Les solutions FlexPod

FlexPod

NetApp
January 21, 2025

Sommaire

Les solutions FlexPod

Définition de FlexPod

Spécifications techniques de FlexPod Express

Tr-4293 : spécifications techniques de FlexPod Express

Karthick Radhakrishnan, Arvind Ramakrishnan, Lindsey Street, Savita Kumari, NetApp

FlexPod Express est une architecture préconçue et conforme aux bonnes pratiques. Elle repose sur la gamme Cisco Unified Computing System (Cisco UCS) et sur la gamme de commutateurs Cisco Nexus. La couche de stockage est conçue par la FAS NetApp ou par le stockage NetApp E-Series. FlexPod Express est une plateforme adaptée pour exécuter divers hyperviseurs de virtualisation, systèmes d'exploitation sans système d'exploitation et charges de travail d'entreprise.

FlexPod Express offre non seulement une configuration de base, mais également la possibilité d'être dimensionnée et optimisée afin de répondre à de nombreuses exigences et cas d'utilisation. Ce document catégorise les configurations FlexPod Express basées sur le système de stockage utilisé, FlexPod Express avec NetApp FAS et FlexPod Express avec E-Series.

Plateformes FlexPod

Il existe trois plateformes FlexPod :

- **FlexPod Datacenter** cette plateforme est une infrastructure de data Center virtuel extrêmement évolutive et adaptée aux applications d'entreprise, à la virtualisation, aux infrastructures de postes de travail virtuels et aux clouds publics et privés. Les caractéristiques de FlexPod Datacenter sont propres, et documentées dans "Tr-4036 : spécifications techniques du data Center FlexPod".
- **FlexPod Express.** cette plate-forme est une infrastructure convergente compacte conçue pour les bureaux distants et les bureaux distants.

Ce document présente les spécifications techniques de la plateforme FlexPod Express.

Règles FlexPod

La conception du système FlexPod permet de créer une infrastructure flexible qui englobe de nombreux composants et versions logicielles différents.

Utilisez les jeux de règles comme guide pour construire ou assembler une configuration FlexPod valide. Les chiffres et les règles indiqués dans ce document représentent le minimum requis pour FlexPod. Ils peuvent être étendus aux familles de produits incluses, si nécessaire pour différents environnements et cas d'utilisation.

Prise en charge par rapport aux configurations FlexPod validées

L'architecture FlexPod est définie par l'ensemble des règles décrites dans ce document. Les composants matériels et les configurations logicielles doivent être pris en charge par la liste de compatibilité matérielle Cisco (HCL) et le "Matrice d'interopérabilité NetApp (IMT)".

Chaque conception validée par Cisco (CVD) ou architecture vérifiée NetApp (NVA) est une configuration FlexPod possible. Cisco et NetApp documentent ces combinaisons de configuration et les valident à l'aide de tests complets. Les déploiements FlexPod qui diffèrent de ces configurations sont entièrement pris en charge si ils suivent les consignes décrites dans ce document et que tous les composants sont répertoriés comme compatibles avec Cisco HCL et NetApp "IMT".

Par exemple, l'ajout de contrôleurs de stockage ou de serveurs Cisco UCS et la mise à niveau du logiciel vers des versions plus récentes sont entièrement pris en charge si le logiciel, le matériel et les configurations sont conformes aux directives définies dans ce document.

Logiciel de stockage

FlexPod Express prend en charge les systèmes de stockage exécutant des systèmes d'exploitation NetApp ONTAP ou SANtricity.

NetApp ONTAP

Le logiciel NetApp ONTAP est le système d'exploitation qui s'exécute sur les systèmes de stockage AFF et FAS. ONTAP offre une architecture de stockage hautement évolutive qui garantit la continuité de l'activité, des mises à niveau sans interruption et une infrastructure de données agile.

Pour plus d'informations sur ONTAP, consultez le "Page produit ONTAP".

Logiciels des E-Series SANtricity

Le logiciel E-Series SANtricity est le système d'exploitation qui s'exécute sur les systèmes de stockage E-Series. SANtricity fournit un système extrêmement flexible qui répond à des besoins applicatifs très divers, et assure une haute disponibilité intégrée et de nombreuses fonctionnalités de protection des données.

Pour plus d'informations, reportez-vous à la section "Page produit SANtricity".

Configuration matérielle minimale requise

Cette section décrit la configuration matérielle minimale requise pour les différentes versions de FlexPod Express.

FlexPod Express avec NetApp FAS

Les configurations décrites dans cette section sont les configurations matérielles requises pour les solutions FlexPod Express qui utilisent des contrôleurs NetApp FAS pour le stockage sous-jacent.

Configuration basée sur CIMC (serveurs en rack autonomes)

La configuration Cisco Integrated Management Controller (CIMC) inclut les composants matériels suivants :

- Deux commutateurs Ethernet standard de 10 Gbit/s dans une configuration redondante (Cisco Nexus 31108 est recommandé, avec prise en charge des modèles Cisco Nexus 3000 et 9000)
- Serveurs en rack autonomes Cisco UCS C-Series
- Deux contrôleurs AFF C190, AFF A250, FAS2600 ou FAS 2700 dans une configuration de paire haute disponibilité déployée sous forme de cluster à deux nœuds

Configuration Cisco UCS-Managed

La confirmation gérée par Cisco UCS inclut les composants matériels suivants :

- Deux commutateurs Ethernet standard de 10 Gbits/s dans une configuration redondante (Cisco Nexus 3524 est recommandé)
- Un châssis de serveur lame Cisco UCS 5108 à courant alternatif (CA)
- Deux interconnexions de fabric Cisco UCS 6324
- Serveurs Cisco UCS B-Series (au moins quatre serveurs lames Cisco UCS B200 M5)
- Deux contrôleurs AFF C190, AFF A250, FAS2750 ou FAS2720 dans une configuration de paire haute disponibilité (deux ports UTA2 disponibles pour chaque contrôleur)

FlexPod Express avec E-Series

La configuration matérielle requise pour la FlexPod Express avec E-Series Starter comprend les éléments suivants :

- Deux interconnexions de fabric Cisco UCS 6324
- Un châssis Cisco UCS Mini 5108 AC2 ou DC2 (les interconnexions de fabric Cisco UCS 6324 sont uniquement prises en charge dans les châssis AC2 et DC2)
- Serveurs Cisco UCS B-Series (au moins deux serveurs lames Cisco UCS B200 M4)
- Une configuration par paire haute disponibilité d'un système de stockage E-Series E2824 chargé avec au moins 12 disques
- Deux commutateurs Ethernet standard de 10 Gbits/s dans une configuration redondante (les commutateurs existants du data Center peuvent être utilisés)

Ces composants matériels sont nécessaires pour établir une configuration de démarrage de la solution ; des serveurs lames et des lecteurs de disque supplémentaires peuvent être ajoutés si nécessaire. Le système de stockage E-Series E2824 peut être remplacé par une plateforme plus élevée et peut également être exécuté en tant que système 100 % Flash.

Configuration logicielle minimale requise

Cette section décrit la configuration logicielle minimale requise pour les différentes versions de FlexPod Express.

Configuration logicielle requise pour FlexPod Express avec NetApp AFF ou FAS

Voici les éléments logiciels requis pour le système FlexPod Express avec NetApp FAS :

- ONTAP 9.1 ou version ultérieure
- Cisco NX-OS version 7.0(3)I6(1) ou ultérieure
- Dans la configuration gérée par Cisco UCS, Cisco UCS Manager UCS 4.0(1b)

Tous les logiciels doivent être répertoriés et pris en charge dans le "NetApp IMT". Certaines fonctionnalités logicielles peuvent nécessiter des versions de code plus récentes que les valeurs minimales répertoriées dans les architectures précédentes.

Configuration logicielle requise pour FlexPod Express avec E-Series

Voici les éléments logiciels requis pour le système FlexPod Express avec E-Series :

- Logiciel E-Series SANtricity 11.30 ou version supérieure
- Cisco UCS Manager 4.0(1b).

Tous les logiciels doivent être répertoriés et pris en charge dans le "NetApp IMT".

Les besoins en connectivité

Cette section décrit les conditions de connectivité requises pour les différentes versions de FlexPod Express.

Les besoins en connectivité de FlexPod Express avec NetApp FAS

Les exigences en matière de connectivité de FlexPod Express avec NetApp FAS sont les suivantes :

- Les contrôleurs de stockage NetApp FAS doivent être directement connectés aux commutateurs Cisco Nexus, sauf dans la configuration gérée par Cisco UCS, où les contrôleurs de stockage sont connectés aux éléments Fabric Interconnect.
- Aucun équipement supplémentaire ne peut être placé en ligne entre les composants principaux de FlexPod.
- Les canaux de port virtuels (VPC) sont nécessaires pour connecter les commutateurs de la gamme Cisco Nexus 3000/9000 aux contrôleurs de stockage NetApp.
- Bien qu'elle ne soit pas requise, l'activation de la prise en charge des trames Jumbo est recommandée dans l'ensemble de l'environnement.

Besoins en connectivité pour FlexPod Express avec NetApp E-Series

Les exigences de connectivité relatives à FlexPod Express avec E-Series sont les suivantes :

- Les contrôleurs de stockage E-Series doivent être directement connectés aux interconnexions de fabric.
- Aucun équipement supplémentaire ne doit être placé en ligne entre les composants principaux de FlexPod.
- Les VPC sont requis entre les interconnexions de fabric et les commutateurs Ethernet.

Les besoins en connectivité de FlexPod Express avec NetApp AFF

Les exigences en matière de connectivité de FlexPod Express avec NetApp AFF sont les suivantes :

- Les contrôleurs de stockage NetApp AFF doivent être directement connectés aux commutateurs Cisco Nexus, sauf dans la configuration gérée par Cisco UCS, où les contrôleurs de stockage sont connectés à la structure. interconnexions.
- Aucun équipement supplémentaire ne peut être placé en ligne entre les composants principaux de FlexPod.
- Les canaux de port virtuels (VPC) sont nécessaires pour connecter les commutateurs de la gamme Cisco Nexus 3000/9000 aux contrôleurs de stockage NetApp.
- Bien qu'elle ne soit pas requise, l'activation de la prise en charge des trames Jumbo est recommandée dans l'ensemble de l'environnement.

Autres exigences

Les autres conditions requises pour FlexPod Express sont les suivantes :

- Des contrats de support valides sont requis pour tous les équipements, notamment :
  - Prise en charge de SMARTnet pour les équipements Cisco
  - Le support SupportEdge Advisor ou SupportEdge Premium pour les équipements NetApp
- Tous les composants logiciels doivent être répertoriés et pris en charge dans le "NetApp IMT".
- Tous les composants matériels NetApp doivent être répertoriés et pris en charge sur "NetApp Hardware Universe".
- Tous les composants matériels Cisco doivent être répertoriés et pris en charge sur "Cisco HCL".

Fonctionnalités en option

Cette section décrit les fonctionnalités en option de FlexPod Express.

Option de démarrage iSCSI

L'architecture FlexPod Express utilise un démarrage iSCSI. La configuration minimale requise pour l'option de démarrage iSCSI est la suivante :

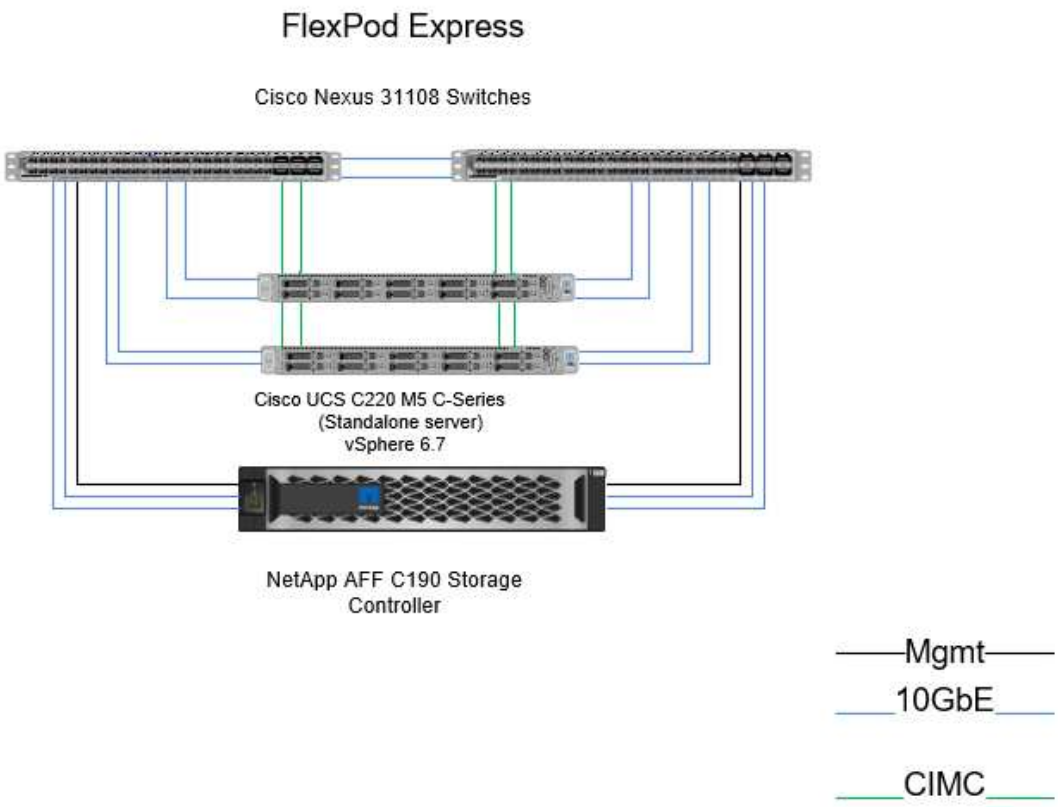
- Licence/fonctionnalité iSCSI activée sur le contrôleur de stockage NetApp
- Un adaptateur Ethernet 10 Gbit/s à deux ports sur chaque nœud de la paire haute disponibilité du contrôleur de stockage NetApp
- Un adaptateur du serveur Cisco UCS capable de démarrer iSCSI

Options de configuration

Cette section fournit des informations supplémentaires sur la configuration requise et validée dans l'architecture FlexPod Express.

FlexPod Express avec Cisco UCS C-Series et AFF C190 Series

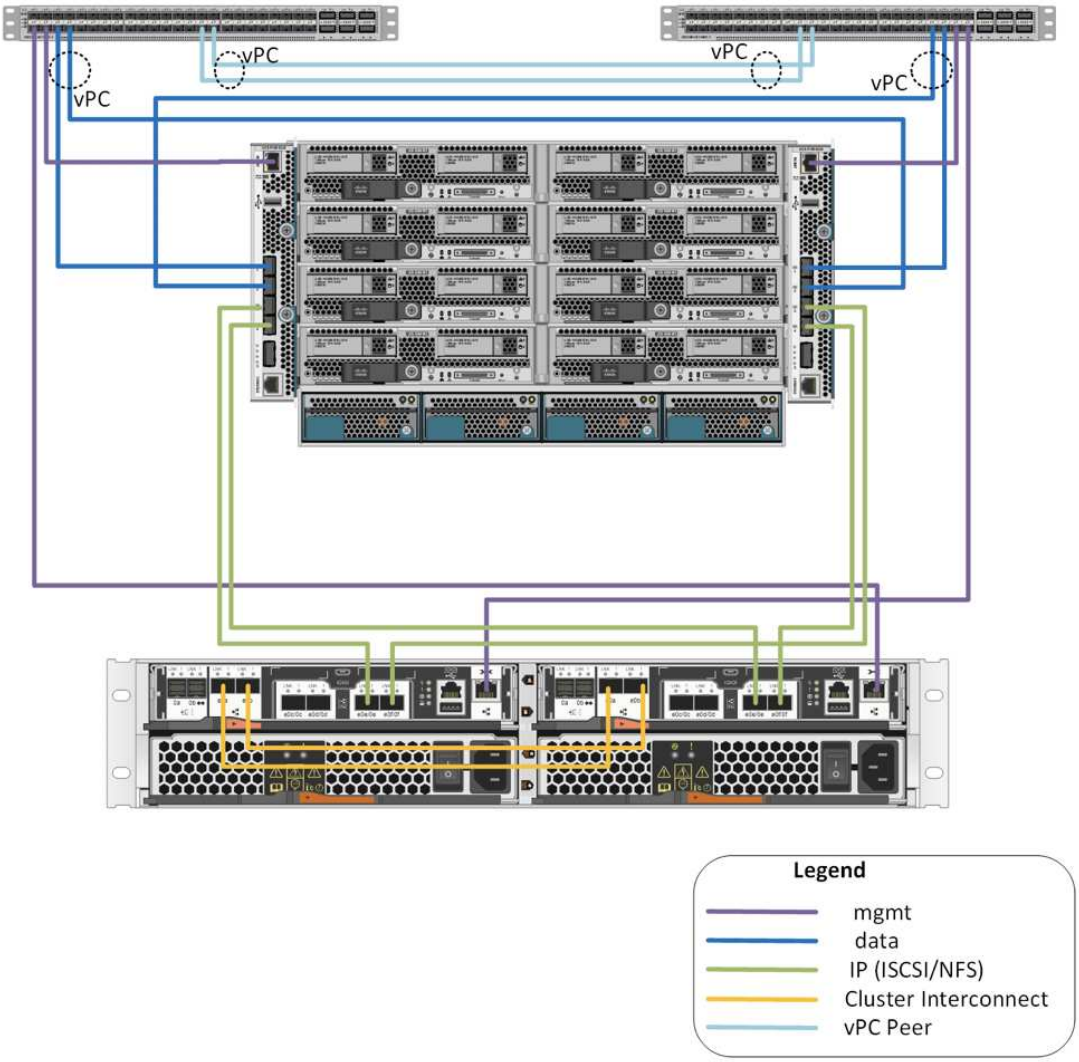
La figure suivante montre l'FlexPod Express avec Cisco UCS C-Series et la gamme AFF C190. Cette solution prend en charge les deux liaisons montantes 10 GbE.



Pour plus d'informations sur cette configuration, consultez le Guide de déploiement NVA FlexPod Express avec VMware vSphere 6.7 et NetApp AFF C190 (en cours).

FlexPod Express avec Cisco UCS Mini, AFF A220 et FAS 2750/2720

La figure suivante illustre le modèle FlexPod Express avec la configuration gérée par Cisco UCS.



Pour plus d'informations sur cette configuration, reportez-vous à "FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage DAS basé sur IP"la section.

Composants Cisco

Cisco apporte une contribution substantielle à la conception et à l'architecture d'FlexPod Express. Il apporte les couches de calcul et de mise en réseau de la solution. Cette section décrit les composants Cisco UCS et Cisco Nexus disponibles pour FlexPod Express.

Options des serveurs lames Cisco UCS B-Series

Les serveurs lames Cisco UCS B-Series actuellement pris en charge par la plateforme Cisco UCS Mini sont les serveurs B200 M5 et B420 M4. Au fur et à mesure que les serveurs lames sont pris en charge par la plateforme Cisco UCS Mini, d'autres lames seront répertoriées dans le tableau suivant.

Serveur Cisco UCS B-Series	Numéro de référence	Caractéristiques techniques
CISCO UCS B200 M5	UCSTM-B200-M5	https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b200-m5-blade-server/model.html
CISCO UCS B200 M4	NGB-B200-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200m4-specsheet.pdf
CISCO UCS B420 M4	NGB-B420-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b420m4-spec-sheet.pdf

Options de serveurs en rack Cisco UCS C-Series

Des serveurs lames Cisco UCS C-Series sont disponibles en un rack et deux racks (RU), avec diverses options de CPU, de mémoire et d'E/S. Les références répertoriées dans le tableau suivant concernent le serveur de base ; elles ne comprennent pas les processeurs, la mémoire, les lecteurs de disque, les cartes PCIe ou les FEX de Cisco. De nombreuses options de configuration sont disponibles et prises en charge dans FlexPod.

Serveur en rack Cisco UCS C-Series	Numéro de référence	Caractéristiques techniques
CISCO UCS C220 M4	UCSC-C220-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
CISCO UCS C240 M4	UCSC-C240-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m4-sff-spec-sheet.pdf
CISCO UCS C460 M4	UCSC-C460-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c460m4_specsheet.pdf

Commutateurs Cisco Nexus

Des commutateurs redondants sont requis pour toutes les architectures FlexPod Express.

L'architecture FlexPod Express avec NetApp AFF ou FAS est conçue à l'aide du commutateur Cisco Nexus 31108. Le FlexPod Express associé à l'architecture Cisco UCS Mini (gérée par Cisco UCS) est validé à l'aide du commutateur Cisco Nexus 3524. Cette configuration peut également être déployée à l'aide d'un commutateur standard.

Le système FlexPod Express avec E-Series peut être déployé avec un switch standard.

Le tableau suivant répertorie les références du châssis de la gamme Cisco Nexus et n'inclut pas de SFP ou de modules d'extension supplémentaires.

Commutateurs de la gamme Cisco Nexus	Numéro de référence	Caractéristiques techniques
Commutateurs Cisco Nexus 3048	N3K-C3048TP-1GE	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-685363.html
Commutateurs Cisco Nexus 31108	N3K-C31108PC-V	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Commutateurs Cisco Nexus 9396	N9K-C9396PX	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729405.html
Commutateurs Cisco Nexus 3172	N3K-C3172	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-729483.html

Options de licence du support Cisco

Des contrats de support SMARTnet valides sont nécessaires sur tous les équipements Cisco de l'architecture FlexPod Express.

Les licences requises et les références de ces licences doivent être vérifiées par votre représentant commercial car elles peuvent varier selon les produits.

Le tableau suivant répertorie les options de licence de prise en charge de Cisco.

Licences du support Cisco	Guide de licence
SMARTnet 24	http://www.cisco.com/web/services/portfolio/product-technical-support/smartnet/index.html

Composants NetApp

Les contrôleurs de stockage NetApp constituent la base du stockage de l'architecture Express de FlexPod pour le stockage des données de démarrage et d'applications. Cette section répertorie les différentes options NetApp disponibles dans l'architecture FlexPod Express.

Options de contrôleurs de stockage NetApp

NetApp FAS

Les contrôleurs redondants AFF C190, AFF A220 ou FAS2750 sont requis dans l'architecture FlexPod Express. Ils exécutent le logiciel ONTAP. Lors de la commande de contrôleurs de stockage, la version logicielle préférée peut être préchargée sur les contrôleurs. Dans le cas d'ONTAP, le cluster peut être déployé avec deux commutateurs d'interconnexion de cluster ou dans une configuration en cluster sans commutateur.

Les références indiquées dans le tableau suivant concernent un contrôleur vide. Plusieurs options et

configurations sont disponibles en fonction de la plateforme de stockage sélectionnée. Pour plus d'informations sur ces composants supplémentaires, adressez-vous à votre représentant commercial.

Contrôleur de stockage	Référence FAS	Caractéristiques techniques
FAS2750	En fonction des options choisies	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
FAS2720	En fonction des options choisies	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
AFF C190	En fonction des options choisies	https://www.netapp.com/us/products/entry-level-aff.aspx
AVEC AFF A220	En fonction des options choisies	https://www.netapp.com/us/documentation/all-flash-fas.aspx
FAS2620	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2650	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx

Stockage E-Series

Une paire haute disponibilité de contrôleurs NetApp E2800 Series est requise dans l'architecture FlexPod Express. Les contrôleurs exécutent le système d'exploitation SANtricity.

Les références indiquées dans le tableau suivant concernent un contrôleur vide. Plusieurs options et configurations sont disponibles en fonction de la plateforme de stockage sélectionnée. Pour plus d'informations sur ces composants supplémentaires, adressez-vous à votre représentant commercial.

Contrôleur de stockage	Numéro de référence	Caractéristiques techniques
E2800	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/e2800/e2800-tech-specs.aspx

Modules d'extension Ethernet NetApp

NetApp FAS

Le tableau suivant répertorie les options d'adaptateur NetApp FAS10GbE.

Composant	Numéro de référence	Caractéristiques techniques
NetApp X1117A	X1117A-R6	https://library.netapp.com/ecm/ecm_download_file/ECMM1280307

Les systèmes de stockage FAS2500 et 2600 sont dotés de ports 10GbE intégrés.

L'adaptateur X1117A NetApp est destiné aux systèmes de stockage FAS8020.

Stockage E-Series

Le tableau suivant répertorie les options des adaptateurs 10GbE du système E-Series.

Composant	Numéro de référence
4 ports iSCSI 10 GbE/FC 16 Gbit/s	X-56025-00-0F-C.
2 ports iSCSI 10 GbE/FC 16 Gbit/s	X-56024-00-0F-C.

> Les systèmes de stockage E2824 sont équipés de ports 10 GbE intégrés.
>
> La carte d'interface hôte (HIC) à 4 ports iSCSI/FC 16 Gbit 10 GbE peut être utilisée pour accroître la densité des ports.

Les ports intégrés et la HIC peuvent fonctionner comme des adaptateurs iSCSI ou FC en fonction de la fonction activée dans SANtricity OS.

Pour plus d'informations sur les options de carte prises en charge, reportez-vous à la section carte réseau de la section "NetApp Hardware Universe".

Tiroirs disques et disques NetApp

NetApp FAS

Un minimum d'un tiroir disque NetApp est requis pour les contrôleurs de stockage. Le type de tiroir NetApp sélectionné détermine les types de disques disponibles au sein de ce tiroir.

Les gammes FAS2700 et FAS2600 sont proposées sous forme de configuration incluant deux contrôleurs de stockage et des disques hébergés dans un même châssis. Cette configuration est proposée avec des disques SATA ou SAS ; par conséquent, des tiroirs disques externes supplémentaires ne sont pas nécessaires, sauf si les exigences en termes de performances ou de capacité requièrent davantage de piles de disques.

> Les références de tous les tiroirs disques correspondent au tiroir vide avec deux blocs d'alimentation CA. Contactez votre ingénieur commercial pour obtenir des références supplémentaires.
>
> Les références de disque varient en fonction de la taille et du format du disque que vous envisagez d'acheter. Contactez votre ingénieur commercial pour obtenir des références supplémentaires.

Le tableau suivant répertorie les options de tiroirs disques NetApp, ainsi que les disques pris en charge pour chaque type de tiroir, disponibles sur NetApp Hardware Universe. Suivez le lien Hardware Universe, sélectionnez la version du ONTAP que vous utilisez, puis sélectionnez le type de tiroir. Sous l'image de tiroir, cliquez sur disques pris en charge pour afficher les disques pris en charge pour des versions spécifiques de ONTAP et des tiroirs disques.

Tiroir disque	Numéro de référence	Caractéristiques techniques
DS212C	DS212C-0-12	"Spécifications techniques des tiroirs disques et des supports de stockage disques pris en charge sur NetApp Hardware Universe"

Tiroir disque	Numéro de référence	Caractéristiques techniques
DS224C	DS224C-0-24	"Spécifications techniques des tiroirs disques et des supports de stockage disques pris en charge sur NetApp Hardware Universe"
DS460C	DS460C-0-60	"Spécifications techniques des tiroirs disques et des supports de stockage disques pris en charge sur NetApp Hardware Universe"
DS2246	X559A-R6	"Spécifications techniques des tiroirs disques et des supports de stockage disques pris en charge sur NetApp Hardware Universe"
DS4246	X24M-R6	"Spécifications techniques des tiroirs disques et des supports de stockage disques pris en charge sur NetApp Hardware Universe"
DS4486	DS4486-144 TO-R5-C.	"Spécifications techniques des tiroirs disques et des supports de stockage disques pris en charge sur NetApp Hardware Universe"

Stockage E-Series

Au moins un tiroir disque NetApp est nécessaire pour les contrôleurs de stockage qui ne hébergent aucun disque dans leur châssis. Le type de tiroir NetApp sélectionné détermine les types de disques disponibles au sein de ce tiroir.

La gamme E2800 de contrôleurs est proposée sous forme de configuration incluant deux contrôleurs de stockage et des disques hébergés dans un tiroir disque pris en charge. Cette configuration est proposée avec des disques SSD ou SAS.

> Les références de disque varient en fonction de la taille et du format du disque que vous envisagez d'acheter. Contactez votre ingénieur commercial pour obtenir des références supplémentaires.

Le tableau suivant répertorie les options de tiroirs disques NetApp et les disques pris en charge pour chaque type de tiroir, disponibles sur NetApp Hardware Universe. Suivez le lien Hardware Universe, sélectionnez la version du ONTAP que vous utilisez, puis sélectionnez le type de tiroir. Sous l'image de tiroir, cliquez sur disques pris en charge pour afficher les disques pris en charge pour des versions spécifiques de ONTAP et des tiroirs disques.

Tiroir disque	Numéro de référence	Caractéristiques techniques
DE460C	E-X5730A-DM-0E-C.	"Tiroirs disques spécifications techniques disques pris en charge disques sur NetApp Hardware Universe"

Tiroir disque	Numéro de référence	Caractéristiques techniques
DE224C	E-X5721A-DM-0E-C.	"Tiroirs disques spécifications techniques disques pris en charge disques sur NetApp Hardware Universe"
DE212C	E-X5723A-DM-0E-C.	"Tiroirs disques spécifications techniques disques pris en charge disques sur NetApp Hardware Universe"

Options NetApp de licences logicielles

NetApp FAS

Le tableau suivant répertorie les options de licence logicielle de NetApp FAS.

Licences logicielles NetApp	Référence	Caractéristiques techniques
Licence de cluster de base	Contactez votre équipe commerciale NetApp pour en savoir plus sur les licences.	

Stockage E-Series

Le tableau suivant répertorie les options de licence logicielle des baies E-Series.

Licences logicielles NetApp	Numéro de référence	Caractéristiques techniques
Caractéristiques standard	Contactez votre équipe commerciale NetApp pour en savoir plus sur les licences.	
Fonctionnalités premium		

Options de licence du support NetApp

Les licences SupportEdge Premium sont requises et les références associées à ces licences varient en fonction des options sélectionnées dans la conception FlexPod Express.

NetApp FAS

Le tableau suivant répertorie les options de licence de support NetApp pour NetApp FAS.

Licences du support NetApp	Numéro de référence	Caractéristiques techniques
SupportEdge Premium4 heures sur place ; mois : 36	CS-O2-4HR	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf

Stockage E-Series

Le tableau suivant répertorie les options de licence de support NetApp pour le stockage E-Series.

Licences du support NetApp	Numéro de référence	Caractéristiques techniques
Support matériel Premium 4 heures sur site ; mois : 36	SVC-O2-4HR-E	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf
Support logiciel	SW-SSP-O2-4HR-E	
Installation initiale	SVC-INST-O2-4HR-E	

Exigences en matière de puissance électrique et de câblage

Cette section décrit les exigences minimales en matière de consommation électrique et de câblage pour une conception FlexPod Express.

Les besoins en alimentation électrique

Les exigences d'alimentation électrique sont basées sur les exigences des États-Unis Spécifications et suppose l'utilisation de l'alimentation CA. D'autres pays peuvent avoir des exigences d'alimentation différentes. Des options d'alimentation à courant continu sont également disponibles pour la plupart des composants. Pour plus de données sur la puissance maximale requise et d'autres informations détaillées sur l'alimentation, consultez les spécifications techniques détaillées de chaque composant matériel.

Pour en savoir plus sur les données de puissance Cisco UCS, consultez le "Calculateur de puissance Cisco UCS".

Le tableau suivant répertorie les ports d'alimentation requis par périphérique.

Commutateurs Cisco Nexus	Câbles d'alimentation requis
Commutateurs Cisco Nexus 3048	2 câbles d'alimentation C13/C14 pour chaque commutateur Cisco Nexus série 3000
Commutateurs Cisco Nexus 3524	2 câbles d'alimentation C13/C14 pour chaque commutateur Cisco Nexus série 3000
Commutateurs Cisco Nexus 9396	2 câbles d'alimentation C13/C14 pour chaque commutateur Cisco Nexus série 9000

Châssis Cisco UCS	Câbles d'alimentation requis
Cisco UCS 5108	2 CAB-US515P-C19-US/CAB-US520-C19-US pour chaque châssis Cisco UCS

Serveurs Cisco UCS B-Series	Câbles d'alimentation requis
CISCO UCS B200 M4	N/A ; le serveur lame est alimenté par le châssis
CISCO UCS B420 M4	N/A ; le serveur lame est alimenté par le châssis
CISCO UCS B200 M5	N/A ; le serveur lame est alimenté par le châssis
CISCO UCS B480 M5	N/A ; le serveur lame est alimenté par le châssis

Serveurs Cisco UCS C-Series	Ports d'alimentation requis
CISCO UCS C220 M4	2 câbles d'alimentation C13/C14 pour chaque serveur Cisco UCS
CISCO UCS C240 M4	
CISCO UCS C460 M4 CISCO UCS C220 M5 CISCO UCS C240 M5 CISCO UCS C480 M5	

Contrôleurs NetApp FAS	Ports d'alimentation requis (par paire haute disponibilité)
FAS2554	2 C13/C14
FAS2552	2 C13/C14
FAS2520	2 C13/C14
FAS8020	2 C13/C14

Contrôleurs E-Series	Ports d'alimentation requis (par paire haute disponibilité)
E2824	2 x C14/C20

Tiroirs disques NetApp FAS	Ports d'alimentation requis
DS212C	2 C13/C14
DS224C	2 C13/C14
DS460C	2 C13/C14
DS2246	2 C13/C14
DS4246	4 C13/C14

Tiroirs disques E-Series	Ports d'alimentation requis
DE460C	2 x C14/C20
DE224C	2 x C14/C20
DE212C	2 x C14/C20

Exigences minimales en matière de câblage

Cette section décrit la configuration minimale requise pour les câbles d'une conception FlexPod Express. La plupart des implémentations FlexPod requièrent des câbles supplémentaires, mais leur nombre varie en fonction de la taille et de l'étendue du déploiement.

Le tableau suivant répertorie le nombre minimal de câbles requis pour chaque périphérique.

Commutateurs Cisco Nexus série 3000	Câbles requis
Commutateurs Cisco Nexus 31108	Au moins deux câbles Twinax ou fibre 10GbE par commutateur
Cisco Nexus 3172PQ	
Commutateurs Cisco Nexus 3048	
Commutateurs Cisco Nexus 3524	
Commutateurs Cisco Nexus 9396	
DS212C	
DS2246	Le nombre de câbles SAS dépend de la configuration spécifique des tiroirs disques
DS460C	
DS224C	
DS4246	
E2800	• Au moins un câble Gigabit Ethernet (1GbE) pour la gestion par contrôleur • Au moins deux câbles 10GbE par contrôleur (pour iSCSI) ou deux câbles FC correspondant aux exigences de vitesse
DE460C	2 câbles HD Mini-SAS par tiroir disque
DE224C	2 câbles HD Mini-SAS par tiroir disque
DE212C	2 câbles HD Mini-SAS par tiroir disque

Spécifications techniques et références

Cette section décrit les spécifications techniques importantes de chaque composant de FlexPod Express.

Serveurs lames Cisco UCS B-Series

Le tableau suivant répertorie les options de serveur lame Cisco UCS B-Series.

Composant	CISCO UCS B200 M4	CISCO UCS B420 M4	CISCO UCS B200 M5
Prise en charge du processeur	Intel Xeon E5-2600	Intel Xeon E5-4600	Processeurs évolutifs Intel Xeon
Capacité de mémoire maximale	24 DIMM pour un maximum de 768 Go	48 DIMM pour un maximum de 3 To	24 DIMM pour un maximum de 3072 Go
Taille et vitesse de la mémoire	DDR4 32 Go ; 2133 MHz	64 Go de DDR4 ; 2 400 MHz	16 Go, 32 Go, 64 Go et 128 Go de DDR4 ; 2666 MHz
Prise en charge du démarrage SAN	Oui.	Oui.	Oui.

Composant	CISCO UCS B200 M4	CISCO UCS B420 M4	CISCO UCS B200 M5
Emplacements d'adaptateur d'E/S mezzanine	2	3	2, avant et arrière, avec prise en charge des GPU
Débit d'E/S maximal	80 Gbit/s.	160 Gbit/s.	80 Gbit/s.

Serveurs en rack Cisco UCS C-Series

Le tableau suivant répertorie les options de serveurs en rack Cisco UCS C-Series.

Composant	CISCO UCS C220 M4	CISCO UCS C240 M4	CISCO UCS C460 M4	CISCO UCS C220 M5
Prise en charge du processeur	1 ou 2 processeurs Intel E5-2600	1 ou 2 processeurs Intel Xeon E5-2600	2 ou 4 Intel Xeon E7-4800/8800	Processeurs évolutifs Intel Xeon (1 ou 2)
Capacité de mémoire maximale	1,5 GO	1,5 TO	6 TO	3072 GO
Emplacements PCIe	2	6	10	2
Format	1RU	2RU	4RU	1 RU

Le tableau suivant répertorie les fiches techniques des options de serveurs en rack Cisco UCS C-Series.

Composant	Fiche technique Cisco UCS
CISCO UCS C220 M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
CISCO UCS C240 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m4-rack-server/datasheet-c78-732455.html
CISCO UCS C460 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c460-m4-rack-server/datasheet-c78-730907.html
CISCO UCS C220 M5	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf

Commutateurs Cisco Nexus série 3000

Le tableau suivant répertorie les options des commutateurs Cisco Nexus 3000.

Composant	Commutateurs Cisco Nexus 3048	Commutateurs Cisco Nexus 3524	Commutateurs Cisco Nexus 31108	Cisco Nexus 3172PQ
Format	1RU	1RU	1RU	1 RU

Composant	Commutateurs Cisco Nexus 3048	Commutateurs Cisco Nexus 3524	Commutateurs Cisco Nexus 31108	Cisco Nexus 3172PQ
Nombre maximum de ports 1 Gbit/s	48	24	48 (10/40/100 Gbit/s)	72 ports 1/10GbE ou 48 ports 1/10GbE plus six ports 40 GbE
Taux de transfert	132 Mbit/s.	360 Mbit/s	1.2Bpps	1 Bpps
Prise en charge des trames Jumbo	Oui.	Oui.	Oui.	Oui.

Le tableau suivant répertorie les fiches techniques des options des commutateurs Cisco Nexus 3000.

Composant	Fiche technique Cisco Nexus
Commutateurs Cisco Nexus 31108	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 3172PQ	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Commutateurs Cisco Nexus 3048	https://www.cisco.com/c/en/us/products/switches/nexus-3048-switch/index.html
Cisco Nexus 3172PQ-XL	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3548 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html
Commutateurs Cisco Nexus 3548	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Commutateurs Cisco Nexus 3524	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html

Le tableau suivant répertorie les options des commutateurs Cisco Nexus 9000.

Composant	Commutateurs Cisco Nexus 9396	Commutateurs Cisco Nexus 9372
Format	2RU	1RU
Nombre maximal de ports	60	54
Ports uplink SFP+ 10 Gbits/s.	48	48

Le tableau suivant répertorie les fiches techniques des options des commutateurs de la gamme Cisco Nexus 9000.

Composant	Fiche technique Cisco Nexus
Commutateurs Cisco Nexus 9396	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html

Composant	Fiche technique Cisco Nexus
Commutateurs Cisco Nexus 9372	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Nexus 9396X	https://www.cisco.com/c/en/us/products/switches/nexus-9396px-switch/index.html?dtid=osscdc000283

Contrôleurs de stockage NetApp FAS

Le tableau suivant répertorie les options actuelles de contrôleur de stockage NetApp FAS.

Composant actuel	FAS2620	FAS2650
Configuration	2 contrôleurs dans un châssis 2U	2 contrôleurs dans un châssis 4U
Capacité brute maximale	1440 TO	123TO
Disques internes	12	24
Nombre maximal de disques (internes plus externes)	144	144
Taille maximale des volumes	100 TO	
Taille maximale des agrégats	4 TO	
Nombre maximal de LUN	2,048 par contrôleur	
Réseaux de stockage pris en charge	ISCSI, FC, FCoE, NFS et CIFS	
Nombre maximal de volumes NetApp FlexVol	1,000 par contrôleur.	
Nombre maximal de copies NetApp Snapshot	255,000 par contrôleur	
Mise en cache intelligente des données NetApp Flash Pool maximale	24 TO	

Pour plus d'informations sur l'option de contrôleur de stockage FAS, reportez-vous au "Modèles FAS" De la section Hardware Universe. Pour AFF, voir "Modèles AFF" section.

Le tableau suivant répertorie les caractéristiques d'un système de contrôleur FAS8020.

Composant	FAS8020
Configuration	2 contrôleurs dans un châssis 3U
Capacité brute maximale	2880 TO
Nombre maximal de disques	480
Taille maximale des volumes	70 TO
Taille maximale des agrégats	324 TO

Composant	FAS8020
Nombre maximal de LUN	8,192 par contrôleur
Réseaux de stockage pris en charge	ISCSI, FC, NFS et CIFS
Nombre maximal de volumes FlexVol	1,000 par contrôleur
Nombre maximal de copies Snapshot	255,000 par contrôleur
Mise en cache intelligente des données NetApp Flash cache maximum	3TO
Mise en cache des données Flash Pool maximale	24 TO

Le tableau suivant répertorie les fiches techniques des contrôleurs de stockage NetApp.

Composant	Fiche technique du contrôleur de stockage
Gamme FAS2600	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
Gamme FAS2500	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
Gamme FAS8000	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

Adaptateurs Ethernet NetApp FAS

Le tableau suivant répertorie les adaptateurs 10GbE de NetApp FAS.

Composant	X1117A-R6
Nombre de ports	2
Type d'adaptateur	SFP+ avec fibre optique

L'adaptateur X1117A-R6 SFP+ est pris en charge sur les contrôleurs de la gamme FAS8000.

Les systèmes de stockage FAS2600 et FAS2500 sont dotés de ports 10GbE intégrés. Pour plus d'informations, reportez-vous à la section "Fiche technique sur l'adaptateur 10GbE NetApp".

Pour plus de détails sur la carte basée sur le modèle AFF ou FAS, reportez-vous au "Section adaptateur" Dans le Hardware Universe.

Tiroirs disques NetApp FAS

Le tableau suivant répertorie les options actuelles de tiroirs disques FAS de NetApp.

Composant	DS460C	DS224C	DS212C	DS2246	DS4246
Format	4RU	2RU	2RU	2RU	4RU
Disques par boîtier	60	24	12	24	24

Composant	DS460C	DS224C	DS212C	DS2246	DS4246
Format de disque	grand format : 3.5 »	petit format : 2.5"	grand format : 3.5 »	petit format : 2.5"	grand format : 3.5 »
Modules E/S à tiroirs	Modules IOM12 doubles	Modules IOM12 doubles	Modules IOM12 doubles	Modules IOM6 doubles	Modules IOM6 doubles

Pour en savoir plus, consultez la fiche technique des tiroirs disques NetApp.

Pour en savoir plus sur les tiroirs disques, consultez la Hardware Universe NetApp "Section tiroirs disques".

Disques NetApp FAS

Les spécifications techniques des disques NetApp incluent la taille de format, la capacité du disque, les tours/min des disques, les exigences relatives à la prise en charge des contrôleurs et les versions Data ONTAP, et se trouvent dans la section disques, le "NetApp Hardware Universe".

Contrôleurs de stockage E-Series

Le tableau suivant répertorie les options actuelles du contrôleur de stockage E-Series.

Composant actuel	E2812	E2824	E2860
Configuration	2 contrôleurs dans un châssis 2U	2 contrôleurs dans un châssis 2U	2 contrôleurs dans un châssis 4U
Capacité brute maximale	1800 TO	1756,8 TO	1800 TO
Disques internes	12	24	60
Nombre maximal de disques (internes plus externes)	180		
SSD maximal	120		
Taille maximale du volume de pool de disques	1024 TO		
Nombre maximum de disques pools	20		
Réseaux de stockage pris en charge	ISCSI et FC		
Nombre maximal de volumes	512		

Le tableau suivant répertorie les fiches techniques du contrôleur de stockage E-Series actuel.

Composant	Fiche technique du contrôleur de stockage
E2800	https://www.netapp.com/pdf.html?item=/media/7573-ds-3805.pdf

Adaptateurs E-Series

Le tableau suivant répertorie les adaptateurs E-Series.

Composant	X-56023-00-0F-C.	X-56025-00-0F-C.	X-56027-00-0F-C.	X-56024-00-0F-C.	X-56026-00-0F-C.
Nombre de ports	2	4	4	2	2
Type d'adaptateur	10 Gbit/s base-T	FC 16 Gbit/s et iSCSI 10GbE	SAS	FC 16 Gbit/s et iSCSI 10GbE	SAS

Tiroirs disques E-Series

Le tableau suivant répertorie les options de tiroirs disques E-Series.

Composant	DE212C	DE224C	DE460C
Format	2RU	2RU	4RU
Disques par boîtier	12	24	60
Format de disque	petit format : 2.5" 3.5"	2.5 »	petit format : 2.5" 3.5"
Modules E/S à tiroirs	IOM12	IOM12	IOM12

Disques E-Series

Les spécifications techniques des disques NetApp incluent la taille, la capacité du disque, les tours/min des disques, les exigences relatives à la prise en charge des contrôleurs et la version SANtricity, et se trouvent dans la section disques, le "NetApp Hardware Universe".

Architectures et équipements antérieurs

FlexPod est une solution flexible qui permet aux clients d'utiliser à la fois les équipements existants et nouveaux actuellement en vente par Cisco et NetApp. Parfois, certains modèles d'équipements Cisco et NetApp sont désignés en fin de vie.

Bien que ces modèles d'équipement ne soient plus disponibles, les clients qui ont acheté un de ces modèles avant la date de fin de vente peuvent utiliser cet équipement dans une configuration FlexPod.

De plus, les architectures FlexPod Express sont régulièrement mises à jour pour introduire les derniers matériels et logiciels Cisco et NetApp dans la solution FlexPod Express. Cette section répertorie les anciennes architectures FlexPod Express et le matériel qui y est utilisé.

Précédentes architectures FlexPod Express

Cette section décrit les précédentes architectures FlexPod Express.

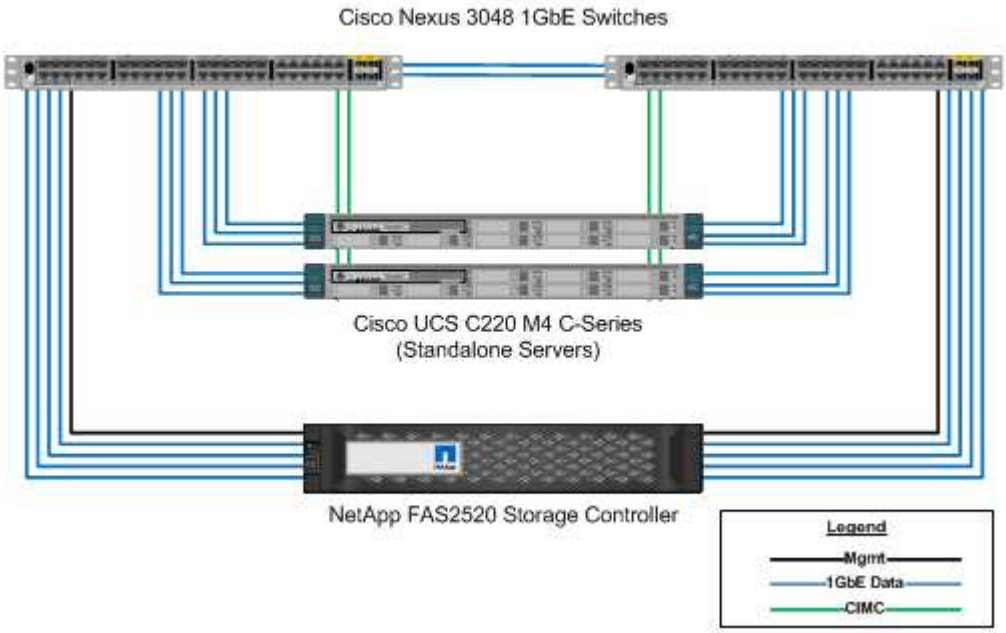
Petites et moyennes configurations FlexPod Express

Les configurations de petite et moyenne taille FlexPod Express incluent les composants suivants :

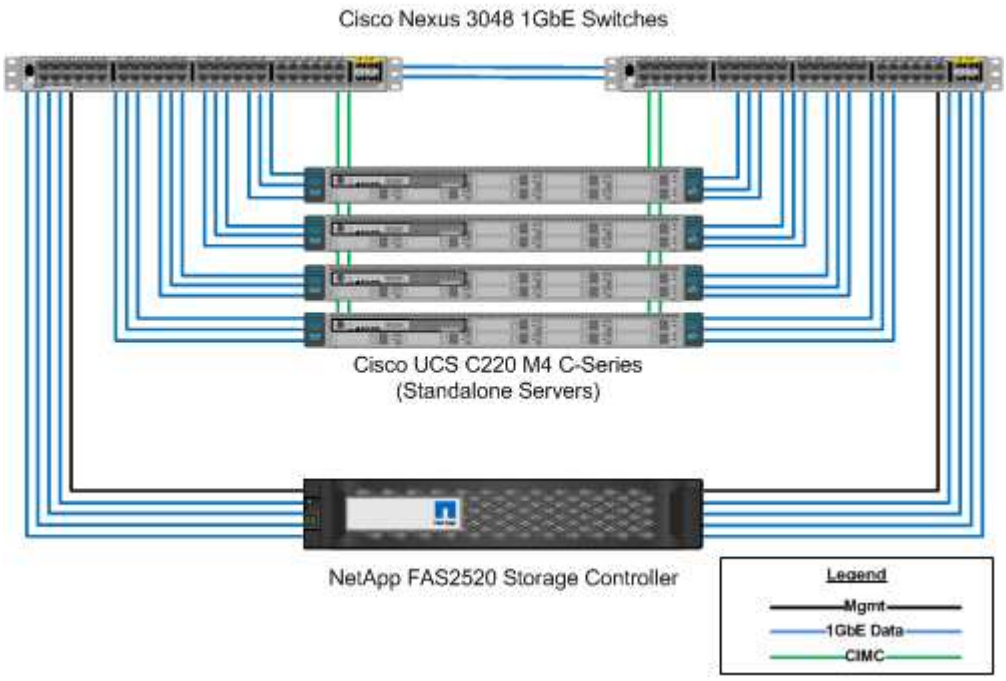
- Deux commutateurs Cisco Nexus 3048 dans une configuration redondante
- Au moins deux serveurs rack Cisco UCS C-Series

- Deux contrôleurs FAS2200 ou FAS2500 en configuration de paires haute disponibilité

La figure suivante illustre la petite configuration de FlexPod Express.



La figure suivante illustre la configuration de support de FlexPod Express.



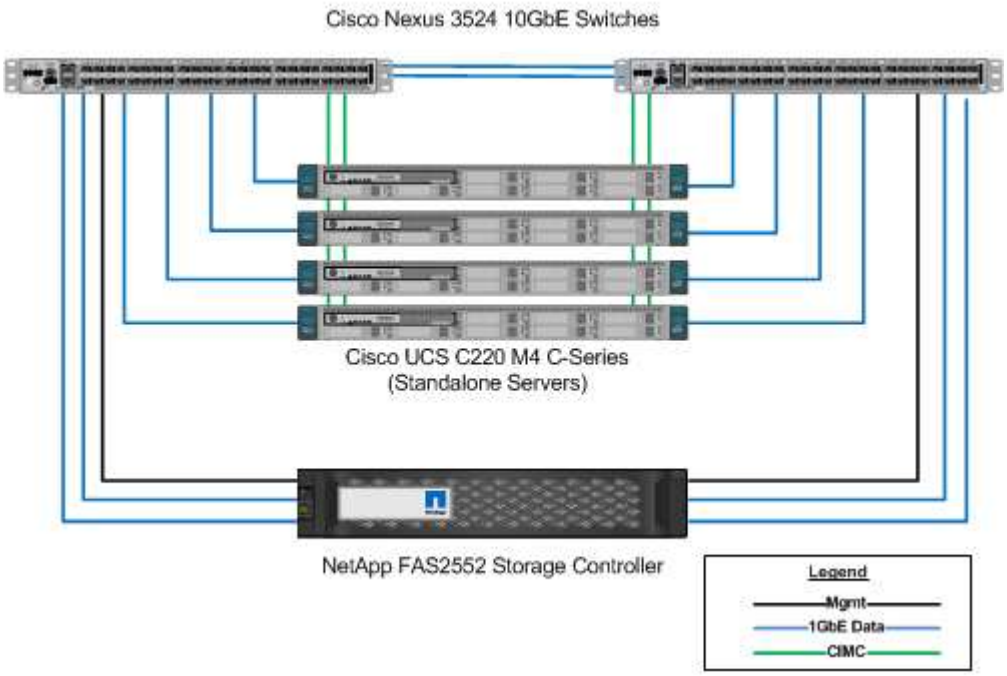
Grande configuration de FlexPod Express

La configuration grand format de FlexPod Express inclut les composants suivants :

- Deux commutateurs Cisco Nexus 3500 ou Cisco Nexus 9300 en configuration redondante

- Au moins deux serveurs rack Cisco UCS C-Series
- Deux contrôleurs FAS2552, FAS2554 ou FAS8020 en configuration de paires haute disponibilité (requiert deux ports 10GbE par contrôleur)
- Un tiroir disque NetApp avec n'importe quel type de disque pris en charge (lorsque le système FAS8020 est utilisé)

La figure suivante illustre la grande configuration de FlexPod Express.



Précédentes architectures vérifiées FlexPod Express

Les précédentes architectures vérifiées FlexPod Express sont toujours prises en charge. Les documents relatifs à l'architecture et au déploiement sont les suivants :

- "FlexPod Express avec Cisco UCS C-Series et NetApp FAS2500 Series"
- "FlexPod Express avec VMware vSphere 6.0 : petites et moyennes configurations"
- "FlexPod Express avec VMware vSphere 6.0 : grande configuration"
- "FlexPod Express avec Microsoft Windows Server 2012 R2 Hyper-V : petites et moyennes configurations"
- "FlexPod Express avec Microsoft Windows Server 2012 R2 Hyper-V : grande configuration"

Matériel précédent

Le tableau suivant répertorie le matériel utilisé dans les précédentes architectures FlexPod Express.

Matériel utilisé dans les architectures précédentes	Caractéristiques techniques (si disponibles)
CISCO UCS C220 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c220-m3-rack-server/data_sheet_c78-700626.html
CISCO UCS C24 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706103.html

Matériel utilisé dans les architectures précédentes	Caractéristiques techniques (si disponibles)
CISCO UCS C22 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706101.html
CISCO UCS C240 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m3-rack-server/data_sheet_c78-700629.html
CISCO UCS C260 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/c260m2_specsheet.pdf
CISCO UCS C420 M3	http://www.cisco.com/en/US/products/ps12770/index.html
CISCO UCS C460 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf
CISCO UCS B200 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b200-m3-blade-server/data_sheet_c78-700625.html
CISCO UCS B420 M3	S/O
CISCO UCS B22 M3	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b22m3_specsheet.pdf
Commutateurs Cisco Nexus 3524	http://www.cisco.com/c/en/us/products/switches/nexus-3524-switch/index.html
FAS2240	
FAS2220	http://www.netapp.com/us/products/storage-systems/fas2200/fas2200-tech-specs.aspx
DS4243	S/O

Équipement existant

Le tableau suivant répertorie les options de contrôleurs de stockage NetApp classiques.

Contrôleur de stockage	Référence FAS	Caractéristiques techniques
FAS2520	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	En fonction des options choisies	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

Le tableau suivant répertorie les options de tiroirs disques NetApp pour NetApp FAS.

Tiroir disque	Numéro de référence	Caractéristiques techniques
DE1600	E-X5682A-DM-0E-R6-C	"Tiroirs disques spécifications techniques disques pris en charge disques sur NetApp Hardware Universe"
DE5600	E-X4041A-12-R6	"Tiroirs disques spécifications techniques disques pris en charge disques sur NetApp Hardware Universe"
DE6600	X-48564-00-R6	"Tiroirs disques spécifications techniques disques pris en charge disques sur NetApp Hardware Universe"

Contrôleurs FAS NetApp hérités

Le tableau suivant répertorie les options de contrôleurs NetApp FAS hérités.

Composant actuel	FAS2554	FAS2552	FAS2520
Configuration	2 contrôleurs dans un châssis 4U	2 contrôleurs dans un châssis 2U	2 contrôleurs dans un châssis 2U
Capacité brute maximale	576 TO	509 TO	36 TO
Disques internes	24	24	12
Nombre maximal de disques (internes plus externes)	144	144	84
Taille maximale des volumes	60 TO		
Taille maximale des agrégats	120 TO		
Nombre maximal de LUN	2,048 par contrôleur		
Réseaux de stockage pris en charge	ISCSI, FC, FCoE, NFS et CIFS		ISCSI, NFS et CIFS
Nombre maximal de volumes NetApp FlexVol	1,000 par contrôleur		
Nombre maximal de copies NetApp Snapshot	255,000 par contrôleur		

Pour plus de modèles NetApp FAS, consultez le "Section modèles FAS" Dans le Hardware Universe.

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce document, consultez ces documents et sites web :

- Centre de documentation du système AFF et FAS

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

- Page des ressources de documentation AFF

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

- Page Ressources de documentation sur les systèmes de stockage FAS

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- Documentation NetApp

  "https://docs.netapp.com"

Caractéristiques techniques des data centers FlexPod

Tr-4036 : spécifications techniques du data Center FlexPod

Arvind Ramakrishnan, et Jyh-shing Chen, NetApp

La plateforme FlexPod est une architecture de data Center préconçue et conforme aux bonnes pratiques. Elle repose sur la plateforme Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus et les contrôleurs de stockage NetApp (systèmes AFF, ASA ou FAS).

FlexPod est une plateforme adaptée pour exécuter divers hyperviseurs de virtualisation, ainsi que des systèmes d'exploitation sans système d'exploitation et des charges de travail d'entreprise. FlexPod offre non seulement une configuration de base, mais également la possibilité d'être dimensionnée et optimisée afin de répondre à de nombreuses exigences et cas d'utilisation.

> Avant de commander une configuration FlexPod complète, reportez-vous au "Infrastructure convergée FlexPod" page netapp.com pour connaître la dernière version de ces spécifications techniques.

"Ensuite : plateformes FlexPod."

Plateformes FlexPod

Il existe deux plateformes FlexPod :

- **FlexPod Datacenter** cette plateforme est une infrastructure de data Center virtuel extrêmement évolutive et adaptée aux charges de travail des applications d'entreprise, de la virtualisation, de l'infrastructure de postes de travail virtuels (VDI) et des clouds publics, privés et hybrides.
- **FlexPod Express.** Il s'agit d'une infrastructure convergée compacte conçue pour les bureaux distants et la périphérie. Les spécifications de FlexPod Express sont décrites dans le "Spécifications techniques de FlexPod Express."

Ce document présente les spécifications techniques de la plateforme FlexPod Datacenter.

Règles FlexPod

La conception de FlexPod permet de créer une infrastructure flexible qui englobe de nombreux composants et versions logicielles différents.

Utilisez les jeux de règles comme guide pour construire ou assembler une configuration FlexPod valide. Les nombres et les règles indiqués dans ce document représentent le minimum requis pour une configuration de FlexPod. Elles peuvent être étendues aux familles de produits incluses, selon les besoins de divers environnements et cas d'utilisation.

Prise en charge par rapport aux configurations FlexPod validées

L'architecture FlexPod est définie par l'ensemble de règles décrites dans ce document. Les composants matériels et les configurations logicielles doivent être pris en charge par le "Liste de compatibilité matérielle et logicielle Cisco UCS" et le "Matrice d'interopérabilité NetApp (IMT)".

Chaque conception validée par Cisco (CVD) ou architecture vérifiée NetApp (NVA) est une configuration FlexPod possible. Cisco et NetApp documentent ces combinaisons de configuration et les valident à l'aide de tests complets. Les déploiements FlexPod qui diffèrent de ces configurations sont entièrement pris en charge s'ils suivent les consignes décrites dans ce document et si tous les composants sont répertoriés comme compatibles dans la liste de compatibilité matérielle et logicielle Cisco UCS et avec NetApp "IMT".

Par exemple, l'ajout de contrôleurs de stockage ou de serveurs Cisco UCS et la mise à niveau du logiciel vers des versions plus récentes sont entièrement pris en charge si le logiciel, le matériel et les configurations sont conformes aux directives définies dans ce document.

NetApp ONTAP

Le logiciel NetApp ONTAP est installé sur tous les systèmes NetApp FAS, AFF et ASA (All SAN Array) de AFF. FlexPod est validé avec le logiciel ONTAP. Son architecture de stockage hautement évolutive garantit la continuité de l'activité, des mises à niveau sans interruption et une infrastructure de données agile.

Pour plus d'informations sur ONTAP, consultez le "Logiciel de gestion des données ONTAP" page produit.

Modes de fonctionnement du commutateur Cisco Nexus

Plusieurs produits Cisco Nexus peuvent être utilisés comme composant de commutation pour un déploiement FlexPod donné. La plupart de ces options reposent sur le système d'exploitation traditionnel Cisco Nexus OS ou NX-OS. La gamme de commutateurs Cisco

Nexus offre différentes fonctionnalités dans ses gammes de produits. Ces fonctionnalités sont détaillées dans ce document.

L'offre de Cisco dans le domaine des réseaux définis par logiciel s'appelle l'infrastructure axée sur les applications (ACI). La gamme de produits Cisco Nexus qui prend en charge le mode ACI, également appelée fabric, est la gamme Cisco Nexus 9300. Ces switchs peuvent également être déployés en mode NX-OS ou autonome.

L'ACI Cisco est destinée aux déploiements de data Center axés sur les besoins d'une application spécifique. Les applications sont instanciées via une série de profils et de contrats permettant la connectivité de l'hôte ou de la machine virtuelle (VM) jusqu'au stockage.

FlexPod est validé avec les deux modes de fonctionnement des commutateurs Cisco Nexus. Pour plus d'informations sur l'ACI et les modes NX-OS, consultez les pages Cisco suivantes :

- "Application Centric Infrastructure (ACI) de Cisco"
- "Logiciel Cisco NX-OS"

Configuration matérielle minimale requise

Une configuration FlexPod Datacenter présente des exigences matérielles minimales, y compris, mais sans s'y limiter, les commutateurs, les interconnexions de fabric, les serveurs et les contrôleurs de stockage NetApp.

Vous devez utiliser des serveurs Cisco UCS. Les serveurs C-Series et B-Series ont été utilisés dans les designs validés. Les Cisco Nexus Fabric Extender (FEXs) sont disponibles en option avec des serveurs C-Series.

Une configuration FlexPod présente la configuration matérielle minimale suivante :

- Deux commutateurs Cisco Nexus dans une configuration redondante. Cette configuration peut consister en deux commutateurs redondants des gammes Cisco Nexus 5000, 7000 ou 9000. Les deux commutateurs doivent être du même modèle et être configurés dans le même mode de fonctionnement.

  Si vous déployez une architecture ACI, vous devez respecter les exigences supplémentaires suivantes :

  - Déployez les commutateurs Cisco Nexus 9000 Series en topologie Leaf-Spine.
  - Utilisez trois contrôleurs d'infrastructure des politiques d'applications Cisco (contrôleurs APIC).
- Deux Cisco UCS 6200, 6300 ou 6400 Series Fabric Interconnect dans une configuration redondante.
- Serveurs Cisco UCS :
  - Si la solution utilise des serveurs B-Series, un châssis de serveur lame Cisco UCS 5108 B-Series et deux serveurs lames Cisco UCS B-Series et deux modules d'E/S (IOM) de 2104, 2204/8, 2408 ou 2304.
  - Si la solution utilise des serveurs C-Series, deux serveurs en rack Cisco UCS C-Series.

    Pour des déploiements de serveurs en rack Cisco UCS C-Series plus importants, vous pouvez choisir une paire de modules FEX 22 32PP. Toutefois, le 2232PP n'est pas obligatoire en termes de matériel.
- Deux contrôleurs de stockage NetApp dans une configuration de paires haute disponibilité :

  Cette configuration peut se composer de n'importe quel contrôleur de stockage NetApp FAS, AFF ou ASA

pris en charge. Voir la "NetApp Hardware Universe" Application pour une liste actuelle des modèles de contrôleurs FAS, AFF et ASA pris en charge.

  - La configuration haute disponibilité requiert deux interfaces redondantes par contrôleur pour l'accès aux données ; les interfaces peuvent être FCoE, FC ou Ethernet 10/25 Gb (GbE).
  - Si la solution utilise NetApp ONTAP, une topologie d'interconnexion de cluster approuvée par NetApp est requise. Pour plus d'informations, reportez-vous à la section "Commutateurs" De l'onglet NetApp Hardware Universe.
  - Si la solution utilise le protocole ONTAP, deux ports 10/25 GbE supplémentaires par contrôleur sont requis pour l'accès aux données.
  - Dans le cas de clusters ONTAP avec deux nœuds, vous pouvez configurer un cluster à deux nœuds sans commutateur.
  - Pour les clusters ONTAP de plus de deux nœuds, une paire de commutateurs d'interconnexion de cluster est requise.
- Un tiroir disque NetApp avec tous les types de disques pris en charge. Voir l'onglet étagères du "NetApp Hardware Universe" vous trouverez la liste actuelle des modèles de tiroirs disques pris en charge.

Configuration logicielle minimale requise

Une configuration FlexPod présente la configuration logicielle minimale suivante :

- NetApp ONTAP :
  - La version du logiciel ONTAP nécessite ONTAP 9.1 ou une version ultérieure
- Versions de Cisco UCS Manager :
  - Interconnexion de fabric Cisco UCS 6200 Series—2.2(8a)
  - Fabric Interconnect Cisco UCS 6300 série 3.1(1e)
  - Fabric Interconnect Cisco UCS 6400 Series, 4.0(1)
- Cisco Intersight Managed mode :
  - Fabric Interconnect Cisco UCS 6400 Series – 4.1(2)
- Pour les commutateurs Cisco Nexus 5000, le logiciel Cisco NX-OS version 5.0(3)N1(1c) ou ultérieure, incluant NX-OS 5.1.x
- Pour les commutateurs Cisco Nexus 7000 Series :
  - Le châssis à 4 slots nécessite la version 6.1(2) ou ultérieure du logiciel Cisco NX-OS
  - Le châssis à 9 slots nécessite la version 5.2 ou ultérieure du logiciel Cisco NX-OS
  - Le châssis à 10 slots nécessite la version 4.0 ou ultérieure du logiciel Cisco NX-OS
  - Le châssis à 18 slots nécessite la version 4.1 ou ultérieure du logiciel Cisco NX-OS
- Pour les commutateurs Cisco Nexus 9000, le logiciel Cisco NX-OS version 6.1(2) ou ultérieure

Les logiciels utilisés dans une configuration FlexPod doivent être répertoriés et pris en charge par le système NetApp "IMT". Certaines fonctionnalités peuvent nécessiter des versions plus récentes du logiciel que celles répertoriées.

Les besoins en connectivité

Une configuration FlexPod présente les exigences de connectivité suivantes :

- Tous les composants doivent utiliser un réseau de gestion hors bande Ethernet 100 Mbit/s distinct.
- NetApp vous recommande d'activer la prise en charge des trames Jumbo dans l'ensemble de l'environnement, mais pas requise.
- Les ports d'appliance Cisco UCS Fabric Interconnect sont recommandés uniquement pour les connexions iSCSI et NAS.
- Aucun équipement supplémentaire ne peut être placé en ligne entre les composants principaux de FlexPod.

Connexions de liaison montante :

- Les ports des contrôleurs de stockage NetApp doivent être connectés aux commutateurs des gammes Cisco Nexus 5000, 7000 ou 9000 pour prendre en charge les canaux de ports virtuels (VPC).
- Les VPC sont requis des commutateurs Cisco Nexus 5000, 7000 ou 9000 vers les contrôleurs de stockage NetApp.
- Les VPC sont requis des commutateurs Cisco Nexus 5000, 7000 ou 9000 vers les interconnexions de fabric.
- Un minimum de deux connexions est requis pour un VPC. Le nombre de connexions au sein d'un VPC peut être augmenté en fonction des exigences de charge et de performances de l'application.

Connexions directes :

- Les ports des contrôleurs de stockage NetApp directement connectés aux Fabric Interconnect peuvent être regroupés pour activer un canal de port. VPC n'est pas pris en charge pour cette configuration.
- Les canaux de port FCoE sont recommandés pour les conceptions FCoE de bout en bout.

Démarrage SAN :

- Les solutions FlexPod sont conçues autour d'une architecture de démarrage SAN qui utilise les protocoles iSCSI, FC ou FCoE. L'utilisation des technologies Boot-from-SAN offre la configuration la plus flexible pour l'infrastructure de data Center et permet d'accéder aux fonctionnalités avancées disponibles dans chaque composant de l'infrastructure. Bien que le démarrage à partir du SAN soit la configuration la plus efficace, le démarrage à partir du stockage du serveur local est une configuration valide et prise en charge.
- Le démarrage SAN via FC-NVME n'est pas pris en charge.

Autres exigences

Une architecture FlexPod nécessite une interopérabilité et des exigences de support supplémentaires :

- Tous les composants matériels et logiciels doivent être répertoriés et pris en charge par le système NetApp "IMT", le "Liste de compatibilité matérielle et logicielle Cisco UCS", Et la matrice d'interopérabilité logicielle et matérielle Cisco UCS.
- Des contrats de support valides sont requis pour tous les équipements, notamment :
  - Prise en charge Smart Net Total Care (SmartNet) pour les équipements Cisco
  - Le support SupportEdge Advisor ou SupportEdge Premium pour les équipements NetApp

Pour plus d’informations, visitez le site NetApp "IMT".

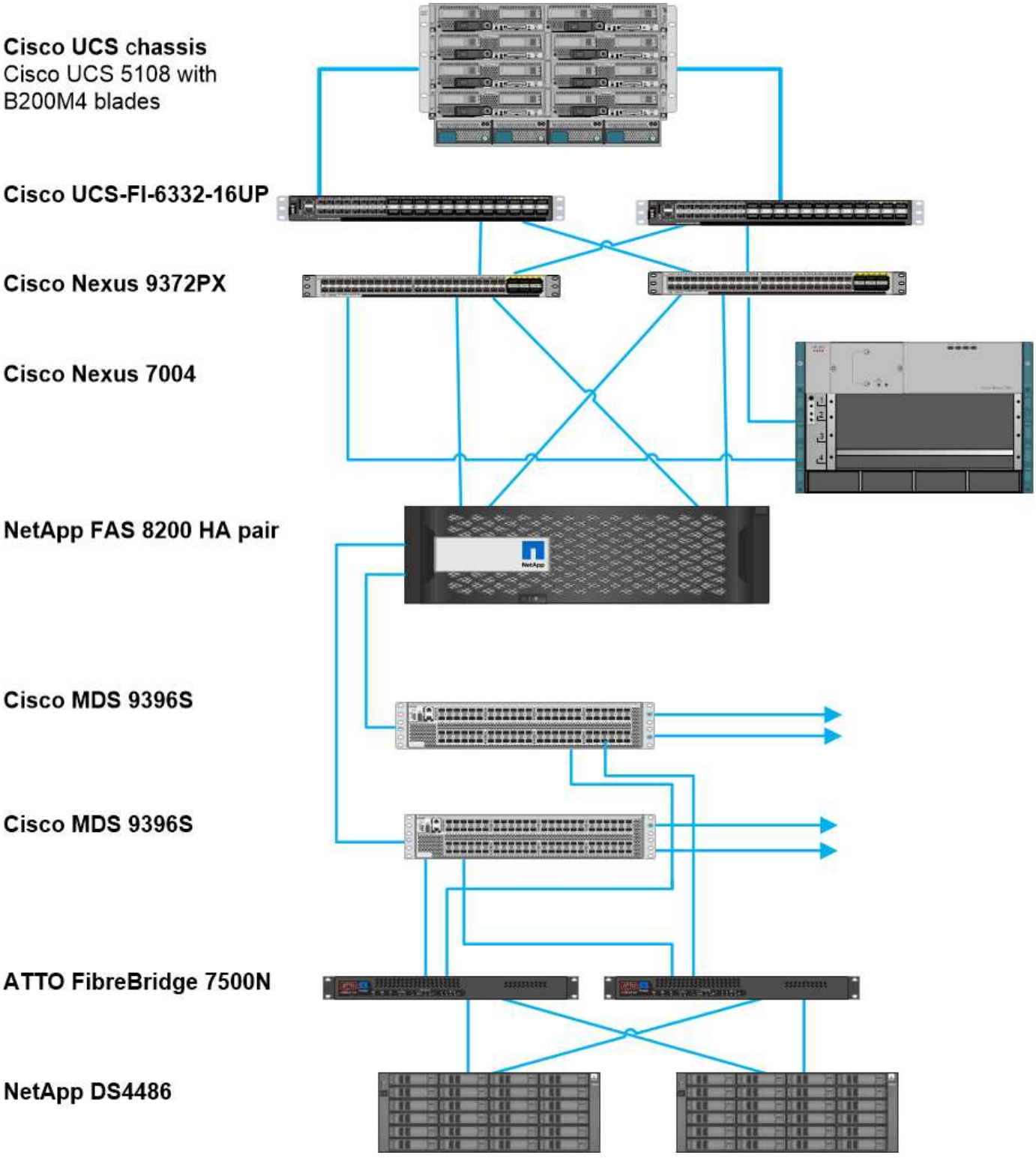
Fonctionnalités en option

NetApp prend en charge plusieurs composants facultatifs pour améliorer encore les architectures FlexPod Datacenter. Les composants facultatifs sont décrits dans les sous-sections suivantes.

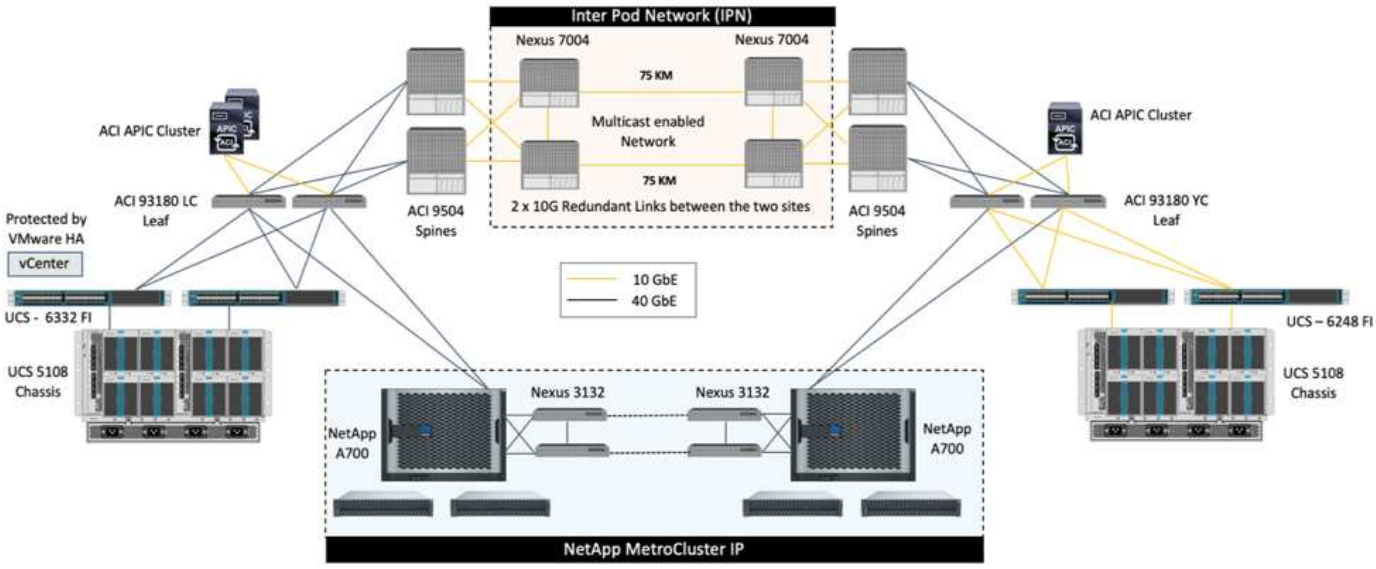
MetroCluster

FlexPod prend en charge les deux versions du logiciel NetApp MetroCluster pour une disponibilité sans interruption dans des configurations en cluster à deux ou quatre nœuds. MetroCluster permet une réplication synchrone des workloads stratégiques. Il requiert une configuration à deux sites connectée aux commutateurs Cisco. La distance maximale prise en charge entre les sites est d’environ 186 km pour les systèmes MetroCluster FC et est supérieure à 435 km pour l’IP MetroCluster. Les figures suivantes illustrent une architecture FlexPod Datacenter avec NetApp MetroCluster et FlexPod Datacenter avec architecture NetApp MetroCluster IP, respectivement.

La figure suivante représente FlexPod Datacenter avec architecture NetApp MetroCluster.

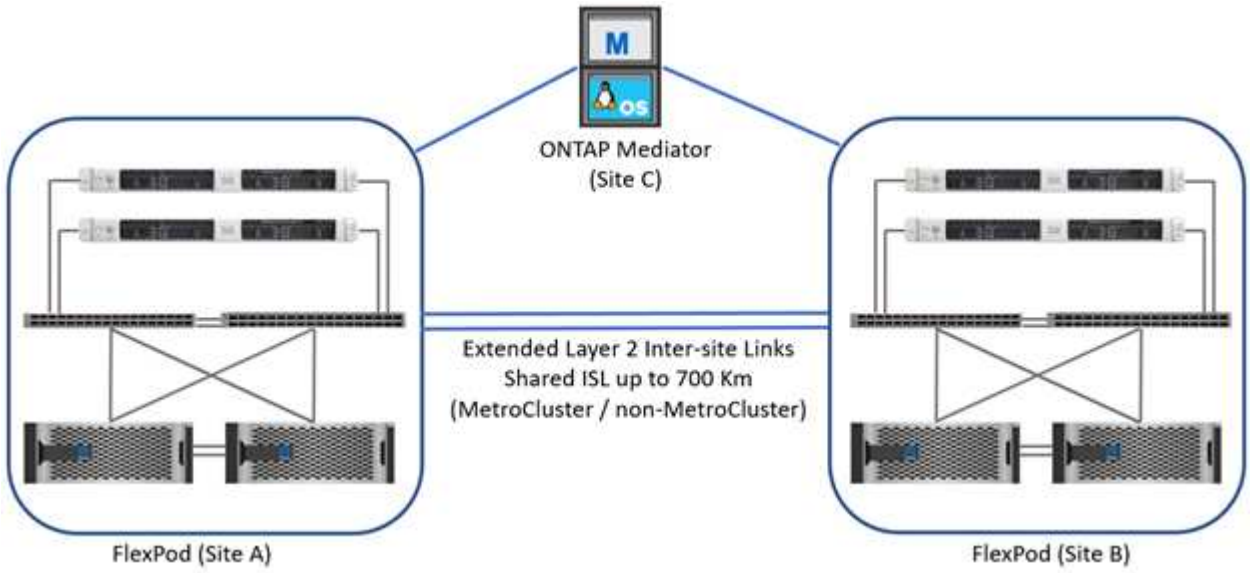


La figure suivante illustre le data Center FlexPod avec l'architecture MetroCluster IP de NetApp.



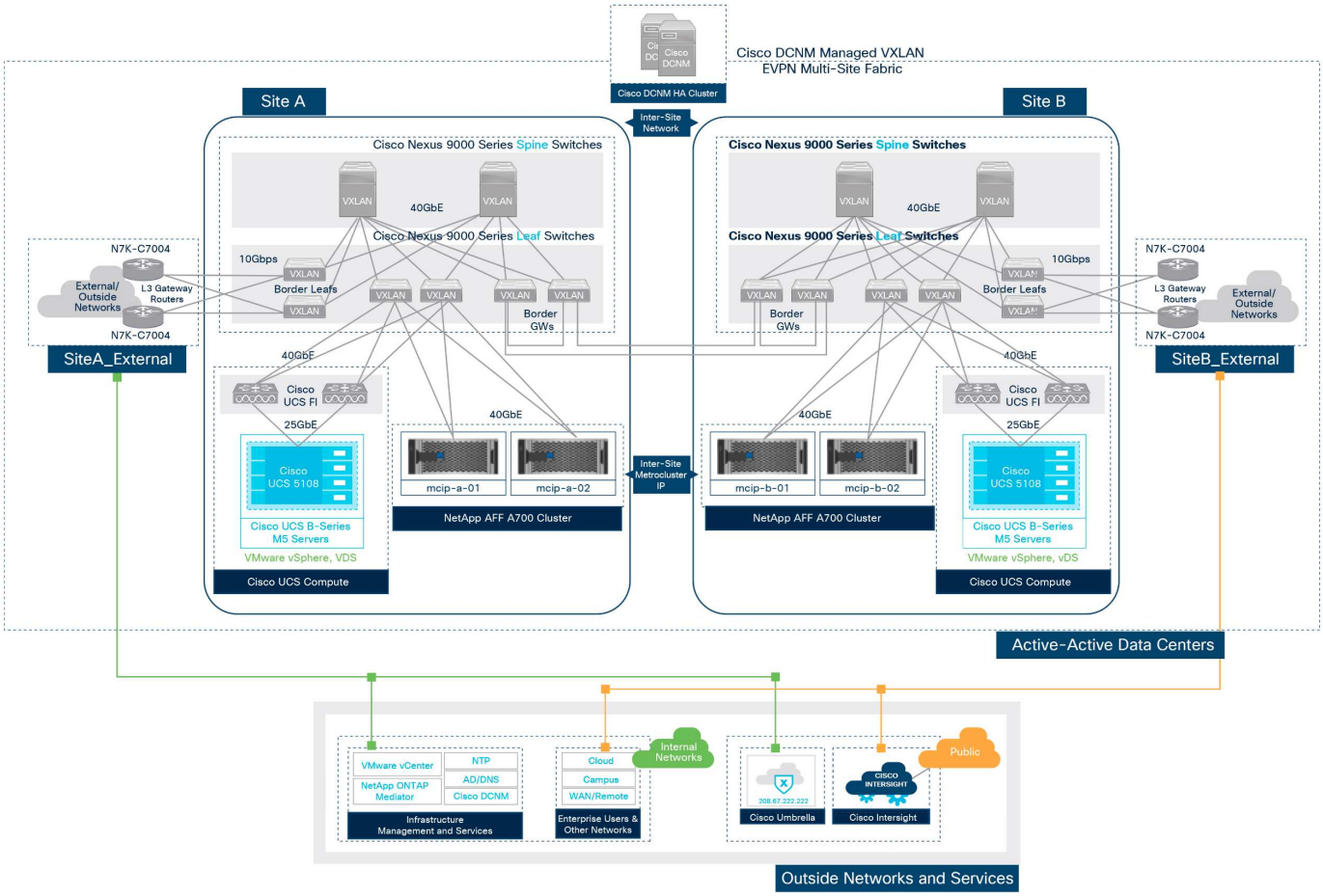
À partir de ONTAP 9.8, ONTAP Mediator peut être déployé sur un troisième site pour surveiller la solution IP MetroCluster et faciliter le basculement non planifié automatisé lorsqu'un incident de site se produit.

Dans le cas d'un déploiement de solution IP FlexPod MetroCluster avec une connectivité site à site étendue couche 2, vous pouvez réaliser des économies en partageant des liens ISL et en utilisant des commutateurs FlexPod comme commutateurs IP MetroCluster conformes si la bande passante réseau et les commutateurs répondent aux exigences indiquées dans la figure suivante, Qui représente la solution IP de FlexPod MetroCluster avec partage de liens ISL et commutateurs conformes.

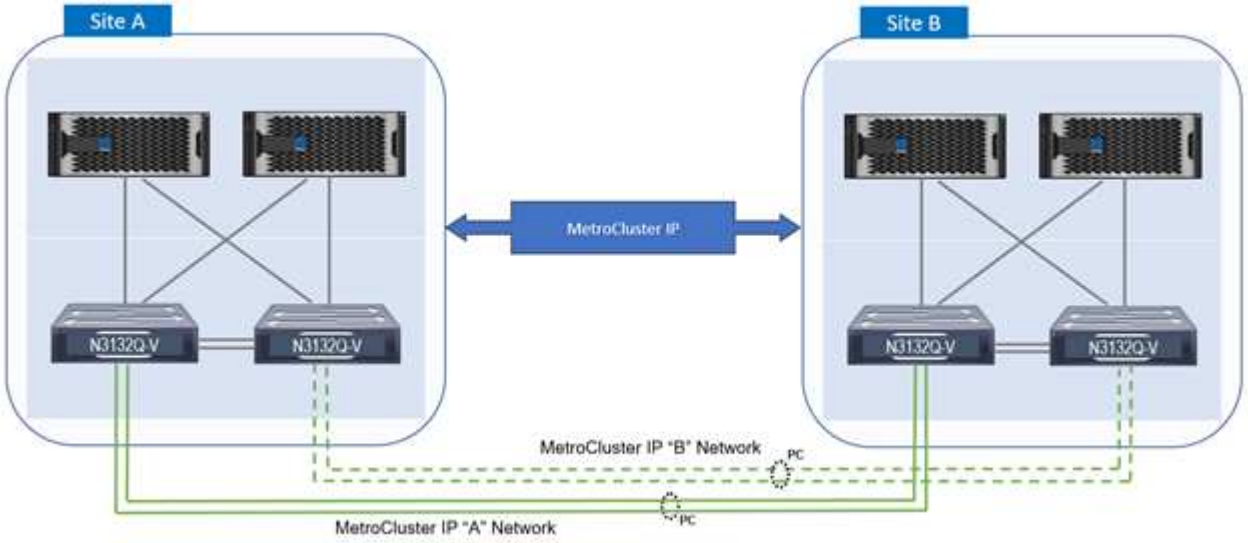


Les deux figures suivantes illustrent la structure multi-sites VXLAN et la structure de stockage IP MetroCluster pour une solution IP FlexPod MetroCluster avec déploiement de structure multisite VXLAN.

- Structure multisite VXLAN pour solution IP FlexPod MetroCluster



- Structure de stockage IP MetroCluster pour solution FlexPod MetroCluster IP



FC-NVMe de bout en bout

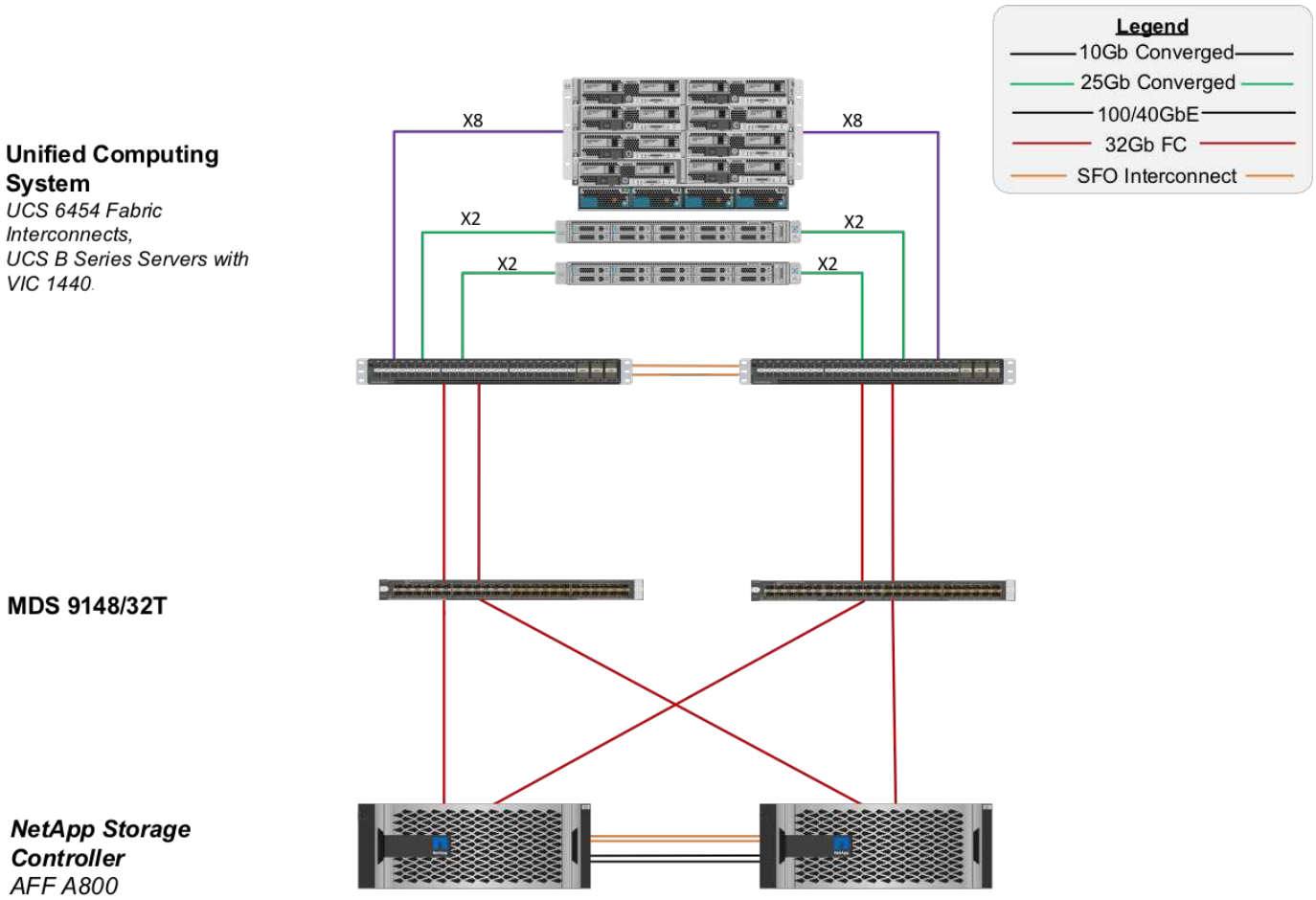
Une connectivité FC-NVMe de bout en bout étend de manière transparente l'infrastructure SAN existante du client aux applications en temps réel, tout en offrant une amélioration des IOPS et du débit avec une latence réduite.

Un transport SAN FC 32 G existant peut être utilisé pour transporter simultanément les charges de travail NVMe et SCSI.

La figure suivante illustre le data Center FlexPod pour FC avec Cisco MDS.

Pour plus d'informations sur la configuration de FlexPod et ses avantages en termes de performances, consultez "Livre blanc NVMe de bout en bout pour FlexPod :"

Pour plus d'informations sur la mise en œuvre de ONTAP, reportez-vous à "Tr-4684 : implémentation et configuration des SAN modernes avec NVMe"la section.



Démarrage SAN FC via Cisco MDS

Pour offrir une meilleure évolutivité grâce à un réseau SAN dédié, FlexPod prend en charge FC via des commutateurs Cisco MDS et Nexus avec prise en charge FC tels que Cisco Nexus 93108TC-FX. L'option de démarrage FC SAN via Cisco MDS présente les exigences matérielles et de licence suivantes :

- Au moins deux ports FC par contrôleur de stockage NetApp ; un port pour chaque structure SAN
- Une licence FC sur chaque contrôleur de stockage NetApp
- Les switchs Cisco MDS et les versions de firmware pris en charge sur le système NetApp "IMT"

Pour plus de conseils sur une conception MDS, consultez le CVD "Guide de déploiement de FlexPod Datacenter avec VMware vSphere 6.7U1 Fibre Channel et iSCSI".

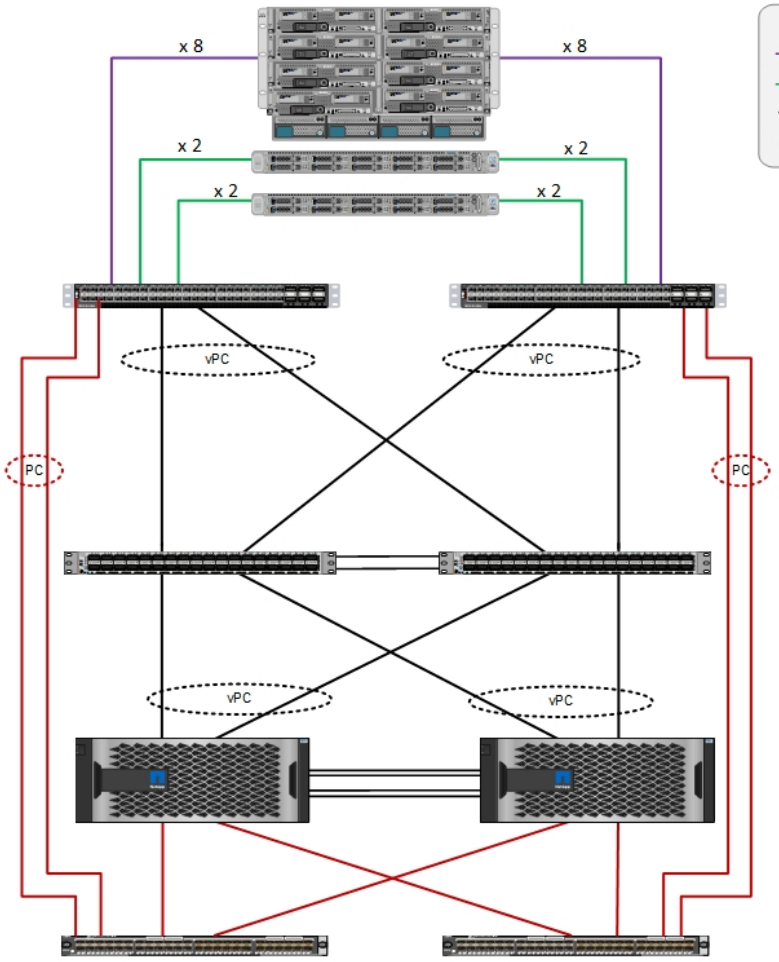
Les figures suivantes illustrent un exemple de data Center FlexPod pour FC avec connectivité MDS et FlexPod Datacenter pour FC avec Cisco Nexus 93180YC-FX, respectivement.

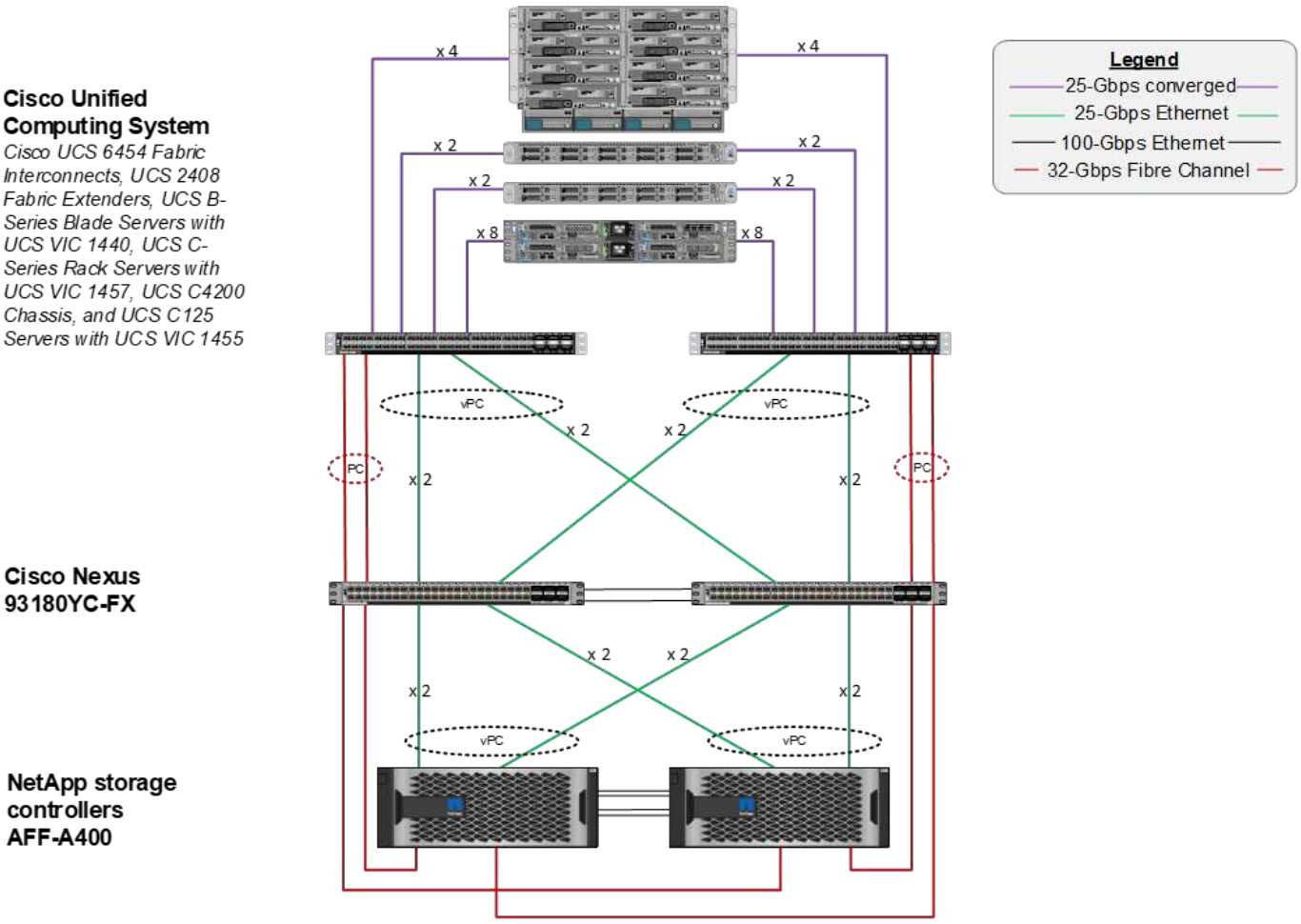
Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS B-Series Blade Servers with UCS VIC 1440, and UCS C-Series Rack Servers with UCS VIC 1457

Cisco Nexus 9336C-FX2

NetApp storage controllers AFF-A800

Cisco MDS 9148T or 9132T switch





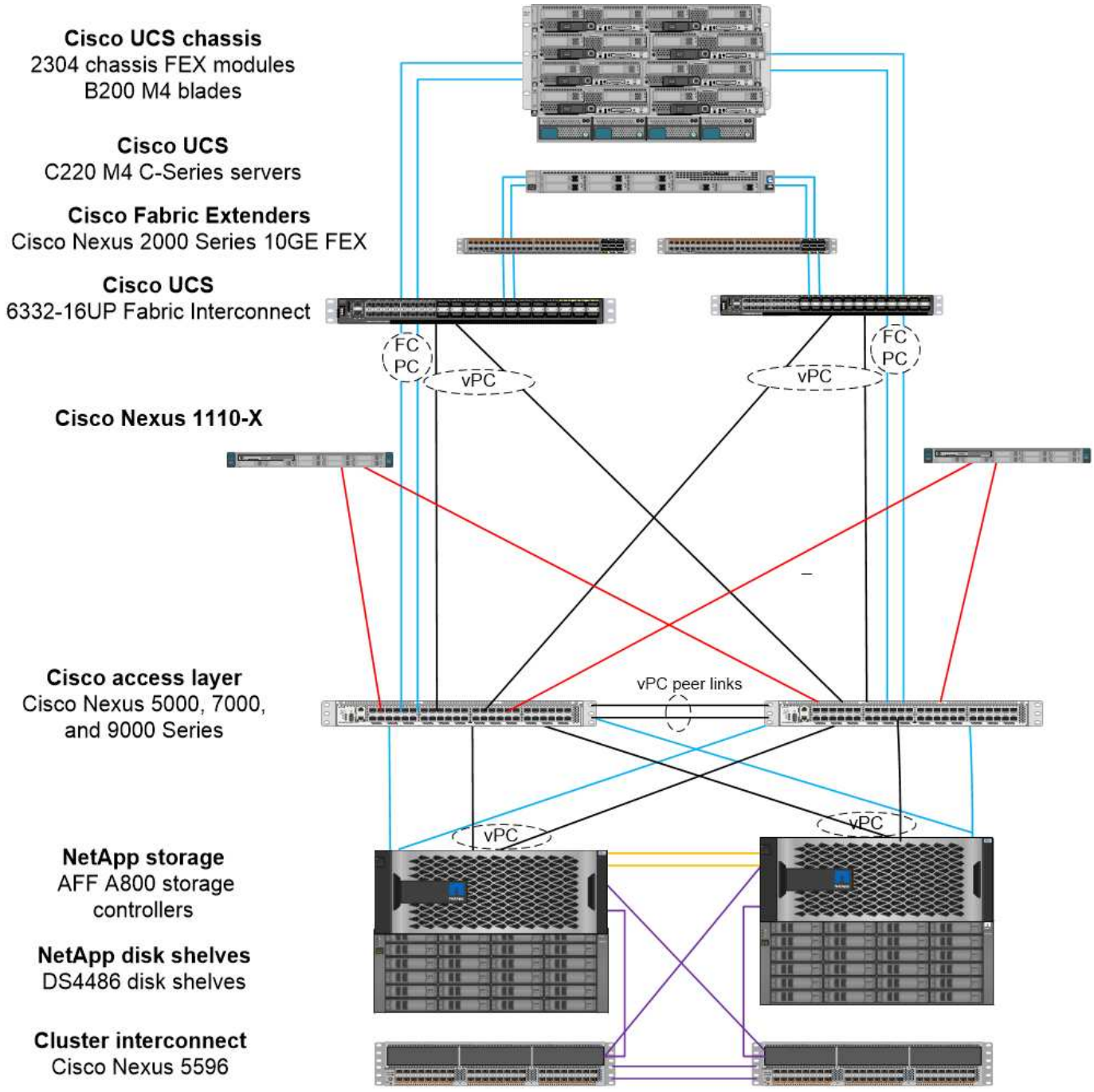
Démarrage SAN FC avec Cisco Nexus

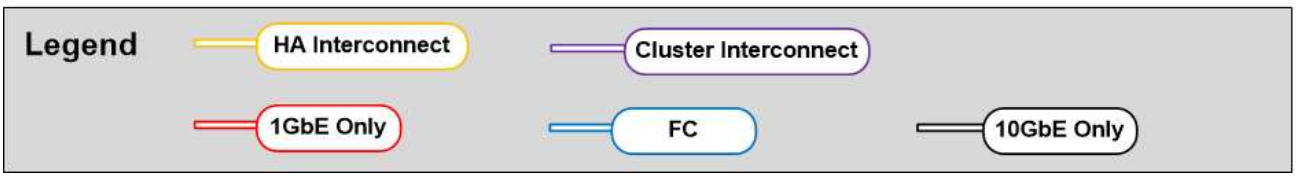
L'option de démarrage FC SAN classique présente les exigences matérielles et de licence suivantes :

- Lorsque la segmentation FC est effectuée sur le commutateur Cisco Nexus 5000 Series, une licence Storage Protocols Service Package pour les commutateurs Cisco Nexus 5000 Series (FC_FEATURES_PKG) est requise.
- Lors d'une segmentation FC sur le commutateur Cisco Nexus série 5000, des liaisons SAN sont requises entre le Fabric Interconnect et le commutateur Cisco Nexus série 5000. Pour une redondance supplémentaire, les canaux de port SAN sont recommandés entre les liaisons.
- Les commutateurs Cisco Nexus 5010, 5020 et 5548P nécessitent un module FC ou universel distinct (UP) pour la connectivité dans l'interconnexion de structure Cisco UCS et dans le contrôleur de stockage NetApp.
- Le Cisco Nexus 93180YC-FX requiert une licence FC pour permettre l'activation de FC.
- Chaque contrôleur de stockage NetApp nécessite au moins deux ports FC 8/16 Gb pour la connectivité.
- Une licence FC est requise sur le contrôleur de stockage NetApp.

> L'utilisation des commutateurs Cisco Nexus 7000 ou 9000 s'oppose à l'utilisation de FC classiques, sauf si un zoning FC est effectué dans l'interconnexion de fabric. Dans ce cas, les liaisons ascendantes SAN vers le commutateur ne sont pas prises en charge.

La figure suivante montre une configuration de la connectivité FC.





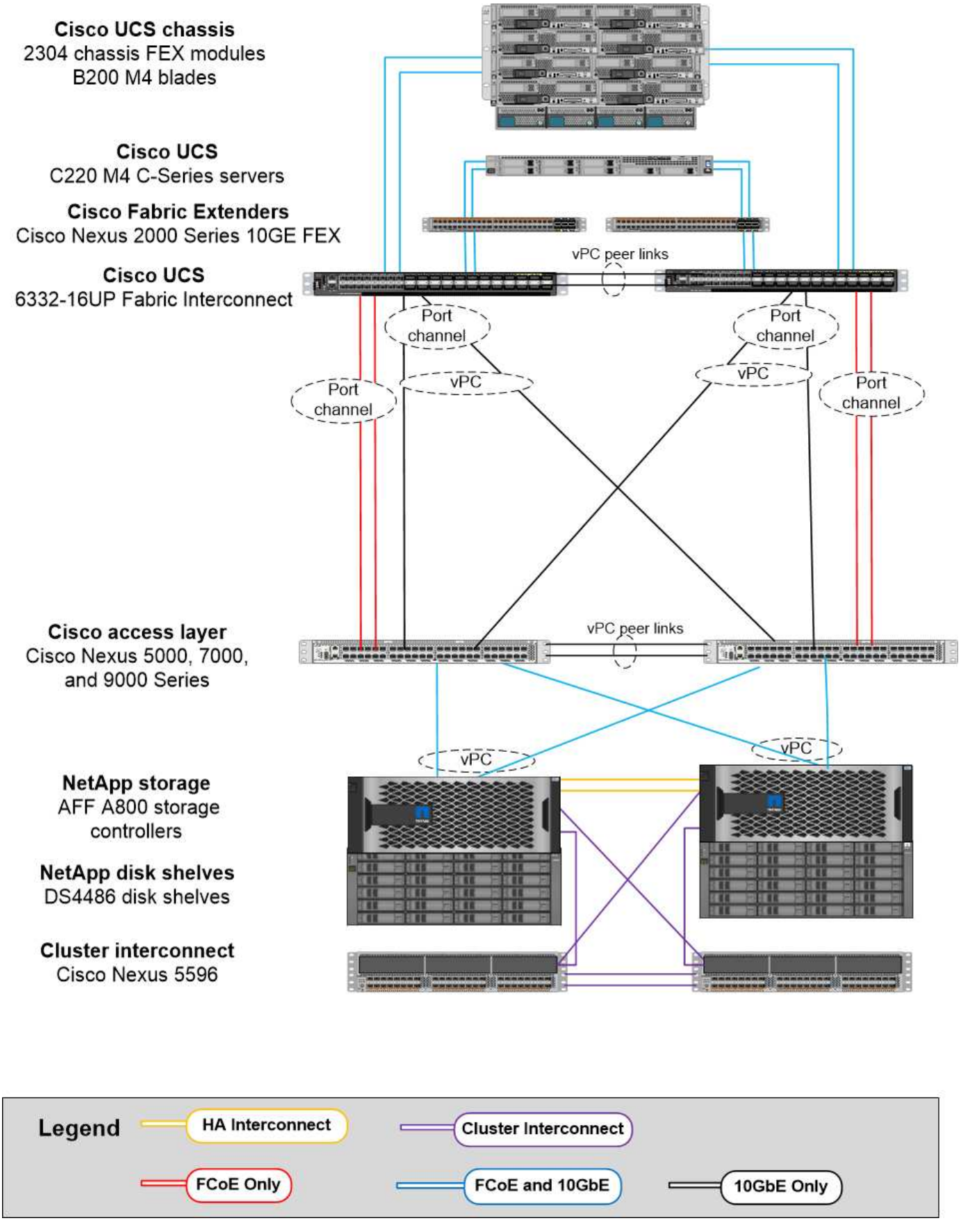
Option de démarrage SAN FCoE

L'option de démarrage SAN FCoE nécessite les licences et la configuration matérielle suivantes :

- Lorsque la segmentation FC est effectuée sur le commutateur, une licence Storage Protocols Service Pack pour les commutateurs Cisco Nexus 5000 ou 7000 (`FC_FEATURES_PKG`) est obligatoire.
- Lors de la segmentation FC sur le commutateur, des liaisons montantes FCoE sont nécessaires entre l'interconnexion de structure et les commutateurs des gammes Cisco Nexus 5000 ou 7000. Pour une redondance supplémentaire, les canaux de port FCoE sont également recommandés entre les liaisons.
- Chaque contrôleur de stockage NetApp nécessite au moins une carte d'extension (UTA) à double port pour la connectivité FCoE, sauf si des ports UTA2 (adaptateurs « Unified Target 2 ») intégrés sont présents.
- Cette option requiert une licence FC sur le contrôleur de stockage NetApp.
- Si vous utilisez les commutateurs Cisco Nexus 7000 Series et que la segmentation FC est effectuée sur le commutateur, une carte de ligne capable de prendre en charge le protocole FCoE est nécessaire.

> L'utilisation de commutateurs Cisco Nexus 9000 Series évite l'utilisation de FCoE, sauf si la segmentation FC est effectuée dans l'interconnexion de structure et que le stockage est connecté aux interconnexions de fabric avec les ports de type appliance. Dans ce cas, les liaisons montantes FCoE vers le commutateur ne sont pas prises en charge.

La figure suivante montre un scénario de démarrage FCoE.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
Port channel
Port channel
vPC
vPC
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

Option de démarrage iSCSI

L’option de démarrage iSCSI présente les licences et la configuration matérielle suivantes :

- Une licence iSCSI est requise sur le contrôleur de stockage NetApp.
- Vous devez disposer d’un adaptateur du serveur Cisco UCS capable de démarrer iSCSI.
- Un adaptateur Ethernet 10Gb/s à deux ports sur le contrôleur de stockage NetApp est requis.

La figure suivante montre une configuration Ethernet uniquement qui est démarrée à l’aide d’iSCSI.

Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades

Cisco UCS
C220 M4 C-Series servers

Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX

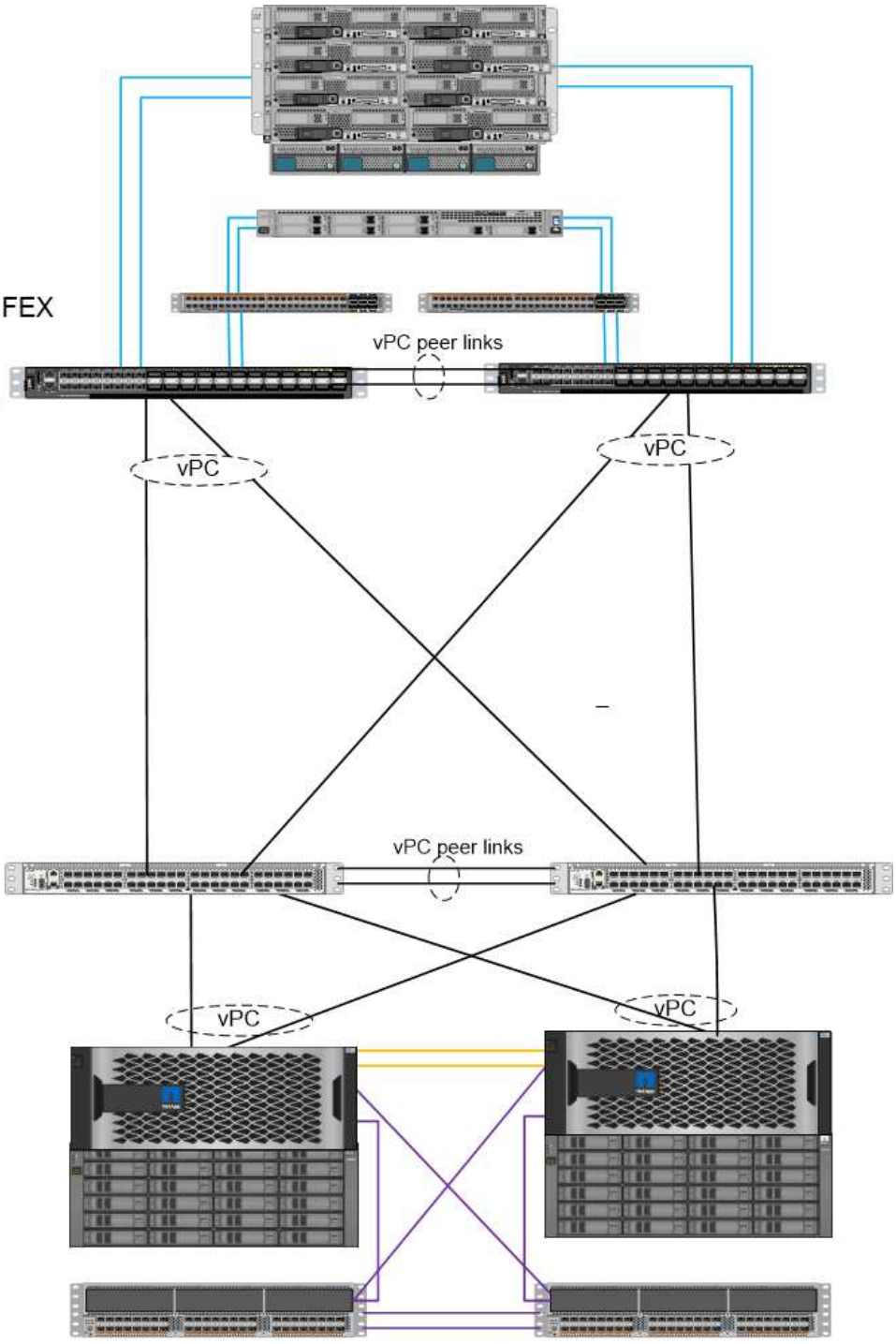
Cisco UCS
6332-16UP Fabric Interconnect

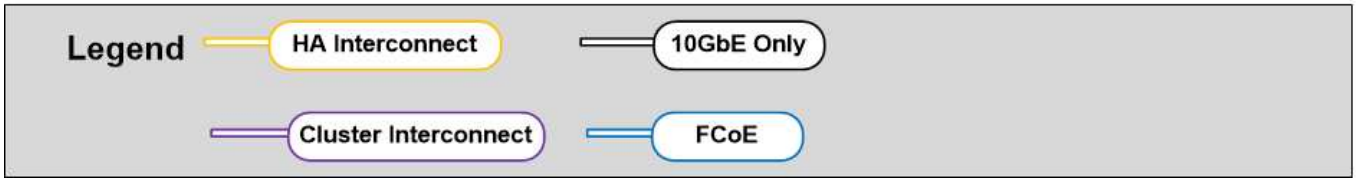
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series

NetApp storage
AFF A800 storage controllers

NetApp disk shelves
DS4486 Disk shelves

Cluster Interconnect
Cisco Nexus 5596





Cisco UCS Direct Connect avec le stockage NetApp

Les contrôleurs NetApp AFF et FAS peuvent être directement connectés aux interconnexions de fabric Cisco UCS sans commutateur SAN en amont.

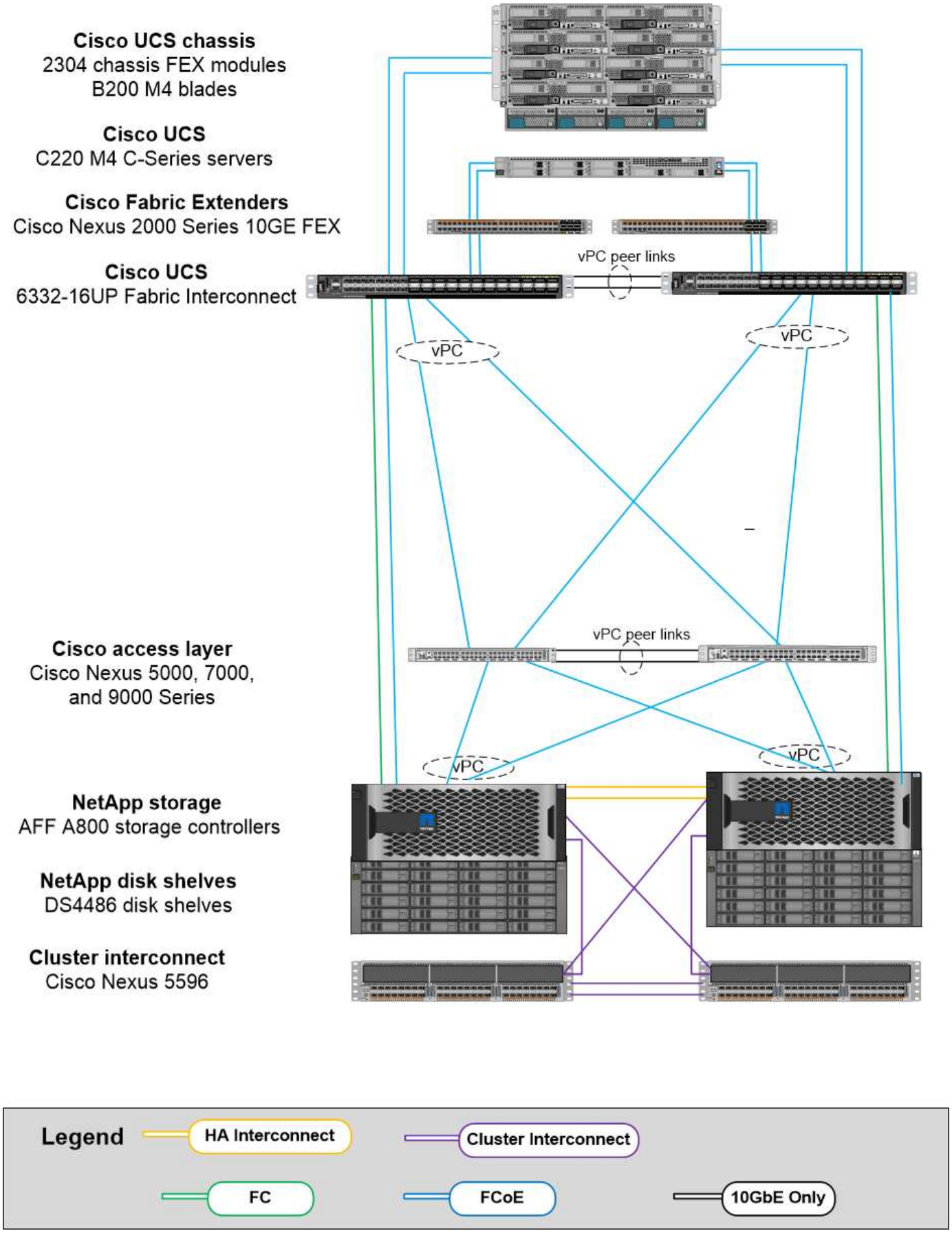
Quatre types de ports Cisco UCS peuvent être utilisés pour la connexion directe au stockage NetApp :

- **Port Storage FC** Connectez directement ce port à un port FC sur le système de stockage NetApp.
- **Port Storage FCoE** Connectez directement ce port à un port FCoE sur le système de stockage NetApp.
- **Port appliance.** Connectez directement ce port à un port 10GbE sur le système de stockage NetApp.
- **Port de stockage unifié.** connectez directement ce port à une UTA NetApp.

La configuration matérielle et de licence est la suivante :

- Une licence de protocole est requise sur le contrôleur de stockage NetApp.
- Un adaptateur Cisco UCS (initiateur) est requis sur le serveur. Pour obtenir la liste des adaptateurs Cisco UCS pris en charge, consultez le site NetApp "IMT".
- Un adaptateur cible est requis sur le contrôleur de stockage NetApp.

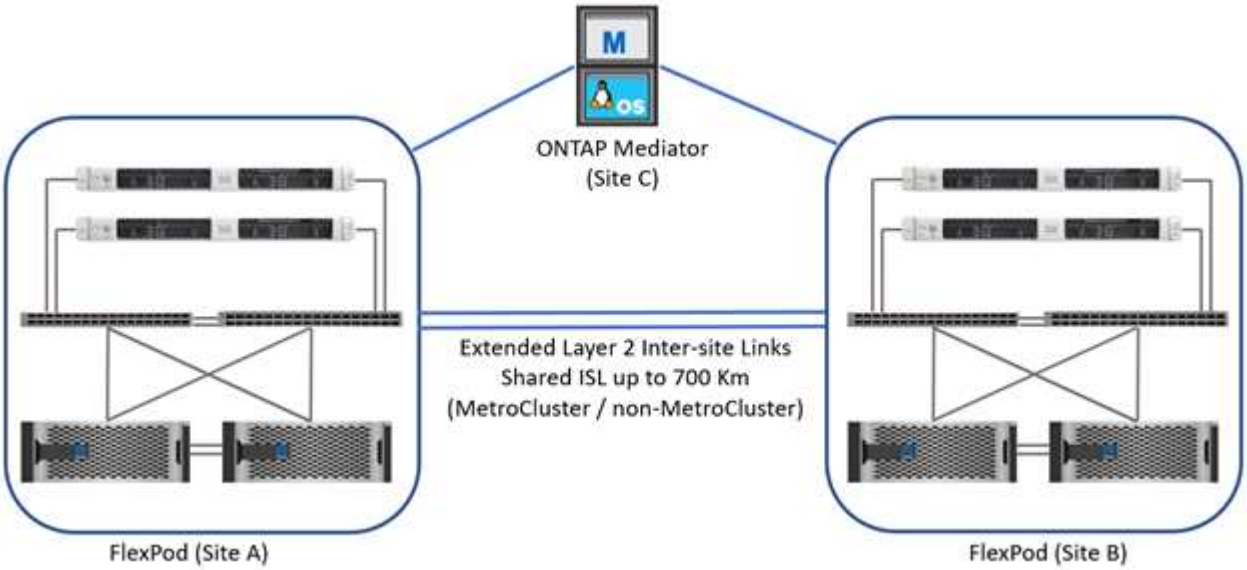
La figure suivante présente une configuration FC à connexion directe.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

Notes:

- Cisco UCS est configuré en mode commutation FC.
- Les ports FCoE de la cible aux interconnexions de fabric sont configurés en tant que ports de stockage FCoE.
- Les ports FC de la cible aux interconnexions de fabric sont configurés en tant que ports de stockage FC.

La figure suivante présente une configuration iSCSI/IP Direct-Connect unifiée.



Notes:

- Cisco UCS est configuré en mode de commutation Ethernet.
- Les ports iSCSI de la cible aux interconnexions de fabric sont configurés en tant que ports de stockage Ethernet pour les données iSCSI.
- Les ports Ethernet de la cible aux interconnexions de fabric sont configurés en tant que ports de stockage Ethernet pour les données CIFS/NFS.

Composants Cisco

Cisco a considérablement contribué au design et à l'architecture de FlexPod, couvrant les couches de calcul et de réseau de la solution. Cette section décrit les options Cisco UCS et Cisco Nexus disponibles pour FlexPod. FlexPod prend en charge les serveurs Cisco UCS B-Series et C-Series.

Options d'interconnexion de fabric Cisco UCS

Des interconnexions de fabric redondantes sont requises dans l'architecture FlexPod. Lorsque vous ajoutez plusieurs châssis Cisco UCS à une paire d'interconnexions de fabric, n'oubliez pas que le nombre maximal de châssis dans un environnement est déterminé par une limite architecturale et par un nombre de ports.

Les références indiquées dans le tableau suivant concernent les interconnexions de structure de base. Ils ne comprennent pas l'unité d'alimentation (PSU), le SFP+, le QSFP+ ou les modules d'extension. D'autres interconnexions de fabric sont prises en charge ; voir "NetApp IMT" pour obtenir une liste complète.

Interconnexion de fabric Cisco UCS	Numéro de référence	Caractéristiques techniques
Cisco UCS 6332UP	UCS-FI-6332-UP	"Fabric Interconnect Cisco UCS 6332"
Cisco UCS 6454	UCS-FI-6454-U	"Fabric Interconnect Cisco UCS 6454"

Cisco UCS 6454

La gamme Cisco UCS 6454 40 propose une connectivité FCoE et Ethernet 10/25/100 GbE sans perte, à fréquence de ligne, avec faible latence et sans perte, ainsi que des ports unifiés capables d'opérer sur des réseaux Ethernet ou FC. Les ports 44 10/25 Gbit/s peuvent fonctionner comme Ethernet 10 Gbit/s ou 25 Gbit/s convergés, dont huit sont des ports unifiés capables d'opérer à 8/16/32 Gbit/s pour FC. Quatre ports fonctionnent à 1/10 Gbit/s pour la connectivité héritée et six ports QSFP servent de ports de liaison montante ou de ports de dérivation 40/100 Gbit/s. Vous pouvez établir une connectivité réseau de bout en bout à 100 Gbit/s avec des contrôleurs de stockage NetApp qui prennent en charge des adaptateurs 100 Gbit/s. Pour la prise en charge des adaptateurs et des plates-formes, reportez-vous à la section "NetApp Hardware Universe".

Pour plus de détails sur les ports, reportez-vous à la section "Fabric Interconnect Cisco UCS 6454" Fiche technique.

Pour connaître les spécifications techniques des modules de données QSFP 100 Gb, consultez le "Fiche technique des modules QSFP Cisco 100GBASE".

Option de châssis Cisco UCS B-Series

Pour utiliser des serveurs lames Cisco UCS B-Series, vous devez disposer d'un châssis Cisco UCS B-Series. Le tableau ci-dessous décrit l'option de châssis Cisco UCS BSeries.

Châssis Cisco UCS B-Series	Numéro de référence	Caractéristiques techniques
Cisco UCS 5108	N20-C6508	"Châssis de serveur lame Cisco UCS 5100 Series"

Chaque châssis lame Cisco UCS 5108 doit disposer de deux IOM Cisco UCS 2200/2300/2400 Series pour assurer une connectivité redondante avec les interconnexions de fabric.

Options des serveurs lames Cisco UCS B-Series

Les serveurs lames Cisco UCS B-Series sont disponibles en deux largeurs et pleine largeur, avec plusieurs options de processeur, de mémoire et d'E/S. Les références répertoriées dans le tableau suivant concernent le serveur de base. Ils ne comprennent pas le processeur, la mémoire, les disques ou les cartes d'adaptateur mezzanine. De nombreuses options de configuration sont disponibles et prises en charge dans l'architecture FlexPod.

Serveurs lames Cisco UCS B-Series	Numéro de référence	Caractéristiques techniques
CISCO UCS B200 M6	NGB-B200-M6	"Serveur lame Cisco UCS B200 M6"

Des générations précédentes de serveurs lames Cisco UCS B-Series peuvent être utilisées dans l'architecture FlexPod, s'ils sont pris en charge sur le système "Liste de compatibilité matérielle et logicielle Cisco UCS". Les

serveurs lames Cisco UCS B-Series doivent également être couverts par un contrat de support SmartNet valide.

Option de châssis Cisco UCS X-Series

Pour utiliser les nœuds de calcul Cisco UCS X-Series, vous devez disposer d'un châssis Cisco UCS X-Series. Le tableau suivant décrit l'option de châssis Cisco UCS X-Series.

Des serveurs lames Cisco UCS X-Series	Numéro de référence	Caractéristiques techniques
Cisco UCS 9508 M6	NGCX-9508	"Châssis Cisco UCX9508 série X"

Chaque châssis Cisco UCS 9508 doit disposer de deux modules de structure intelligente Cisco UCS 9108 pour assurer une connectivité redondante avec les interconnexions de fabric.

Options de périphériques Cisco UCS X-Series

Les nœuds de calcul Cisco UCS X-Series sont disponibles avec plusieurs options de CPU, de mémoire et d'E/S. Les références répertoriées dans le tableau suivant concernent le nœud de base. Ils ne comprennent pas le processeur, la mémoire, les disques ou les cartes d'adaptateur mezzanine. De nombreuses options de configuration sont disponibles et prises en charge dans l'architecture FlexPod.

Nœuds de calcul Cisco UCS X-Series	Numéro de référence	Caractéristiques techniques
Cisco UCS X210c M6	NGCX-210C-M6	"Nœud de calcul Cisco UCS X210c M6"

Options de serveurs en rack Cisco UCS C-Series

Les serveurs rack Cisco UCS C-Series sont disponibles en un ou deux types d'unités de rack (RU), avec diverses options de CPU, de mémoire et d'E/S. Les références répertoriées dans le deuxième tableau ci-dessous concernent le serveur de base. Ils n'incluent pas les processeurs, la mémoire, les disques, les cartes PCIe ou le Fabric Extender Cisco. De nombreuses options de configuration sont disponibles et prises en charge dans l'architecture FlexPod.

Le tableau suivant répertorie les options des serveurs en rack Cisco UCS C-Series.

Serveur en rack Cisco UCS C-Series	Numéro de référence	Caractéristiques techniques
CISCO UCS C220 M6	UCSC-C220-M6	"Serveur en rack Cisco UCS C220 M6"
CISCO UCS C225 M6	UCSC-C225-M6	"Serveur rack Cisco UCS C225 M6"
CISCO UCS C240 M6	UCSC-C240-M6	"Serveur en rack Cisco UCS C240 M6"
CISCO UCS C245 M6	UCSC-C245-M6	"Serveur rack Cisco UCS C245 M6"

Des générations précédentes de serveurs Cisco UCS C-Series peuvent être utilisées dans l'architecture FlexPod, s'ils sont pris en charge sur le système "Liste de compatibilité matérielle et logicielle Cisco UCS". Les serveurs Cisco UCS C-Series doivent également être couverts par un contrat de support SmartNet valide.

Options de commutateurs Cisco Nexus 5000 Series

L'architecture FlexPod requiert des commutateurs redondants Cisco Nexus 5000, 7000 ou 9000. Les références indiquées dans le tableau ci-dessous concernent le châssis Cisco Nexus 5000 Series et n'incluent pas de modules SFP, de modules d'extension FC ou Ethernet.

Commutateur Cisco Nexus série 5000	Numéro de référence	Caractéristiques techniques
Cisco Nexus 56128P	N5K-C56128P	"Commutateurs de plateforme Cisco Nexus 5600"
Cisco Nexus 5672UP-16G	N5K-C5672UP-16G	
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Commutateurs Cisco Nexus 5548 et 5596"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Options des commutateurs Cisco Nexus 7000 Series

L'architecture FlexPod requiert des commutateurs redondants Cisco Nexus 5000, 7000 ou 9000. Les références répertoriées dans le tableau ci-dessous concernent le châssis Cisco Nexus 7000 Series ; elles ne incluent pas de modules SFP, de cartes de ligne ou de blocs d'alimentation, mais elles incluent également des tiroirs de ventilateurs.

Commutateur Cisco Nexus série 7000	Numéro de référence	Caractéristiques techniques
Commutateurs Cisco Nexus 7004	N7K-C7004	"Commutateur Cisco Nexus à 7000 4 emplacements"
Commutateurs Cisco Nexus 7009	N7K-C7009	"Commutateur Cisco Nexus à 7000 9 emplacements"
Commutateurs Cisco Nexus 7702	N7K-C7702	"Commutateur Cisco Nexus 7700 à 2 emplacements"
Commutateurs Cisco Nexus 7706	N77-C7706	"Commutateur Cisco Nexus à 7700 6 emplacements"

Options des commutateurs Cisco Nexus 9000 Series

L'architecture FlexPod requiert des commutateurs redondants Cisco Nexus 5000, 7000 ou 9000. Les références répertoriées dans le tableau ci-dessous s'applique au châssis Cisco Nexus 9000 Series et ne incluent pas de modules SFP ou Ethernet.

Commutateur Cisco Nexus série 9000	Référence	Caractéristiques techniques
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Commutateurs Cisco Nexus 9300 Series"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Cisco Nexus 9336PQ ACI Rachis	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	

Commutateur Cisco Nexus série 9000	Référence	Caractéristiques techniques
Cisco Nexus 92304QC	N9K-C92304QC	"Commutateurs Cisco Nexus 9200 Series"
Cisco Nexus 9236C	N9K-9236C	

Certains commutateurs Cisco Nexus 9000 sont disponibles en versions supplémentaires. Ces variantes sont prises en charge dans le cadre de la solution FlexPod. Pour obtenir la liste complète des commutateurs Cisco Nexus 9000 Series, consultez "Commutateurs Cisco Nexus 9000 Series" Sur le site Web de Cisco.

Options APIC Cisco

Lors du déploiement de Cisco ACI, vous devez configurer les trois APIC Cisco en plus des éléments de la section "Commutateurs Cisco Nexus 9000 Series". Pour plus d'informations sur les tailles des APIC Cisco, consultez le "Fiche technique de l'infrastructure axée sur les applications Cisco."

Pour plus d'informations sur les caractéristiques des produits APIC, reportez-vous aux tableaux 1 à 3 du "Fiche technique de Cisco application Policy Infrastructure Controller".

Options des extenseur de fabric Cisco Nexus

Les FEXs redondants montés en rack Cisco Nexus 2000 sont recommandés pour les grandes architectures FlexPod utilisant des serveurs C-Series. Le tableau ci-dessous décrit quelques options Cisco Nexus FEX. D'autres modèles FEX sont également pris en charge. Pour plus d'informations, reportez-vous à la section "Liste de compatibilité matérielle et logicielle Cisco UCS".

FEX en rack Cisco Nexus	Numéro de référence	Caractéristiques techniques
Cisco Nexus 2232PP	N2K-C232PP	"Fabric Extender Cisco Nexus 2000 Series"
Cisco Nexus 2232TM-E	N2K-C232TM-E	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Fabric Extender Cisco Nexus 2300 pour plateforme"
Cisco Nexus 2348TQCisco Nexus 2348TQ-E	N2K-C2348TQN2K-C2348TQ-E	

Options Cisco MDS

Les commutateurs Cisco MDS sont un composant facultatif de l'architecture FlexPod. Des structures de commutateurs SAN redondants sont requises lorsque vous implémentez le commutateur Cisco MDS pour SAN FC. Le tableau ci-dessous répertorie les références et les détails d'un sous-ensemble des commutateurs Cisco MDS pris en charge. Voir la "NetApp IMT" et "Liste de compatibilité matérielle et logicielle Cisco" Pour obtenir la liste complète des commutateurs SAN pris en charge.

Commutateur Cisco MDS 9000 Series	Numéro de référence	Description
Cisco MDS 9148T	DS-C9148T-24IK	"Commutateurs Cisco MDS 9100 Series"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Commutateurs Cisco MDS 9300 Series"

Options de licences logicielles Cisco

Des licences sont nécessaires pour activer les protocoles de stockage sur les commutateurs Cisco Nexus. Les commutateurs Cisco Nexus 5000 et 7000 exigent tous une licence de services de stockage pour activer le protocole FC ou FCoE dans le cadre des implémentations de démarrage SAN. Pour le moment, les commutateurs Cisco Nexus 9000 ne prennent pas en charge FC ou FCoE.

Les licences requises et les références associées à ces licences varient en fonction des options que vous sélectionnez pour chaque composant de la solution FlexPod. Par exemple, les numéros de référence des licences logicielles varient en fonction du nombre de ports et des commutateurs Cisco Nexus 5000 ou 7000 de votre choix. Consultez votre ingénieur commercial pour obtenir les références exactes. Le tableau ci-dessous répertorie les options de licence logicielle de Cisco.

Licences logicielles Cisco	Numéro de référence	Informations de licence
Licence de stockage Cisco Nexus 5500, 8, 48 et 96 ports	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"Licences des fonctionnalités du logiciel Cisco NX-OS"
Licence pour les protocoles de stockage Cisco Nexus 5010/5020	N5010-SSK9/N5020-SSK9	
Licence pour les protocoles de stockage Cisco Nexus 5600	N56-16P-SSK9/N5672-72P-SSK9/N56128-128P-SSK9	
Licence d'entreprise de stockage Cisco Nexus 7000	N7K-SAN1K9	
Licence Cisco Nexus 9000 Enterprise Services	N95-LAN1K9/N93-LAN1K9	

Options de licence de prise en charge par Cisco

Des contrats de support SmartNet valides sont requis sur tous les équipements Cisco de l'architecture FlexPod.

Les licences requises et les références de ces licences doivent être vérifiées par votre représentant commercial car elles peuvent varier en fonction des différents produits. Le tableau ci-dessous répertorie les options de licence de support de Cisco.

Licences du support Cisco	Guide de licence
Smart Net Total Care Premium sur site	"Service Cisco Smart Net Total Care"

Composants NetApp

Les contrôleurs de stockage NetApp constituent la base du stockage de l'architecture FlexPod pour le stockage des données de démarrage et d'applications. Les composants NetApp sont notamment des contrôleurs de stockage, des commutateurs d'interconnexion de cluster, des disques et des tiroirs disques, ainsi que des options de licence.

Options de contrôleurs de stockage NetApp

Des contrôleurs NetApp FAS, AFF ou AFF ASA redondants sont requis dans l'architecture FlexPod. Ils exécutent le logiciel ONTAP. Lorsque les contrôleurs de stockage sont commandés, la version logicielle

préférée peut être préchargée sur les contrôleurs. Pour ONTAP, un cluster complet est commandé. Un cluster complet inclut une paire de contrôleurs de stockage et une interconnexion de cluster (commutateur ou sans commutateur).

Différentes options et configurations sont disponibles, en fonction de la plateforme de stockage sélectionnée. Pour plus d'informations sur ces composants supplémentaires, adressez-vous à votre représentant commercial.

Les gammes de contrôleurs répertoriées dans le tableau ci-dessous peuvent être utilisées dans une solution de data Center FlexPod, car leur connexion aux commutateurs Cisco Nexus est transparente. Voir la "NetApp Hardware Universe" pour en savoir plus sur la compatibilité de chaque modèle de contrôleur.

Gamme de contrôleurs de stockage	Caractéristiques techniques
Gamme AFF A-Series	"Documentation AFF A-Series"
GAMME AFF ASA A-SERIES	"Documentation AFF ASA A-Series"
Gamme FAS	"Documentation sur la gamme FAS"

Options de commutateurs d'interconnexion de cluster

Le tableau suivant répertorie les commutateurs d'interconnexion de cluster Nexus disponibles pour les architectures FlexPod. Par ailleurs, FlexPod prend en charge tous les commutateurs en cluster pris en charge par ONTAP, y compris les commutateurs non Cisco, à condition qu'ils soient compatibles avec la version de ONTAP déployée. Voir la "NetApp Hardware Universe" pour plus de détails sur la compatibilité des modèles de commutateurs spécifiques.

Commutateur d'interconnexion de cluster	Caractéristiques techniques
Cisco Nexus 3132Q-V	"Documentation NetApp : commutateurs Cisco Nexus 3132Q-V"
Cisco Nexus 9336C-FX2	"Documentation NetApp : commutateurs Cisco Nexus 9336C-FX2"

Options de tiroirs disques et de disques NetApp

Tous les contrôleurs de stockage doivent utiliser un minimum d'un tiroir disque NetApp.

Le type de tiroir NetApp sélectionné détermine les types de disques disponibles dans ce tiroir.

Pour connaître les références de tous les tiroirs disques et des disques, adressez-vous à votre ingénieur commercial.

Pour plus d'informations sur les disques pris en charge, cliquez sur le lien NetApp Hardware Universe dans le tableau suivant, puis sélectionnez disques pris en charge.

Tiroir disque	Caractéristiques techniques
DS224C	"Tiroirs disques et supports de stockage disques pris en charge sur NetApp Hardware Universe"
DS212C	
DS460C	
NS224	

Options NetApp de licences logicielles

Le tableau suivant répertorie les options de licence logicielle NetApp disponibles pour l'architecture FlexPod Datacenter. Le logiciel NetApp est sous licence au niveau du contrôleur FAS et AFF.

Licences logicielles NetApp	Numéro de référence	Caractéristiques techniques
SW, BNDL complet (contrôleur), -C.	SW-8XXX-COMP-BNDL-C.	"Bibliothèque de produits A–Z."
SW, ONTAP Essentials (contrôleur), -C.	SW-8XXX-ONTAP 9-C.	

Options de licences de support NetApp

Des licences NetApp SupportEdge Premium sont requises pour l'architecture FlexPod, mais les références associées à ces licences varient en fonction des options sélectionnées dans la conception FlexPod. Par exemple, les références des licences logicielles diffèrent en fonction du contrôleur FAS choisi. Pour plus d'informations sur les numéros de référence exacts des licences d'assistance individuelles, consultez votre représentant commercial. Le tableau ci-dessous présente un exemple de licence SupportEdge.

Licences de support NetApp	Numéro de référence	Caractéristiques techniques
SupportEdge Premium 4 heures sur site (mois : 36)	CS-O2-4HR	"NetApp SupportEdge Premium"

Exigences en matière de puissance électrique et de câblage

La conception d'une FlexPod présente des exigences minimales en matière d'alimentation et de câblage.

Les besoins en alimentation électrique

Les exigences en termes d'alimentation pour le data Center FlexPod diffèrent selon l'emplacement où la configuration FlexPod Datacenter est installée.

Pour plus de données sur la puissance maximale requise et pour obtenir d'autres informations détaillées sur l'alimentation, consultez les spécifications techniques de chaque composant matériel répertorié dans la section "Spécifications techniques et références : composants matériels".

Pour en savoir plus sur les données de puissance Cisco UCS, consultez le "Calculateur de puissance Cisco UCS".

Pour connaître les données d'alimentation des contrôleurs de stockage NetApp, consultez le "NetApp Hardware Universe". Sous les plateformes, sélectionnez la plateforme de stockage à utiliser dans la configuration (FAS/V-Series ou AFF). Sélectionnez la version ONTAP et le contrôleur de stockage, puis cliquez

sur le bouton Afficher les résultats.

Exigences minimales en matière de câblage

Le nombre et le type de câbles et d'adaptateurs requis varient selon le déploiement de FlexPod Datacenter. Le type de câble, le type d'émetteur-récepteur et le numéro sont déterminés pendant le processus de conception en fonction de vos besoins. Le tableau ci-dessous répertorie le nombre minimal de câbles requis.

Sous-jacent	Numéro de modèle	Câbles requis
Châssis Cisco UCS	Cisco UCS 5108	Au moins deux câbles Twinax par module Cisco UCS 2104XP, 2204XP ou 2208XP
Interconnexions de fabric Cisco UCS	Cisco UCS 6248UP	• Deux câbles Cat5e pour les ports de gestion • Deux câbles Cat5e pour les interconnexions L1 et L2, par paire d'interconnexions de fabric • Au moins quatre câbles Twinax par interconnexion de fabric • Au moins quatre câbles FC par Fabric Interconnect
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• Deux câbles Cat5e pour les ports de gestion • Deux câbles Cat5e pour les interconnexions L1 et L2, par paire d'interconnexions de fabric • Au moins quatre câbles Twinax par interconnexion de fabric	Cisco UCS 6324
	• Deux ports de gestion 10/100/1000Mbps • Au moins deux câbles Twinax par interconnexion de structure	Commutateurs Cisco Nexus 5000 et 7000
	Cisco Nexus 5000 Series	
• Au moins deux câbles fibre 10 GbE ou Twinax par commutateur • Au moins deux câbles FC par commutateur (si la connectivité FC/FCoE est requise)	Cisco Nexus 7000 Series	Commutateurs Cisco Nexus 9000 Series

Sous-jacent	Numéro de modèle	Câbles requis
Cisco Nexus 9000 Series	Au moins deux câbles 10GbE par commutateur	Contrôleurs NetApp FAS
Gamme AFF A-Series	• Paire de câbles SAS ou SATA par contrôleur de stockage • En cas d'utilisation d'un câble FC existant, au moins deux câbles FC par contrôleur • Au moins deux câbles 10GbE par contrôleur • Au moins un câble GbE pour la gestion par contrôleur • Pour ONTAP, huit câbles Twinax courts sont requis par paire de commutateurs d'interconnexion de cluster	
Gamme FAS	Tiroirs disques NetApp	DS212C
Deux câbles SAS, SATA ou FC par tiroir disque		DS224C
		DS460C
		NS224

Spécifications techniques et références

Les spécifications techniques fournissent des détails sur les composants matériels d'une solution FlexPod, tels que les châssis, les FEXs, les serveurs, les commutateurs, et de stockage netapp.

Châssis de serveur lame Cisco UCS B-Series

Les spécifications techniques du châssis de serveur lame Cisco UCS B-Series, comme illustré dans le tableau ci-dessous, incluent les composants suivants :

- Nombre d'unités de rack
- Nombre maximum de lames
- Fonctionnalité de structure unifiée
- Bande passante d'E/S moyenne par serveur
- Nombre de baies d'E/S pour les FEXs

Composant	Châssis de serveur lame Cisco UCS 5100 Series
Unités en rack	6
Lames pleine largeur maximum	4
Lames demi-largeur maximum	8

Composant	Châssis de serveur lame Cisco UCS 5100 Series
Capacité de la structure unifiée	Oui.
E/S du fond de panier central	Jusqu'à 80 Gbit/s de bande passante d'E/S par serveur
Baies d'E/S pour FEXs	Deux baies pour Cisco UCS 2104XP, 2204/8XP, 2408XP et 2304 FEXs

Pour plus d'informations, reportez-vous à la section "Fiche technique sur les châssis de serveur lame Cisco UCS 5100 Series".

Serveurs lames Cisco UCS B-Series

Les spécifications techniques des serveurs lames Cisco UCS B-Series, comme illustré dans le tableau ci-dessous, incluent les composants suivants :

- Nombre de sockets du processeur
- Prise en charge du processeur
- Capacité de la mémoire
- Dimensionnement et vitesse
- Prise en charge du démarrage SAN
- Nombre de logements d'adaptateur mezzanine
- Débit d'E/S maximal
- Format
- Nombre maximal de serveurs par châssis

Composant	Fiche technique Cisco UCS
CISCO UCS B200 M6	"Serveur lame Cisco UCS B200 M6"

Serveurs en rack Cisco UCS C-Series

Les spécifications techniques des serveurs en rack Cisco UCS C-Series incluent la prise en charge du processeur, la capacité de mémoire maximale, le nombre de connecteurs PCIe et la taille du format. Pour plus d'informations sur les modèles de serveur UCS compatibles, consultez le "Compatibilité matérielle Cisco" liste. Les tableaux suivants illustrent les fiches techniques du serveur rack C-Series et l'option de châssis Cisco UCS C-Series, respectivement.

Composant	Fiche technique Cisco UCS
CISCO UCS C220 M6	"Serveur en rack Cisco UCS C220 M6"
CISCO UCS C225 M6	"Serveur rack Cisco UCS C225 M6"
CISCO UCS C240 M6	"Serveur en rack Cisco UCS C240 M6"
CISCO UCS C245 M6	"Serveur rack Cisco UCS C245 M6"

Châssis Cisco UCS X-Series

Les spécifications techniques du châssis Cisco UCS X-Series, comme illustré dans le tableau ci-dessous, incluent les composants suivants :

- Nombre d'unités de rack
- Nombre maximal de nœuds
- Fonctionnalité de structure unifiée
- Nombre de baies d'E/S pour IFMS

Composant	Châssis de nœud de calcul Cisco UCS 9508 X-Series
Unités en rack	7
Nombre maximal de nœuds	8
Capacité de la structure unifiée	Oui.
Baies d'E/S pour IFMS	Deux baies pour les modules de structure intelligente Cisco UCS 9108 (IFMS)

Pour plus d'informations, reportez-vous à la section "Fiche technique sur le châssis Cisco UCS X9508 X-Series".

Nœud de calcul Cisco UCS X-Series

Les spécifications techniques du nœud de calcul Cisco UCS X-Series, comme illustré dans le tableau ci-dessous, incluent les composants suivants :

- Nombre de sockets du processeur
- Prise en charge du processeur
- Capacité de la mémoire
- Dimensionnement et vitesse
- Prise en charge du démarrage SAN
- Nombre de logements d'adaptateur mezzanine
- Débit d'E/S maximal
- Format
- Nombre maximal de nœuds de calcul par châssis

Composant	Fiche technique Cisco UCS
Cisco UCS X210c M6	"Nœud de calcul Cisco UCS X210c M6"

Recommandation de processeurs graphiques pour FlexPod ai, ML et DL

Les serveurs en rack Cisco UCS C-Series répertoriés dans le tableau ci-dessous peuvent être utilisés dans une architecture FlexPod pour héberger des charges de travail d'IA, DE ML et de DL. Les serveurs Cisco UCS C480 ML M5 sont dédiés aux charges de travail d'IA, DE ML et de DL, ainsi qu'aux processeurs graphiques SXM2 de NVIDIA, tandis que les autres serveurs utilisent des processeurs graphiques PCIe.

Le tableau ci-dessous répertorie également les GPU recommandés qui peuvent être utilisés avec ces serveurs.

Serveur	GPU
CISCO UCS C220 M6	NVIDIA T4
CISCO UCS C225 M6	NVIDIA T4
CISCO UCS C240 M6	NVIDIA TESLA A10, A100
CISCO UCS C245 M6	NVIDIA TESLA A10, A100

Les adaptateurs Cisco UCS VIC pour serveurs lames Cisco UCS B-Series

Les spécifications techniques des adaptateurs Cisco UCS Virtual interface Card (VIC) pour serveurs lames Cisco UCS B-Series incluent les composants suivants :

- Nombre de ports de liaison ascendante
- Performances par port (IOPS)
- Puissance
- Nombre d'orifices de lame
- Déchargement matériel
- Prise en charge de la virtualisation d'entrée/sortie racine unique (SR-IOV)

Toutes les architectures FlexPod actuellement validées utilisent un système Cisco UCS VIC. D'autres adaptateurs sont pris en charge s'ils sont répertoriés sur le système NetApp "IMT" Et sont compatibles avec votre déploiement de FlexPod, mais ils ne fournissent peut-être pas toutes les fonctionnalités présentées dans les architectures de référence correspondantes. Le tableau suivant illustre les fiches techniques de l'adaptateur VIC de Cisco UCS.

Composant	Fiche technique Cisco UCS
Adaptateurs d'interface virtuelle Cisco UCS	"Fiches techniques Cisco UCS VIC"

Interconnexions de fabric Cisco UCS

Les spécifications techniques des interconnexions de fabric Cisco UCS incluent la taille du format, le nombre total de ports et de connecteurs d'extension, ainsi que la capacité de débit. Le tableau suivant illustre les fiches techniques d'interconnexion de structure Cisco UCS.

Composant	Fiche technique Cisco UCS
Cisco UCS 6248UP	"Cisco UCS 6200 Series Fabric Interconnect"
Cisco UCS 6296UP	
Cisco UCS 6324	"Fabric Interconnect Cisco UCS 6324"
Cisco UCS 6300	"Cisco UCS 6300 Series Fabric Interconnect"
Cisco UCS 6454	"Cisco UCS 6400 Series Fabric Interconnect"

Commutateurs Cisco Nexus série 5000

Les spécifications techniques des commutateurs Cisco Nexus 5000 Series, y compris la taille au format, le nombre total de ports et la prise en charge des modules et des cartes filles de couche 3, sont fournies dans la fiche technique de chaque famille de modèles. Ces fiches techniques sont disponibles dans le tableau suivant.

Composant	Fiche technique Cisco Nexus
Cisco Nexus 5548UP	"Commutateur Cisco Nexus 5548UP"
Cisco Nexus 5596UP (2U)	"Commutateur Cisco Nexus 5596UP"
Cisco Nexus 56128P	"Commutateur Cisco Nexus 56128P"
Cisco Nexus 5672UP	"Commutateur Cisco Nexus 5672UP"

Commutateurs Cisco Nexus série 7000

Les spécifications techniques des commutateurs Cisco Nexus 7000 Series, y compris la taille au format et le nombre maximal de ports, sont indiquées dans la fiche technique de chaque gamme de modèles. Ces fiches techniques sont disponibles dans le tableau suivant.

Composant	Fiche technique Cisco Nexus
Commutateurs Cisco Nexus 7004	"Commutateurs Cisco Nexus 7000 Series"
Commutateurs Cisco Nexus 7009	
Commutateurs Cisco Nexus 7010	
Commutateurs Cisco Nexus 7018	
Commutateurs Cisco Nexus 7702	"Commutateurs Cisco Nexus 7700 Series"
Commutateurs Cisco Nexus 7706	
Commutateurs Cisco Nexus 7710	
Commutateurs Cisco Nexus 7718	

Commutateurs Cisco Nexus série 9000

Les spécifications techniques des commutateurs Cisco Nexus 9000 Series figurent dans la fiche technique de chaque modèle. Les spécifications incluent la taille du format, le nombre de superviseurs, le module de structure et les logements de carte de ligne, ainsi que le nombre maximum de ports. Ces fiches techniques sont disponibles dans le tableau suivant.

Composant	Fiche technique Cisco Nexus
Cisco Nexus 9000 Series	"Commutateurs Cisco Nexus 9000 Series"
Cisco Nexus 9500 Series	"Commutateurs Cisco Nexus 9500 Series"
Cisco Nexus 9300 Series	"Commutateurs Cisco Nexus 9300 Series"
Commutateur Cisco Nexus 9336PQ ACI Spine Switch	"Commutateur Cisco Nexus 9336PQ ACI Spine Switch"
Cisco Nexus 9200 Series	"Commutateurs de plateforme Cisco Nexus 9200"

Contrôleur d'infrastructure des politiques d'applications Cisco

Lorsque vous déployez Cisco ACI, en plus des éléments de la section "Commutateurs Cisco Nexus 9000 Series", Vous devez configurer trois circuits intégrés Cisco. Le tableau suivant répertorie la fiche technique du contrôleur APIC Cisco.

Composant	Fiche technique de Cisco application Policy Infrastructure
Contrôleur d'infrastructure des politiques d'applications Cisco	"Fiche technique du contrôleur APIC Cisco"

Détails du extenseur de fabric Cisco Nexus

Les spécifications techniques de Cisco Nexus FEX incluent la vitesse, le nombre de ports et de liaisons fixes ainsi que la taille des formats.

Le tableau suivant répertorie la fiche technique FEX de Cisco Nexus 2000 Series.

Composant	Fiche technique sur les extenseur de fabric Cisco Nexus
Fabric Extender Cisco Nexus 2000 Series	"Fiche technique FEX de la gamme Nexus 2000"

Modules SFP

Pour plus d'informations sur les modules SFP, consultez les ressources suivantes :

- Pour plus d'informations sur le module SFP 10 Gbit/s Cisco, reportez-vous à la section "Modules Cisco 10 Gigabit".
- Pour plus d'informations sur le module SFP 25 Gb Cisco, reportez-vous à la section "Modules Cisco 25 Gigabit".
- Pour plus d'informations sur le module QSFP Cisco, reportez-vous au "Fiche technique sur les modules QSFP Cisco 40GBASE".
- Pour plus d'informations sur le SFP Cisco 100 Gb, consultez la page "Modules Cisco 100 Gigabit".
- Pour plus d'informations sur le module SFP Cisco FC, reportez-vous au "Fiche technique sur les émetteurs-récepteurs enfichables de la gamme Cisco MDS 9000".
- Pour plus d'informations sur tous les modules SFP et émetteurs-récepteurs Cisco pris en charge, reportez-vous à la section "Notes d'installation du module SFP et SFP+ Cisco" et "Modules émetteurs-récepteurs Cisco".

Contrôleurs de stockage NetApp

Les spécifications techniques des contrôleurs de stockage NetApp incluent les composants suivants :

- Configuration de châssis
- Nombre d'unités de rack
- Quantité de mémoire
- Mise en cache NetApp FlashCache
- Taille de l'agrégat

- Taille du volume
- Nombre de LUN
- Stockage réseau pris en charge
- Nombre maximal de volumes NetApp FlexVol
- Nombre maximal d'hôtes SAN pris en charge
- Nombre maximal de copies Snapshot

Gamme FAS

Tous les modèles de contrôleurs de stockage FAS disponibles sont pris en charge dans un data Center FlexPod. Les spécifications détaillées de tous les contrôleurs de stockage FAS sont disponibles dans le "NetApp Hardware Universe". Pour plus d'informations sur un modèle FAS spécifique, reportez-vous à la documentation spécifique à la plate-forme répertoriée dans le tableau suivant.

Composant	Documentation sur la plateforme des contrôleurs de la gamme FAS
Gamme FAS9000	"Fiche technique sur la gamme FAS9000"
Gamme FAS8700	"Fiche technique des baies FAS8700"
Gamme FAS8300	"Fiche technique FAS8300 Series"
Gamme FAS500f	"Fiche technique sur la gamme FAS500f"
Gamme FAS2700	"Fiche technique des systèmes FAS2700 Series"

Gamme AFF A-Series

Tous les modèles actuels de contrôleurs de stockage NetApp AFF A-Series sont pris en charge dans FlexPod. Vous trouverez des informations supplémentaires dans la "Caractéristiques techniques des systèmes AFF" fiche technique et dans le "NetApp Hardware Universe". Pour plus d'informations sur un modèle AFF spécifique, reportez-vous à la documentation spécifique à la plate-forme répertoriée dans le tableau suivant.

Composant	Documentation sur la plateforme du contrôleur AFF A-Series
NetApp AFF A800	"Documentation de la plateforme AFF A800"
NetApp AFF A700	"Documentation sur la plateforme AFF A700"
NetApp AFF A700s	"Documentation de la plateforme AFF A700s"
NetApp AFF A400	"Documentation sur la plateforme AFF A400"
NetApp AFF A250	"Documentation de la plateforme AFF A250"

GAMME AFF ASA A-SERIES

Tous les modèles actuels de contrôleurs de stockage NetApp AFF ASA A-Series sont pris en charge dans FlexPod. Pour plus d'informations, consultez les documents relatifs à la baie SAN uniquement, le rapport technique sur les baies SAN 100 % Flash de ONTAP AFF et le rapport NetApp Hardware Universe. Pour plus d'informations sur un modèle AFF spécifique, reportez-vous à la documentation spécifique à la plate-forme répertoriée dans le tableau suivant.

Composant	Documentation sur la plateforme du contrôleur AFF A-Series
NETAPP AFF ASA A800	"Documentation de la plateforme AFF ASA A800"
NETAPP AFF ASA A700	"Documentation sur la plateforme AFF ASA A700"
NETAPP AFF ASA A400	"Documentation sur la plateforme AFF ASA A400"
NETAPP AFF ASA A250	"Documentation de la plateforme AFF ASA A250"
AVEC AFF ASA A220	"Documentation de la plateforme AFF ASA A220"

Tiroirs disques NetApp

Les spécifications techniques des tiroirs disques NetApp incluent la taille, le nombre de disques par boîtier et les modules d'E/S de tiroir. Cette documentation est disponible dans le tableau suivant. Pour plus d'informations, reportez-vous à la section "Spécifications techniques des tiroirs disques et des supports de stockage NetApp" et le "NetApp Hardware Universe".

Composant	Documentation du tiroir disque FAS/AFF NetApp
Tiroir disque NetApp DS212C	"Documentation des tiroirs disques DS212C"
Tiroir disque NetApp DS224C	"Documentation du tiroir disque DS224C"
Tiroir disque DS460C NetApp	"Documentation des tiroirs disques DS460C"
Tiroir disque SSD NVMe-NS224 de NetApp	"Documentation du tiroir disque NS224"

Disques NetApp

Les spécifications techniques des disques NetApp incluent la taille, la capacité du disque, les tours/min des disques, les contrôleurs et les exigences de version ONTAP. Ces spécifications sont disponibles dans la section entraînements du "NetApp Hardware Universe".

Équipement existant

FlexPod est une solution flexible qui vous permet d'utiliser votre équipement existant et vos nouveaux équipements actuellement commercialisés par Cisco et NetApp. Il arrive que certains modèles d'équipements Cisco et NetApp soient fin de vie.

Bien que ces modèles d'équipement ne soient plus disponibles, si vous avez acheté un de ces modèles avant la date de fin de disponibilité, vous pouvez utiliser cet équipement dans une configuration FlexPod. Vous pouvez consulter la liste complète des anciens modèles pris en charge par FlexPod et non commercialisés sur le "Index de fin de disponibilité des programmes de services et de produits NetApp".

Pour plus d'informations sur les équipements Cisco hérités, consultez les avis de fin de vie et de fin de disponibilité de Cisco pour "Serveurs en rack Cisco UCS C-Series", "Serveurs lames Cisco UCS B-Series", et "Commutateurs Nexus".

La prise en charge du protocole FC existant inclut les éléments suivants :

- Fabric 2 Go
- Structure 4 Go

Les logiciels hérités incluent les éléments suivants :

- NetApp Data ONTAP 7-mode, version 7.3.5 et ultérieure
- ONTAP 8.1.x à 9.0.x
- Cisco UCS Manager 1.3 et versions ultérieures
- Cisco UCS Manager 2.1 à 2.2.7

Où trouver des informations complémentaires

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

- Documentation produit NetApp

  "https://docs.netapp.com/"

- Communications du support NetApp

  "https://mysupport.netapp.com/info/communications/index.html"

- Matrice d'interopérabilité NetApp (IMT)

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe

  "https://hwu.netapp.com/"

- Support NetApp

  "https://mysupport.netapp.com/"

Data Center FlexPod

FlexPod datacenter avec NetApp SnapMirror Business Continuity et ONTAP 9.10

Tr-4920 : continuité de l'activité pour FlexPod Datacenter avec NetApp SnapMirror et ONTAP 9.10

Jyh-shing Chen, NetApp

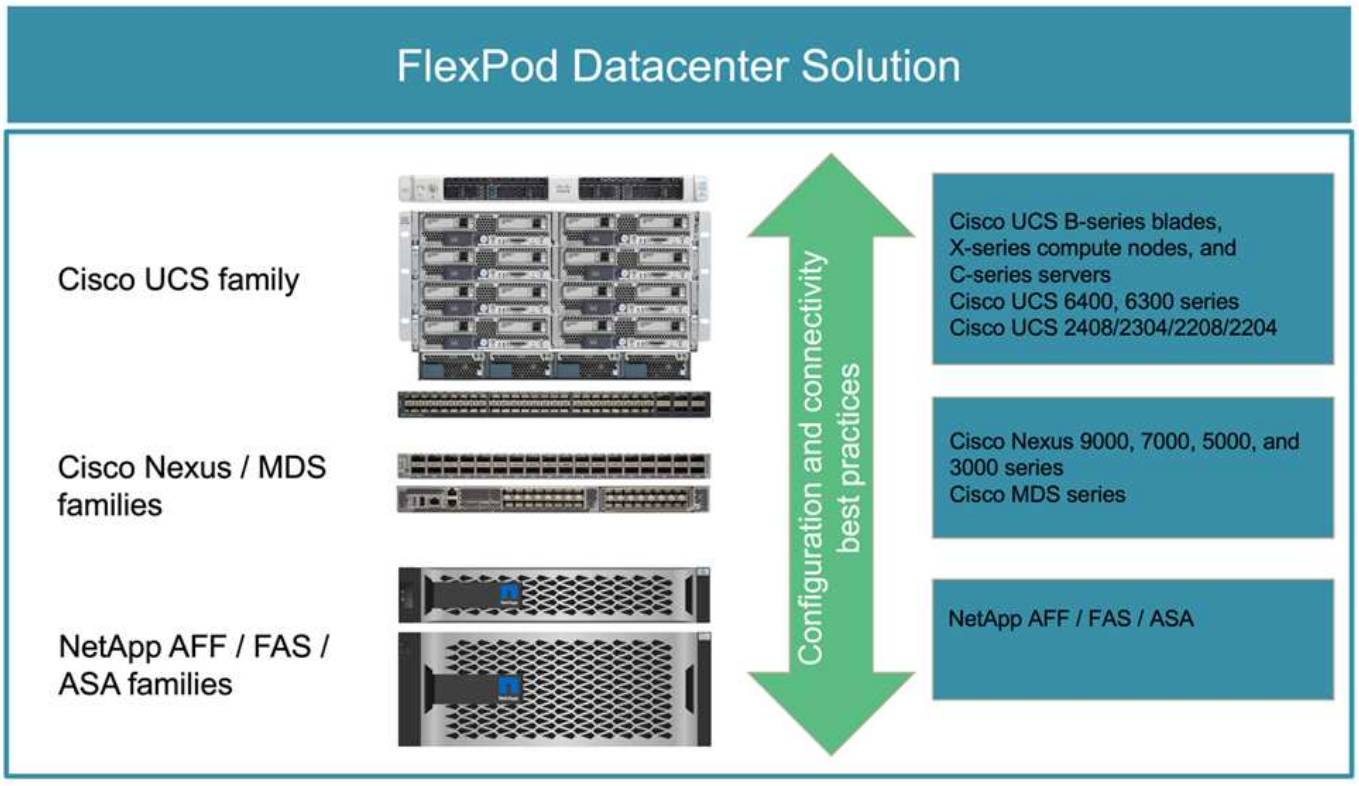
Introduction

Solution FlexPod

FlexPod est une architecture de data Center basée sur les bonnes pratiques. Elle inclut les composants suivants de Cisco et NetApp :

- Serveurs Cisco Unified Computing System (Cisco UCS)
- Gammes de commutateurs Cisco Nexus et MDS
- Systèmes NetApp FAS, NetApp AFF et ASA

La figure suivante décrit certains des composants utilisés pour créer des solutions FlexPod. Ces composants sont connectés et configurés conformément aux meilleures pratiques recommandées par Cisco et NetApp pour fournir une plateforme idéale pour exécuter en toute confiance une variété de charges de travail d'entreprise.



Un large portefeuille de conceptions validées Cisco (CVD) et d'architectures vérifiées NetApp (NVA) est

disponible. Ces CVD et NVA couvrent l'ensemble des charges de travail majeures des data centers et résultent d'une collaboration et d'innovations continues entre NetApp et Cisco sur les solutions FlexPod.

En intégrant des tests et des validations déjà exhaustifs dans le processus de création, les conformément aux CVD et aux NVA de FlexPod fournissent des conceptions d'architecture de solutions de référence et des guides de déploiement détaillés pour aider les partenaires et les clients à déployer et à adopter les solutions FlexPod. En utilisant ces CVD et les NVA comme guides de conception et d'implémentation, les entreprises peuvent réduire les risques, réduire les temps d'indisponibilité de la solution et augmenter la disponibilité, l'évolutivité, la flexibilité et la sécurité des solutions FlexPod qu'elles déploient.

Chacune des familles de composants FlexPod présentées (Cisco UCS, commutateurs Cisco Nexus/MDS et stockage NetApp) offre des options de plateforme et de ressources pour faire évoluer l'infrastructure de manière verticale ou horizontale, tout en prenant en charge les fonctionnalités requises selon les meilleures pratiques de configuration et de connectivité de FlexPod. FlexPod peut également évoluer horizontalement pour les environnements nécessitant plusieurs déploiements cohérents en déployant des piles FlexPod supplémentaires.

Assurer une reprise après incident rapide et la continuité de l'activité

Plusieurs méthodes permettent aux entreprises de récupérer rapidement leurs applications et services de données en cas d'incident. La mise en place d'un plan de reprise après incident et de continuité de l'activité, l'implémentation d'une solution qui répond aux objectifs métier et l'exécution de tests réguliers des scénarios d'incident permettent aux entreprises de bénéficier d'une reprise après incident et de continuer les services stratégiques après une situation d'incident.

Les exigences en matière de reprise après incident et de continuité de l'activité peuvent être différentes pour les types de services d'applications et de données. Certaines applications et données ne sont pas nécessaires en cas d'urgence ou d'incident, alors que d'autres doivent être disponibles en continu pour répondre aux exigences de l'entreprise.

Pour les applications stratégiques et les services de données qui risquent de perturber votre activité alors qu'ils ne sont pas disponibles, une évaluation minutieuse est nécessaire pour répondre à des questions telles que le type de maintenance et les scénarios d'incident auxquels l'entreprise doit tenir compte, quelle quantité de données l'entreprise peut se permettre de perdre en cas d'incident, et la rapidité à laquelle la reprise peut et doit avoir lieu.

Pour les entreprises qui ont recours à des services de données pour générer du chiffre d'affaires, les services de données doivent être protégés par une solution capable de résister à plusieurs scénarios de défaillance unique, mais aussi à un scénario de panne sur site dans le but d'assurer la continuité de l'activité.

Objectifs de point de restauration et de délai de restauration

L'objectif de point de restauration (RPO) mesure la quantité de données générée, en termes de temps, vous pouvez vous permettre de perdre ou bien le point auquel vous pouvez récupérer vos données. Avec un plan de sauvegarde quotidien, une entreprise risque de perdre une journée de données, car les modifications apportées aux données depuis la dernière sauvegarde pourraient être perdues en cas d'incident. Pour les services de données stratégiques et stratégiques, vous avez besoin d'un RPO nul et d'un plan et d'infrastructures associés pour protéger vos données sans aucune perte.

L'objectif de délai de restauration (RTO) mesure le temps que vous pouvez vous permettre d'éviter que les données ne soient disponibles ou la rapidité à laquelle les services de données doivent être mis en service. Par exemple, une entreprise peut disposer d'une implémentation de la sauvegarde et de la restauration qui utilise des bandes traditionnelles pour certains jeux de données en raison de sa taille. Par conséquent, la restauration des données à partir des bandes de sauvegarde peut prendre plusieurs heures, voire des jours, en cas de défaillance de l'infrastructure. Il faut également comprendre le temps nécessaire pour sauvegarder

l'infrastructure et restaurer les données. Pour les services de données stratégiques, vous pourriez avoir besoin d'un RTO très faible et vous ne pouvez tolérer qu'un temps de basculement de quelques secondes ou minutes pour remettre en ligne les services de données pour assurer la continuité de l'activité.

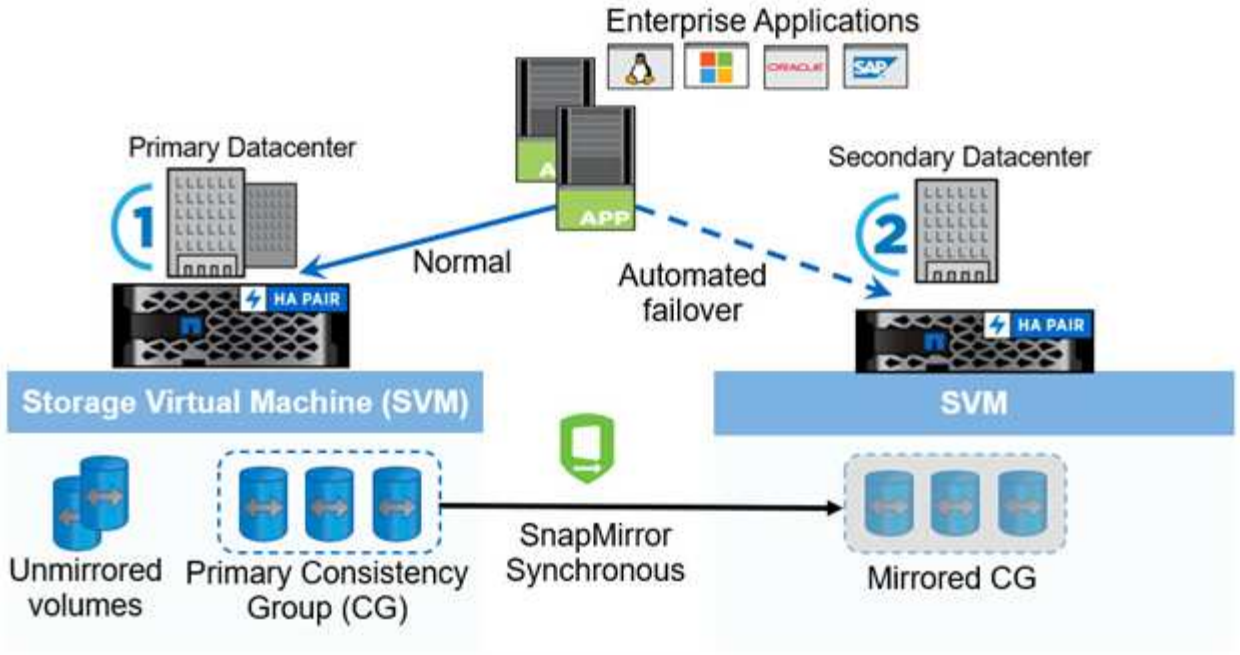
SM-BC

Depuis ONTAP 9.8, vous pouvez protéger les charges de travail SAN pour un basculement transparent des applications avec NetApp SM-BC. Vous pouvez créer des relations de groupes de cohérence entre deux clusters AFF ou deux clusters ASA pour la réplication des données afin d'atteindre un RPO nul et un RTO proche de zéro.

La solution SM-BC réplique les données à l'aide de la technologie SnapMirror synchrone sur un réseau IP. Elle offre une granularité au niveau des applications et un basculement automatique pour protéger vos services de données stratégiques, tels que Microsoft SQL Server, Oracle, etc. Avec des LUN SAN basées sur des protocoles iSCSI ou FC. Un médiateur ONTAP déployé sur un troisième site surveille la solution SM-BC et active le basculement automatique en cas d'incident sur site.

Un groupe de cohérence est une collection de volumes FlexVol qui offre une garantie de cohérence de l'ordre d'écriture pour la charge de travail applicative qui doit être protégée pour la continuité de l'activité. Elle permet d'effectuer simultanément des copies Snapshot cohérentes après panne d'un ensemble de volumes à un point dans le temps. Une relation SnapMirror, également appelée relation de groupe de cohérence, est établie entre un groupe de cohérence source et un groupe de cohérence de destination. Le groupe de volumes sélectionnés pour faire partie d'un groupe de cohérence peut être mappé à une instance d'application, à un groupe d'instances d'applications ou à une solution complète. En outre, les relations de groupe de cohérence SM-BC peuvent être créées ou supprimées à la demande en fonction des exigences et des changements de l'entreprise.

Comme illustré dans la figure suivante, les données du groupe de cohérence sont répliquées sur un second cluster ONTAP pour la reprise sur incident et la continuité de l'activité. Les applications disposent d'une connectivité aux LUN des deux clusters ONTAP. Les E/S sont généralement servies par le cluster primaire et reprises automatiquement à partir du cluster secondaire si un incident se produit sur le cluster primaire. Lors de la conception d'une solution SM-BC, les nombres d'objets pris en charge pour les relations CG (par exemple, un maximum de 20 CGS et un maximum de 200 noeuds finaux) doivent être observés pour éviter de dépasser les limites prises en charge.



"Suivant : solution FlexPod SM-BC."

Solution FlexPod SM-BC

"Précédent : introduction."

Présentation de la solution

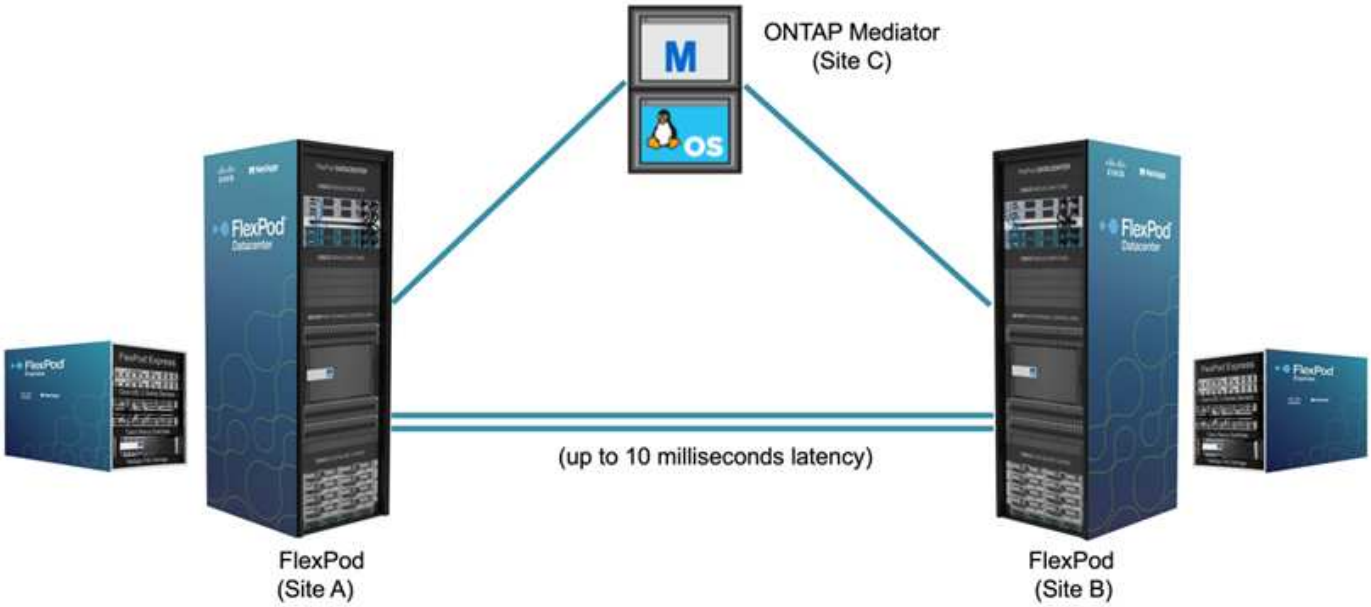
À un haut niveau, la solution FlexPod SM-BC est composée de deux systèmes FlexPod, situés sur deux sites séparés par une certaine distance, connectés et associés, afin d'offrir une solution de data Center hautement disponible, extrêmement flexible et extrêmement fiable, capable d'assurer la continuité de l'activité malgré une défaillance sur un site.

Outre le déploiement de deux nouvelles infrastructures FlexPod pour créer une solution FlexPod SM-BC, la solution peut également être implémentée sur deux infrastructures FlexPod existantes compatibles avec SM-BC ou en ajoutant un nouveau FlexPod pour être homologue avec un FlexPod existant.

Les deux systèmes FlexPod d'une solution FlexPod SM-BC n'ont pas besoin d'être identiques dans les configurations. Cependant, les deux clusters ONTAP doivent être des mêmes familles de stockage, deux systèmes AFF ou deux systèmes ASA, mais pas nécessairement du même modèle matériel. La solution SM-BC ne prend pas en charge les systèmes FAS.

Les deux sites FlexPod nécessitent une connectivité réseau qui répond aux exigences de bande passante et de qualité de service de la solution. Ils offrent une latence aller-retour inférieure à 10 millisecondes (10 ms) entre les sites, comme l'exige la solution ONTAP SM-BC. Pour la validation de cette solution FlexPod SM-BC, les deux sites FlexPod sont interconnectés via un réseau de couche 2 étendu dans le même laboratoire.

La solution NetApp ONTAP SM-BC assure une réplication synchrone entre les deux clusters de stockage NetApp pour une haute disponibilité et la reprise après incident dans un campus ou une zone métropolitaine. Le médiateur ONTAP déployé sur un troisième site surveille la solution et permet un basculement automatique en cas d'incident sur site. La figure suivante fournit une vue d'ensemble des composants de la solution.



Avec la solution FlexPod SM-BC, vous pouvez déployer un cloud privé basé sur VMware vSphere sur une infrastructure distribuée mais intégrée. La solution intégrée permet de coordonner plusieurs sites en tant qu'infrastructure unique afin de protéger les services de données contre différents scénarios de point de défaillance unique et une défaillance complète du site.

Ce rapport technique met en évidence certaines des considérations de conception de bout en bout de la solution FlexPod SM-BC. Les professionnels sont encouragés à obtenir des informations de référence disponibles dans les CVD et les NVA d'FlexPod pour d'autres détails d'implémentation de la solution FlexPod.

Bien que la solution ait été validée en déployant deux systèmes FlexPod basés sur les meilleures pratiques de FlexPod, comme décrit dans les CVD, elle tient compte des exigences de la solution SM-BC. La solution FlexPod SM-BC déployée décrite dans ce rapport a été validée pour la résilience et la tolérance aux pannes dans différents scénarios de défaillance, ainsi qu'une simulation de défaillance d'un site.

De la solution

La solution FlexPod SM-BC est conçue pour répondre aux exigences clés suivantes :

- Continuité de l'activité pour les applications et les services de données stratégiques en cas de défaillance complète du data Center
- Placement flexible des workloads distribués avec mobilité des workloads dans l'ensemble des data centers
- Affinité avec les sites dans lesquels les données des machines virtuelles sont accessibles localement, à partir du même site de data Center, pendant les opérations normales
- Restaurez rapidement vos données sans aucune perte en cas de défaillance d'un site

Composants de la solution

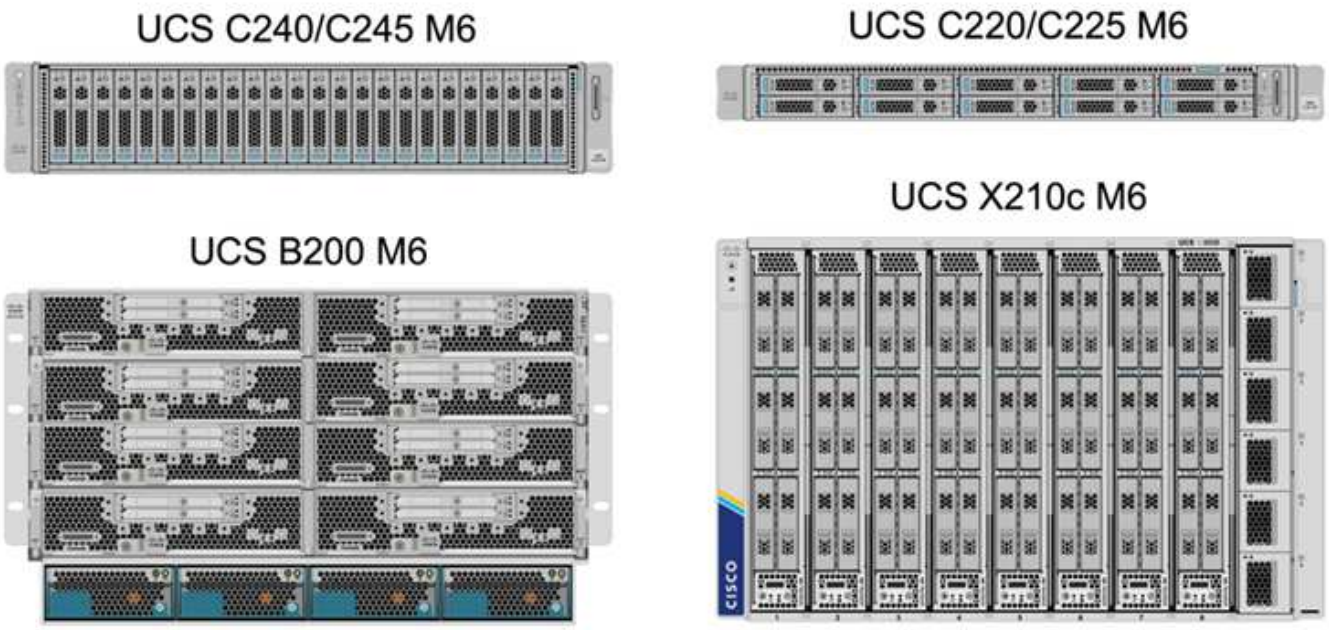
Composants de calcul Cisco

Cisco UCS est une infrastructure informatique intégrée qui offre des ressources informatiques unifiées, une structure unifiée et une gestion unifiée. Elle permet aux entreprises d'automatiser et d'accélérer le déploiement des applications, y compris la virtualisation et les charges de travail sans système d'exploitation. Cisco UCS prend en charge de nombreuses utilisations dans le cadre du déploiement, notamment les bureaux distants, les succursales, les data centers et le cloud hybride. Selon les exigences spécifiques de la solution, la mise en œuvre des ressources de calcul FlexPod et Cisco peut utiliser différents composants à différentes échelles.

Les sous-parties suivantes fournissent des informations supplémentaires sur certains composants UCS.

Serveur UCS et nœud de calcul

La figure suivante présente quelques exemples de composants de serveur UCS, dont des serveurs en rack UCS C-Series, des châssis UCS 5108 avec serveurs lames B-Series et le nouveau châssis UCS X9508 avec nœuds de calcul X-Series. Les serveurs en rack Cisco UCS C-Series sont disponibles dans un ou deux formats d'unité de rack (RU), avec processeurs Intel et AMD, ainsi que dans plusieurs vitesses de CPU, cœurs, mémoire et options d'E/S. Les serveurs lames Cisco UCS B-Series et les nouveaux nœuds de calcul X-Series sont également disponibles avec plusieurs options de processeur, de mémoire et d'E/S, et tous sont pris en charge dans l'architecture FlexPod pour répondre aux diverses exigences de l'entreprise.



En plus des serveurs rack M6 nouvelle génération C220/C225/C240/C245, des serveurs lames B200 M6 et des nœuds de calcul X210c illustrés dans cette figure, les générations précédentes de serveurs rack et lame peuvent également être utilisées si elles sont toujours prises en charge.

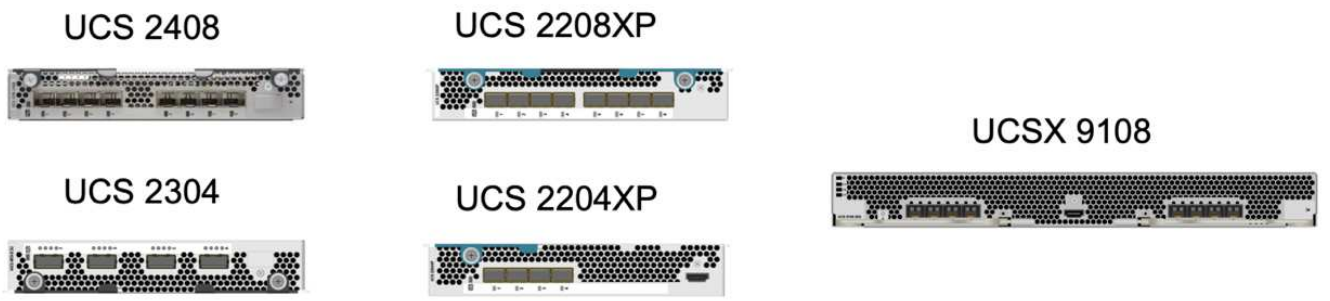
Module d'E/S et module de structure intelligente

Le module d'E/S (IOM)/Fabric Extender et le module de structure intelligente (IFM) offrent une connectivité de structure unifiée pour le châssis de serveurs lames Cisco UCS 5108 et le châssis Cisco UCS X9508 X-Series, respectivement.

La quatrième génération d'UCS IOM 2408 possède huit ports Ethernet unifiés 25 G pour la connexion du châssis UCS 5108 avec Fabric Interconnect (FI). Chaque 2408 dispose de quatre ports Ethernet de fond de panier 10 G par le biais du fond de panier central à chaque serveur lame du châssis.

Le contrôleur UCSTM X 9108 25G IFM est doté de huit ports Ethernet unifiés 25-G pour la connexion des serveurs lames dans le châssis UCS X9508 avec des interconnexions de fabric. Chaque 9108 dispose de quatre connexions 25-G vers chaque nœud de calcul UCS X210c dans le châssis X9108. Le 9108 IFM fonctionne également de concert avec le Fabric Interconnect pour gérer l'environnement du châssis.

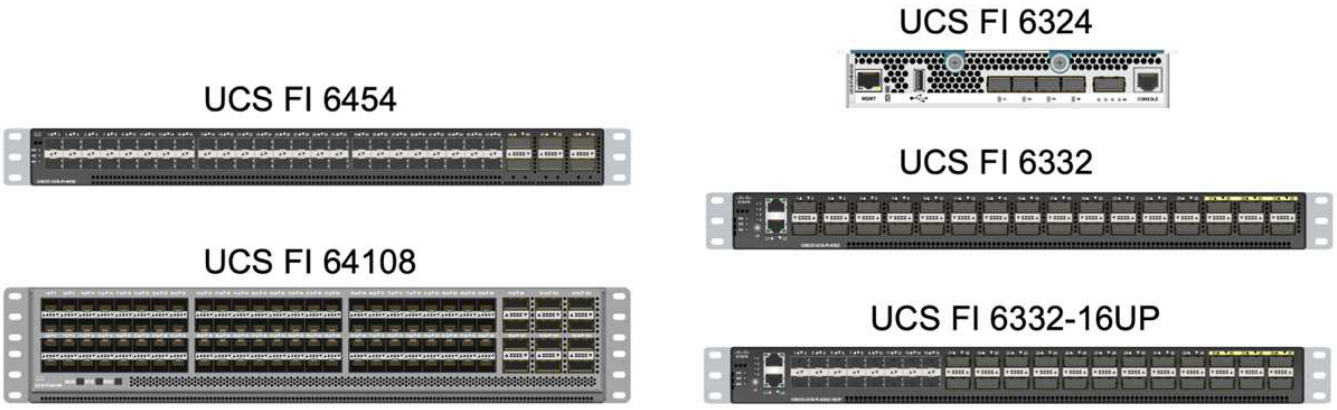
La figure suivante représente les générations d'IOM UCS 2408 et antérieures pour le châssis UCS 5108 et le module 9108 IFM pour le châssis X9508.



Interconnexions de fabric UCS

Les interconnexions de fabric Cisco UCS (IF) offrent une connectivité et une gestion à l'ensemble du système Cisco UCS. Généralement déployées en tant que paire active/active, les interfaces de contrôle de la qualité du système intègrent tous les composants dans un domaine de gestion unique et hautement disponible, contrôlé par Cisco UCS Manager ou Cisco Intersight. Il s'agit d'une structure unifiée unique pour le système avec une faible latence et sans perte, des commutateurs coupe-circuit qui prennent en charge le trafic LAN, SAN et de gestion à l'aide d'un seul jeu de câbles.

Il existe deux variantes pour les IFI Cisco UCS de quatrième génération : UCS FI 6454 et 64108. Ils comprennent la prise en charge de ports Ethernet 10/25 Gbit/s, de ports Ethernet 1/10/25 Gbit/s, de ports Ethernet UP-link 40/100 Gbit/s et de ports unifiés prenant en charge les ports Ethernet 10/25 Gbit/s ou Fibre Channel 8/16/32 Gbit/s. La figure suivante montre les IFI Cisco UCS de quatrième génération, ainsi que les modèles de troisième génération également pris en charge.



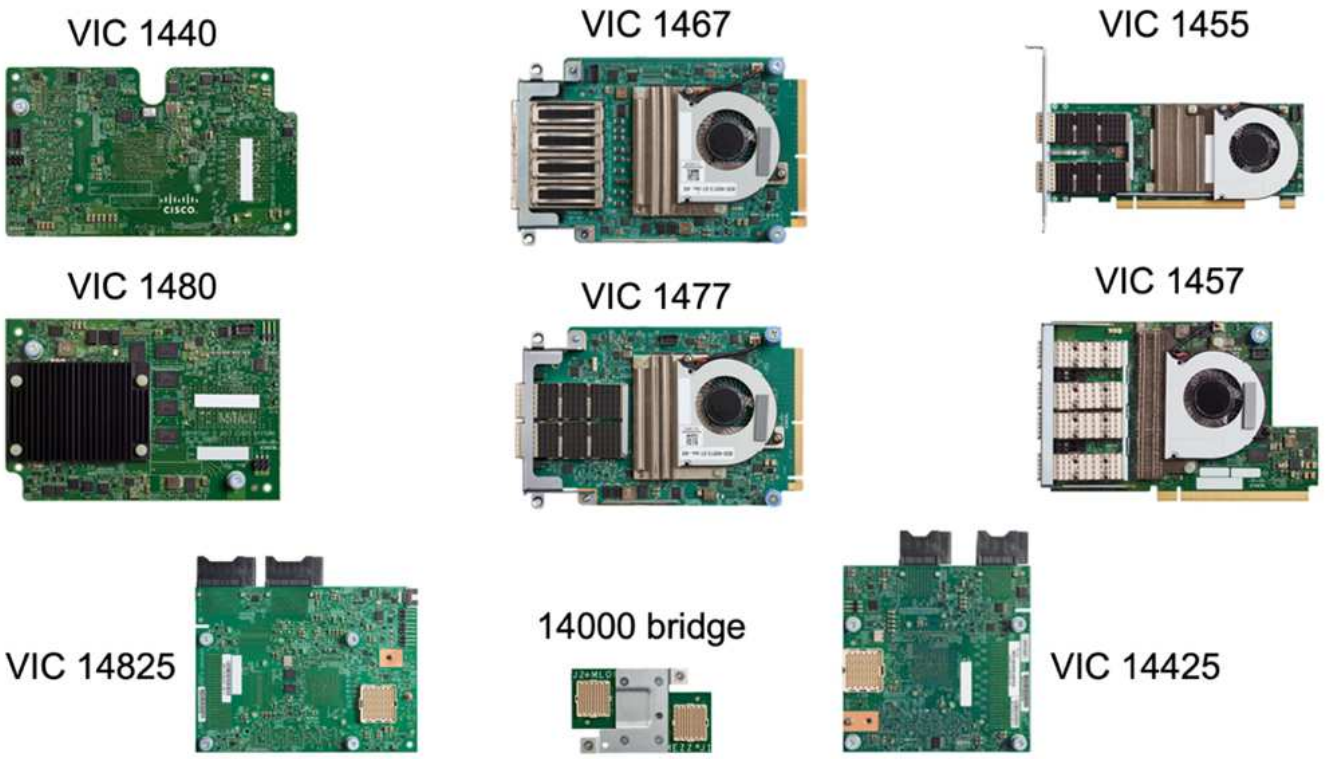
Pour prendre en charge le châssis Cisco UCS X-Series, des interconnexions de fabric de quatrième génération configurées en mode géré InterSight (IMM) sont requises. Cependant, le châssis Cisco UCS 5108 B-series peut être pris en charge aussi bien en mode IMM qu'en mode géré UCSM.

Le système UCS FI 6324 utilise le format de module d'E/S et est intégré dans un châssis UCS Mini pour les déploiements qui requièrent uniquement un petit domaine UCS.

Cartes d'interface virtuelle UCS

Les cartes d'interface virtuelle Cisco UCS (VICS) unifient la gestion des systèmes et la connectivité LAN et SAN pour les serveurs rack et lames. Il prend en charge jusqu'à 256 périphériques virtuels, soit en tant que cartes d'interface réseau virtuelles (vNIC), soit en tant que cartes de bus hôte virtuelles (vHBA) utilisant la

technologie Cisco SingleConnect. Suite à la virtualisation, les cartes VIC simplifient considérablement la connectivité réseau et réduisent le nombre d'adaptateurs réseau, de câbles et de ports de commutation nécessaires au déploiement de la solution. La figure suivante présente certaines des Cisco UCS VICS disponibles pour les serveurs B-Series et C-Series, ainsi que les nœuds de calcul X-Series.



Les différents modèles d'adaptateurs prennent en charge différents serveurs lame et rack avec différents nombres de ports, vitesses de port et formats de LAN modulaire sur la carte mère (mLOM), cartes mezzanine et interfaces PCIe. Les adaptateurs prennent en charge certaines combinaisons de Ethernet 10/25/40/100-G et FCoE (Fibre Channel over Ethernet). Ils intègrent la technologie CNA (Converged Network adapter) de Cisco, prennent en charge un ensemble complet de fonctionnalités et simplifient la gestion des adaptateurs et le déploiement des applications. Par exemple, le VIC prend en charge la technologie VM-FEX (Data Center Virtual machine Fabric Extender) de Cisco, qui étend les ports d'interconnexion de structure Cisco UCS aux machines virtuelles, simplifiant ainsi le déploiement de la virtualisation des serveurs.

Avec une combinaison de Cisco VIC dans les configurations mLOM, mezzanine, module d'extension de port et carte pont, vous pouvez tirer pleinement parti de la bande passante et de la connectivité disponibles pour les serveurs lames. Par exemple, en utilisant les deux liaisons 25 G sur le VIC 14825 (mLOM) et 14425 (mezzanine) et le 14000 (carte de pont) pour le nœud de calcul X210c, la bande passante combinée VIC est de 2 x 50-G + 2 x 50-G, Ou 100 G par fabric/IFM et 200 G au total par serveur avec la configuration IFM double.

Pour plus d'informations sur les gammes de produits Cisco UCS, les spécifications techniques et la documentation, consultez le "Cisco UCS" site web pour information.

Composants de commutation Cisco

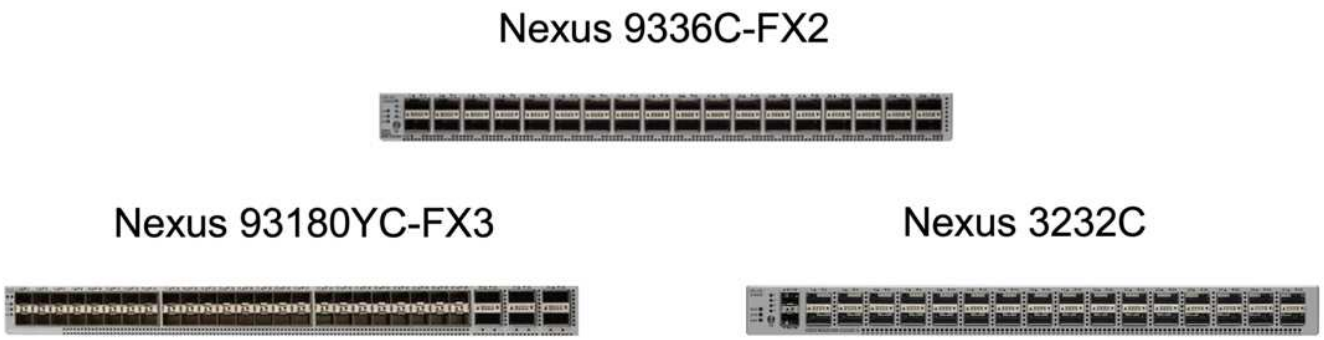
Commutateurs Nexus

FlexPod utilise des commutateurs Cisco Nexus Series afin de fournir une structure de commutation Ethernet pour les communications entre Cisco UCS et les contrôleurs de stockage NetApp. Tous les modèles de commutateurs Cisco Nexus actuellement pris en charge, y compris les gammes Cisco Nexus 3000, 5000,

7000 et 9000, sont pris en charge pour le déploiement de FlexPod.

Dans le choix d'un modèle de switch pour un déploiement FlexPod, de nombreux facteurs sont à prendre en compte, notamment les performances, la vitesse de port, la densité de port, la latence de commutation, Et des protocoles tels que la prise en charge ACI et VXLAN, pour vos objectifs de conception ainsi que la durée de prise en charge des commutateurs.

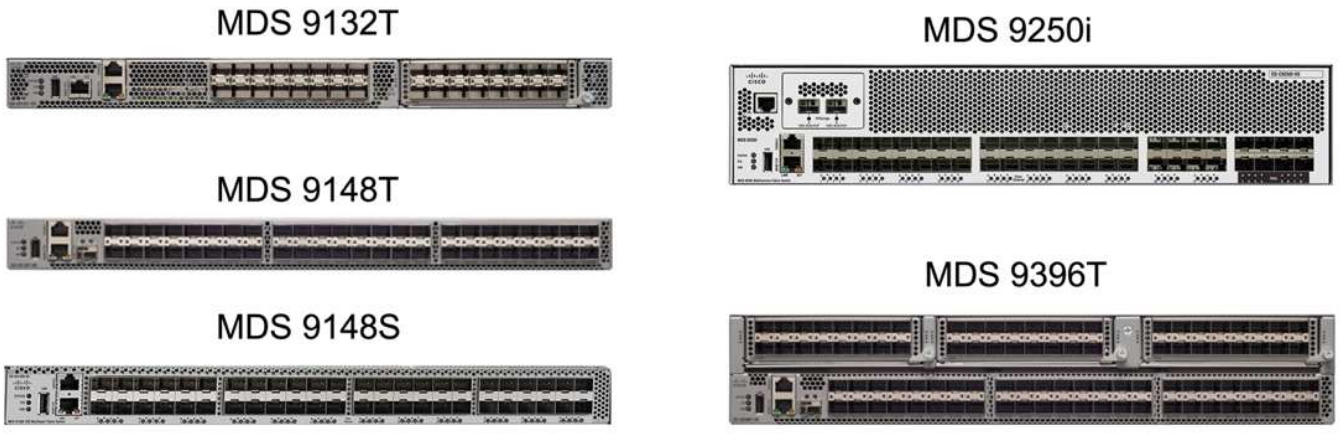
La validation de nombreux CVD récents de FlexPod utilise des commutateurs Cisco Nexus 9000, tels que les Nexus 9336C-FX2 et Nexus 93180YC-FX3. Ils offrent des ports haute performance 40/100G et 10//25G, une faible latence et une efficacité énergétique exceptionnelle dans un format compact 1U. Des vitesses supplémentaires sont prises en charge via des ports de liaison ascendante et des câbles de dérivation. La figure ci-dessous présente quelques switchs Cisco Nexus 9k et 3K, notamment les Nexus 9336C-FX2 et Nexus 3232C utilisés pour cette validation.



Voir "Commutateurs pour data Center Cisco" Pour plus d'informations sur les commutateurs Nexus disponibles ainsi que leurs spécifications et leurs documentations.

Switchs MDS

Les switchs de fabric Cisco MDS 9100/9200/9300 sont des composants facultatifs pour l'architecture FlexPod. Ces commutateurs sont extrêmement fiables, hautement flexibles, sécurisés et offrent une visibilité sur le flux du trafic dans le maillage. La figure suivante présente quelques exemples de commutateurs MDS qui peuvent être utilisés pour créer des structures SAN FC redondantes pour une solution FlexPod, afin de répondre aux besoins des applications et de l'entreprise.



Les commutateurs Cisco MDS 9132T/9148T/9396T haute performance 32G Multilayer Fabric sont économiques et extrêmement fiables, flexibles et évolutifs. Les fonctionnalités avancées du réseau de stockage facilitent la gestion et sont compatibles avec l'ensemble de la gamme Cisco MDS 9000 pour une

implémentation SAN fiable.

Ces fonctionnalités de télémétrie et d'analytique SAN dernière génération sont intégrées à cette plateforme matérielle nouvelle génération. Les données de télémétrie extraites de l'inspection des en-têtes de trame peuvent être transmises à une plateforme de visualisation analytique, y compris Cisco Data Center Network Manager. Les commutateurs MDS qui prennent en charge Fibre Channel 16 Gbit/s, comme le MDS 9148S, sont également pris en charge dans FlexPod. De plus, les commutateurs multiservice MDS, comme le MDS 9250i, qui prend en charge les protocoles FCoE et FCIP en plus du protocole FC, font également partie de la gamme de solutions FlexPod.

Sur les commutateurs MDS semi-modulaires tels que le 9132T et le 9396T, des licences de port et de module d'extension de port supplémentaires peuvent être ajoutées pour prendre en charge la connectivité de périphérique supplémentaire. Sur les commutateurs fixes comme le 9148T, des licences de port supplémentaires peuvent être ajoutées si nécessaire. Cette flexibilité de facturation à l'utilisation fournit une composante des dépenses d'exploitation qui permet de réduire les dépenses d'investissement relatives à la mise en œuvre et à l'exploitation d'une infrastructure SAN de commutateur MDS.

Voir "Commutateurs de structure Cisco MDS" Pour plus d'informations sur les commutateurs MDS Fabric disponibles, consultez le "NetApp IMT" et "Liste de compatibilité matérielle et logicielle Cisco" Pour obtenir la liste complète des commutateurs SAN pris en charge.

Composants NetApp

Les contrôleurs NetApp AFF ou ASA redondants qui exécutent le logiciel ONTAP 9.8 ou des versions ultérieures sont requis pour créer une solution FlexPod SM-BC. La dernière version d'ONTAP, actuellement 9.10.1, est recommandée pour le déploiement de SM-BC afin de tirer parti des innovations, des performances et des améliorations de qualité continues de ONTAP, ainsi que du nombre maximal d'objets pour la prise en charge de SM-BC.

Les contrôleurs NetApp AFF et ASA, dotés de performances et d'innovations de pointe, assurent la protection des données d'entreprise et proposent des fonctionnalités avancées de gestion des données. Les systèmes AFF et ASA prennent en charge les technologies NVMe de bout en bout, y compris les disques SSD connectés via NVMe et la connectivité hôte front-end NVMe over Fibre Channel (NVMe/FC). Vous pouvez améliorer le débit des workloads et réduire la latence d'E/S en adoptant une infrastructure SAN NVMe/FC. Toutefois, les datastores NVMe/FC ne peuvent actuellement être utilisés que pour les charges de travail qui ne sont pas protégées par SM-BC, car la solution SM-BC ne prend actuellement en charge que les protocoles iSCSI et FC.

NetApp AFF et les contrôleurs de stockage ASA fournissent également une base solide pour le cloud hybride qui permet aux clients de profiter des avantages de la mobilité transparente des données grâce à NetApp Data Fabric. Data Fabric vous permet d'accéder facilement aux données de la périphérie jusqu'au cœur, où elles sont générées, ainsi qu'au cloud, pour exploiter l'élasticité de calcul, d'IA et DE ML des informations exploitables à la demande.

Comme le montre la figure suivante, NetApp propose différents contrôleurs de stockage et tiroirs disques afin de répondre à vos exigences en termes de performances et de capacité. Pour plus d'informations sur les fonctionnalités et les spécifications des contrôleurs NetApp AFF et ASA, consultez le tableau suivant et consultez les liens vers les pages produits.

AFF A700/A900, ASA A700

AFF/ASA A400/A800

AFF/ASA A250, AFF C190

DS 224C/2246

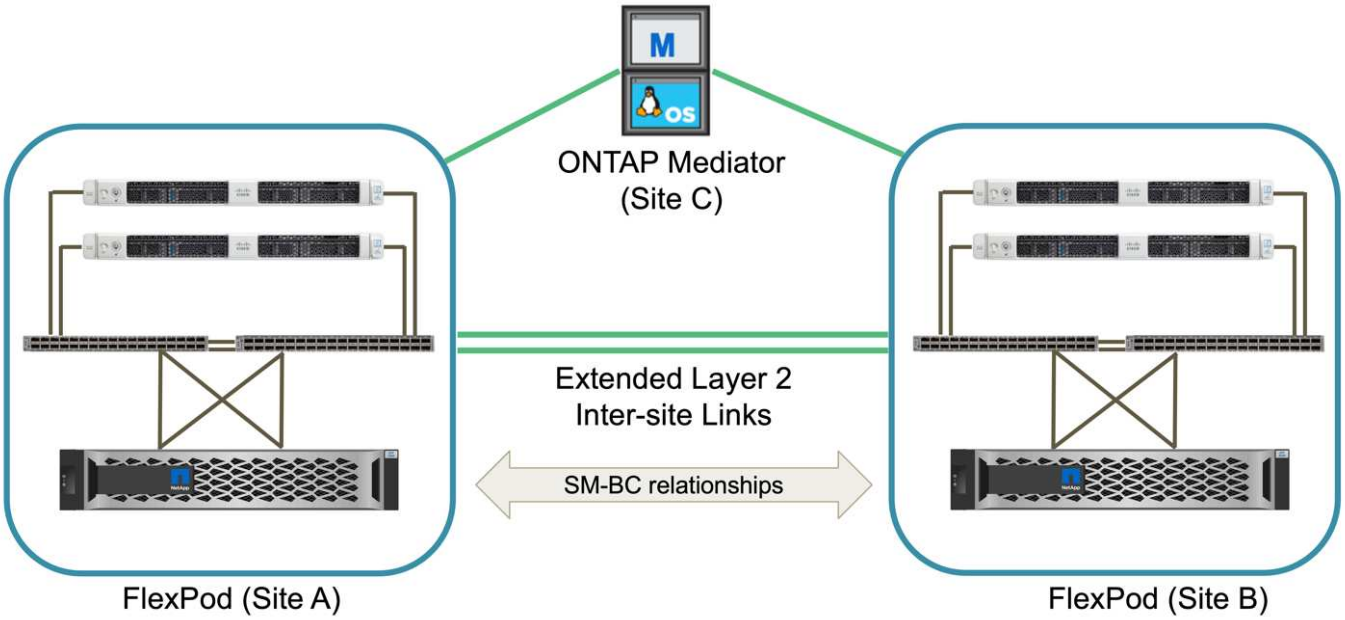
NS 224

Famille de produits	Caractéristiques techniques
Gamme AFF	"Documentation sur la gamme AFF"
Gamme ASA	"Documentation sur la gamme ASA"

Consulter le "Documentation relative aux tiroirs disques et aux supports de stockage NetApp" et "NetApp Hardware Universe" pour en savoir plus sur les tiroirs disques et les tiroirs disques pris en charge pour chaque modèle de contrôleur de stockage.

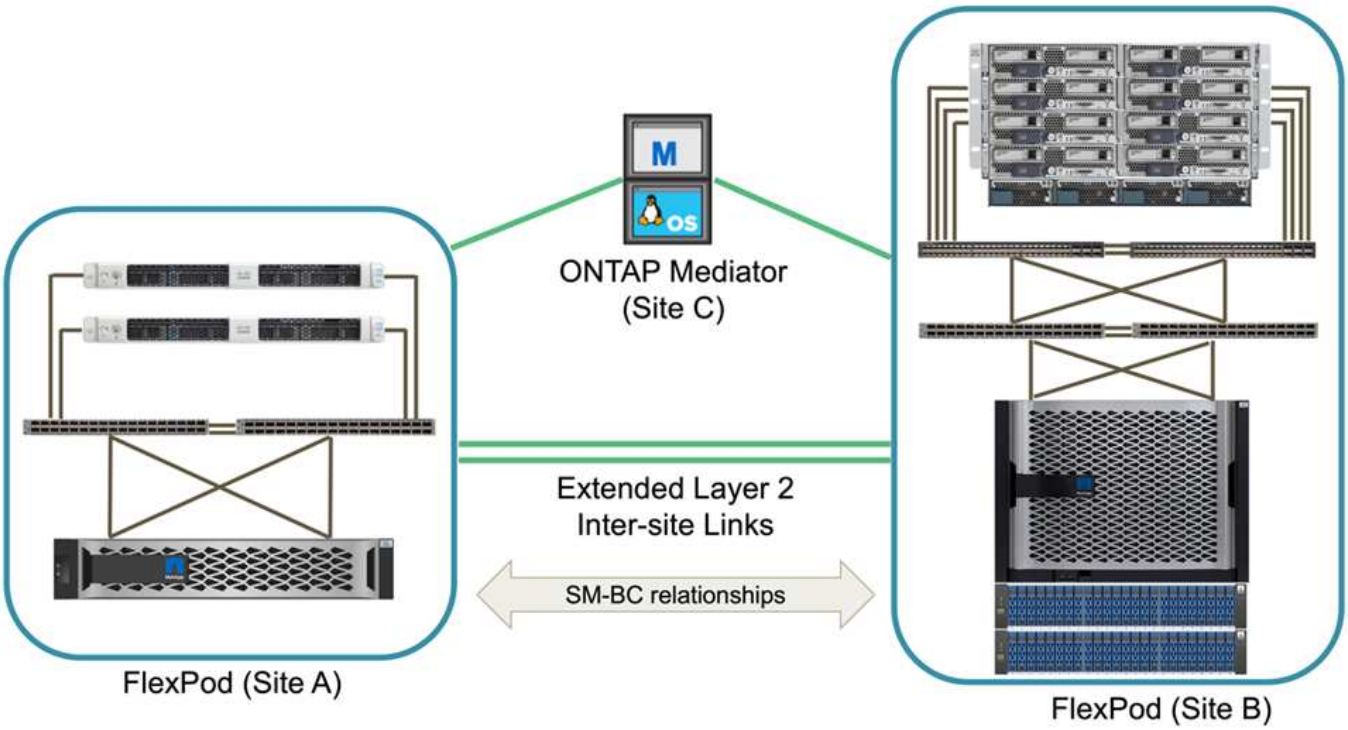
Topologies de solution

Les solutions FlexPod sont flexibles en topologie et peuvent évoluer verticalement ou horizontalement pour répondre à différents besoins. Une solution qui exige une protection de continuité de l'activité et qui ne contient que des ressources minimales de calcul et de stockage peuvent exploiter une topologie de la solution simple, comme l'illustre la figure suivante. Cette topologie simple utilise les serveurs rack UCS C-Series et les contrôleurs AFF/ASA avec des disques SSD dans le contrôleur sans tiroirs disques supplémentaires.



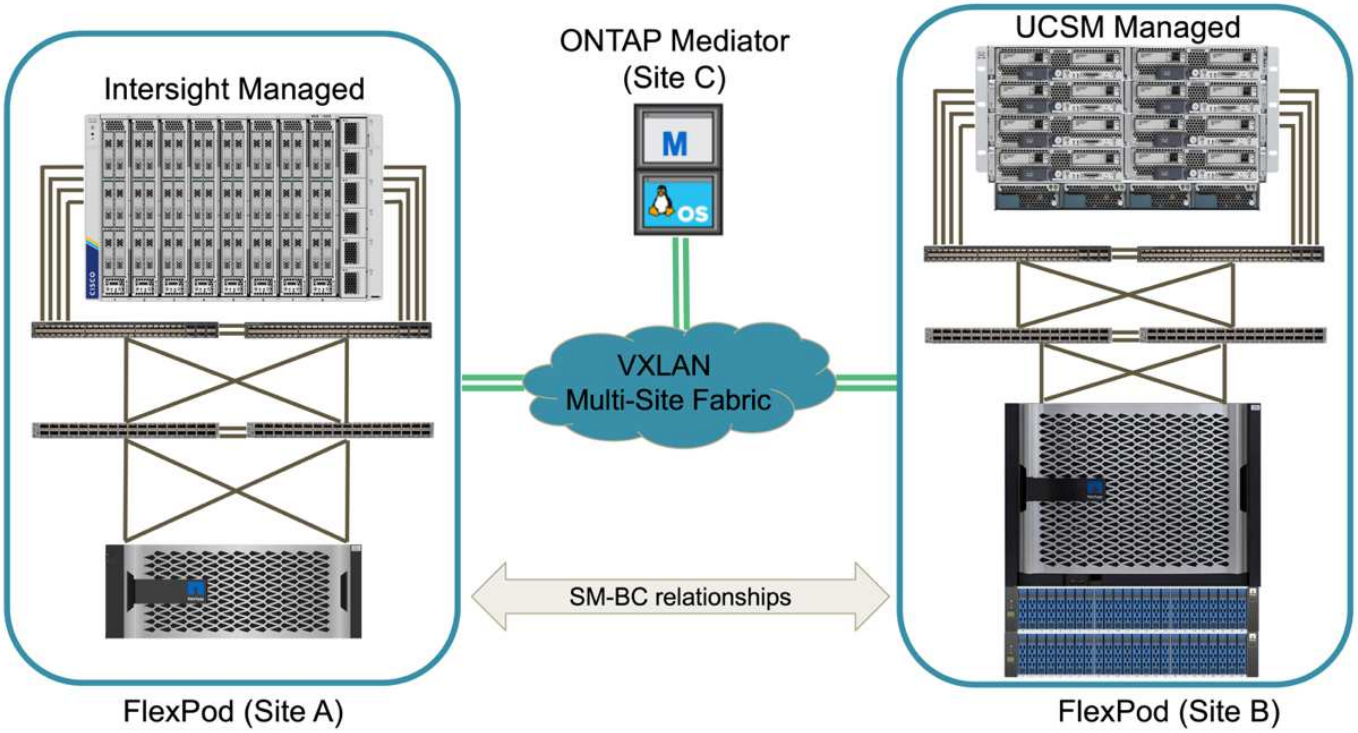
Ses composants redondants de calcul, de réseau et de stockage sont interconnectés par la connectivité redondante entre les composants. Ce design haute disponibilité assure la résilience de la solution et permet de résister à un seul point de défaillance. La conception multisite et les relations de réplication de données synchrone ONTAP SM-BC fournissent des services de données stratégiques, malgré un risque de défaillance d'un stockage sur un seul site.

Une topologie de déploiement asymétrique qui pourrait être utilisée par les entreprises entre un data Center et une succursale dans une zone métropolitaine pourrait ressembler à la figure suivante. Pour ce design asymétrique, le data Center requiert un FlexPod plus performant avec davantage de ressources de calcul et de stockage. Cependant, les besoins de la succursale sont moins importants et peuvent être satisfaits par un FlexPod beaucoup plus petit.

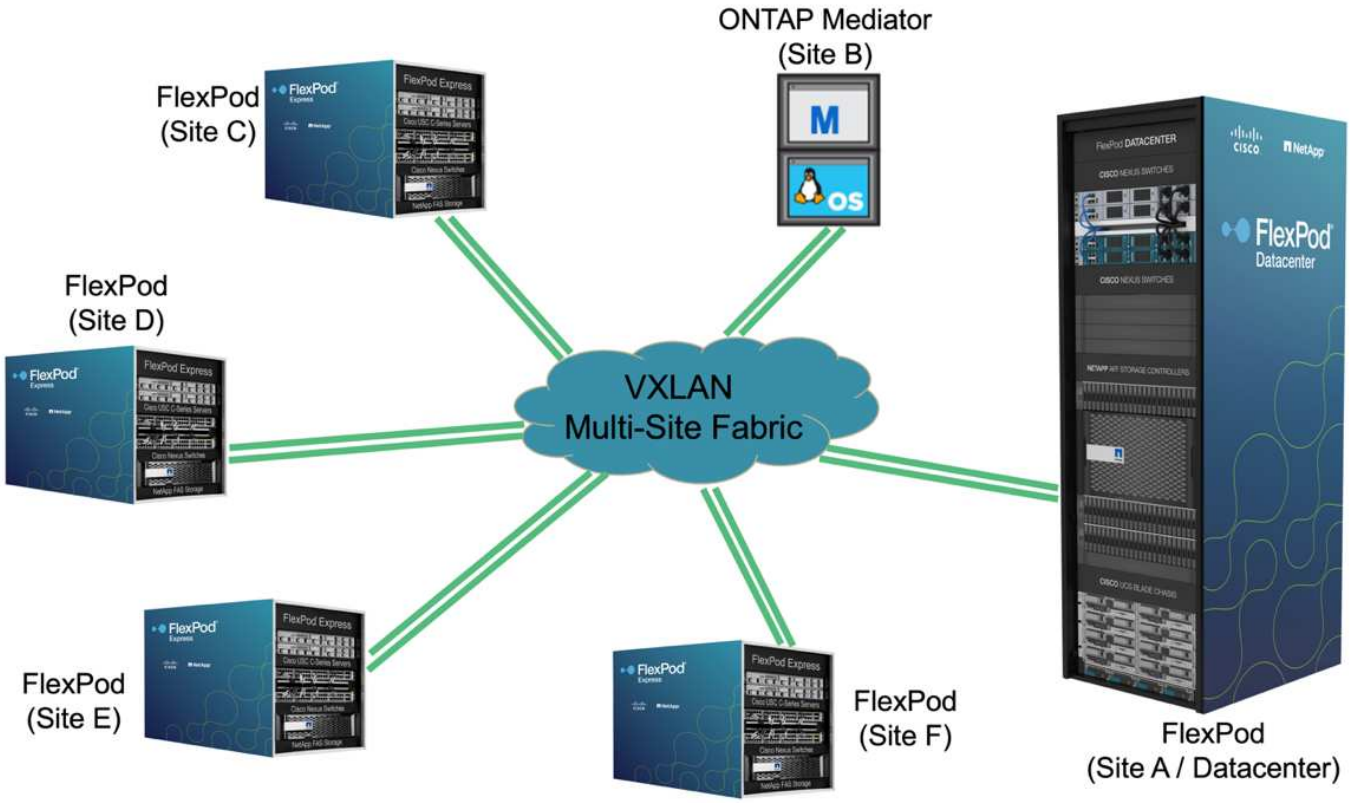


Pour les entreprises dont les besoins en ressources de calcul et de stockage sont plus importants et sur plusieurs sites, une structure multisite basée sur VXLAN permet à plusieurs sites d'avoir une structure réseau transparente afin de faciliter la mobilité des applications et de servir une application depuis n'importe quel site.

Il peut y avoir une solution FlexPod existante au moyen de châssis Cisco UCS 5108 et de serveurs lames B-Series qui doivent être protégés par une nouvelle instance FlexPod. La nouvelle instance FlexPod peut utiliser le tout dernier châssis UCS X9508 avec des nœuds de calcul X210c gérés par Cisco Intersight, comme l'illustre la figure suivante. Dans ce cas, les systèmes FlexPod de chaque site sont connectés à une structure de data Center plus vaste, et les sites sont connectés via un réseau d'interconnexion pour former une structure multisite VXLAN.



Pour les entreprises disposant d'un data Center et de plusieurs succursales dans une zone métropolitaine, qui doivent tous être protégées afin d'assurer la continuité de l'activité, La topologie de déploiement FlexPod SM-BC illustrée dans la figure suivante peut être mise en œuvre pour protéger les services d'applications et de données stratégiques afin d'atteindre un RPO nul et un RTO proche de zéro pour toutes les succursales.



Pour ce modèle de déploiement, chaque succursale établit les relations SM-BC et les groupes de cohérence dont elle a besoin avec le centre de données. Vous devez tenir compte des limites d'objets SM-BC prises en charge, de sorte que les relations de groupes de cohérence et le nombre de points de terminaison globaux ne dépassent pas les valeurs maximales prises en charge au niveau du datacenter.

"Ensuite : présentation de la validation de la solution."

Validation des solutions

Validation des solutions : présentation

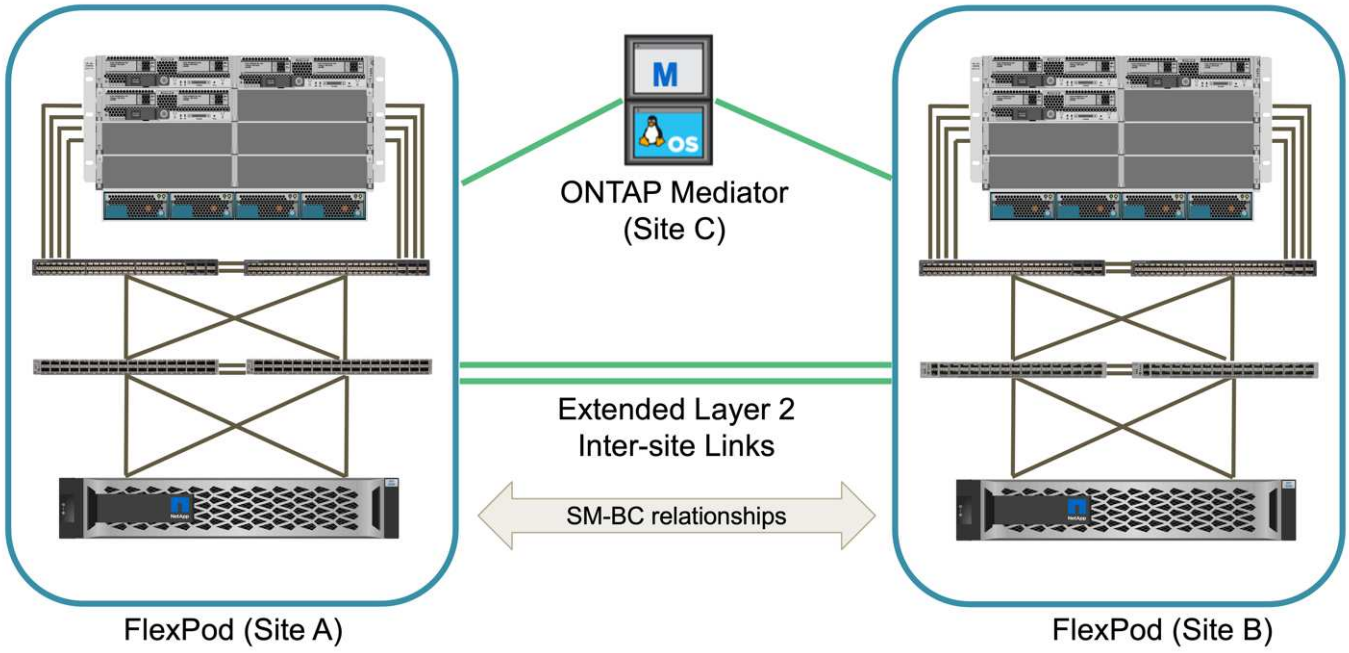
"Précédent : solution FlexPod SM-BC."

Les détails de la conception et de l'implémentation de la solution FlexPod SM-BC dépendent des objectifs spécifiques de la configuration et de la solution FlexPod. Une fois les exigences générales de continuité de l'activité définies, la solution FlexPod SM-BC peut être créée en implémentant une toute nouvelle solution avec deux nouveaux systèmes FlexPod, en ajoutant un nouveau système FlexPod sur un autre site pour une paire avec un FlexPod existant, ou en associant deux systèmes FlexPod existants.

Les solutions FlexPod étant par nature flexibles dans ses configurations, tous les composants et configurations FlexPod pris en charge peuvent être utilisés. Le reste de cette section fournit des informations sur les validations d'implémentation effectuées pour une solution d'infrastructure virtuelle basée sur VMware. À l'exception des aspects liés à SM-BC, l'implémentation suit les processus standard de déploiement FlexPod. Pour en savoir plus sur l'implémentation FlexPod, consultez les CVD et les NVA FlexPod disponibles, en fonction de vos configurations spécifiques.

Topologie de validation

À des fins de validation de la solution FlexPod SM-BC, les composants technologiques pris en charge par NetApp, Cisco et VMware sont utilisés. La solution comprend des paires HA AFF A250 de NetApp exécutant ONTAP 9.10.1, deux switchs Cisco Nexus 9336C-FX2 sur le site A et deux switchs Cisco Nexus 3232C sur le site B, ou Cisco UCS 6454 Fi sur les deux sites, Et trois serveurs Cisco UCS B200 M5 sur chaque site exécutant VMware vSphere 7.0u2 et gérés par UCS Manager et le serveur VMware vCenter. La figure suivante montre la topologie de validation de solution au niveau des composants avec deux systèmes FlexPod s'exécutant sur le site A et le site B connectés par des liens inter-sites étendus de couche 2 et un médiateur ONTAP s'exécutant sur le site C.



Matériel et logiciels

Le tableau suivant répertorie le matériel et les logiciels utilisés pour la validation de la solution. Il est important de noter que Cisco, NetApp et VMware disposent de matrices d'interopérabilité permettant de déterminer la prise en charge de toute implémentation spécifique de FlexPod :

- "http://support.netapp.com/matrix/"
- "Outil d'interopérabilité matérielle et logicielle Cisco UCS"
- "http://www.vmware.com/resources/compatibility/search.php"

Catégorie	Composant	Version logicielle	Quantité
Calcul	Fabric Interconnect Cisco UCS 6454	4.2(1f)	4 (2 par site)
	Serveurs Cisco UCS B200 M5	4.2(1f)	6 (3 par site)
	MODULE D'E/S CISCO UCS 2204XP	4.2(1f)	4 (2 par site)
	CISCO VIC 1440 (PID : UCSTM-MLOM-40G-04)	5.2(1a)	2 (1 par site)

Catégorie	Composant	Version logicielle	Quantité
	CISCO VIC 1340 (PID : UCSTM-MLOM-40G-03)	4.5(1a)	4 (2 par site)
Le réseau	Cisco Nexus 9336C-FX2	9.3(6)	2 (site A)
	Cisco Nexus 3232C	9.3(6)	2 (site B)
Stockage	NetApp AFF A250	9.10.1	4 (2 par site)
	NetApp System Manager	9.10.1	2 (1 par site)
	NetApp Active IQ Unified Manager	9.10	1
	Outils NetApp ONTAP pour VMware vSphere	9.10	1
	Plug-in NetApp SnapCenter pour VMware vSphere	4.6	1
	Médiateur ONTAP	1.3	1
	Boîte NAbox	3.0.2	1
	Récolte NetApp	21.11.1-1	1
Virtualisation	VMware ESXi	7.0U2	6 (3 par site)
	Pilote Ethernet nenic VMware ESXi	1.0.35.0	6 (3 par site)
	VMware vCenter	7.0U2	1
	Plug-in NetApp NFS pour VMware VAAI	2.0	6 (3 par site)
Test	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6 (3 par site)
	Iometer	1.1.0	6 (3 par site)

"Validation de la solution - calcul."

Validation des solutions : calcul

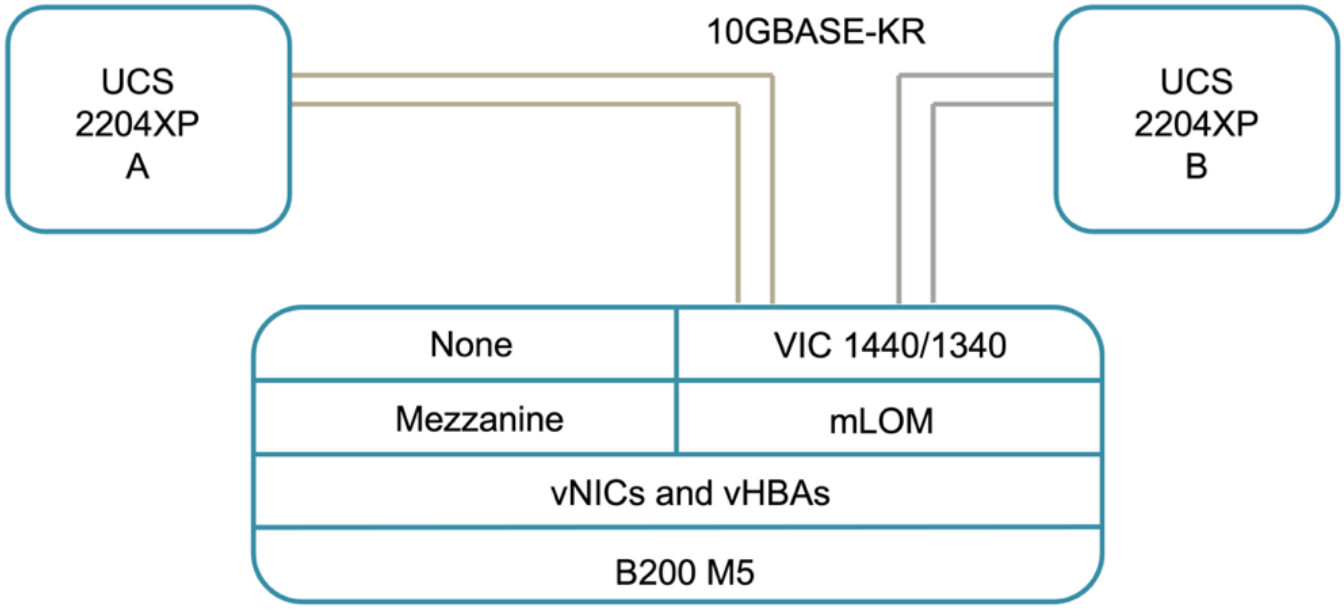
"Preivous : validation de la solution - Présentation."

La configuration de calcul de la solution FlexPod SM-BC suit les bonnes pratiques des solutions FlexPod classiques. Les sections suivantes mettent en évidence certaines des connexions et configurations utilisées pour la validation. Certaines des considérations liées au SM-BC sont également mises en évidence pour fournir des références et des

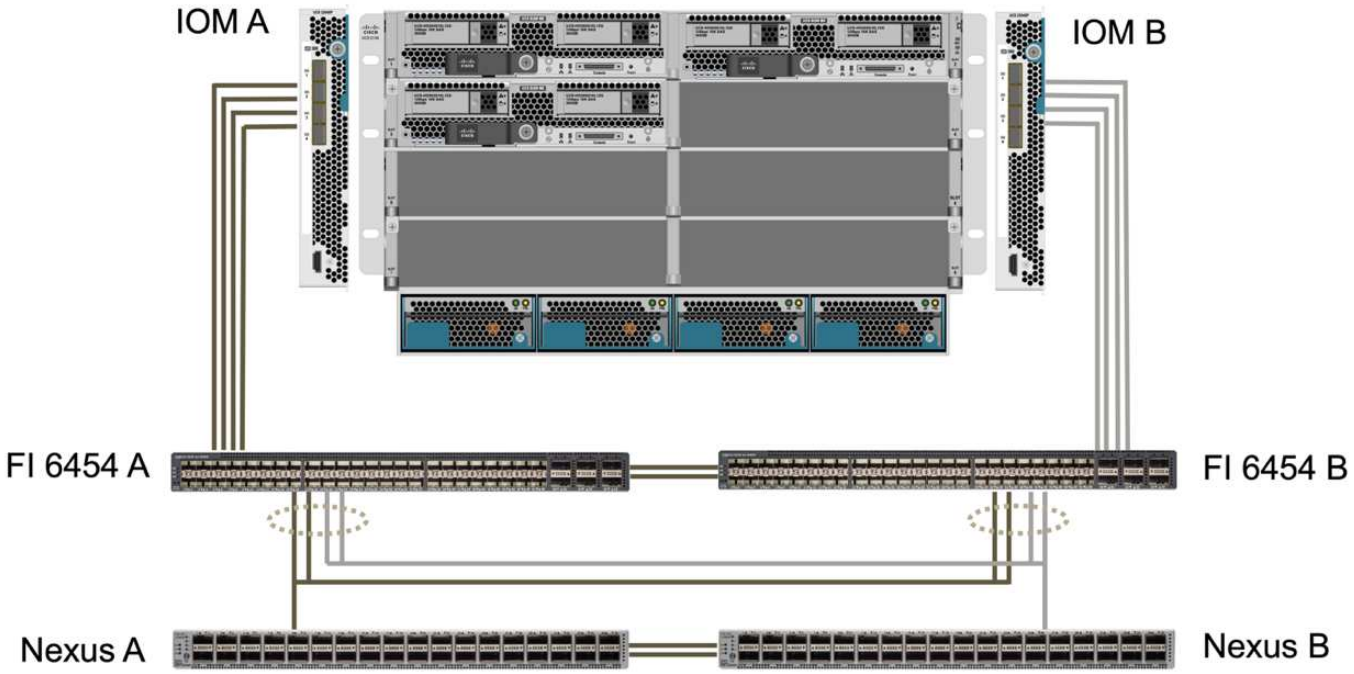
conseils sur la mise en œuvre.

Connectivité

La connectivité entre les serveurs lames UCS B200 et les IOM est fournie par la carte VIC UCS 5108 via les connexions de fond de panier du châssis UCS. UCS 2204XP Fabric Extender utilisé pour la validation possède 16 ports 10G chacun pour la connexion aux huit serveurs lames demi-largeur, par exemple deux pour chaque serveur. Pour augmenter la bande passante de connectivité du serveur, vous pouvez ajouter un VIC supplémentaire basé sur mezzanine pour connecter le serveur au module UCS 2408 IOM alternatif qui fournit quatre connexions 10G à chaque serveur.



La connectivité entre le châssis UCS 5108 et les IF UCS 6454 utilisés pour la validation sont assurées par le module IOM 2204XP qui utilise quatre connexions 10G. Les ports FI 1 à 4 sont configurés comme ports serveur pour ces connexions. Les ports FI 25 à 28 sont configurés en tant que ports de liaison ascendante du réseau vers les commutateurs Nexus A et B du site local. Les figures et tableaux suivants présentent le schéma de connectivité et les détails de connexion des ports pour les serveurs UCS 6454 IFF permettant de se connecter au châssis UCS 5108 et aux switchs Nexus.



Périphérique local	Port local	Périphérique distant	Port distant
UCS 6454 FI A	1	MODULE D'E/S A	1
	2		2
	3		3
	4		4
	25	Nexus A	24/13/1
	26		24/13/2
	27	Nexus B	24/13/3
	28		24/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	MODULE D'E/S B	1
	2		2
	3		3
	4		4
	25	Nexus A	24/13/3
	26		24/13/4
	27	Nexus B	24/13/1
	28		24/13/2
	L1	UCS 6454 FI A	L1

Périphérique local	Port local	Périphérique distant	Port distant
	L2		L2

Les connexions ci-dessus sont similaires pour les deux sites A et B, malgré l'utilisation du site A avec des switchs Nexus 9336C-FX2et du site B avec des switchs Nexus 3232C. Des câbles de dérivation 40G à 4x10G sont utilisés pour les connexions Nexus vers FI. Les connexions FI au Nexus utilisent le canal de port et les canaux de port virtuel sont configurés sur les commutateurs Nexus afin d'agréger les connexions à chaque FI.

Si vous utilisez une autre combinaison de composants IOM, FI et Nexus, veillez à utiliser les câbles et la vitesse de port appropriés pour la combinaison d'environnement.

Une bande passante supplémentaire peut être obtenue en utilisant des composants qui prennent en charge des connexions plus rapides ou plus de connexions. Pour assurer une redondance supplémentaire, il est possible d'ajouter des connexions supplémentaires avec des composants qui les prennent en charge.

Profils de services

Un châssis de serveur lame avec des Fabric Interconnect gérés par UCS Manager (UCSM) ou Cisco Intersight peut extraire les serveurs à l'aide des profils de service disponibles dans UCSM et les profils de serveurs. Cette validation utilise UCSM et les profils de service pour simplifier la gestion des serveurs. Avec les profils de service, il est possible de remplacer ou mettre à niveau un serveur simplement en associant le profil de service d'origine au nouveau matériel.

Les profils de service créés prennent en charge les éléments suivants pour les hôtes VMware ESXi :

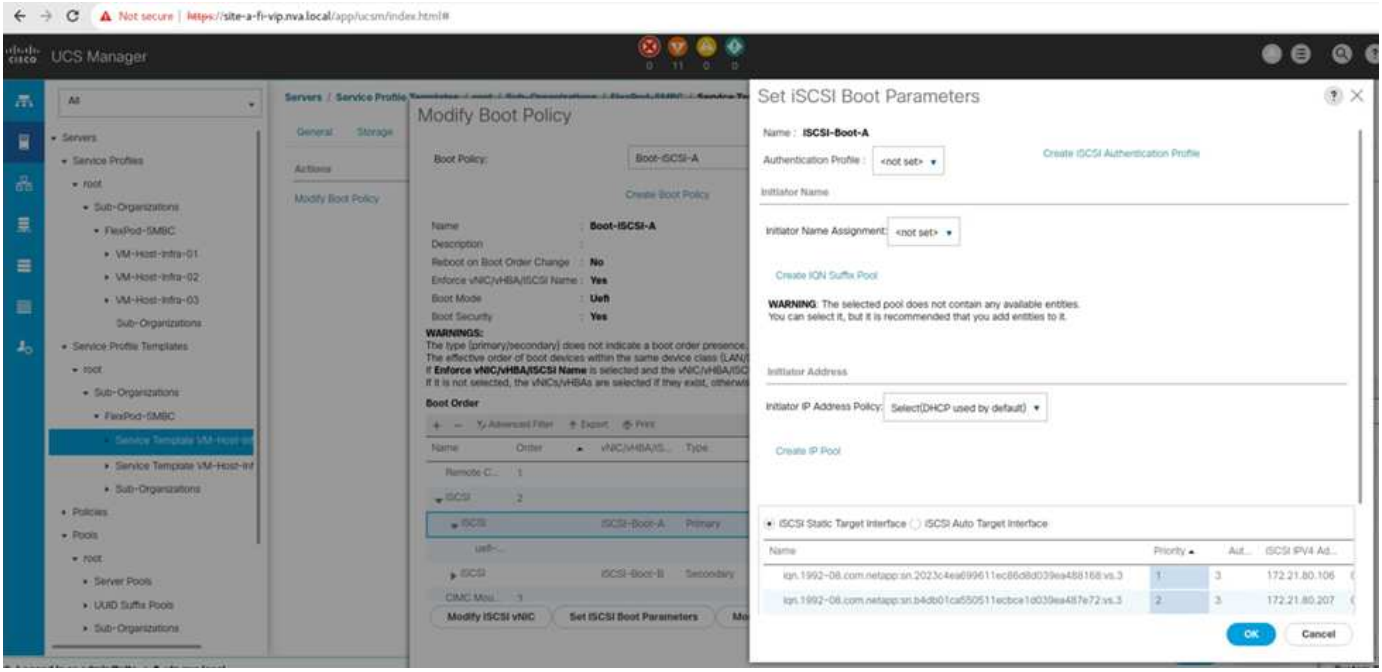
- Démarrage SAN depuis le système de stockage AFF A250 sur n'importe quel site, au moyen du protocole iSCSI.
- Six vNIC sont créés pour les serveurs où :
  - Deux cartes vNIC redondantes (vSwitch0-A et vSwitch0-B) transportent le trafic de gestion sur bande. Éventuellement, ces vNIC peuvent également être utilisés par des données de protocole NFS qui ne sont pas protégées par SM-BC.
  - Deux vNIC redondants (VDS-A et VDS-B) sont utilisés par le commutateur distribué vSphere pour supporter le trafic VMware vMotion et d'autres applications.
  - ISCSI-A vNIC utilisé par iSCSI-A vSwitch pour fournir un accès au chemin iSCSI-A.
  - VNIC iSCSI-B utilisé par le vSwitch iSCSI-B pour fournir un accès au chemin iSCSI-B.

Démarrage SAN

Dans le cas de la configuration de démarrage SAN iSCSI, les paramètres de démarrage iSCSI sont définis pour autoriser le démarrage iSCSI à partir des deux matrices iSCSI. Pour prendre en charge le scénario de basculement SM-BC dans lequel une LUN de démarrage SAN iSCSI est desservie à partir du cluster secondaire lorsque le cluster principal n'est pas disponible, la configuration cible statique iSCSI doit inclure des cibles à partir du site A et du site B. De plus, pour optimiser la disponibilité des LUN de démarrage, configurez les paramètres de démarrage iSCSI pour qu'ils démarrent à partir de tous les contrôleurs de stockage.

La cible statique iSCSI peut être configurée dans la stratégie d'amorçage des modèles de profil de service sous la boîte de dialogue définir le paramètre d'amorçage iSCSI, comme illustré dans la figure suivante. La configuration recommandée des paramètres d'amorçage iSCSI est indiquée dans le tableau suivant, qui

implémente la stratégie d'amorçage décrite ci-dessus pour obtenir une haute disponibilité.



Structure iSCSI	Priorité	Cible iSCSI	LIF iSCSI
ISCSI A	1	Site Une cible iSCSI	Site A Controller 1 iSCSI A LIF
	2	Cible iSCSI du site B	Contrôleur B 2 iSCSI A LIF
ISCSI B	1	Cible iSCSI du site B	Contrôleur B 1 LIF iSCSI B du site B
	2	Site Une cible iSCSI	Site A contrôleur 2 iSCSI B LIF

"Suivant : validation de la solution - réseau."

Validation de la solution : réseau

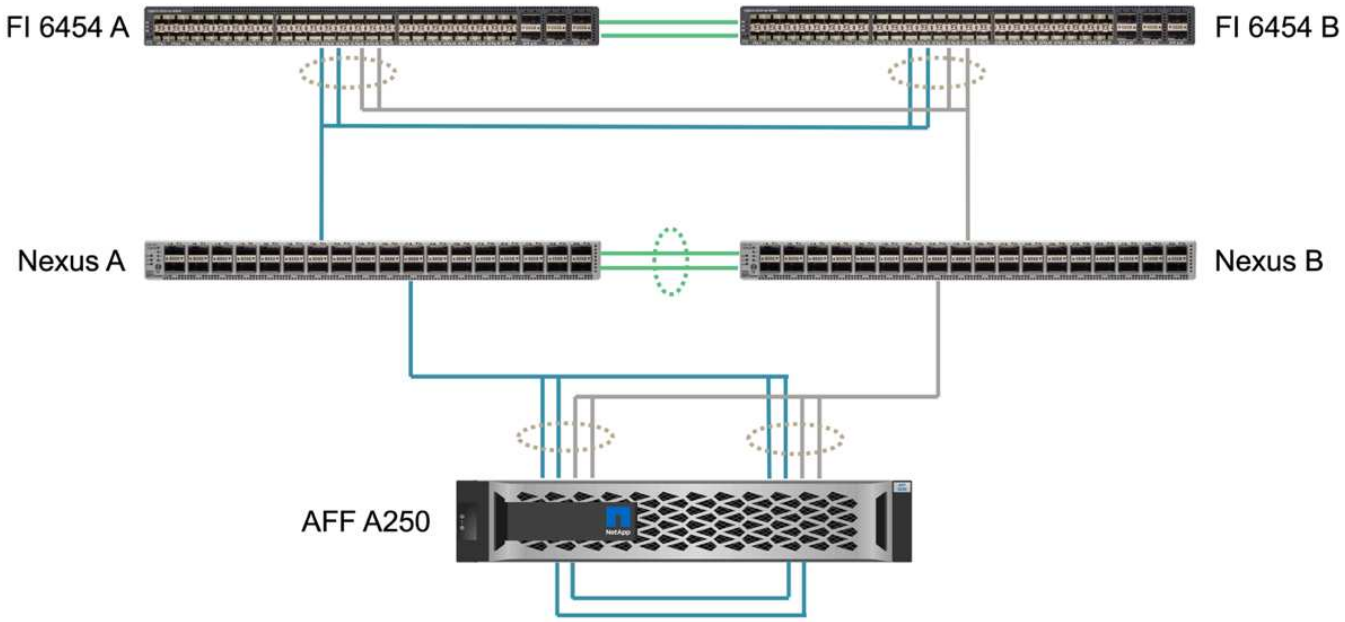
"Précédente : validation de la solution - calcul."

La configuration réseau de la solution FlexPod SM-BC suit les meilleures pratiques typiques des solutions FlexPod sur chaque site. Pour la connectivité entre sites, la configuration de validation de la solution connecte les switchs FlexPod Nexus sur les deux sites afin d'assurer une connectivité entre sites qui étend les VLAN entre les deux sites. Les sections suivantes mettent en évidence certaines des connexions et configurations utilisées pour la validation.

Connectivité

Les switchs FlexPod Nexus de chaque site procurent une connectivité locale entre le calcul UCS et le stockage ONTAP dans une configuration haute disponibilité. Les composants redondants et la connectivité redondante offrent la résilience aux scénarios de point de défaillance unique.

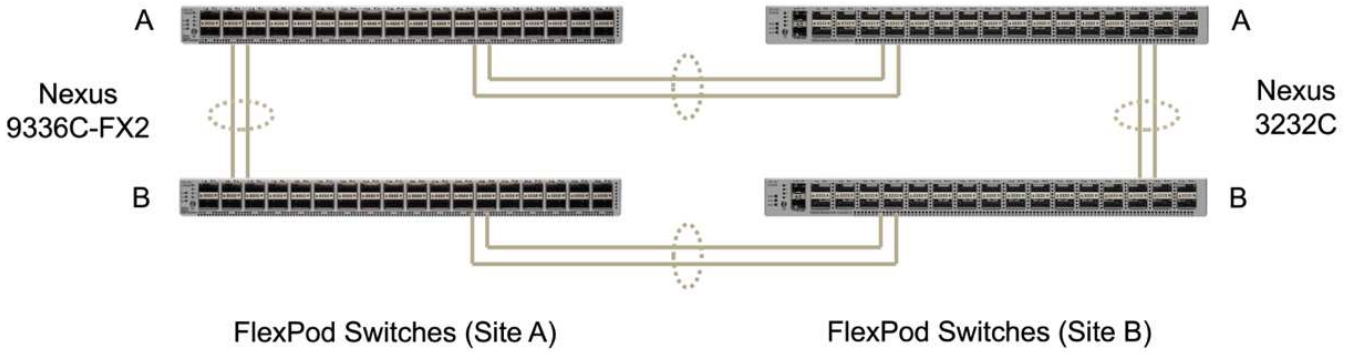
Le schéma suivant présente la connectivité locale du commutateur Nexus sur chaque site. Outre ce qui est illustré dans le schéma, il existe aussi des connexions au réseau de gestion et de console pour chaque composant qui ne sont pas affichés. Les câbles de dérivation 40G à 4 x 10G sont utilisés pour connecter les commutateurs Nexus aux serveurs d'accès UCS ainsi qu'aux contrôleurs de stockage ONTAP AFF A250. Il est également possible d'utiliser des câbles de dérivation 100G à 4 x 25G pour accroître la vitesse de communication entre les commutateurs Nexus et les contrôleurs de stockage AFF A250. Pour plus de simplicité, les deux contrôleurs AFF A250 sont présentés côte à côte pour illustrer le câblage. Les deux connexions entre les deux contrôleurs de stockage permettent au système de stockage de former un cluster sans commutateur.



Le tableau suivant montre la connectivité entre les switchs Nexus et les contrôleurs de stockage AFF A250 sur chaque site.

Périphérique local	Port local	Périphérique distant	Port distant
Nexus A	24/10/1	AFF A250 A	e1a
	24/10/2		e1b
	24/10/3	AFF A250 B	e1a
	24/10/4		e1b
Nexus B	24/10/1	AFF A250 A	e1c
	24/10/2		e1d
	24/10/3	AFF A250 B	e1c
	24/10/4		e1d

La connectivité entre les commutateurs FlexPod du site A et du site B est illustrée dans la figure suivante avec les détails de câblage répertoriés dans le tableau ci-dessous. Les connexions entre les deux commutateurs de chaque site correspondent aux liaisons VPC Peer. D'autre part, les connexions entre les commutateurs entre les sites fournissent les liaisons intersites. Les liaisons étendent les VLAN sur plusieurs sites pour la communication intercluster, la réplication des données SM-BC, la gestion intrabande et l'accès aux données pour les ressources des sites distants.



Périphérique local	Port local	Périphérique distant	Port distant
Commutateur a du site	33	Commutateur a du site B	31
	34		32
	25	Commutateur du site A B	25
	26		26
Commutateur du site A B	33	Commutateur du site B	31
	34		32
	25	Commutateur a du site	25
	26		26
Commutateur a du site B	31	Commutateur a du site	33
	32		34
	25	Commutateur du site B	25
	26		26
Commutateur du site B	31	Commutateur du site A B	33
	32		34
	25	Commutateur a du site B	25
	26		26

Le tableau ci-dessus répertorie la connectivité du point de vue de chaque commutateur FlexPod. Par conséquent, le tableau contient des informations dupliquées pour leur lisibilité.

Canal de port et canal de port virtuel

Le canal de port active l'agrégation de liens à l'aide du protocole LACP (Link Aggregation Control Protocol) pour l'agrégation de la bande passante et la résilience des pannes de liaison. Le canal de port virtuel (VPC) permet que les connexions des canaux de port entre deux commutateurs Nexus apparaissent logiquement comme une seule. Ceci améliore davantage la résilience des pannes pour les situations telles qu'une panne de liaison unique ou une défaillance de commutateur unique.

Le trafic du serveur UCS vers le système de stockage chemins entre l'E/S A et LES E/S B et LA FI B avant d'atteindre les commutateurs Nexus. Au fur et à mesure que les connexions FI aux commutateurs Nexus

utilisent le canal de port du côté FI et le canal de port virtuel du côté du commutateur Nexus, le serveur UCS peut utiliser efficacement les chemins via les deux commutateurs Nexus et résister aux scénarios de défaillance unique. Entre les deux sites, les commutateurs Nexus sont interconnectés, comme illustré dans la figure précédente. Il y a deux liaisons pour connecter les paires de commutateurs entre les sites et ils utilisent également une configuration de canal de port.

La connectivité des protocoles de stockage des données intrabande, inter-cluster et iSCSI/NFS est assurée par l'interconnexion des contrôleurs de stockage de chaque site aux switchs Nexus locaux dans une configuration redondante. Chaque contrôleur de stockage est relié à deux commutateurs Nexus. Les quatre connexions sont configurées en tant que partie d'un groupe d'interface sur le stockage pour une résilience améliorée. Du côté du commutateur Nexus, ces ports font également partie d'un VPC entre les commutateurs.

Le tableau suivant répertorie l'ID et l'utilisation du canal de port sur chaque site.

ID de canal de port	Du stockage
10	Lien homologue Nexus local
15	Fabric Interconnect A liens
16	Liaisons Fabric Interconnect B
27	Le contrôleur de stockage A relie
28	Liaisons du contrôleur de stockage B
100	Liaisons a du commutateur inter-site
200	Liaisons du commutateur intersite B

VLAN

Le tableau suivant répertorie les réseaux VLAN configurés pour la configuration de l'environnement de validation de la solution FlexPod SM-BC et leur utilisation.

Nom	ID VLAN	Du stockage
VLAN natif	2	VLAN 2 utilisé comme VLAN natif au lieu du VLAN par défaut (1)
OOB-MGMT-VLAN	3333	VLAN de gestion hors bande pour les périphériques
IB-MGMT-VLAN	3334	VLAN de gestion intrabande pour les hôtes ESXi, la gestion des VM, etc
NFS-VLAN	3335	VLAN NFS facultatif pour le trafic NFS
ISCSI-A-VLAN	3336	San iSCSI-A Fabric pour le trafic iSCSI
ISCSI-B-VLAN	3337	San fabric iSCSI-B pour le trafic iSCSI
VMotion-VLAN	3338	VLAN pour le trafic VMware vMotion

Nom	ID VLAN	Du stockage
VM-trafic-VLAN	3339	VLAN pour le trafic des machines virtuelles VMware
VLAN-intercluster	3340	VLAN intercluster pour les communications entre clusters ONTAP

Bien que SM-BC ne prend pas en charge les protocoles NFS ou CIFS pour la continuité de l'activité, vous pouvez les utiliser pour les workloads qui n'ont pas besoin d'être protégés pour la continuité de l'activité. Les datastores NFS n'ont pas été créés pour cette validation.

"Suivant : validation de la solution - stockage."

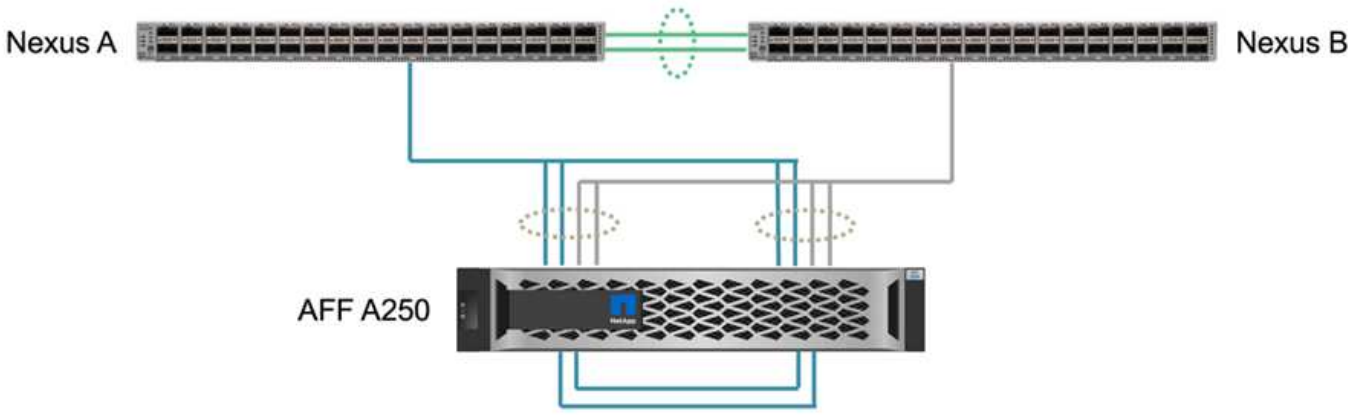
Validation de la solution : stockage

"Précédent : validation de la solution - réseau."

La configuration du stockage pour la solution FlexPod SM-BC suit les meilleures pratiques typiques des solutions FlexPod sur chaque site. Pour le peering de clusters et la réplication des données de SM-BC, ils utilisent les liaisons intersites établies entre les commutateurs FlexPod sur les deux sites. Les sections suivantes mettent en évidence certaines des connexions et configurations utilisées pour la validation.

Connectivité

La connectivité de stockage aux IF et aux serveurs lames UCS locaux est fournie par les commutateurs Nexus sur le site local. La connectivité du switch Nexus entre les sites permet au stockage d'être accessible par les serveurs lames UCS distants. La figure et le tableau ci-dessous présentent le schéma de connectivité du stockage et une liste des connexions des contrôleurs de stockage de chaque site.



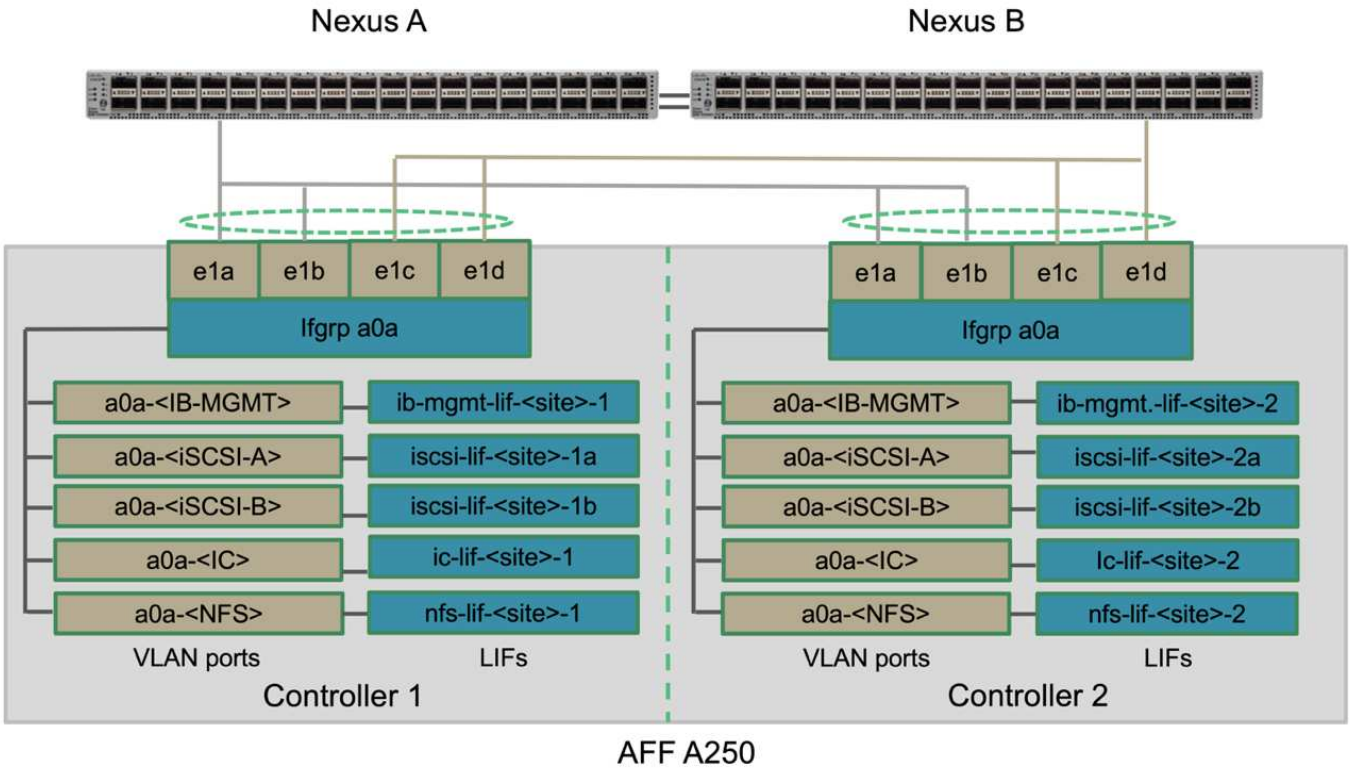
Périphérique local	Port local	Périphérique distant	Port distant
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A	24/10/1

Périphérique local	Port local	Périphérique distant	Port distant
	e1b		24/10/2
	e1c	Nexus B	24/10/1
	e1d		24/10/2
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	e1a	Nexus A	24/10/3
	e1b		24/10/4
	e1c	Nexus B	24/10/3
	e1d		24/10/4

Connexions et interfaces

Deux ports physiques de chaque contrôleur de stockage sont connectés à chaque commutateur Nexus afin d'assurer l'agrégation de la bande passante et la redondance pour cette validation. Ces quatre connexions participent à une configuration de groupe d'interface sur le système de stockage. Les ports correspondants des commutateurs Nexus font partie d'un VPC pour assurer l'agrégation de liens et la résilience.

Les protocoles de stockage des données intrabande et inter-cluster et NFS/iSCSI utilisent des VLAN. Les ports VLAN sont créés sur le groupe d'interface pour isoler les différents types de trafic. Les interfaces logiques (LIF) des fonctions respectives sont créées en plus des ports VLAN correspondants. La figure suivante montre la relation entre les connexions physiques, les groupes d'interfaces, les ports VLAN et les interfaces logiques.

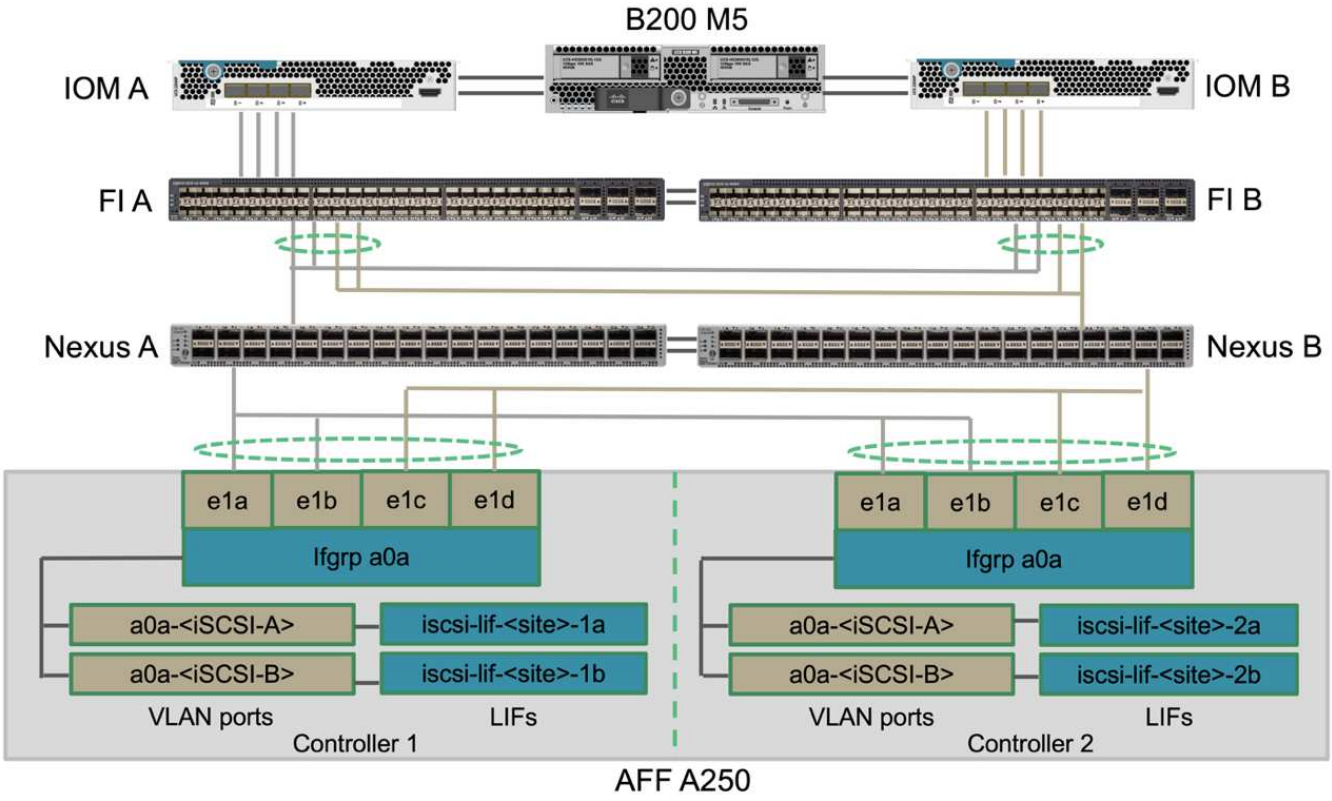


Démarrage SAN

NetApp recommande l'implémentation d'un démarrage SAN pour les serveurs Cisco UCS dans la solution FlexPod. L'implémentation du démarrage SAN vous permet de sécuriser le système d'exploitation au sein du système de stockage NetApp, vous offrant ainsi de meilleures performances et une plus grande flexibilité. Pour cette solution, le démarrage SAN iSCSI a été validé.

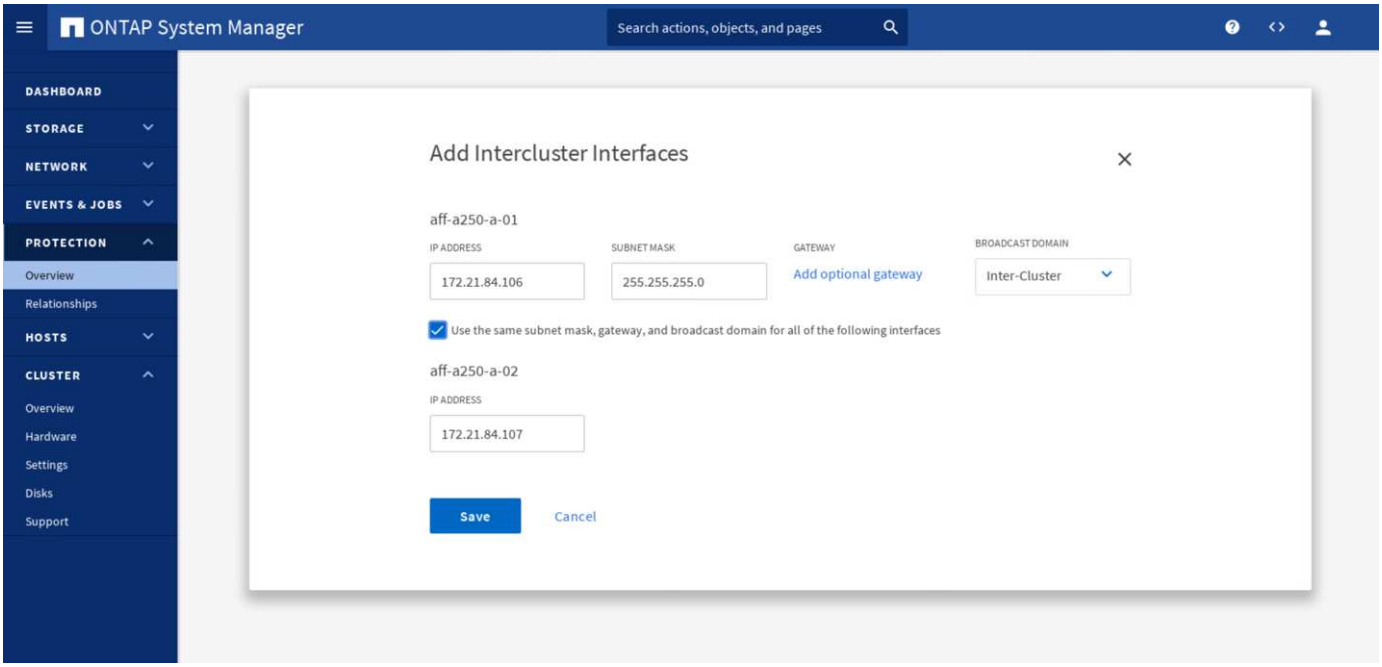
La figure suivante décrit la connectivité du démarrage SAN iSCSI du serveur Cisco UCS du stockage NetApp. Lors du démarrage SAN iSCSI, chaque serveur Cisco UCS est affecté à deux vNIC iSCSI (une pour chaque structure SAN) qui fournissent une connectivité redondante depuis le serveur jusqu'au stockage. Les ports de stockage Ethernet 10/25-G connectés aux commutateurs Nexus (dans cet exemple e1a, e1b, e1c et e1d) sont regroupés pour former un groupe d'interface (ifgrp) (dans cet exemple, a0A). Les ports VLAN iSCSI sont créés sur le ifgrp et les LIFs iSCSI sont créés sur les ports VLAN iSCSI.

Chaque LUN de démarrage iSCSI est mappée sur le serveur qui s'amorce à partir de celle-ci via les LIFs iSCSI en associant la LUN de démarrage aux noms qualifiés iSCSI (IQN) du serveur dans son groupe initiateur de démarrage. Le groupe initiateur d'initialisation du serveur contient deux IQN, un pour chaque structure vNIC/SAN. Cette fonctionnalité permet uniquement au serveur autorisé d'accéder à la LUN de démarrage créée spécifiquement pour ce serveur.



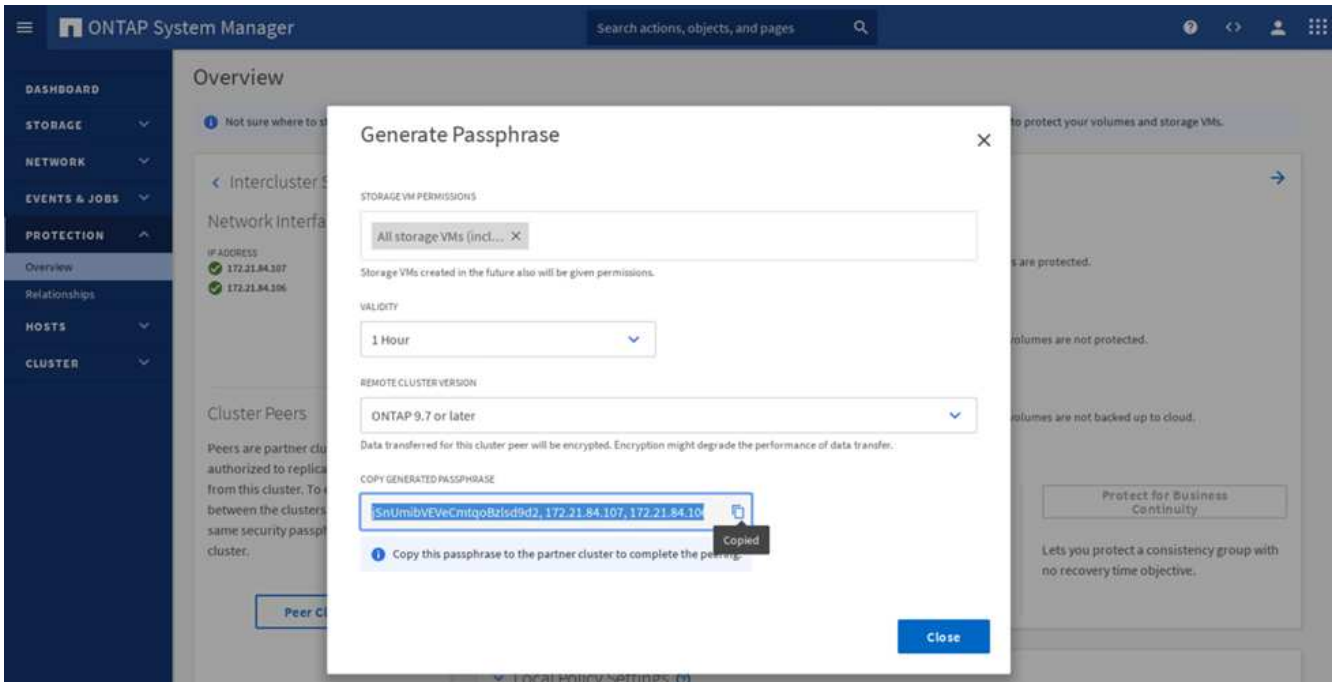
Peering de clusters

Les pairs de cluster ONTAP communiquent via les LIFs intercluster. En utilisant ONTAP System Manager pour les deux clusters, vous pouvez créer les LIF intercluster nécessaires sous le volet protection > Présentation.

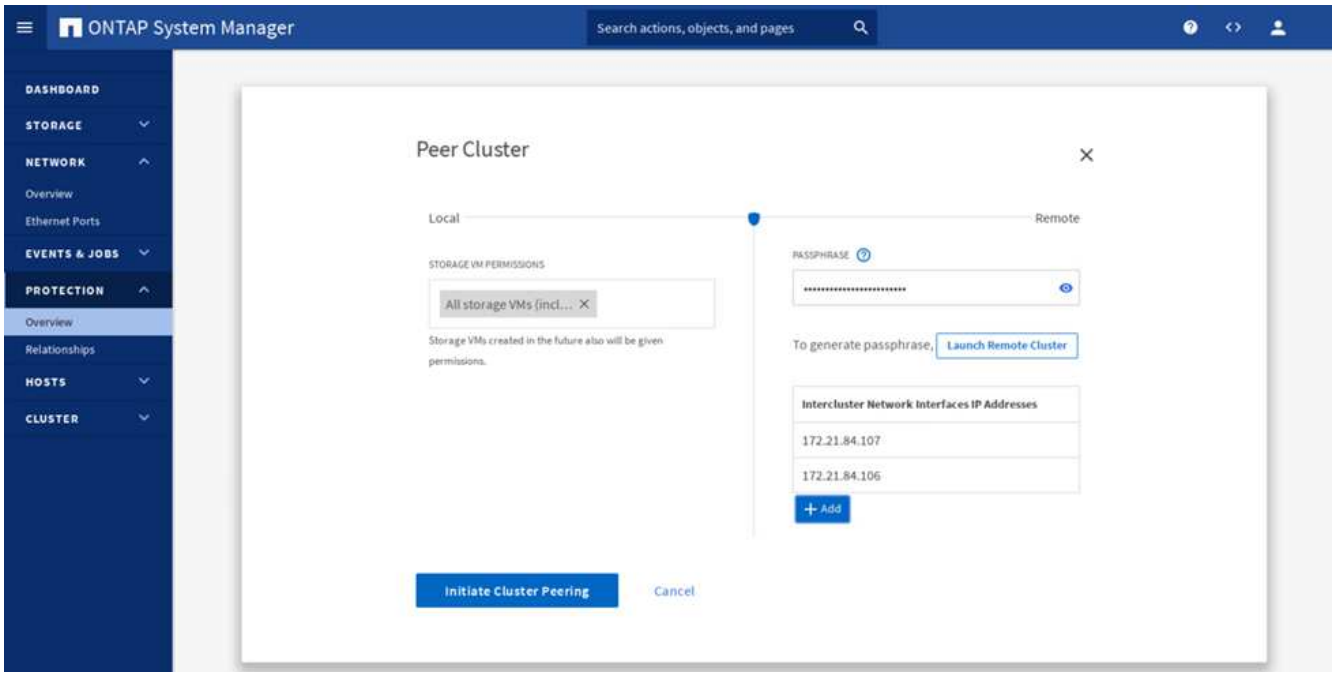


Pour pairs les deux clusters, effectuez la procédure suivante :

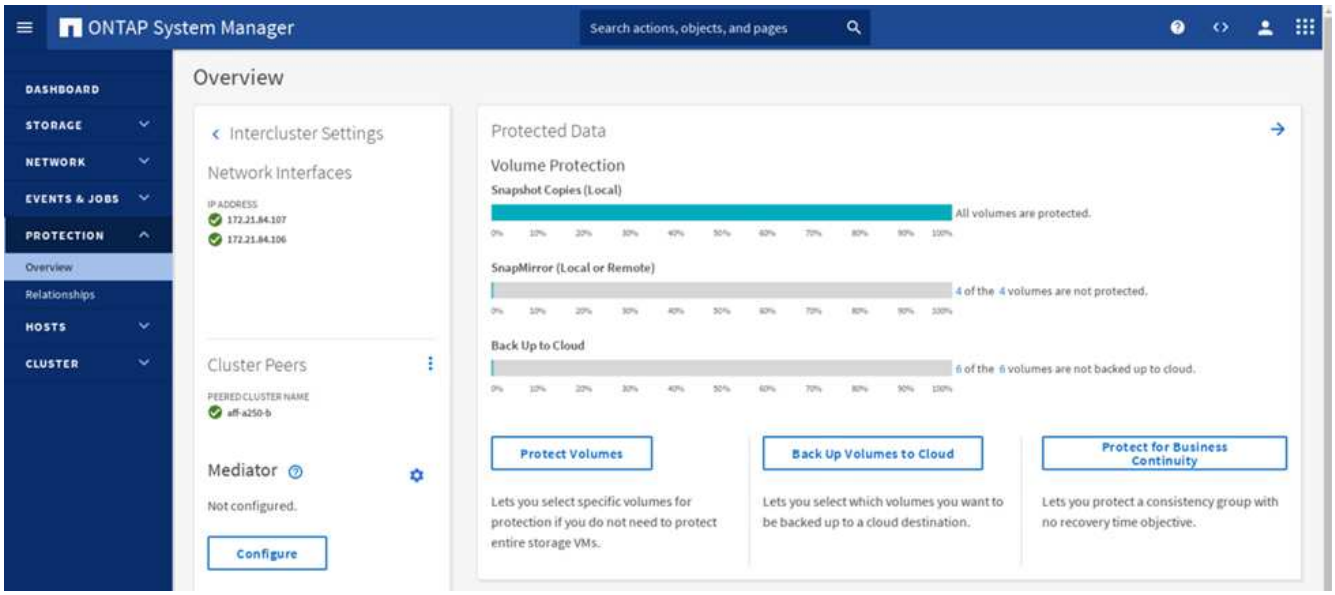
1. Générer la phrase de passe de peering de cluster dans le premier cluster.



2. Appeler l’option Peer Cluster dans le second cluster et fournir la phrase de passe et les informations LIF intercluster



3. Le volet protection > Présentation de System Manager affiche les informations sur les pairs de cluster.

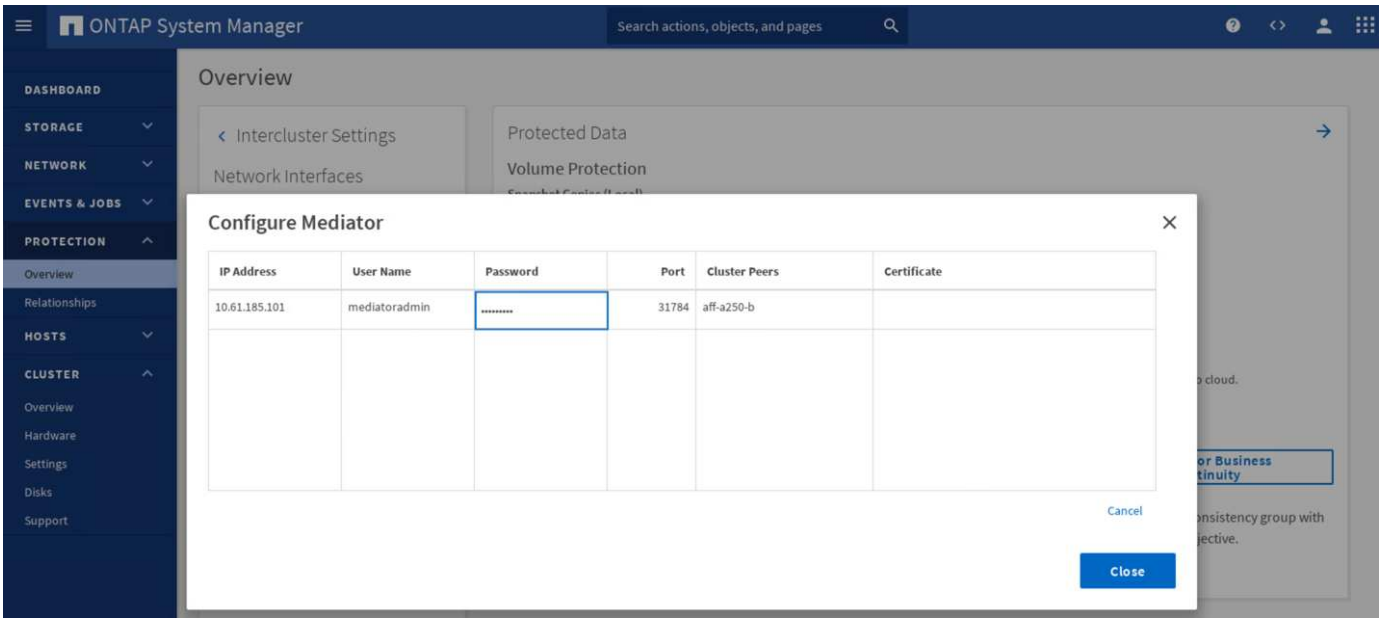


Installation et configuration du médiateur ONTAP

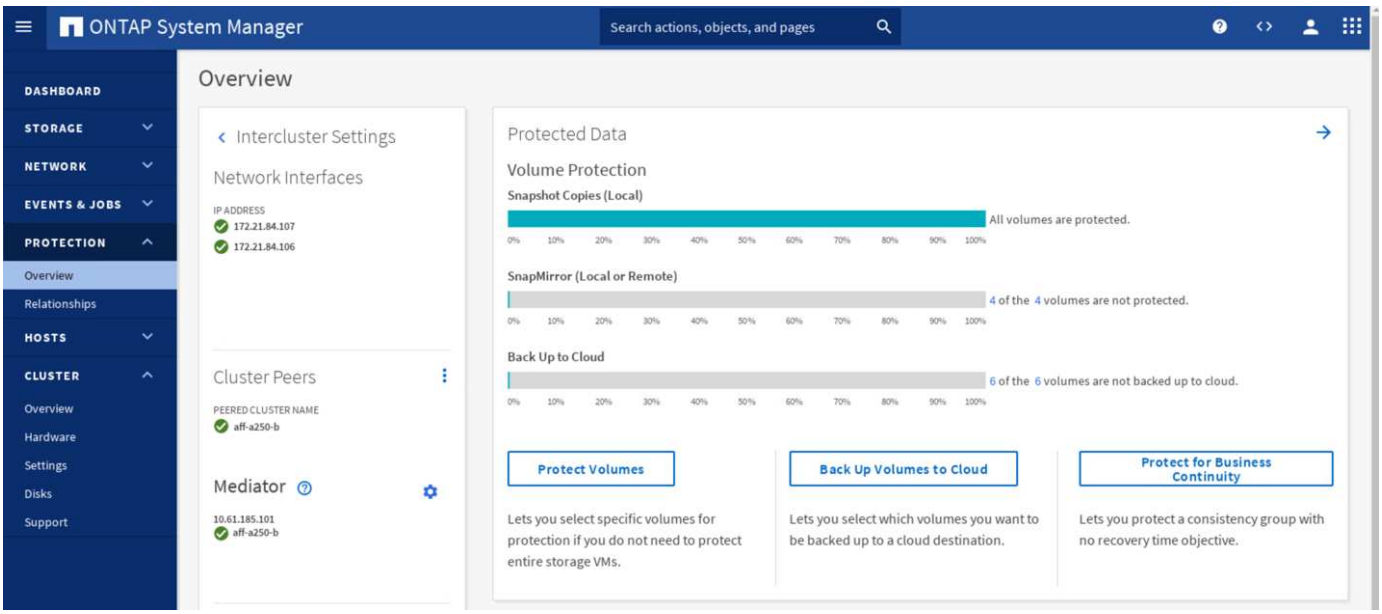
Le médiateur ONTAP établit un quorum pour les clusters ONTAP dans une relation SM-BC. Il coordonne le basculement automatique en cas de défaillance et aide à éviter les scénarios où chaque cluster tente simultanément d'établir le contrôle en tant que cluster principal.

Avant d'installer le médiateur ONTAP, consultez le "Installez ou mettez à niveau le service ONTAP Mediator" Page pour les prérequis, les versions Linux prises en charge et les procédures d'installation sur les différents systèmes d'exploitation Linux pris en charge.

Une fois le médiateur ONTAP installé, vous pouvez ajouter le certificat de sécurité du médiateur ONTAP aux clusters ONTAP, puis configurer le médiateur ONTAP dans le volet protection du gestionnaire système > vue d'ensemble. La capture d'écran suivante montre l'interface graphique de configuration du médiateur ONTAP.



Après avoir indiqué les informations nécessaires, le médiateur ONTAP configuré apparaît dans le volet protection du gestionnaire de système > vue d'ensemble.



Groupe de cohérence SM-BC

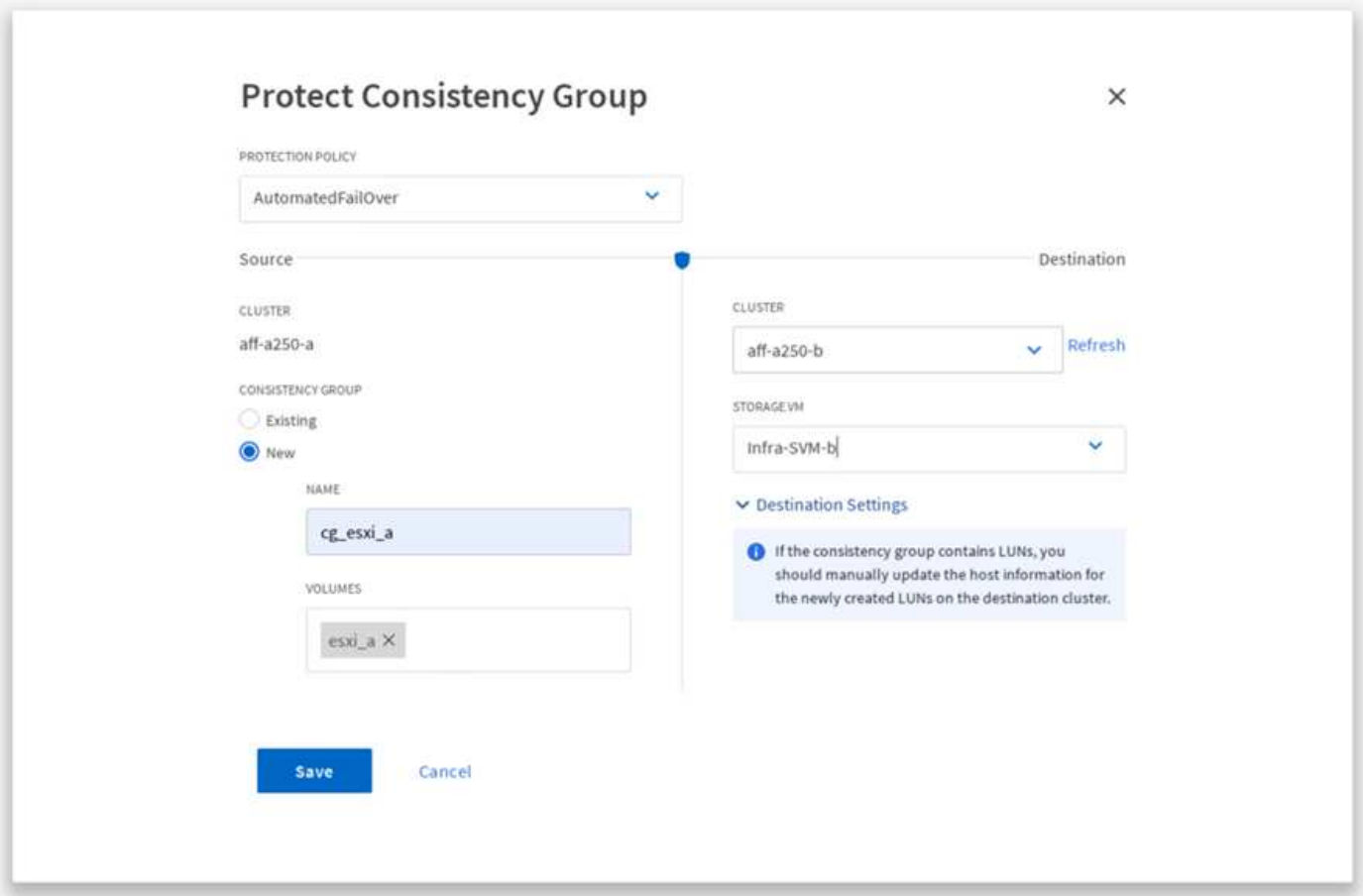
Un groupe de cohérence assure la cohérence d'ordre d'écriture d'une charge de travail d'application couvrant un ensemble de volumes spécifiés. Pour ONTAP 9.10.1, voici quelques-unes des restrictions importantes.

- Le nombre maximal de relations de groupe de cohérence SM-BC dans un cluster est de 20.
- Le nombre maximal de volumes pris en charge par relation SM-BC est de 16.
- Le nombre maximal de terminaux source et de destination dans un cluster est de 200.

Pour plus de détails, consultez la documentation du SM-BC de ONTAP sur le "restrictions et limites".

Pour la configuration de validation, ONTAP System Manager a été utilisé pour créer les groupes de cohérence afin de protéger à la fois les LUN de démarrage ESXi et les LUN de datastore partagé pour les deux sites. La

boîte de dialogue de création de groupes de cohérence est accessible en sélectionnant protection > Présentation > protection pour la continuité de l'activité > protéger le groupe de cohérence. Pour créer un groupe de cohérence, fournissez les volumes source, le cluster de destination et les informations de machine virtuelle de stockage de destination nécessaires à la création.

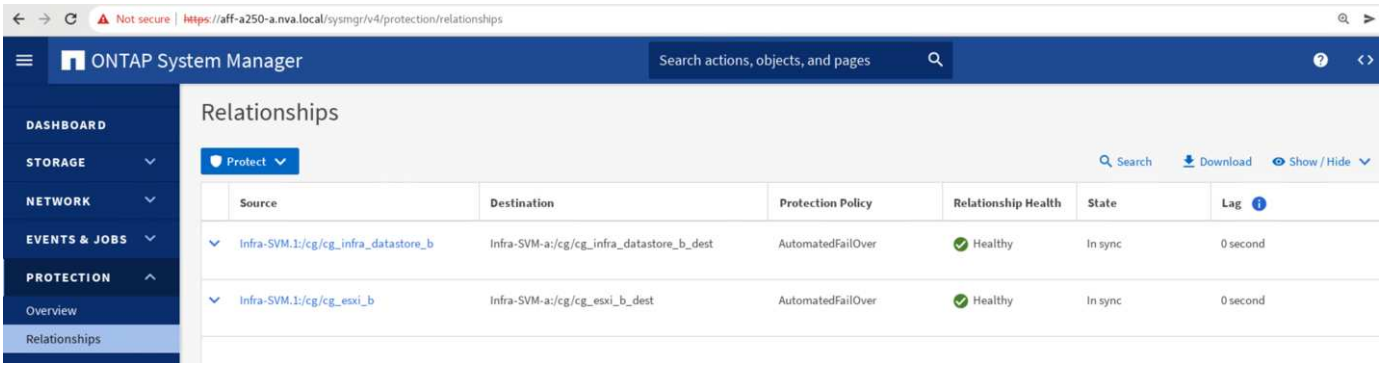


Le tableau suivant répertorie les quatre groupes de cohérence créés et les volumes inclus dans chaque groupe de cohérence pour le test de validation.

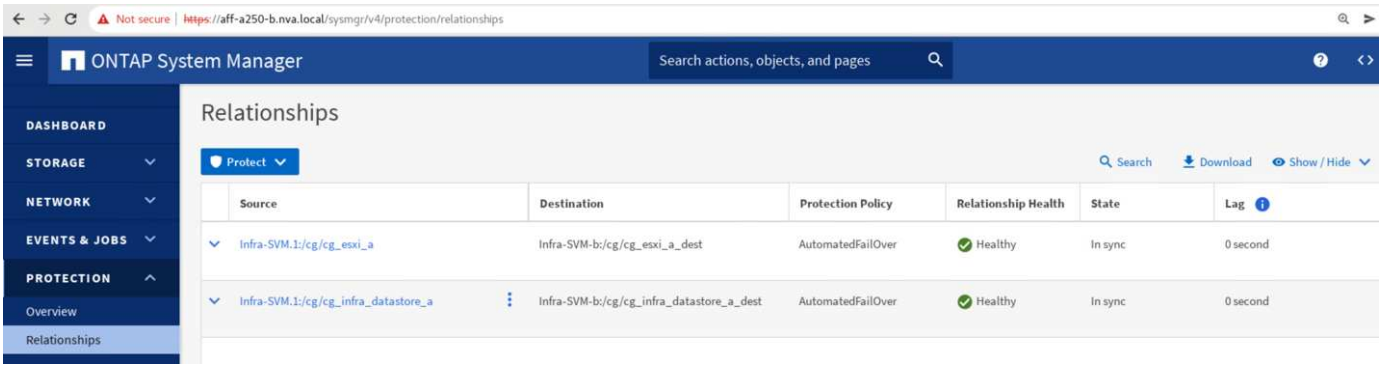
System Manager	Groupe de cohérence	Volumes
Site A	cg_esxi_a	esxi_a
Site A	cg_infra_datastore_a	infra_datastore_a_01 infra_datastore_a_02
Site B	cg_esxi_b	esxi_b
Site B	cg_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

Une fois les groupes de cohérence créés, ils s'affichent sous les relations de protection respectives sur le site A et sur le site B.

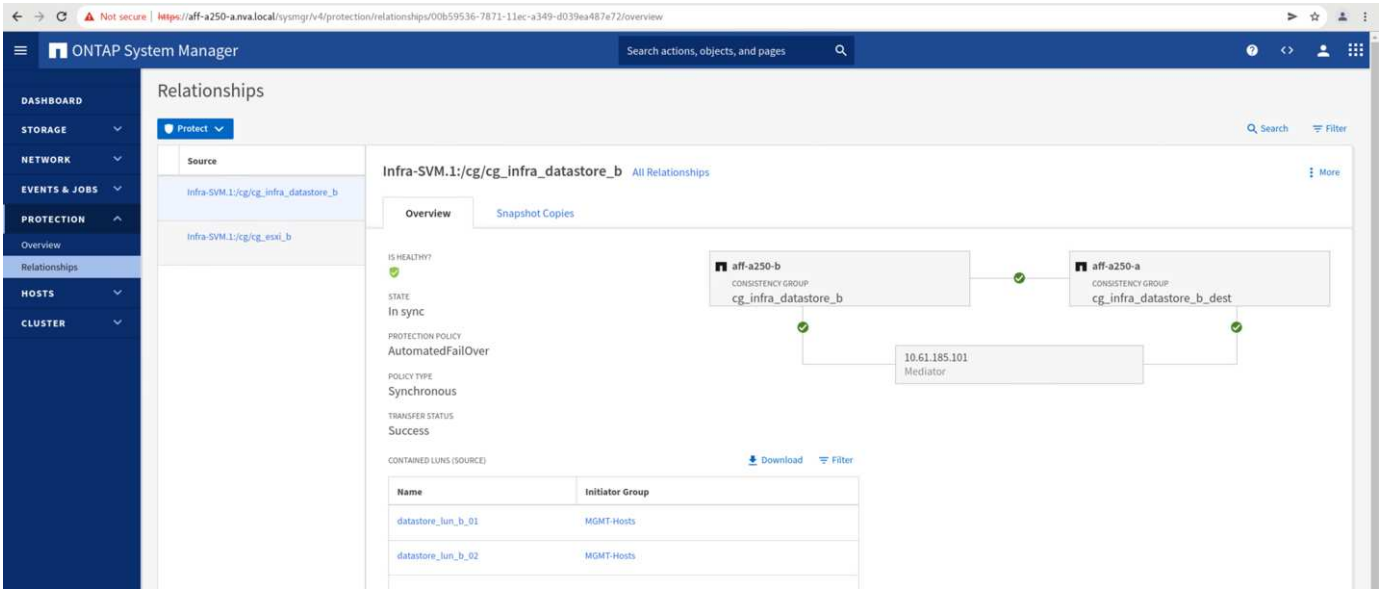
Cette capture d'écran affiche les relations de groupe de cohérence sur le site A.



Cette capture d'écran affiche les relations de groupe de cohérence sur le site B.



Cette capture d'écran affiche les détails de la relation de groupe de cohérence pour le groupe cg_infra_datastore_b.



Volumes, LUN et mappages d'hôtes

Une fois les groupes de cohérence créés, SnapMirror synchronise les volumes source et de destination pour que les données soient toujours synchronisées. Les volumes de destination du site distant portent les noms des volumes avec la fin _dest. Par exemple, pour le volume esxi_a du site Un cluster, il existe un volume ESXi_a_dest de protection des données (DP) correspondant sur le site B.

Cette capture d'écran affiche les informations de volume du site A.

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Cette capture d’écran affiche les informations de volume du site B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Pour faciliter le basculement transparent des applications, les LUN SM-BC en miroir doivent également être mappés sur les hôtes à partir du cluster de destination. Cela permet aux hôtes de voir correctement les chemins d’accès aux LUN depuis les clusters source et de destination. Le `igroup show` et `lun show` Les sorties du site A et du site B sont saisies dans les deux captures d’écran suivantes. Avec les mappages créés, chaque hôte ESXi du cluster voit son propre LUN de démarrage SAN comme ID 0 et les quatre LUN de datastore iSCSI partagés.

Cette capture d’écran montre les groupes initiateurs hôtes et le mappage de LUN pour le site A cluster.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01             VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02             VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03             VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                     MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01        VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02        VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03        VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b                MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

Cette capture d’écran montre les groupes initiateurs hôtes et le mappage de LUN pour le cluster du site B.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Validation de la solution - virtualisation."

Validation de la solution : virtualisation

"Précédente : validation de la solution - stockage."

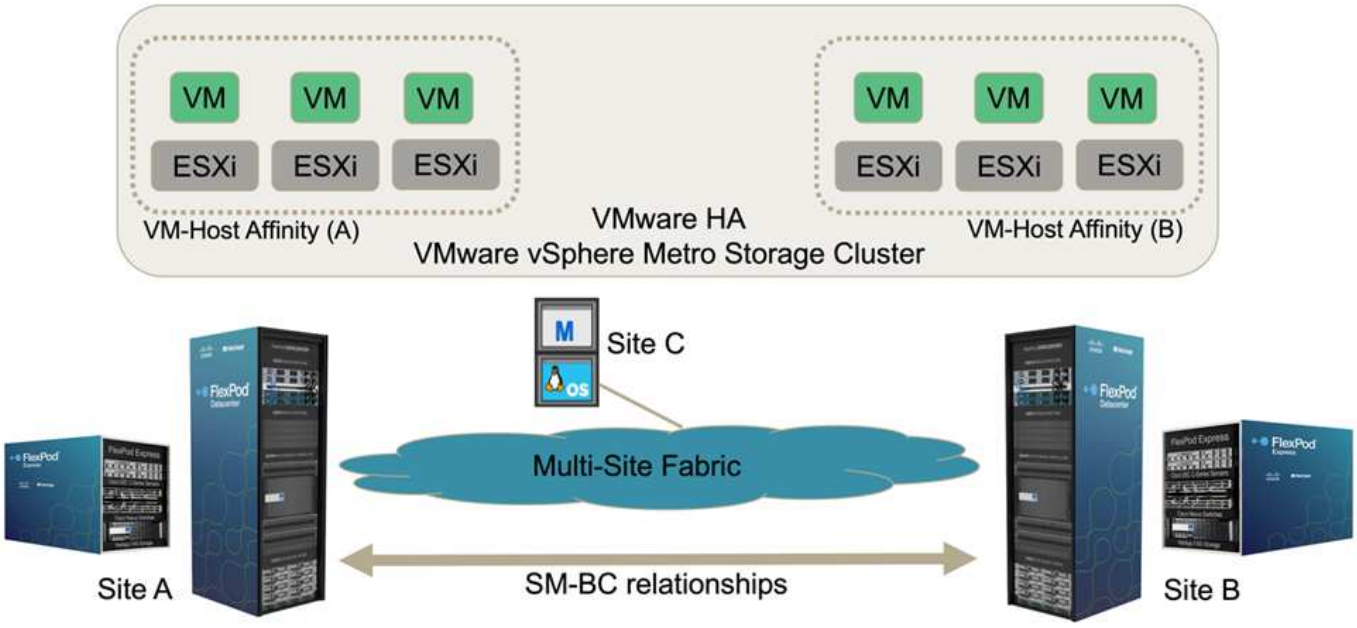
Dans la solution multisite FlexPod SM-BC, un seul VMware vCenter gère les ressources de l'infrastructure virtuelle pour l'ensemble de la solution. Les hôtes des deux data centers font partie du cluster haute disponibilité VMware unique qui s'étend sur les deux data centers. Les hôtes ont accès à la solution NetApp SM-BC où le stockage avec des relations SM-BC définies est accessible depuis les deux sites.

Le stockage de la solution SM-BC est conforme au modèle d'accès uniforme de la fonctionnalité VMware vSphere Metro Storage Cluster (vMSC) afin d'éviter les incidents et les temps d'indisponibilité. Pour des performances optimales des machines virtuelles, les disques de ces machines doivent être hébergés sur les systèmes locaux AFF A250 de NetApp. La latence et le trafic sur les liaisons WAN doivent ainsi être minimisés en cas de fonctionnement normal.

Dans le cadre de la mise en œuvre de la conception, il est nécessaire de déterminer la répartition des machines virtuelles entre les deux sites. Vous pouvez déterminer l'affinité de site et la distribution des applications de cette machine virtuelle sur les deux sites en fonction des préférences de votre site et des exigences de vos applications. Les groupes VM/hôtes du cluster VMware et les règles VM/hôte sont utilisés pour configurer l'affinité VM/hôte afin de s'assurer que les VM s'exécutent sur les hôtes du site souhaité.

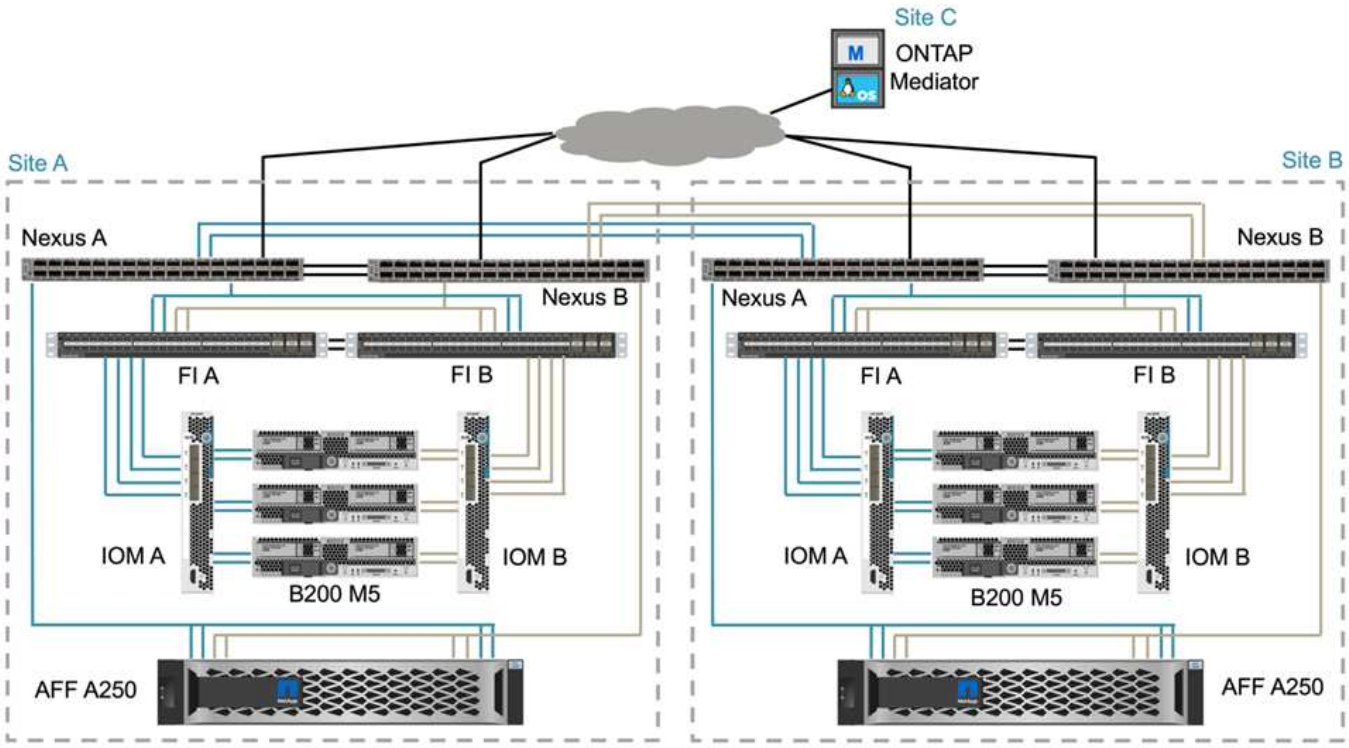
Toutefois, les configurations permettant d'exécuter des machines virtuelles sur les deux sites garantissent la résilience de la solution pour redémarrer les ordinateurs virtuels sur les hôtes du site distant. Pour que les machines virtuelles s'exécutent sur les deux sites, tous les datastores iSCSI partagés doivent être montés sur tous les hôtes ESXi afin de garantir un fonctionnement vMotion fluide des machines virtuelles entre les sites.

La figure suivante montre une vue de virtualisation de la solution FlexPod SM-BC haut de gamme incluant à la fois des fonctionnalités VMware HA et vMSC afin d'offrir la haute disponibilité des services de calcul et de stockage. L'architecture de solution de data Center actif-actif permet la mobilité de la charge de travail entre les sites et assure la reprise après incident et la continuité de l'activité.



Connectivité réseau de bout en bout

La solution FlexPod SM-BC comprend des infrastructures FlexPod sur chaque site, une connectivité réseau entre les sites et un médiateur ONTAP déployé sur un troisième site afin d'atteindre les objectifs RPO et RTO requis. La figure suivante montre une connectivité réseau de bout en bout entre les serveurs Cisco UCS B200M5 sur chaque site et le système de stockage NetApp disposant de fonctionnalités SM-BC sur un site et sur plusieurs sites.



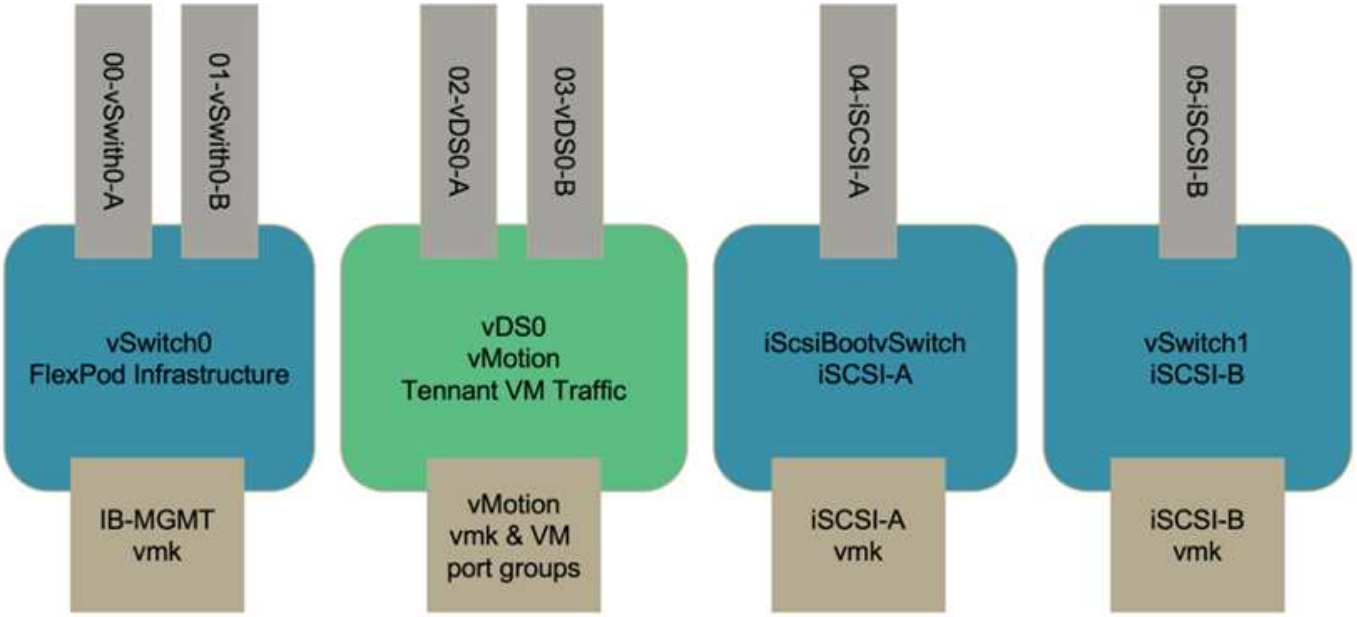
L'architecture de déploiement FlexPod est identique sur chaque site pour la validation de cette solution. Cependant, elle prend en charge les déploiements asymétriques et peut également être ajoutée aux solutions FlexPod existantes s'ils répondent aux exigences.

Une architecture étendue couche 2 est utilisée pour une Data Fabric multisite transparente qui offre une connectivité entre les ressources de calcul Cisco UCS et le stockage NetApp bâbord dans chaque data Center, ainsi que la connectivité entre les data centers. La configuration du canal de port et la configuration du canal de port virtuel, le cas échéant, sont utilisées pour l'agrégation de la bande passante et la tolérance aux pannes entre les couches de calcul, de réseau et de stockage, ainsi que pour les liens intersites. Par conséquent, les serveurs lames UCS offrent une connectivité et un accès multivoie aux systèmes de stockage NetApp locaux et distants.

La mise en réseau virtuelle

Chaque hôte du cluster est déployé à l'aide d'une mise en réseau virtuelle identique, quel que soit son emplacement. La conception sépare les différents types de trafic à l'aide de commutateurs virtuels VMware (vSwitch) et de switchs virtuels VMware (VDS). Le vSwitch VMware est utilisé principalement pour les réseaux d'infrastructure FlexPod et VDS pour les réseaux d'applications, mais il n'est pas nécessaire.

Les commutateurs virtuels (vSwitch, VDS) sont déployés avec deux liaisons ascendantes par commutateur virtuel. Les liaisons ascendantes au niveau de l'hyperviseur ESXi sont appelées vmnics et vNIC virtuels (vNIC) sur le logiciel Cisco UCS. Les vNIC sont créés sur l'adaptateur Cisco UCS VIC de chaque serveur en utilisant des profils de service Cisco UCS. Six vNIC sont définis, deux pour vSwitch0, deux pour vDS0, deux pour vSwitch1 et deux pour les liaisons montantes iSCSI, comme illustré dans la figure suivante.



VSwitch0 est défini lors de la configuration hôte VMware ESXi. Il contient le VLAN de gestion de l'infrastructure FlexPod et les ports VMK (hôte ESXi) pour la gestion. Un groupe de ports de machine virtuelle de gestion d'infrastructure est également placé sur vSwitch0 pour les machines virtuelles de gestion d'infrastructure stratégiques requises.

Il est important de placer ces machines virtuelles d'infrastructure de gestion sur vSwitch0 plutôt que dans le VDS, car si l'infrastructure FlexPod est arrêtée ou mise hors tension et que vous tentez d'activer cette machine virtuelle de gestion sur un hôte autre que l'hôte sur lequel elle était exécutée à l'origine, Il démarre très bien sur le réseau sur vSwitch0. Ce processus est particulièrement important si VMware vCenter est la machine virtuelle de gestion. Si vCenter se trouvaient sur le VDS et était déplacé vers un autre hôte puis démarré, il ne serait pas connecté au réseau après le démarrage.

Deux vswitches de démarrage iSCSI sont utilisés dans cette conception. Le démarrage iSCSI Cisco UCS nécessite des vNIC distincts pour le démarrage iSCSI. Ces vNIC utilisent le VLAN iSCSI de la structure appropriée en tant que VLAN natif et sont connectés au vSwitch de démarrage iSCSI approprié. Vous pouvez également déployer des réseaux iSCSI sur VDS en déployant un nouveau VDS ou en utilisant une existante.

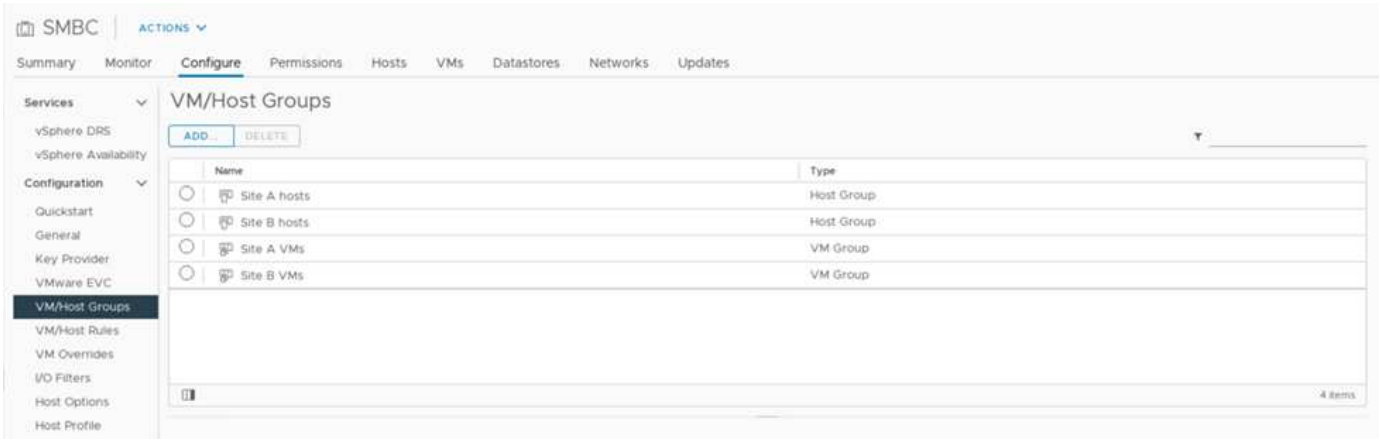
Règles et groupes d'affinité VM-Host

Pour que les machines virtuelles s'exécutent sur n'importe quel hôte ESXi des deux sites SM-BC, tous les hôtes ESXi doivent monter les datastores iSCSI des deux sites. Si les datastores des deux sites sont correctement montés par tous les hôtes ESXi, vous pouvez migrer une machine virtuelle entre tous les hôtes avec vMotion et la machine virtuelle conserve toujours l'accès à tous ses disques virtuels créés à partir de ces datastores.

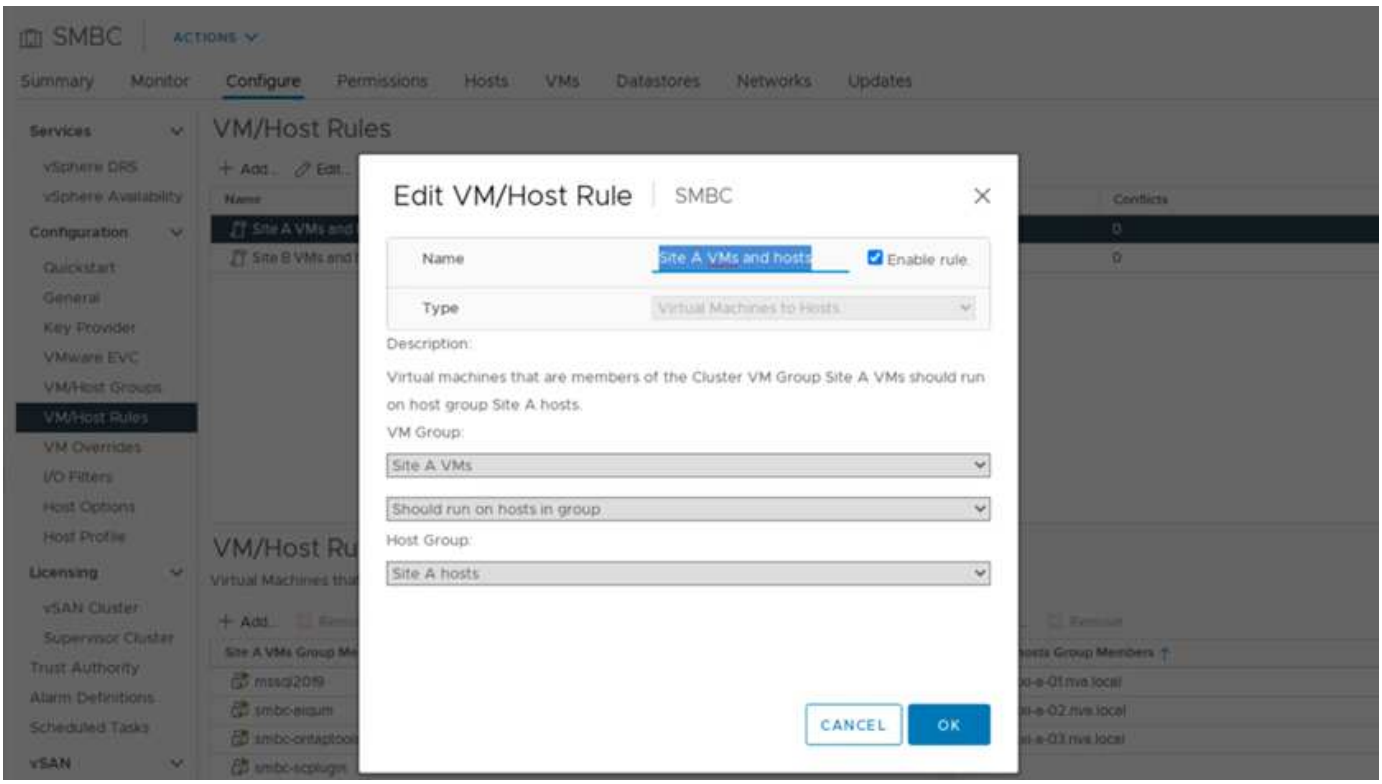
Dans le cas d'une machine virtuelle utilisant des datastores locaux, son accès aux disques virtuels devient distant s'il est migré vers un hôte du site distant et augmente ainsi la latence des opérations de lecture en raison de la distance physique entre les sites. Par conséquent, il est recommandé de conserver les machines virtuelles sur les hôtes locaux et d'utiliser le stockage local sur le site.

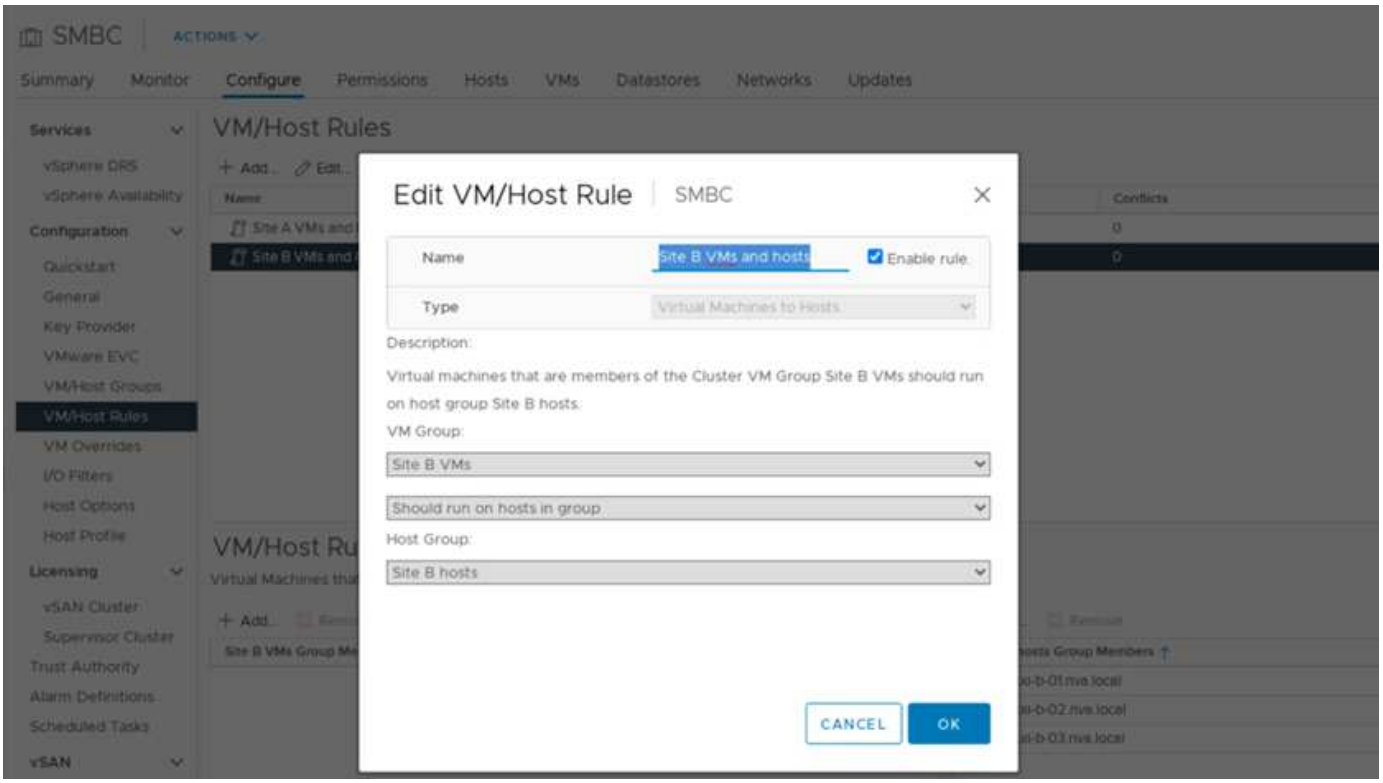
En utilisant un mécanisme d'affinité VM/hôte, vous pouvez utiliser des groupes VM/hôtes pour créer un groupe de VM et un groupe d'hôtes pour les machines virtuelles et les hôtes situés sur un site particulier. Les règles VM/hôte vous permettent de spécifier la règle à suivre pour les VM et les hôtes. Pour permettre la migration de la machine virtuelle entre les sites pendant un scénario de maintenance de site ou de sinistre, utilisez la spécification de stratégie « devrait s'exécuter sur les hôtes du groupe » pour cette flexibilité.

La capture d'écran suivante montre que deux groupes d'hôtes et deux groupes de machines virtuelles sont créés pour les hôtes et les machines virtuelles du site A et du site B.



En outre, les deux figures suivantes montrent les règles VM/hôte créées pour les machines virtuelles du site A et du site B à exécuter sur les hôtes de leurs sites respectifs à l'aide de la stratégie « devrait s'exécuter sur les hôtes du groupe ».

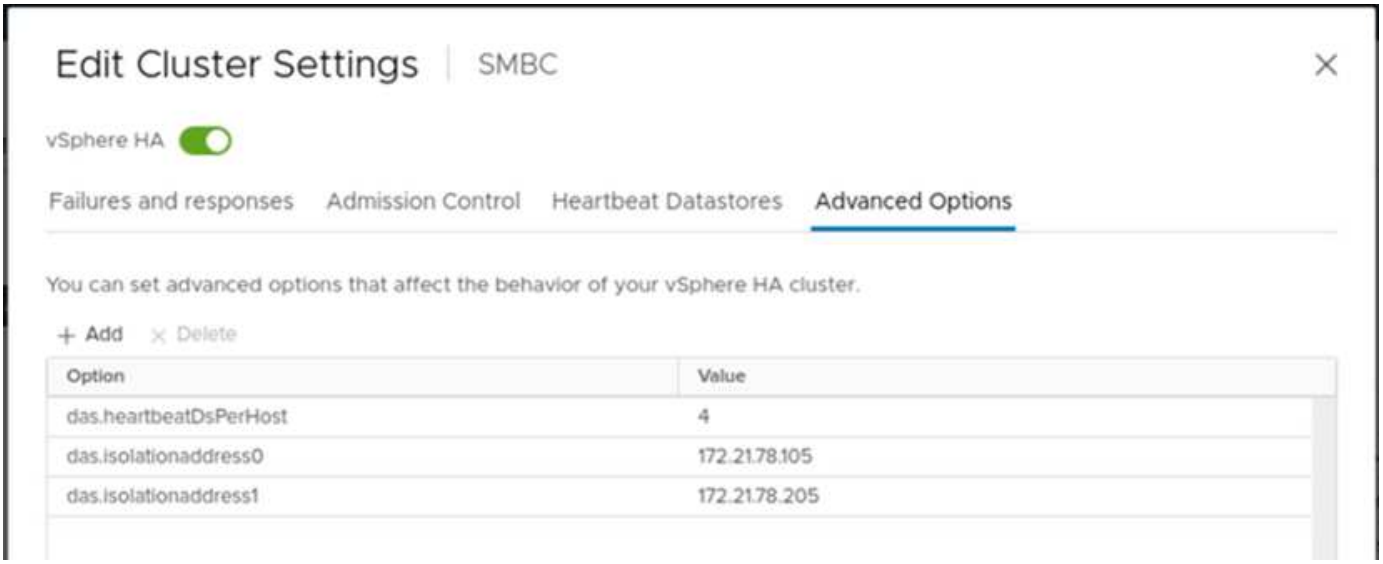




Pulsation vSphere HA

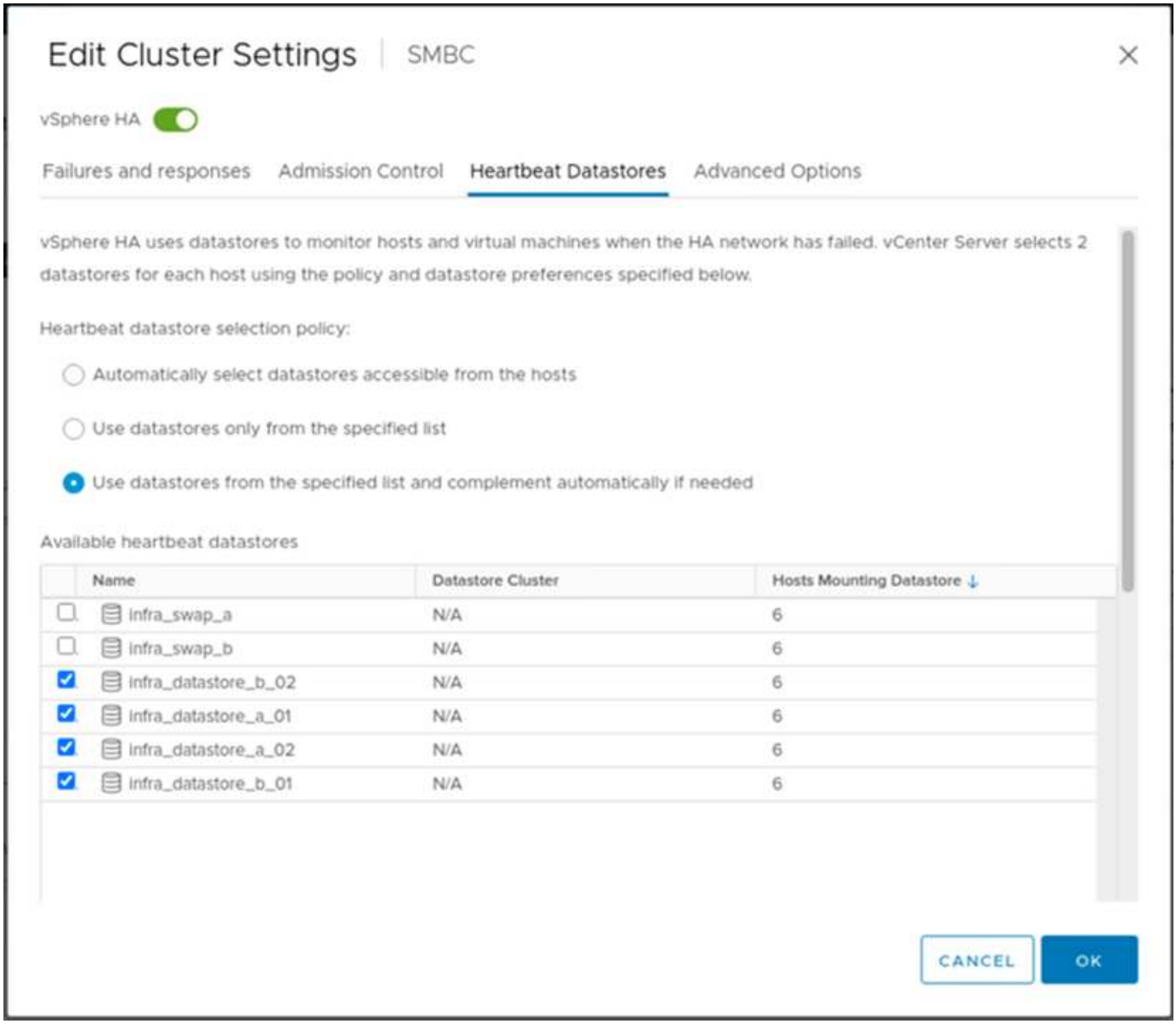
VMware vSphere HA dispose d'un mécanisme de pulsation pour la validation de l'état hôte. Le mécanisme de pulsation principal passe par le réseau, tandis que le mécanisme de pulsation secondaire se fait par l'intermédiaire du datastore. Si les signaux ne sont pas reçus, il décide alors s'ils sont isolés du réseau en envoyant une commande ping à la passerelle par défaut ou aux adresses d'isolation configurées manuellement. Pour le signal de détection du datastore, VMware recommande d'augmenter les datastores de signal de détection de deux à quatre pour un cluster étendu.

Pour la validation de la solution, les deux adresses IP de gestion de cluster ONTAP sont utilisées comme adresse d'isolation. En outre, l'option avancée vSphere HA est recommandée `ds.heartbeatDsPerHost` avec une valeur de 4 a été ajoutée comme indiqué dans la figure suivante.



Pour le datastore de signal de détection, spécifiez les quatre datastores partagés du cluster et complétez

automatiquement, comme illustré dans la figure suivante.



Pour connaître les meilleures pratiques et les configurations pour VMware HA Cluster et VMware vSphere Metro Storage Cluster, consultez "Création et utilisation de clusters HA vSphere", "Cluster de stockage Metro VMware vSphere (vMSC)" Et VMware KB pour "NetApp ONTAP avec NetApp SnapMirror Business Continuity (SM-BC) et VMware vSphere Metro Storage Cluster (vMSC)".

"La validation des solutions : scénarios validés"

Validation des solutions : scénarios validés

"Validation de la solution - virtualisation."

La solution FlexPod Datacenter SM-BC protège les services de données dans de nombreux scénarios de point de défaillance unique et en cas d'incident sur site. La conception redondante implémentée sur chaque site assure une haute disponibilité et l'implémentation de SM-BC avec réplication synchrone des données sur plusieurs sites protège les services de données d'un incident sur l'ensemble d'un site. La solution

déployée est validée pour les fonctions de la solution ainsi que pour les différents scénarios de défaillance pour lesquels la solution est conçue pour la protection.

Validation des fonctions de la solution

Différents cas de test sont utilisés pour vérifier le fonctionnement de la solution et simuler des scénarios de défaillance partielle et complète du site. Pour réduire au minimum la duplication avec les tests déjà effectués dans les solutions de data Center FlexPod existantes dans le cadre du programme de conception validée par Cisco, ce rapport se concentre sur les aspects liés à SM-BC de la solution. Certaines validations FlexPod générales sont incluses pour que les praticiens puissent passer en revue leurs validations de mise en œuvre.

Pour la validation de la solution, une machine virtuelle Windows 10 par hôte ESXi a été créée sur tous les hôtes ESXi des deux sites. L'outil IOMeter a été installé et utilisé pour générer des E/S sur deux disques de données virtuels mappés à partir des datastores iSCSI locaux partagés. Les paramètres de la charge de travail IOMeter configurés étaient à 8 Ko d'E/S, à 75 % de lecture et à 50 % aléatoires, et 8 commandes d'E/S en attente pour chaque disque de données. Dans la plupart des scénarios de test réalisés, la suite des E/S IOMeter montre que le scénario n'a pas provoqué de panne du service de données.

Étant donné que SM-BC est critique pour les applications métier telles que les serveurs de base de données, L'instance Microsoft SQL Server 2019 d'une machine virtuelle Windows Server 2022 a également été incluse dans le cadre des tests pour confirmer que l'application continue à s'exécuter lorsque le stockage sur son site local n'est pas disponible et que le service de données est repris sur le système de stockage du site distant sans application perturbation.

Test de démarrage SAN iSCSI de l'hôte ESXi

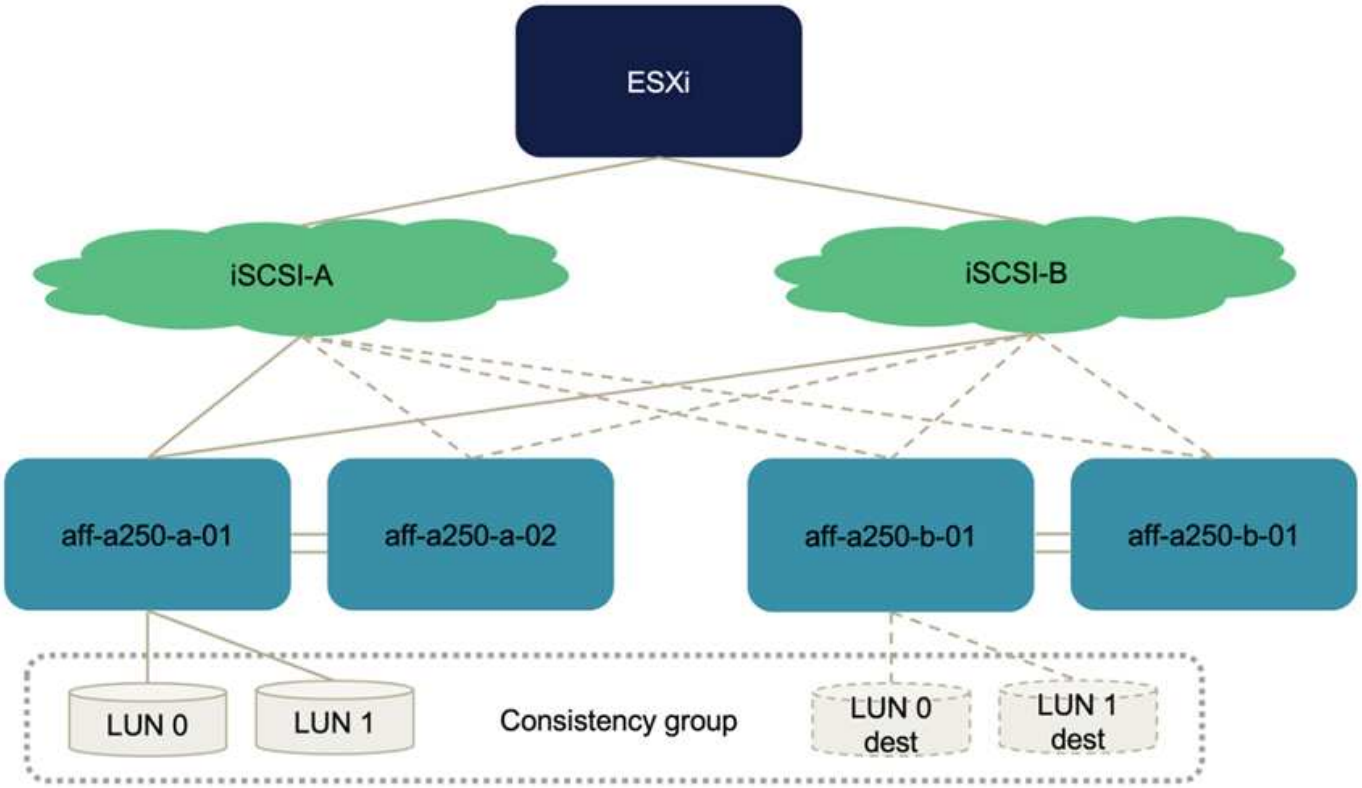
Les hôtes ESXi de la solution sont configurés pour démarrer à partir du SAN iSCSI. L'utilisation du démarrage SAN simplifie la gestion du serveur lors du remplacement d'un serveur car le profil de service du serveur peut être associé à un nouveau serveur pour qu'il démarre sans apporter de modifications de configuration supplémentaires.

En plus de démarrer un hôte ESXi situé sur un site à partir de sa LUN de démarrage iSCSI locale, un test a également été effectué pour démarrer l'hôte ESXi lorsque son contrôleur de stockage local est en état de basculement ou lorsque son cluster de stockage local est totalement indisponible. Ces scénarios de validation garantissent la configuration correcte des hôtes ESXi par conception et peuvent démarrer lors d'une maintenance du stockage ou d'un scénario de reprise après incident afin d'assurer la continuité de l'activité.

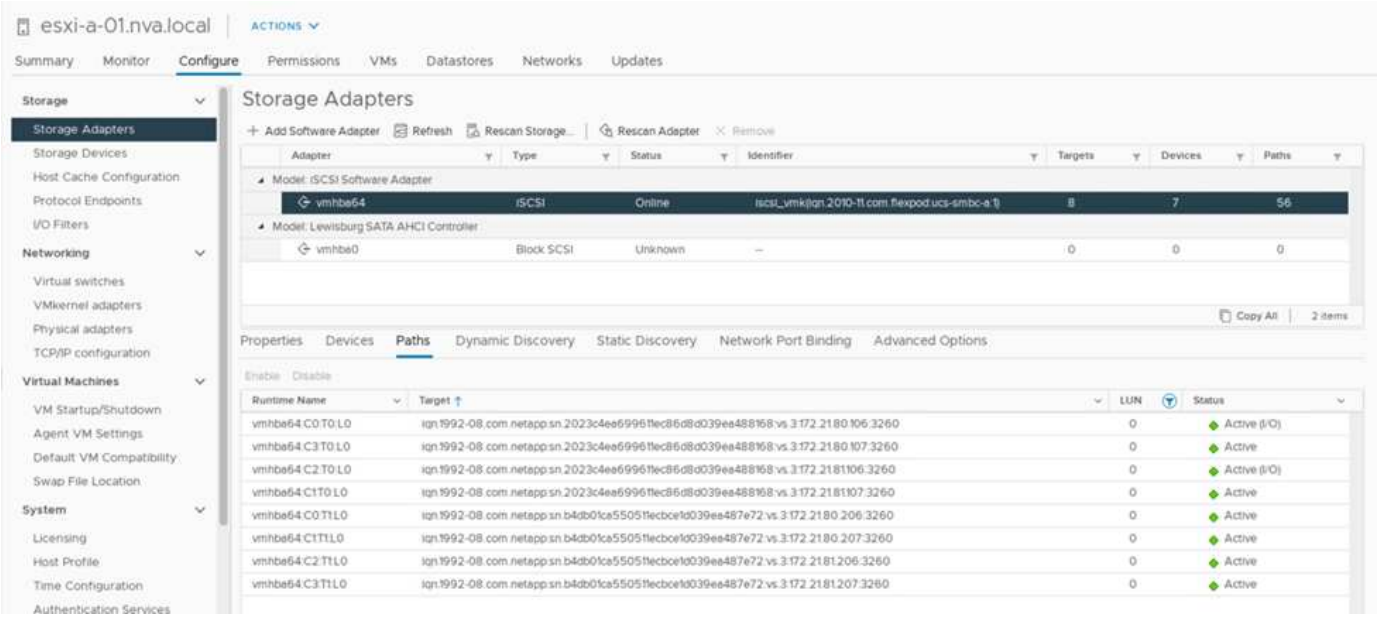
Avant de configurer la relation de groupe de cohérence SM-BC, une LUN iSCSI hébergée par une paire haute disponibilité de contrôleur de stockage dispose de quatre chemins, deux par le biais de chaque structure iSCSI, selon l'implémentation des meilleures pratiques. Un hôte peut passer au LUN via les deux VLAN/fabrics iSCSI vers le contrôleur hôte LUN, ainsi via le partenaire haute disponibilité du contrôleur.

Une fois la relation de groupe de cohérence SM-BC configurée et les LUN en miroir correctement mappées sur les initiateurs, le nombre de chemins d'accès de la LUN double. Pour cette implémentation, il s'agit de disposer de deux chemins actifs/optimisés et de deux chemins actifs/non optimisés, d'avoir deux chemins actifs/optimisés et six chemins actifs/non optimisés.

La figure suivante illustre les chemins qu'un hôte ESXi peut prendre pour accéder à une LUN, par exemple LUN 0. Comme la LUN est connectée au site A contrôleur 01, seuls les deux chemins qui accèdent directement à la LUN via ce contrôleur sont actifs/optimisés et les six chemins restants sont actifs/non optimisés.



La capture d'écran suivante des informations sur le chemin du périphérique de stockage montre comment l'hôte ESXi voit les deux types de chemins de périphérique. Les deux chemins actifs/optimisés sont indiqués comme ayant `active (I/O)` l'état du chemin, alors que les six chemins actifs/non optimisés sont affichés uniquement comme `active`. Notez également que la colonne cible affiche les deux cibles iSCSI et les adresses IP LIF iSCSI respectives pour obtenir les cibles.



Lorsqu'un des contrôleurs de stockage est en panne pour cause de maintenance ou de mise à niveau, les deux chemins qui atteignent le contrôleur de panne ne sont plus disponibles et affichent le chemin d'accès à `dead` à la place.

Si un basculement de groupe de cohérence se produit sur le cluster de stockage principal, soit en raison de

tests de basculement manuels, soit d'un basculement automatique en cas d'incident, le cluster de stockage secondaire continue à fournir les services de données pour les LUN du groupe de cohérence SM-BC. Comme les identités de LUN sont préservées et que les données ont été répliquées de manière synchrone, toutes les LUN de démarrage de l'hôte ESXi protégées par les groupes de cohérence SM-BC restent disponibles depuis le cluster de stockage distant.

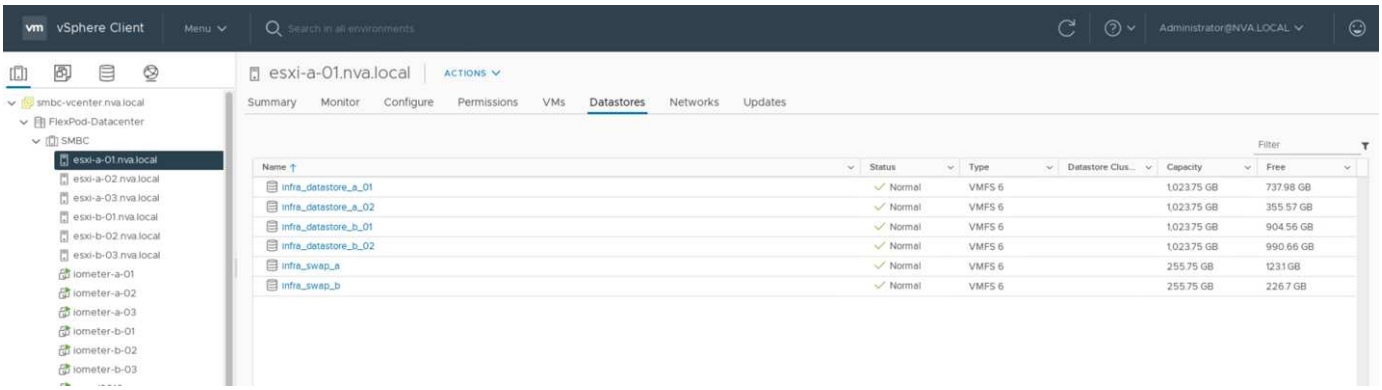
Test d'affinité avec les VM/hôtes VMware vMotion

Bien qu'une solution générique FlexPod VMware Datacenter prenne en charge plusieurs protocoles, tels que FC, iSCSI, NVMe et NFS, la fonctionnalité de la solution FlexPod SM-BC prend en charge les protocoles SAN FC et iSCSI généralement utilisés pour les solutions stratégiques. Cette validation utilise uniquement les datastores basés sur protocole iSCSI et le démarrage SAN iSCSI.

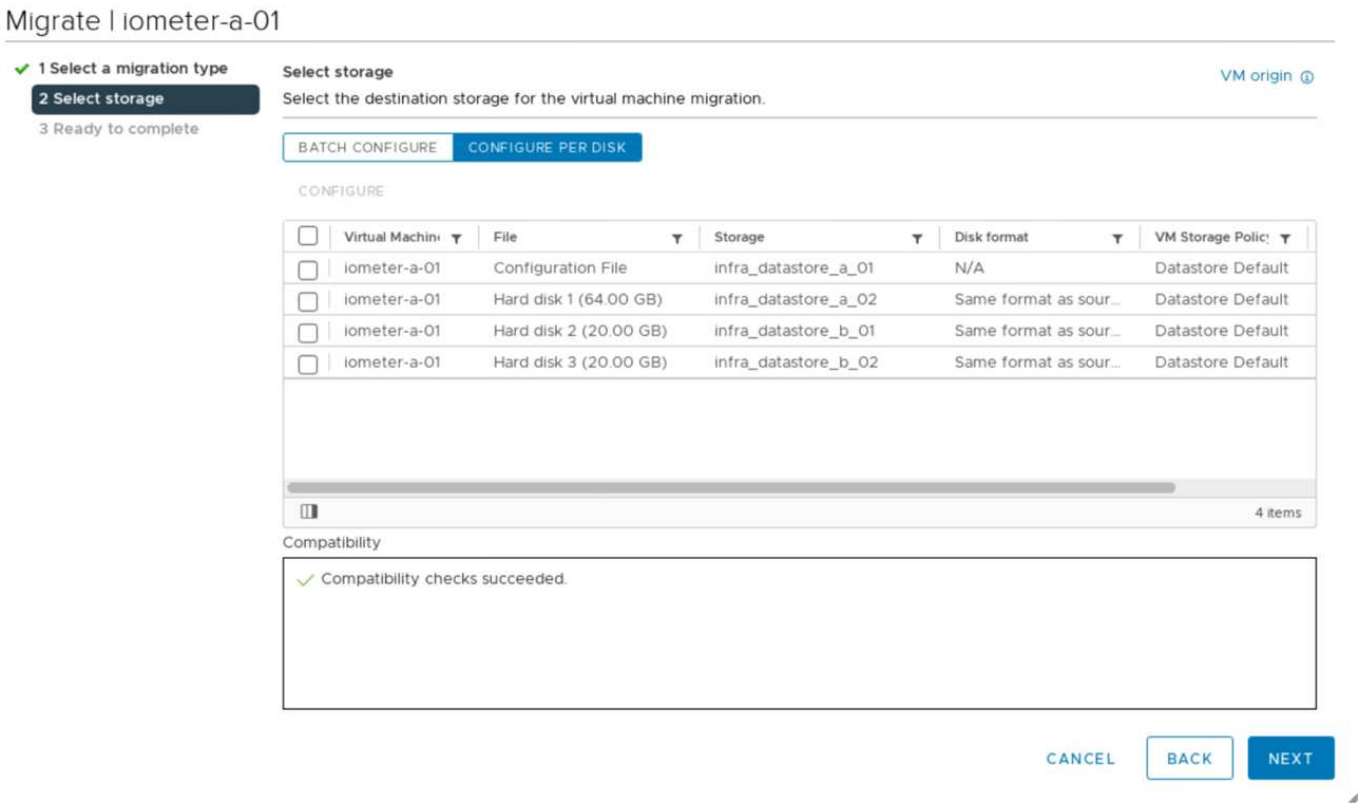
Pour permettre aux machines virtuelles d'utiliser les services de stockage depuis l'un des sites SM-BC, les datastores iSCSI des deux sites doivent être montés par tous les hôtes du cluster afin de permettre la migration des machines virtuelles entre les deux sites et dans le cadre de scénarios de basculement en cas d'incident.

Il est également possible d'utiliser le protocole NFS et les datastores NFS pour les applications exécutées sur l'infrastructure virtuelle qui ne nécessitent pas la protection des groupes de cohérence SM-BC entre les sites. Dans ce cas, il convient d'observer une attention particulière lors de l'allocation du stockage pour les VM afin que les applications stratégiques utilisent correctement les datastores SAN protégés par le groupe de cohérence SM-BC pour assurer la continuité de l'activité.

La capture d'écran suivante montre que les hôtes sont configurés pour monter des datastores iSCSI à partir des deux sites.



Vous pouvez migrer des disques de machines virtuelles entre des datastores iSCSI disponibles depuis les deux sites, comme le montre la figure suivante. Pour considérations de performances, il est optimal de disposer de serveurs virtuels qui utilisent le stockage de leur cluster de stockage local afin de réduire les latences d'E/S des disques. Ceci est particulièrement vrai lorsque les deux sites sont situés à certaines distances, en raison de la latence de distance de aller-retour physique d'environ 1 ms par 100 km de distance.



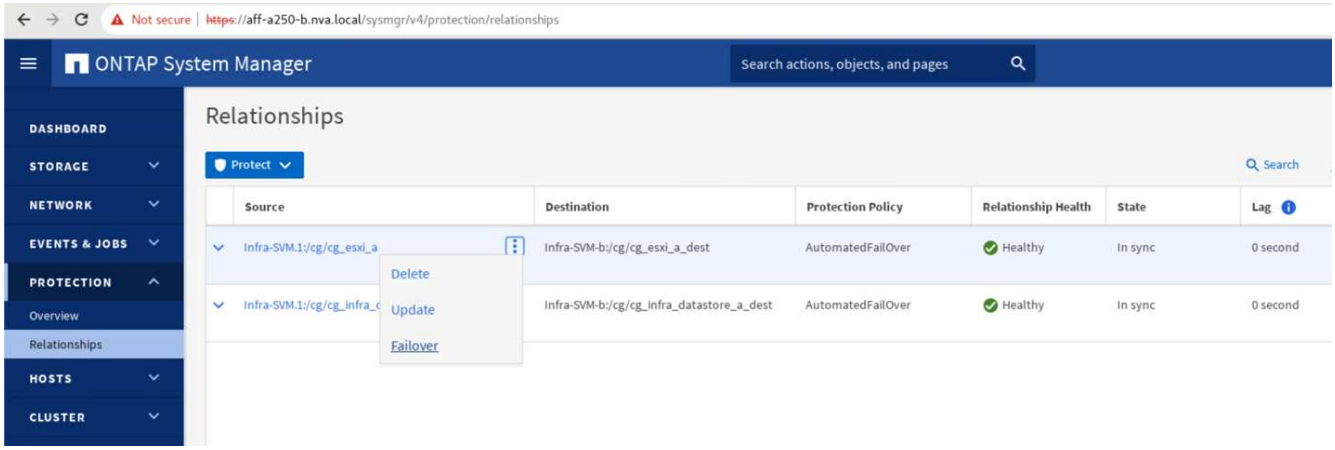
Des tests de vMotion d'machines virtuelles sur un hôte différent au niveau du même site, ainsi que sur plusieurs sites ont été réalisés et ont abouti. Après avoir migré manuellement une machine virtuelle sur plusieurs sites, la règle d'affinité VM/hôte s'active et retransfère la machine virtuelle au groupe où elle appartient dans la condition normale.

Basculement planifié du stockage

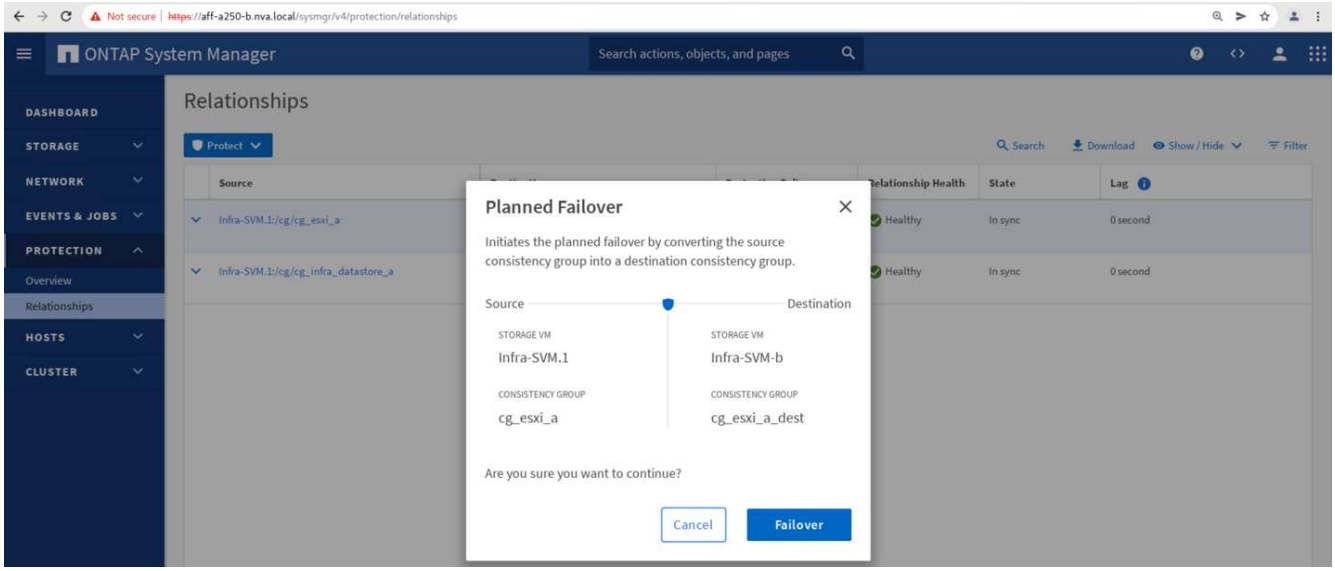
Les opérations planifiées de basculement du stockage doivent être réalisées sur la solution après la configuration initiale afin de déterminer si la solution fonctionne correctement après le basculement du stockage. Ce test peut aider à identifier tout problème de connectivité ou de configuration susceptible d'entraîner des interruptions d'E/S. Les tests et la résolution réguliers de tout problème de connectivité ou de configuration permettent de fournir des services de données sans interruption en cas d'incident sur site réel. Le basculement planifié du stockage peut également être utilisé avant une maintenance planifiée du stockage afin que les services de données puissent être assurés depuis le site non affecté.

Pour lancer un basculement manuel des services de données de stockage du site A vers le site B, vous pouvez utiliser le site B ONTAP System Manager pour effectuer l'action.

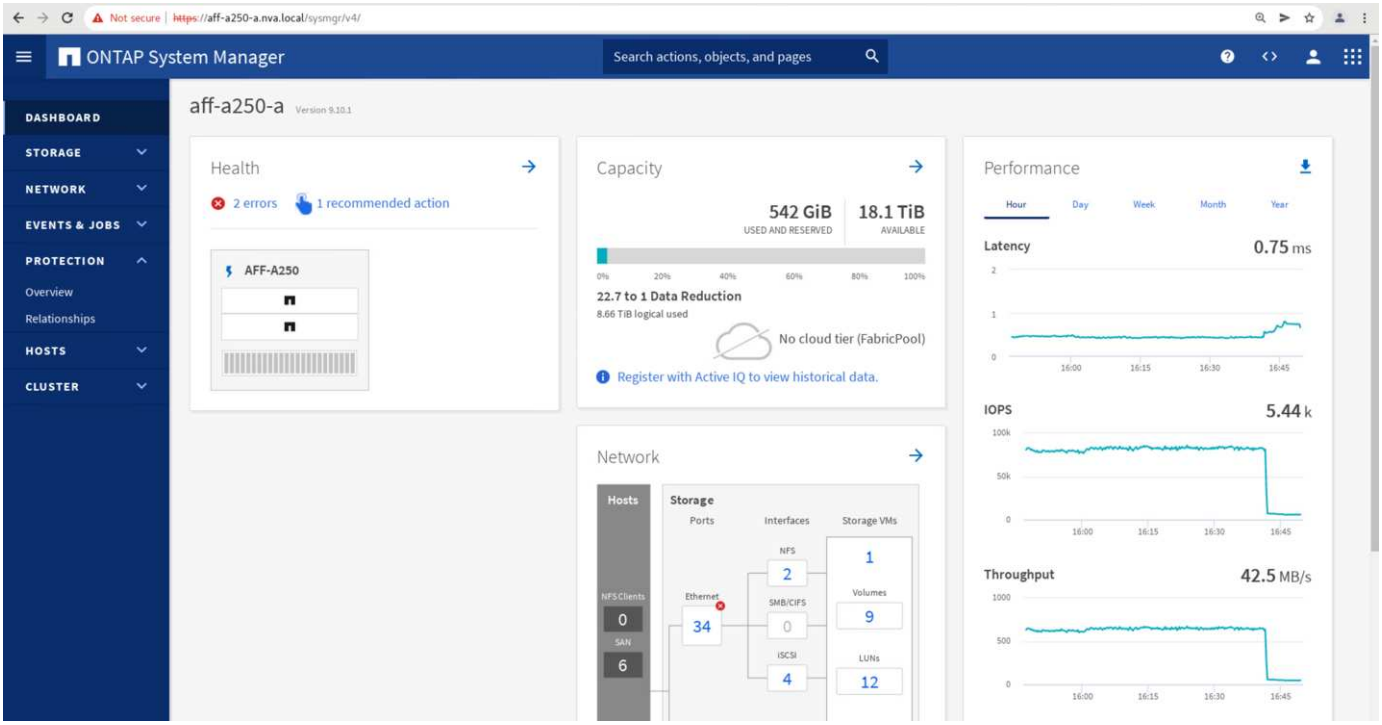
1. Accédez à l'écran protection > relations pour confirmer que l'état de la relation de groupe de cohérence est `In Sync`. S'il se trouve toujours dans le `Synchronizing` attendez que l'état devienne `In Sync` avant d'effectuer un basculement.
2. Développez les points en regard du nom de la source et cliquez sur basculement.



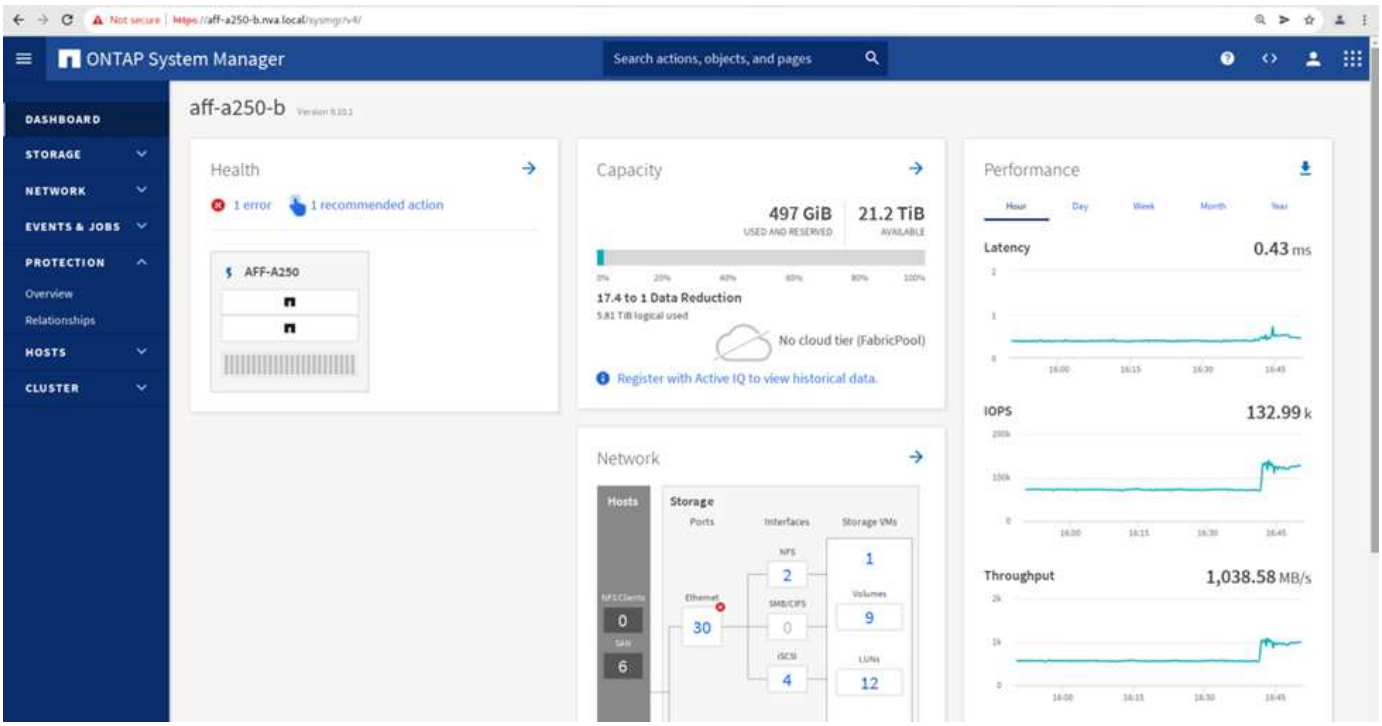
3. Confirmer le basculement pour que l'action démarre.



Peu de temps après le lancement du basculement des deux groupes de cohérence, `cg_esxi_a` et `cg_infra_datastore_a`, Sur l'interface graphique System Manager du site B, les E/S du site A servant à traiter les deux groupes de cohérence déplacés vers le site B. Ainsi, les E/S sur le site A sont considérablement réduites comme indiqué sur le site A volet performances de System Manager.

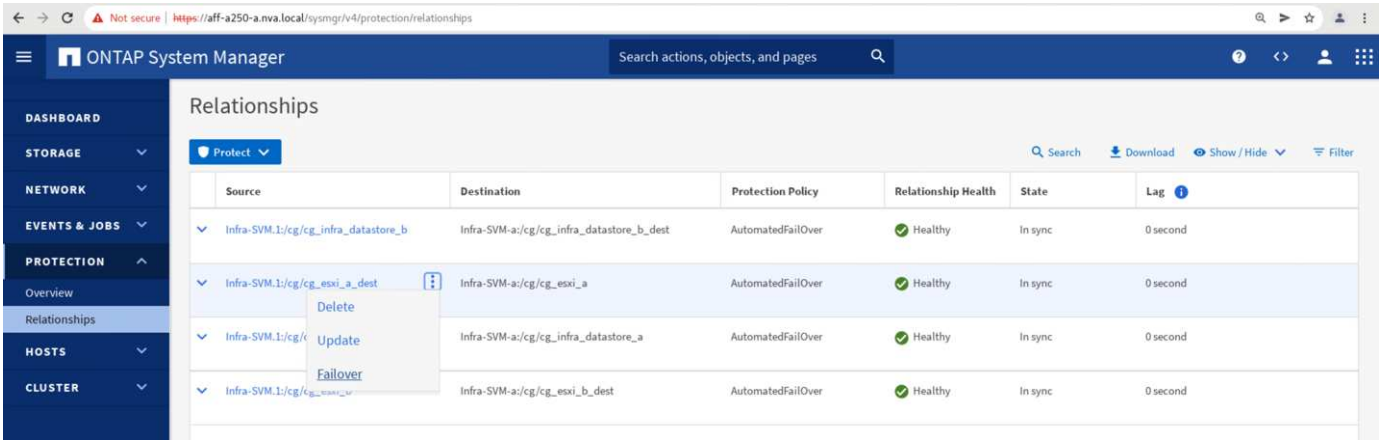


Par contre, le volet performances du tableau de bord du site B System Manager affiche une augmentation significative des IOPS, en raison de la transmission des E/S supplémentaires transférées du site A à environ 130 000 IOPS, De plus, nous avons atteint un débit d'environ 1 Gbit/s, tout en maintenant une latence d'E/S inférieure à la milliseconde.



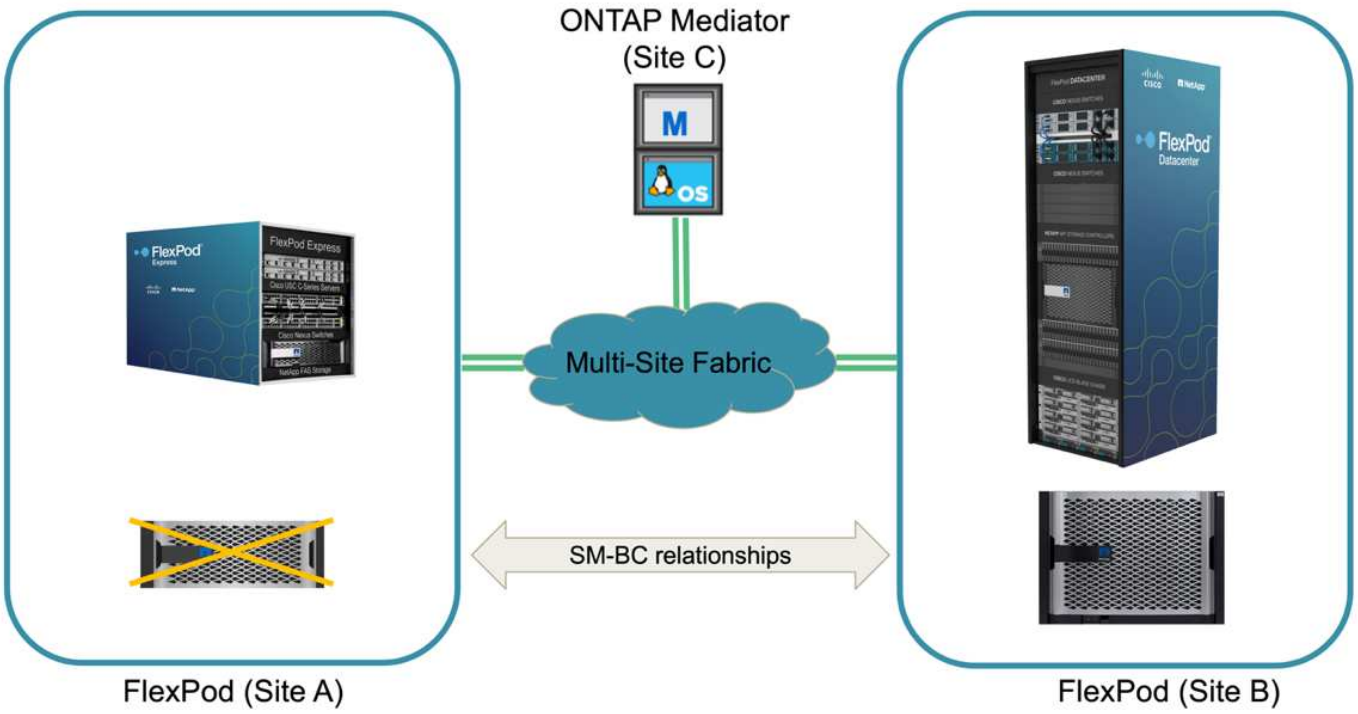
Grâce à la migration transparente des E/S du site A vers le site B, les contrôleurs de stockage du site A peuvent désormais être mis en service afin de planifier la maintenance. Une fois le travail de maintenance ou le test terminé et que le cluster de stockage d'un site est réexécuté et opérationnel, vérifiez et attendez que l'état de protection du groupe de cohérence soit revenir à `In sync` Avant d'effectuer un basculement pour renvoyer les E/S de basculement du site B vers le site A. Notez que plus un site est arrêté pour les opérations de maintenance ou de test, plus il faut de temps pour synchroniser les données et que le groupe de cohérence

est renvoyé au `In sync` état.



Basculement de stockage non planifié

Un basculement de stockage non planifié peut se produire en cas d'incident réel ou lors d'une simulation d'incident. Par exemple, consultez la figure suivante dans laquelle le système de stockage sur le site A subit une panne de courant, un basculement de stockage non planifié est déclenché et les services de données pour les LUN du site A, protégés par les relations SM-BC, continuent à partir du site B.



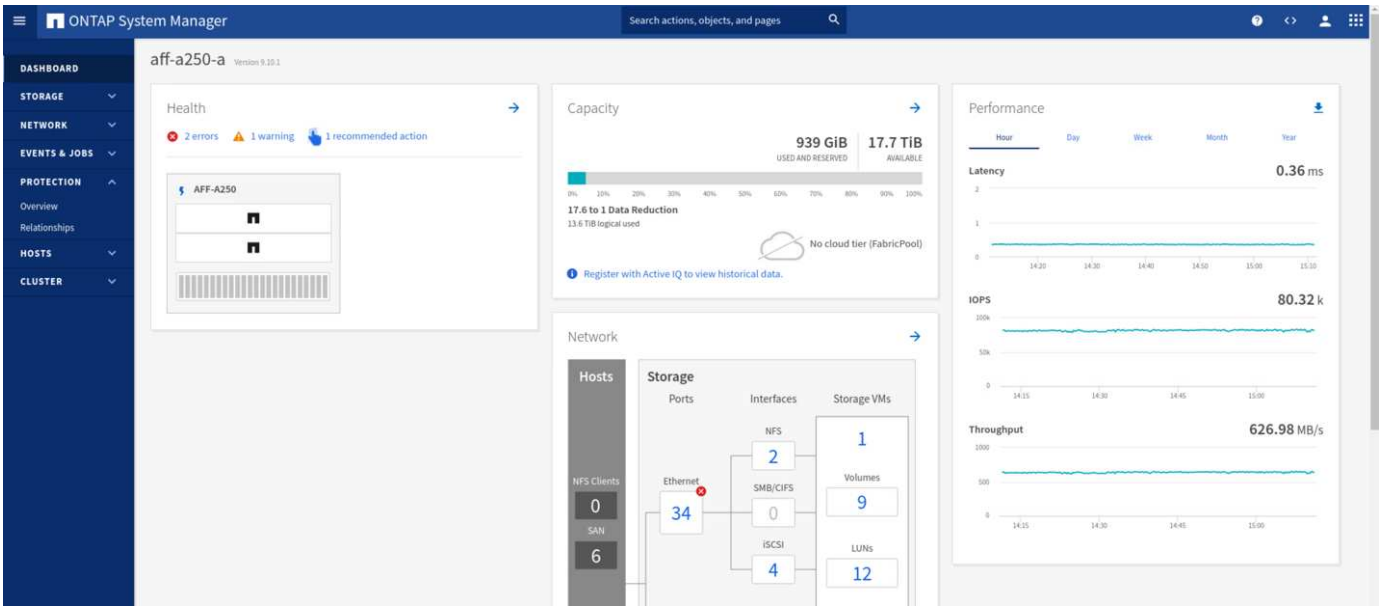
Pour simuler un incident de stockage au niveau du site A, les deux contrôleurs de stockage du site A peuvent être mis hors tension en mettant physiquement l'interrupteur afin de mettre fin à l'alimentation des contrôleurs, ou en utilisant la commande de gestion de l'alimentation système des processeurs de service du contrôleur de stockage pour mettre les contrôleurs hors tension.

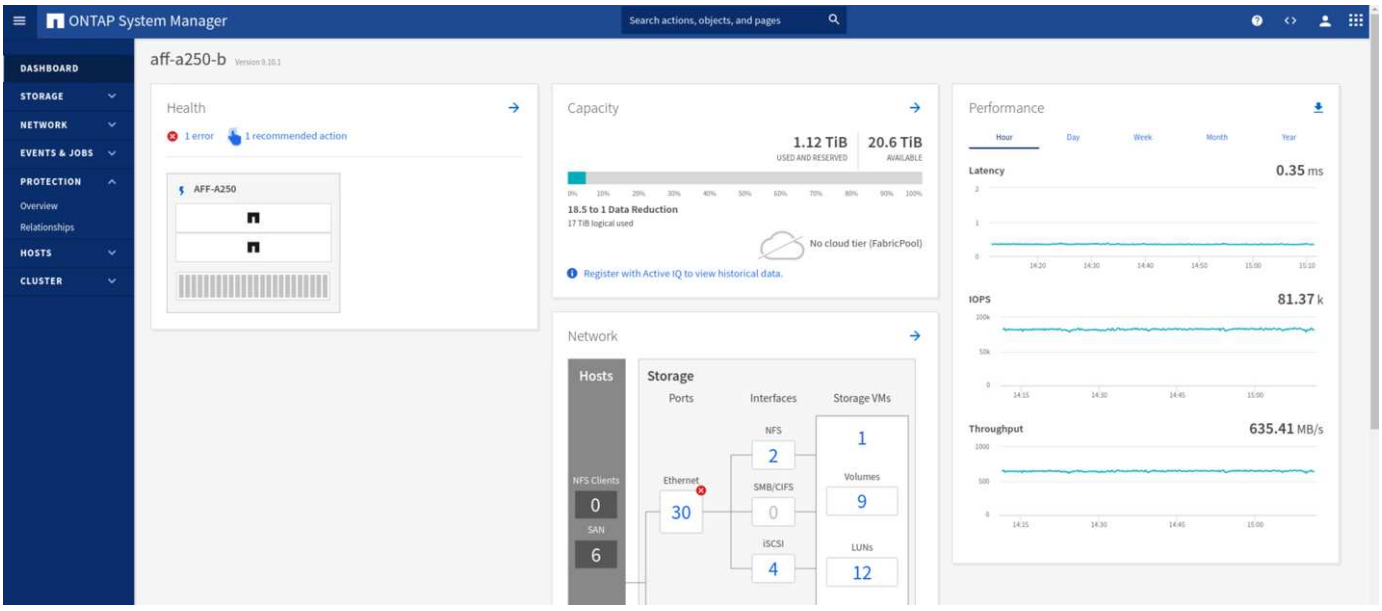
Lorsque le cluster de stockage du site a une perte de puissance, les services de données fournis par le site A du cluster de stockage sont stoppés soudainement. Ensuite, le médiateur ONTAP, qui surveille la solution SM-BC à partir d'un troisième site, détecte une condition de défaillance de stockage du site et permet à la solution SM-BC d'effectuer un basculement non planifié automatisé. Cela permet aux contrôleurs de stockage du site B de continuer les services de données pour les LUN configurés dans les relations du groupe de cohérence SM-

BC avec le site A.

Du point de vue des applications, les services de données font une pause brève fois que le système d'exploitation vérifie l'état du chemin des LUN, puis reprend les E/S sur les chemins disponibles vers les contrôleurs de stockage du site B survivants.

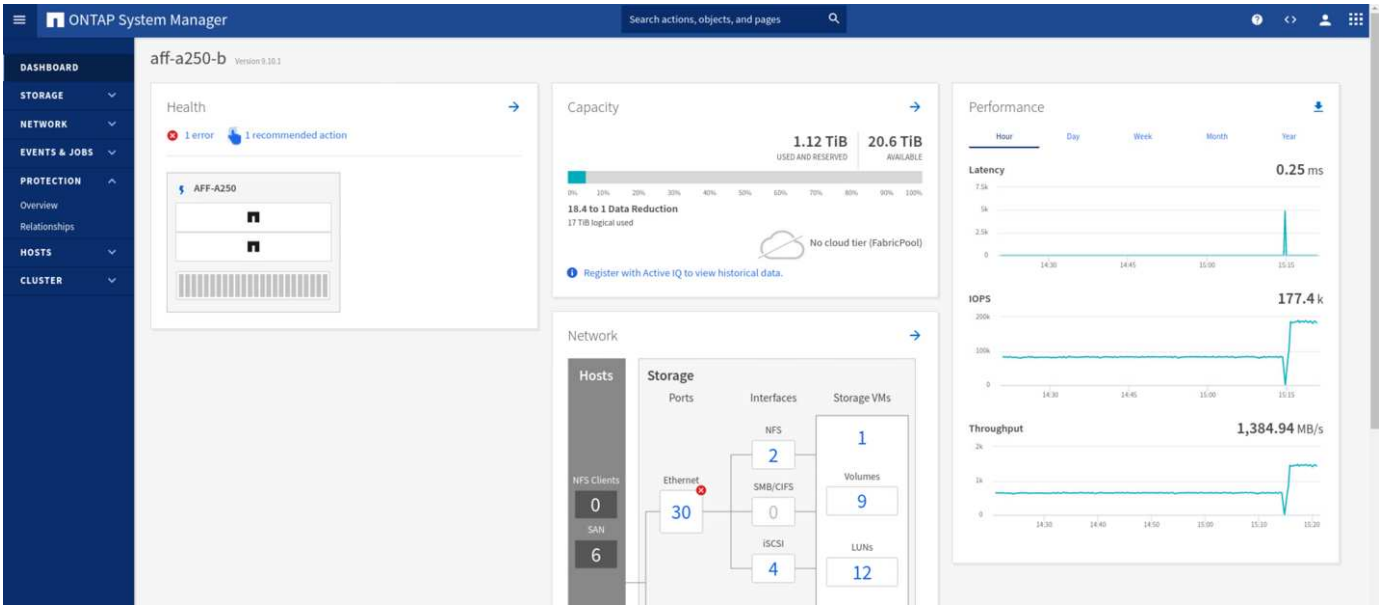
Lors des tests de validation, l'outil IOMeter installé sur les machines virtuelles des deux sites génère des E/S dans leurs datastores locaux. Après la mise hors tension du site D'Un cluster, les E/S sont suspendues brièvement et ont repris ensuite. Reportez-vous aux deux figures suivantes pour les tableaux de bord du cluster de stockage sur le site A et le site B, respectivement avant le sinistre qui montrent environ 80 000 IOPS et un débit de 600 Mo/s sur chaque site.



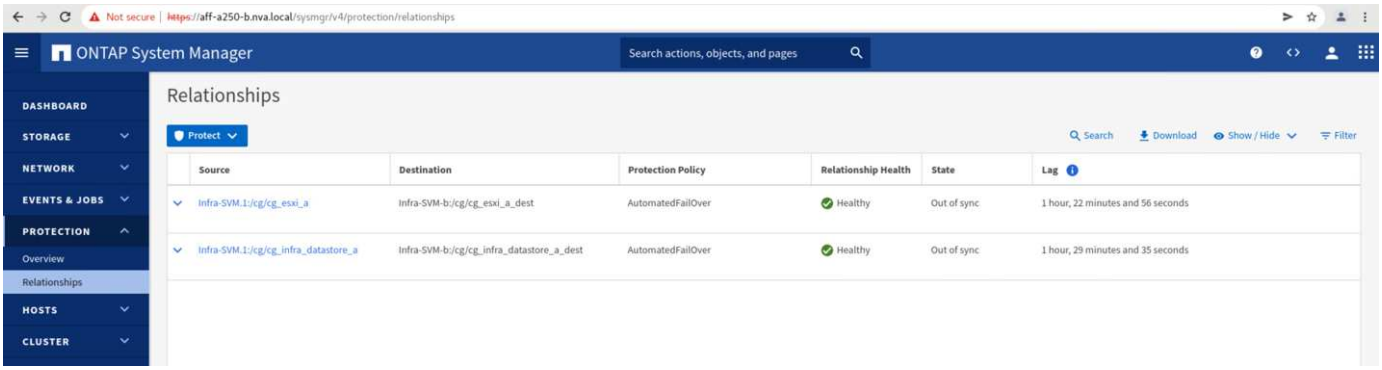


Après la mise hors tension des contrôleurs de stockage sur le site A, nous pouvons vérifier que les E/S du contrôleur de stockage du site B ont nettement augmenté pour fournir des services de données supplémentaires pour le compte du site A (voir la figure suivante). En outre, l'interface graphique des machines virtuelles IOMeter a également démontré la continuité des E/S malgré la panne du cluster de stockage sur le site. Notez que si d'autres datastores sont sauvegardés par des LUN non protégées par des relations SM-BC, ces datastores ne seront plus accessibles en cas d'incident de stockage. Par conséquent, il

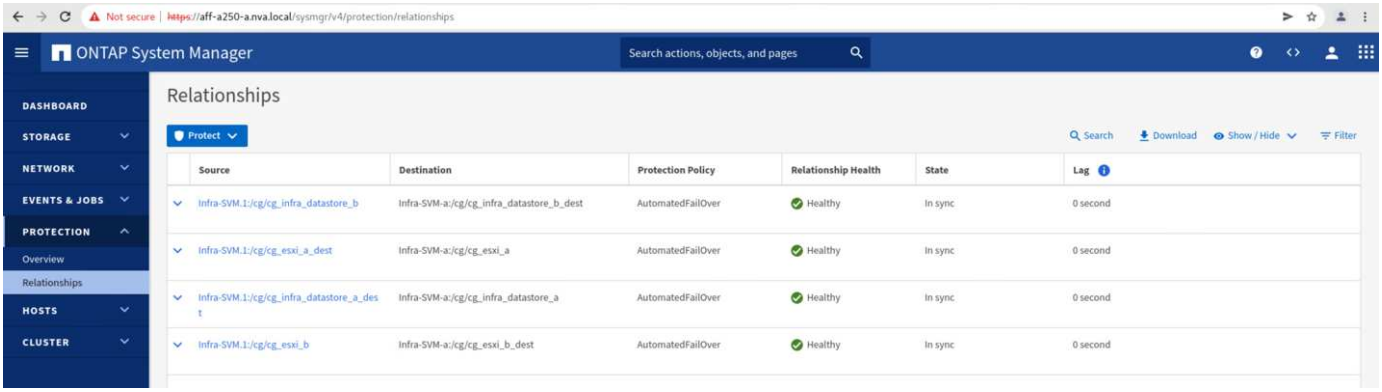
est important d'évaluer les besoins métier des diverses données d'application et de les placer correctement dans des datastores protégés par des relations SM-BC pour assurer la continuité de l'activité.



Le site D'Un cluster ne fonctionne pas, mais les relations des groupes cohérents s'affichent `Out of sync` état comme indiqué dans la figure suivante. Une fois que le système est de nouveau sous tension pour les contrôleurs de stockage du site A, le cluster de stockage démarre et la synchronisation des données entre le site A et le site B se produit automatiquement.



Avant de renvoyer les services de données du site B vers le site A, vous devez consulter le site A System Manager et vérifier que les relations SM-BC sont bien établies et que leur état est de nouveau synchronisé. Après avoir confirmé que les groupes de cohérence sont en cours de synchronisation, une opération de basculement manuel peut être lancée pour renvoyer les services de données dans les relations de groupe de cohérence vers le site A.



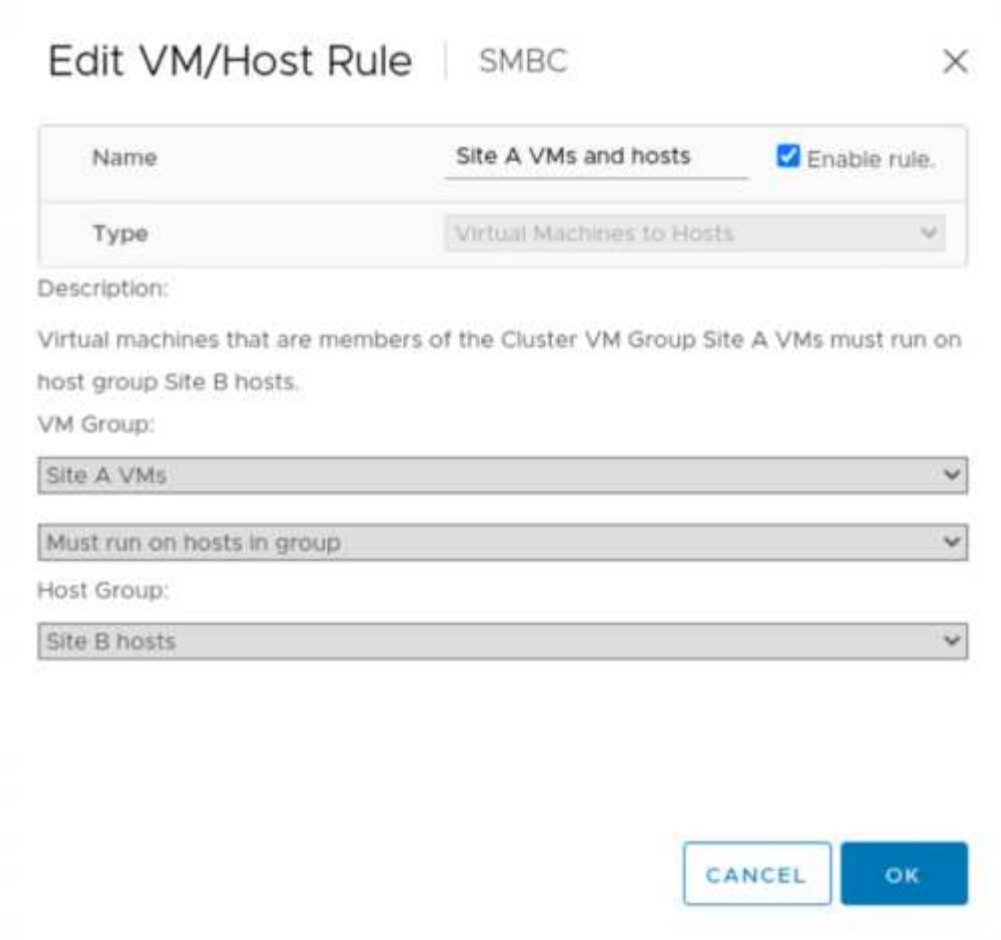
Effectuez les opérations de maintenance du site ou les pannes du site

Un site peut avoir besoin d'une maintenance de site, subir des pannes d'électricité ou être touché par une catastrophe naturelle comme un ouragan ou un tremblement de terre. Par conséquent, il est essentiel que vous pratiiez des scénarios d'échec de site planifiés et non planifiés pour vous assurer que votre solution FlexPod SM-BC est correctement configurée pour résister à de telles défaillances pour l'ensemble de vos applications et services de données stratégiques. Les scénarios suivants relatifs au site ont été validés.

- Scénario de maintenance de site planifié par la migration des machines virtuelles et des services de données critiques vers l'autre site
- Scénario de panne imprévue à l'échelle du site en mettant hors tension les serveurs et les contrôleurs de stockage à des fins de simulation d'incident

Pour préparer un site pour la maintenance planifiée des sites, une combinaison de migration des machines virtuelles concernées hors du site avec vMotion et d'un basculement manuel des relations de groupes de cohérence SM-BC est nécessaire pour migrer les machines virtuelles et les services de données critiques vers l'autre site. Les tests ont été réalisés en deux commandes différentes : VMotion a d'abord été suivi par les basculements SM-BC et SM-BC, puis vMotion, afin de confirmer que les machines virtuelles continuent à fonctionner et que les services de données ne sont pas interrompus.

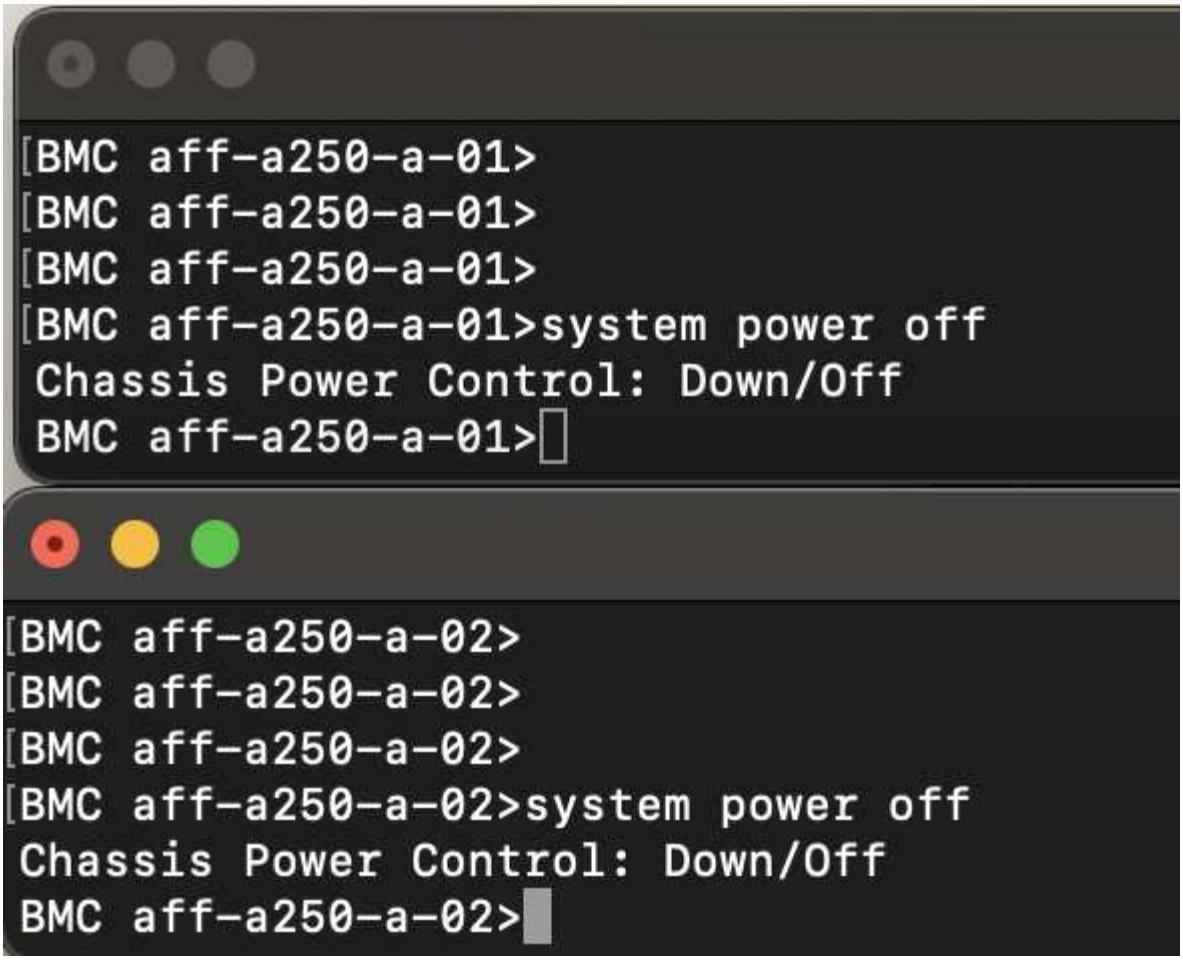
Avant d'effectuer la migration planifiée, mettez à jour la règle d'affinité VM/hôte afin que les machines virtuelles actuellement exécutées sur le site soient automatiquement migrées hors du site en cours de maintenance. La capture d'écran suivante montre un exemple de modification de la règle d'affinité VM/hôte du site A pour que les machines virtuelles migrent automatiquement du site A vers le site B. Au lieu de spécifier que les VM doivent maintenant s'exécuter sur le site B, il est également possible de désactiver temporairement la règle d'affinité pour que les VM puissent être migrées manuellement.



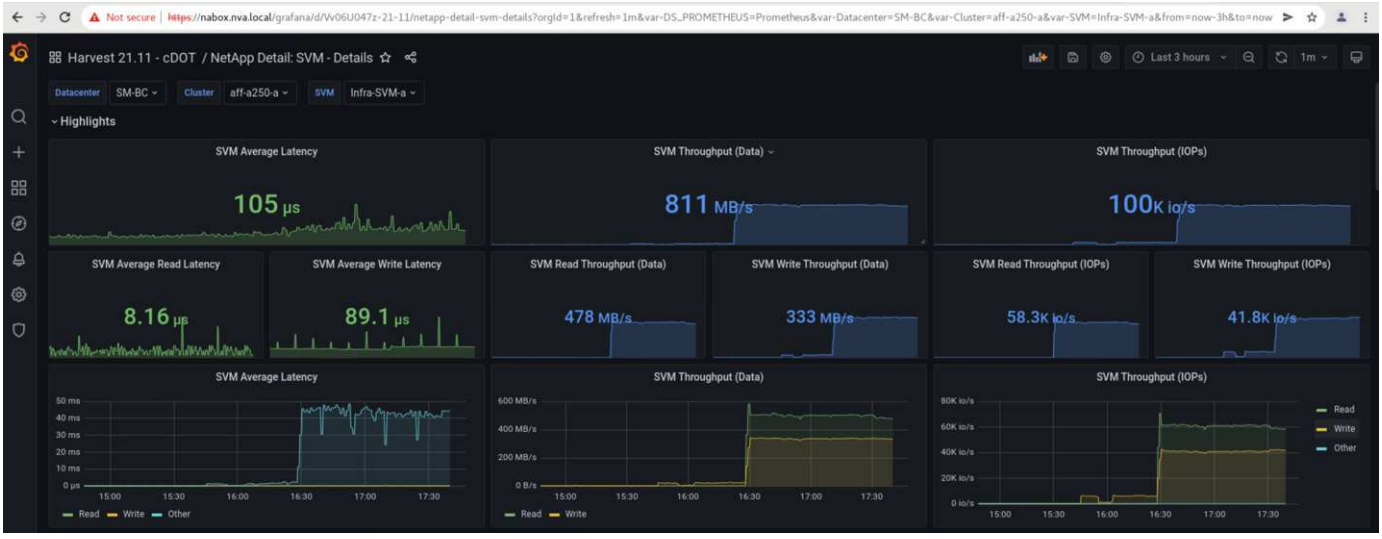
Une fois les ordinateurs virtuels et les services de stockage migrés, vous pouvez mettre hors tension les serveurs, les contrôleurs de stockage, les tiroirs disques et les commutateurs, et réaliser les activités de maintenance du site nécessaires. Une fois la maintenance du site terminée et l'instance FlexPod renvoyée, vous pouvez modifier l'affinité des groupes d'hôtes pour que les VM reprennent leur site d'origine. Ensuite, vous devez modifier la règle d'affinité VM/site hôte "doit être exécuté sur des hôtes dans un groupe" en "devrait s'exécuter sur des hôtes dans un groupe" afin que les machines virtuelles soient autorisées à fonctionner sur des hôtes de l'autre site en cas d'incident. Pour les tests de validation, toutes les machines virtuelles ont été migrées avec succès vers l'autre site et les services de données se sont poursuivis sans problèmes après avoir effectué un basculement pour les relations SM-BC.

Pour la simulation d'incident imprévue à l'échelle du site, les serveurs et les contrôleurs de stockage ont été mis hors tension afin de simuler un incident de site. La fonction VMware HA détecte les machines virtuelles qui sont arrêté et redémarre ces machines virtuelles sur le site survivant. En outre, le médiateur ONTAP fonctionnant sur un troisième site détecte la panne du site et le site survivant lance un basculement et commence à fournir des services de données pour le site en panne comme prévu.

La capture d'écran suivante montre que l'interface de ligne de commande du processeur de service des contrôleurs de stockage a été utilisée pour mettre hors tension le site D'Un cluster brusquement afin de simuler un incident de stockage sur le site.



Les tableaux de bord des machines virtuelles de stockage des clusters, tels que capturés par l'outil NetApp Harvest Data et affichés dans le tableau de bord Grafana dans l'outil de surveillance NAbox, sont présentés dans les deux captures d'écran suivantes. Comme l'indique les graphiques à droite des IOPS et des débits, le cluster du site B récupère les charges de travail de stockage du cluster immédiatement après la panne du site A.

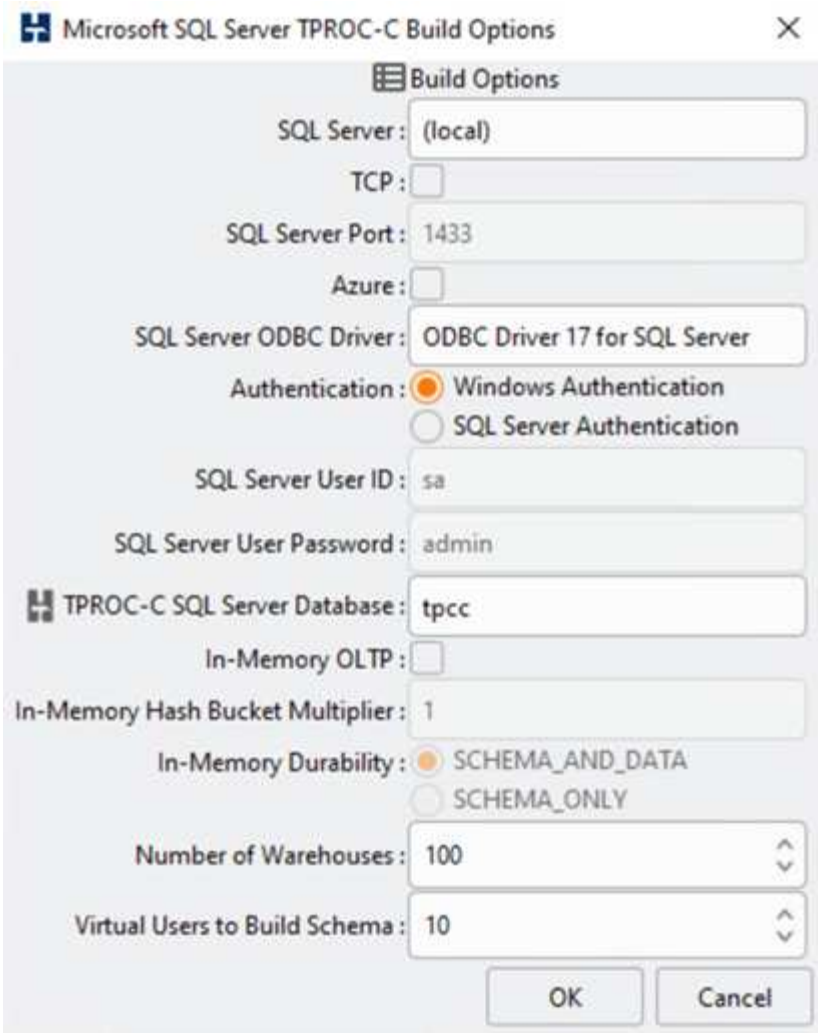


Microsoft SQL Server

Microsoft SQL Server est une plateforme de base de données adoptée et déployée pour LE DÉPARTEMENT INFORMATIQUE de l'entreprise. La version Microsoft SQL Server 2019 apporte beaucoup de nouvelles fonctionnalités et améliorations à ses moteurs relationnels et analytiques. Ce logiciel prend en charge les workloads avec des applications exécutées sur site, dans le cloud et dans un environnement hybride. En outre, il peut être déployé sur plusieurs plateformes, notamment Windows, Linux et les conteneurs.

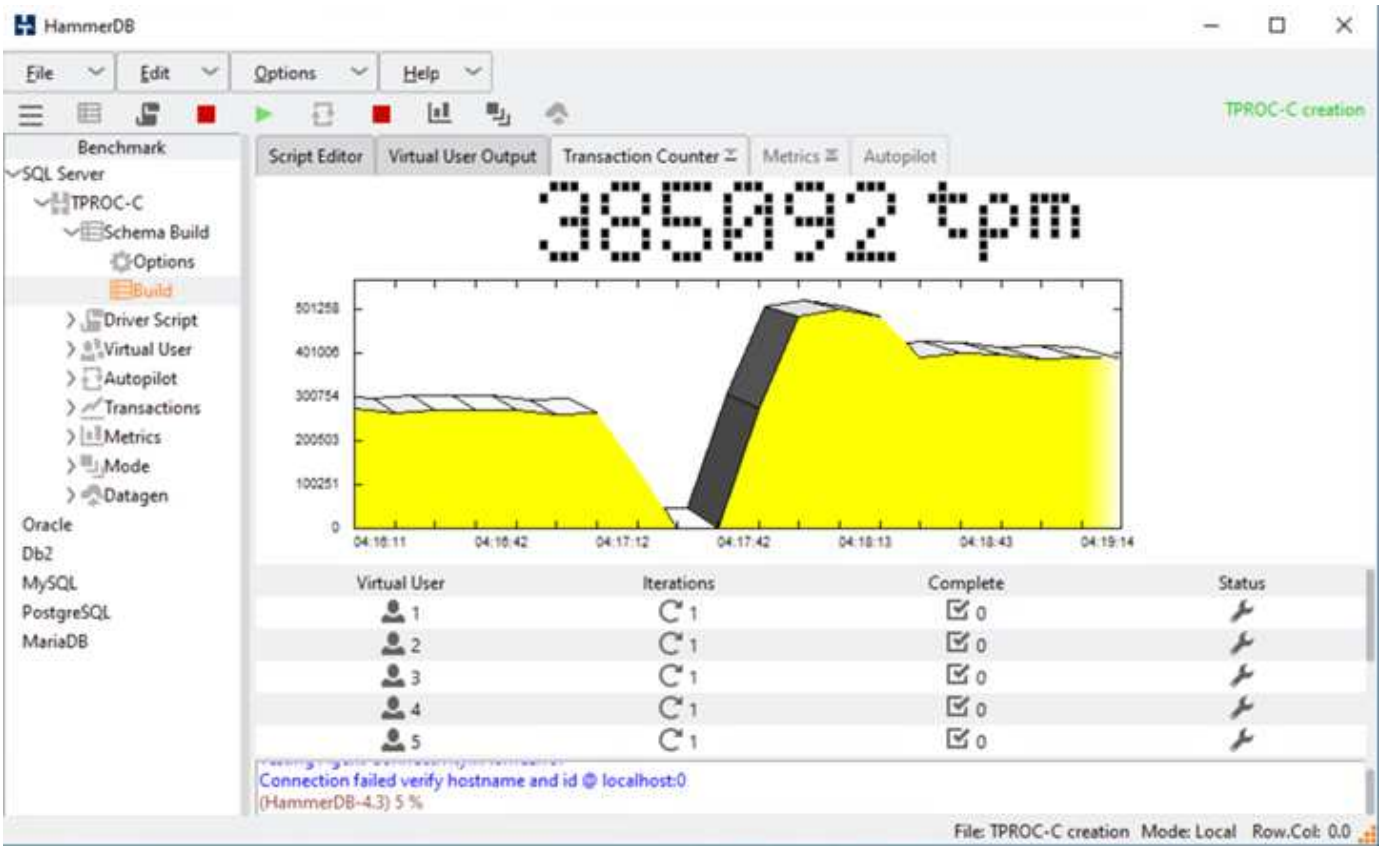
Dans le cadre de la validation des charges de travail stratégiques pour la solution FlexPod SM-BC, Microsoft SQL Server 2019 installé sur une machine virtuelle Windows Server 2022 est inclus avec les machines virtuelles IOMeter pour les tests de basculement du stockage planifiés et non planifiés de SM-BC. Sur la machine virtuelle Windows Server 2022, SQL Server Management Studio est installé pour gérer le serveur SQL. Pour les tests, l'outil base de données HammerDB est utilisé pour générer des transactions de base de données.

L'outil de test de la base de données HammerDB a été configuré pour les tests avec la charge de travail TPROC-C de Microsoft SQL Server. Pour les configurations de construction de schéma, les options ont été mises à jour pour utiliser 100 entrepôts avec 10 utilisateurs virtuels comme indiqué dans la capture d'écran suivante.



Une fois les options de création de schéma mises à jour, le processus de création de schéma a démarré. Quelques minutes plus tard, une erreur simulée de cluster de stockage du site B a été introduite en mettant hors tension les deux nœuds du cluster de stockage AFF A250 à environ la même heure à l'aide des commandes CLI du processeur système.

Après une courte pause des transactions de base de données, le basculement automatique pour la correction des sinistres a débuté et les transactions ont repris. La capture d'écran ci-dessous montre la capture d'écran du compteur de transactions HammerDB. Étant donné que la base de données de Microsoft SQL Server réside généralement dans le cluster de stockage du site B, la transaction a été interrompue brièvement lorsque le stockage sur le site B s'est arrêté, puis reprise après le basculement automatisé.



Les metrics du cluster de stockage ont été capturées à l'aide de l'outil NAbox et de l'outil de surveillance de récolte NetApp installé. Les résultats sont affichés dans les tableaux de bord prédéfinis de Grafana pour la machine virtuelle de stockage et autres objets de stockage. Le tableau de bord fournit des schémas de latence, de débit et d'IOPS, ainsi que des détails supplémentaires avec des statistiques de lecture et d'écriture séparées pour le site B et le site A.

Cette capture d'écran présente le tableau de bord des performances NAbox Grafana pour cluster de stockage site B.

Le cluster de stockage du site B était d'environ 100 000 IOPS avant l'introduction de l'incident. Ensuite, les mesures de performances ont montré une baisse nette de zéro à droite des graphiques dus à l'incident. Comme le cluster de stockage du site B était en panne, aucun élément ne pouvait être collecté à partir du

cluster du site B après l'introduction du sinistre.

À l'inverse, les IOPS du cluster de stockage du site A ont récupéré les charges de travail supplémentaires depuis le site B après le basculement automatisé. La charge de travail supplémentaire est facilement affichée à droite des graphiques IOPS et débit dans la capture d'écran suivante, qui montre le tableau de bord des performances de NAbox Grafana pour site De cluster de stockage.

Le scénario de test d'incident de stockage ci-dessus a confirmé que la charge de travail de Microsoft SQL Server peut survivre à une panne complète du cluster de stockage sur le site B où réside la base de données. Une fois l'incident détecté et le basculement effectué, l'application a utilisé de manière transparente les services de données du site De cluster De stockage.

Au niveau de la couche de calcul, lorsque les machines virtuelles qui s'exécutent sur un site particulier souffrent d'une défaillance d'hôte, les machines virtuelles sont conçues pour être redémarrée automatiquement par la fonctionnalité de haute disponibilité VMware. En cas de panne de calcul de l'ensemble du site, les règles d'affinité VM/hôte permettent de redémarrer les machines virtuelles sur le site survivant. Cependant, pour qu'une application stratégique puisse fournir des services sans interruption, une solution de mise en cluster basée sur des applications telles que Microsoft Failover Cluster ou l'architecture applicative basée sur des conteneurs Kubernetes doit éviter les temps d'indisponibilité des applications. Veuillez vous reporter au document relatif à l'implémentation de la mise en cluster basée sur l'application, qui va au-delà du périmètre de ce rapport technique.

"Suivant: Conclusion."

Conclusion

"Précédent : validation des solutions - scénarios validés"

Le FlexPod Datacenter avec SM-BC utilise une conception de data Center actif-actif afin d'assurer la continuité de l'activité et la reprise après incident pour les workloads stratégiques. La solution interconnecte généralement deux data centers déployés dans des sites séparés géographiquement dispersés dans une zone métropolitaine. La solution NetApp SM-BC utilise une réplication synchrone pour protéger les services de données stratégiques contre une panne sur site. La solution requiert que les deux sites de déploiement FlexPod offrent une latence réseau aller-retour inférieure à 10 millisecondes.

Le médiateur NetApp ONTAP déployé sur un site tiers surveille la solution SM-BC et permet un basculement automatisé en cas d'incident sur site. VMware vCenter avec VMware HA et étendu la configuration du cluster de stockage Metro VMware vSphere fonctionne en toute transparence avec NetApp SM-BC, afin de permettre à la solution de respecter le RPO nul et les objectifs de durée de restauration proches de zéro.

La solution FlexPod SM-BC peut également être déployée sur les infrastructures FlexPod existantes s'ils répondent aux exigences ou en ajoutant une solution FlexPod supplémentaire à un FlexPod existant pour atteindre les objectifs de continuité de l'activité. Des outils supplémentaires de gestion, de contrôle et d'automatisation tels que Cisco InterSight, Ansible et HashiCorp Terraform Automation sont disponibles auprès de NetApp et Cisco. Vous pouvez facilement surveiller la solution, obtenir des informations sur ses opérations et automatiser son déploiement et ses opérations.

Du point de vue d'une application stratégique telle que Microsoft SQL Server, une base de données résidant sur un datastore VMware protégé par une relation de groupe de cohérence ONTAP SM-BC reste disponible malgré une panne du stockage sur site. Comme vérifié lors du test de validation, après une panne de courant du cluster de stockage où réside la base de données, un basculement de la relation SM-BC CG CG CG se produit et les transactions Microsoft SQL Server reprennent sans interruption des applications.

Grâce à la protection granulaire des données des applications, vous pouvez créer des relations ONTAP SM-BC CG pour vos applications stratégiques afin de répondre aux exigences RPO zéro et RTO quasi nul. Afin que le cluster VMware sur lequel l'application Microsoft SQL Server s'exécute puisse survivre à une panne de stockage de site, les LUN de démarrage des hôtes ESXi de chaque site sont également protégées par une relation SM-BC CG CG CG CG.

La flexibilité et l'évolutivité de FlexPod vous permettent de démarrer avec une infrastructure correctement dimensionnée qui peut évoluer et évoluer en fonction des exigences de votre entreprise. Cette conception validée vous permet de déployer de manière fiable un cloud privé VMware vSphere sur une infrastructure intégrée et distribuée. Vous bénéficiez ainsi d'une solution résiliente à de nombreux scénarios de défaillance unique, ainsi qu'une défaillance d'un site, pour protéger les services de données stratégiques.

"Suivant : où trouver des informations supplémentaires et l'historique des versions ?"

Où trouver des informations supplémentaires et l'historique des versions

"Précédent: Conclusion."

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

FlexPod

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Serveurs Cisco - Unified Computing System (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- Documentation produit NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- FlexPod Datacenter avec Cisco UCS 4.2(1) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9 : Guide de conception

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- Guide de déploiement de FlexPod Datacenter avec Cisco UCS 4.2(1) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- Guide de design de FlexPod Datacenter avec Cisco UCS X-Series, VMware 7.0 U2 et NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- Guide de déploiement de FlexPod Datacenter avec Cisco UCS X-Series, VMware 7.0 U2 et NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- Guide de design de FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et baies NetApp AFF/FAS NVA

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- Guide de déploiement de FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et NVA AFF/FAS de NetApp

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP avec structure front-end multisite VXLAN

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- Boîte NAbox

  "https://nabox.org"

- Récolte NetApp

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- Tr-4878 : continuité de l'activité SnapMirror (SM-BC) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Comment supprimer correctement une relation SnapMirror ONTAP 9

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Principes de base de la reprise après incident synchrone de SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Principes de base de la reprise sur incident asynchrone SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Protection des données et reprise d'activité

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Installez ou mettez à niveau le service ONTAP Mediator

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere HA et vSphere Metro Storage Cluster

- Création et utilisation de clusters HA vSphere

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- Cluster de stockage Metro VMware vSphere (vMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Bonnes pratiques pour VMware vSphere Metro Storage Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP avec NetApp SnapMirror Business Continuity (SM-BC) avec VMware vSphere Metro Storage Cluster (vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Protégez les bases de données et les applications de niveau 1 avec VMware vSphere Metro Storage Cluster et ONTAP

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL et HammerDB

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Guide des meilleures pratiques de conception de Microsoft SQL Server sur VMware vSphere

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- Site Web HammerDB

  "https://www.hammerdb.com"

Matrice de compatibilité

- Matrice de compatibilité matérielle Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Matrice d'interopérabilité NetApp

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe

  "https://hwu.netapp.com"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Avril 2022	Version initiale.

Conception du data Center FlexPod avec VMware vSphere 7.0, Cisco VXLAN Single-site Fabric et NetApp ONTAP 9.7

Ramesh Isaac, Cisco Abhinav Singh, NetApp

Les conceptions validées par Cisco (CVD) se composent de systèmes et de solutions conçus, testés et documentés pour faciliter et améliorer les déploiements client. Ces conceptions intègrent une large gamme de technologies et de produits dans une gamme de solutions qui ont été développées pour répondre aux besoins commerciaux des clients. Cisco et NetApp se sont associés pour créer FlexPod, qui sert de base à une variété de workloads, et pour élaborer des architectures robustes, efficaces et évolutives afin de répondre aux besoins des clients. La solution FlexPod est une approche validée

pour le déploiement des technologies et produits Cisco et NetApp afin de créer une infrastructure partagée de cloud privé et public.

"Conception du data Center FlexPod avec VMware vSphere 7.0, Cisco VXLAN Single-site Fabric et NetApp ONTAP 9.7"

FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7 : déploiement

John George, Cisco Sree Lakshmi Lanka, NetApp

Ce document présente le data Center FlexPod de Cisco et NetApp avec NetApp ONTAP 9.7 sur le système de stockage 100 % Flash NetApp AFF A400, le logiciel unifié Cisco UCS Manager version 4.1(2) avec processeurs évolutifs Intel Xeon de deuxième génération et VMware vSphere 7.0. Cisco UCS Manager (UCSM) 4.1(2) assure la prise en charge consolidée des éléments suivants :

- Tous les modèles Cisco UCS Fabric Interconnect : 6200, 6300, 6324 (Cisco UCS Mini)
- 6400
- Série 2200/2300/2400 IOM
- Cisco UCS B-Series
- Cisco UCS C-Series

Elle comprend également les plateformes de gestion SaaS Cisco Intersight et NetApp Active IQ.

Le data Center FlexPod avec NetApp ONTAP 9.7, le logiciel unifié Cisco UCS 4.1(2) et VMware vSphere 7.0 comprend une architecture de data Center préconçue et conforme aux bonnes pratiques, basée sur le système Cisco Unified Computing System (Cisco UCS), la famille de commutateurs Cisco Nexus 9000, les commutateurs de structure multicouche MDS 9000, Et les baies de stockage NetApp AFF A-Series exécutant le logiciel de gestion des données ONTAP 9.7.

"FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7 : déploiement"

FlexPod Datacenter avec Cisco Intersight et NetApp ONTAP 9.7 - conception

John George, Cisco Scott Kovacs, NetApp

Ce document présente la solution FlexPod de Cisco et NetApp, une approche validée pour le déploiement des technologies Cisco et NetApp en tant qu'infrastructure cloud partagée. Cette conception validée fournit une structure pour le déploiement de VMware vSphere, la plateforme de virtualisation la plus populaire dans les data centers d'entreprise, sur FlexPod.

"FlexPod Datacenter avec Cisco Intersight et NetApp ONTAP 9.7 - conception"

FlexPod Datacenter avec Cisco Intersight et NetApp ONTAP 9.7 : déploiement

John George, Cisco Scott Kovacs, NetApp

La tendance actuelle du secteur dans le domaine de la conception de data centers concerne les infrastructures partagées. Grâce à la virtualisation et aux plateformes INFORMATIQUES prévalidées, les entreprises se sont lancées dans la transition vers le cloud en s'éloignant des silos d'applications et en se muant vers une infrastructure partagée qui peut être déployée rapidement, améliorant ainsi l'agilité et réduisant les coûts. Cisco et NetApp se sont associés pour proposer FlexPod, qui utilise les meilleurs composants de stockage, de serveur et de réseau pour servir de base à un large éventail de charges de travail. Les designs d'architecture efficaces peuvent être déployés rapidement et en toute confiance.

"FlexPod Datacenter avec Cisco Intersight et NetApp ONTAP 9.7 : déploiement"

FlexPod Datacenter avec Cisco Intersight et NetApp ONTAP 9.7 - conception

John George, Cisco Scott Kovacs, NetApp

Ce document présente une solution validée pour le déploiement des technologies Cisco et NetApp en tant qu'infrastructure cloud partagée. Cette conception validée fournit une structure pour le déploiement de VMware vSphere, la plateforme de virtualisation la plus populaire dans les data centers d'entreprise, sur FlexPod.

L'infrastructure intégrée de pointe FlexPod prend en charge un large éventail de charges de travail et d'utilisations. Cette solution permet aux clients de déployer rapidement et de manière fiable un cloud privé basé sur VMware vSphere sur une infrastructure intégrée.

"FlexPod Datacenter avec Cisco Intersight et NetApp ONTAP 9.7 - conception"

FlexPod Datacenter avec VMware vSphere 6.7 U2, Cisco UCS pour la structure de dernière génération et NetApp ONTAP 9.6

John George, Cisco Sree Lakshmi Lanka, NetApp

Ce document présente le centre de données Cisco et NetApp FlexPod avec NetApp ONTAP 9.6, le logiciel unifié Cisco UCS Manager version 4.0(4) avec processeurs évolutifs Intel Xeon deuxième génération et VMware vSphere 6.7 U2. Cisco UCS Manager (UCSM) 4.0(4) assure la prise en charge consolidée des éléments suivants :

- Tous les modèles Cisco UCS Fabric Interconnect : 6200, 6300, 6324 (Cisco UCS Mini)
- 6454

- Série 2200/2300/2400 IOM
- Cisco UCS B-Series
- Serveurs Cisco UCS C-Series

Le data Center FlexPod avec NetApp ONTAP 9.6, le logiciel unifié Cisco UCS 4.0(4) et VMware vSphere 6.7 U2 est une architecture de data Center préconçue et conforme aux bonnes pratiques, basée sur le système Cisco Unified Computing System (Cisco UCS), la famille de commutateurs Cisco Nexus 9000, les commutateurs de fabric multicouche MDS 9000, Et les baies de stockage NetApp AFF A-Series exécutant ONTAP 9.

"FlexPod Datacenter avec VMware vSphere 6.7 U2, Cisco UCS quatrième génération Fabric et NetApp ONTAP 9.6"

Centre de données FlexPod avec VMware vSphere 6.7 U1, structure de quatrième génération Cisco UCS et système AFF a-Series NetApp - Design

John George, Cisco Sree Lakshmi Lanka, NetApp

Ce document présente la solution FlexPod de Cisco et NetApp, une approche validée pour le déploiement des technologies Cisco et NetApp en tant qu'infrastructure cloud partagée. Cette conception validée fournit une structure pour le déploiement de VMware vSphere, la plateforme de virtualisation la plus populaire dans les data centers d'entreprise, sur FlexPod.

L'infrastructure intégrée de pointe FlexPod prend en charge un large éventail de charges de travail et d'utilisations. Cette solution permet aux clients de déployer rapidement et de manière fiable un cloud privé basé sur VMware vSphere sur une infrastructure intégrée.

L'architecture de solution recommandée repose sur Cisco Unified Computing System (Cisco UCS) avec la version logicielle unifiée pour prendre en charge les plateformes matérielles Cisco UCS, notamment les serveurs lames Cisco UCS B-Series et les serveurs rack C-Series, les interconnexions de fabric Cisco UCS 6454, les commutateurs Cisco Nexus 9000 Series, les commutateurs Fibre Channel Cisco MDS, Et les baies de stockage NetApp 100 % Flash. De plus, il inclut VMware vSphere 6.7 Update 1, qui offre un certain nombre de nouvelles fonctionnalités permettant d'optimiser l'utilisation du stockage et de faciliter le déploiement d'un cloud privé.

"Centre de données FlexPod avec VMware vSphere 6.7 U1, structure de quatrième génération Cisco UCS et système AFF a-Series NetApp - Design"

Centre de données FlexPod avec VMware vSphere 6.7 U1, structure de quatrième génération Cisco UCS et système AFF A-Series NetApp

John George, Cisco Scott Kovacs, NetApp

Ce document présente le logiciel unifié Cisco et NetApp FlexPod Datacenter avec Cisco UCS Manager version 4.0(2) et VMware vSphere 6.7 U1. Cisco UCS Manager (UCSM) 4.0(2) assure la prise en charge consolidée de tous les modèles Cisco UCS Fabric

Interconnect (6200, 6300, 6324 (Cisco UCS Mini)), d'un module d'E/S de la gamme 6454,2200/2300, de Cisco UCS B-Series et de Cisco UCS C-Series. FlexPod Datacenter avec Cisco UCS Unified Software version 4.0(2) et VMware vSphere 6.7 U1 est une architecture de data Center préconçue et conforme aux bonnes pratiques, basée sur le système Cisco Unified Computing System (UCS), la famille de commutateurs Cisco Nexus 9000, les commutateurs de structure multicouche MDS 9000, Et les baies de stockage NetApp AFF A-Series exécutant le système d'exploitation du stockage ONTAP 9.

"Centre de données FlexPod avec VMware vSphere 6.7 U1, structure de quatrième génération Cisco UCS et système AFF A-Series NetApp"

Design de FlexPod Datacenter avec Cisco ACI Multi-Pod, NetApp MetroCluster IP et VMware vSphere 6.7

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Ce document décrit l'intégration de la solution FlexPod Cisco ACI Multi-Pod et NetApp MetroCluster IP dans le centre de données FlexPod, afin de fournir une solution de data Center Multi-Data. L'architecture à plusieurs data centers permet d'équilibrer les charges de travail entre deux data centers grâce à la mobilité non disruptive des charges de travail. Ainsi, la migration des services entre les sites n'est pas nécessaire de supporter une panne.

La solution FlexPod avec FlexPod ACI Multi-Pod et NetApp MetroCluster IP offre les avantages suivants :

- Mobilité transparente des workloads entre les data centers
- Politiques cohérentes sur tous les sites
- Extension de couche 2 pour les data centers dispersés géographiquement
- Prévention améliorée des temps d'arrêt pendant la maintenance
- Prévention des incidents et reprise d'activité

"Design de FlexPod Datacenter avec Cisco ACI Multi-Pod, NetApp MetroCluster IP et VMware vSphere 6.7"

Déploiement de FlexPod Datacenter avec Cisco ACI Multi-Pod avec NetApp MetroCluster IP et VMware vSphere 6.7

Haseeb Niazi, Cisco Ramesh Issac, Cisco Arvind Ramakrishnan, NetApp

Cisco et NetApp se sont associés pour proposer une gamme de solutions FlexPod compatibles avec des plateformes de data Center stratégiques. La solution FlexPod propose une architecture intégrée qui intègre les meilleures pratiques de conception en matière de calcul, de stockage et de réseau. Cela permet de réduire les risques INFORMATIQUES en validant l'architecture intégrée afin d'assurer la compatibilité entre les différents composants. La solution répond également aux problématiques IT en fournissant des conseils de conception, des conseils de déploiement et un support

documentés qui peuvent être utilisés à différentes étapes (planification, conception et implémentation) d'un déploiement.

"Déploiement de FlexPod Datacenter avec Cisco ACI Multi-Pod avec NetApp MetroCluster IP et VMware vSphere 6.7"

Cloud hybride

Cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic

Tr-4960 : cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic

En partenariat avec : 

Kamini Singh, NetApp

Pour réussir sa transformation digitale, il suffit d'en faire plus avec la donnée. Les hôpitaux génèrent et requièrent d'importants volumes de données pour gérer leur entreprise et servir leurs patients de manière efficace. Les informations sont collectées et traitées lors du traitement des patients et de la gestion des horaires du personnel et des ressources médicales.

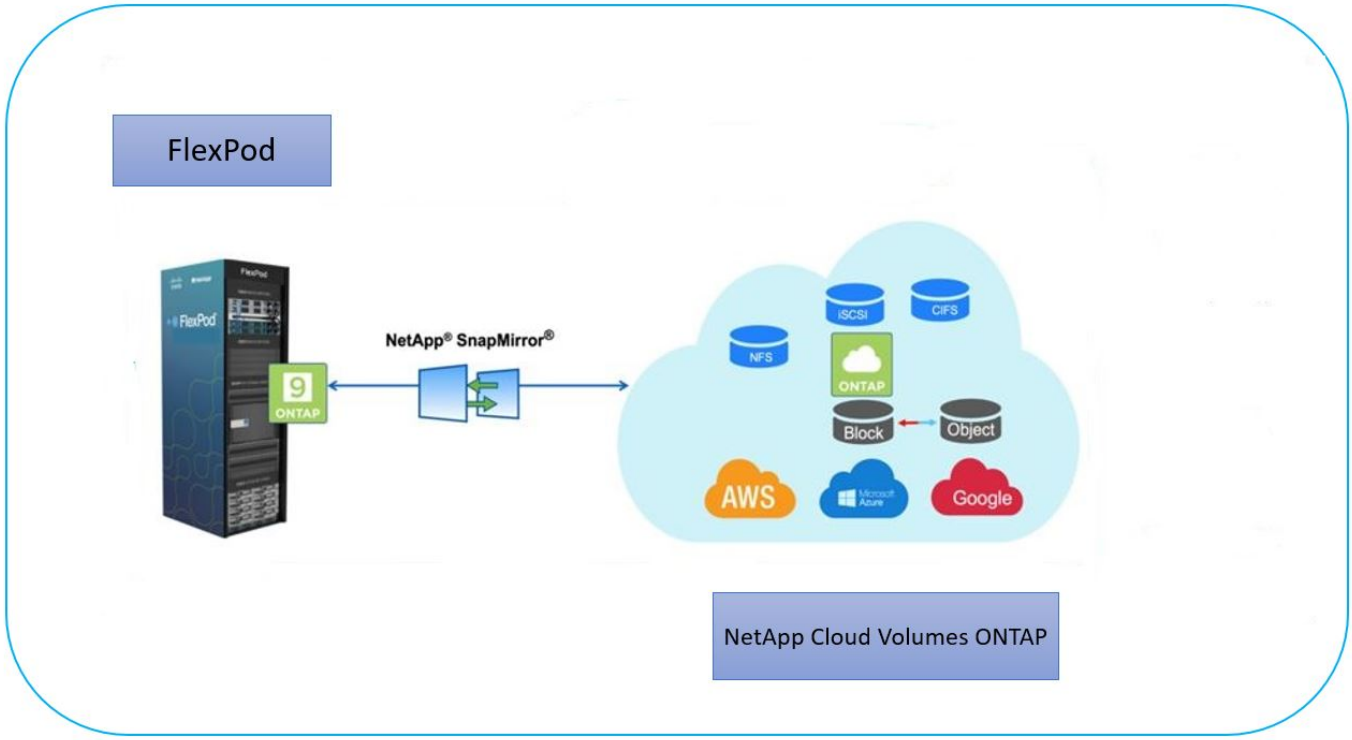
Face à la taille croissante des données de santé et aux informations exploitables qu'elles peuvent fournir, les services de données de santé et la protection des données sont deux aspects à la fois essentiels et complexes. Premièrement, les données de santé doivent être à la fois disponibles et protégées pour répondre aux exigences de restauration des données, de continuité de l'activité médicale et de conformité.

Deuxièmement, les données sur les soins de santé doivent être facilement accessibles pour analyse. Cette analyse utilise souvent des approches basées sur l'intelligence artificielle (IA) et le machine learning (ML) pour aider les entreprises du secteur médical à améliorer leurs solutions et à créer de la valeur commerciale.

Troisièmement, les infrastructures de services de données et les méthodologies de protection des données doivent prendre en charge la croissance des données de santé à mesure que le business médical se développe. De plus, la mobilité des données devient stratégique, car il est nécessaire de déplacer les données de la périphérie au cœur et jusqu'au cloud pour utiliser les ressources disponibles à des fins d'analyse ou d'archivage.

NetApp propose une solution unique de gestion des données pour les applications d'entreprise, y compris le secteur de la santé, et nous pouvons guider les hôpitaux tout au long de leur transition vers la transformation digitale. NetApp Cloud Volumes ONTAP propose une solution de gestion des données de santé dans laquelle les données peuvent être efficacement répliquées à partir d'un data Center FlexPod vers Cloud Volumes ONTAP déployé sur un cloud public tel qu'AWS.

En exploitant des ressources de cloud public sécurisées et économiques, Cloud Volumes ONTAP améliore la reprise après incident dans le cloud grâce à une réplication des données ultra-efficace, des fonctionnalités d'efficacité du stockage intégrées et des tests de reprise d'activité simples. La gestion de ces systèmes se fait par un contrôle unifié et la simplicité de la glisser-déposer. Vous bénéficiez ainsi d'une protection à toute épreuve, peu importe le type d'erreur, de défaillance ou d'incident. Cloud Volumes ONTAP propose la technologie NetApp SnapMirror comme solution de réplication des données de niveau bloc qui assure l'actualisation du volume de destination grâce à des mises à jour incrémentielles.



Public

Ce document est destiné aux ingénieurs solutions partenaires et NetApp, ainsi qu'aux équipes des services professionnels. NetApp suppose que le lecteur possède les connaissances de base suivantes :

- Une solide compréhension des concepts SAN et NAS
- Connaissance technique des systèmes de stockage ONTAP de NetApp
- Connaissance technique de la configuration et de l'administration du logiciel ONTAP

Avantages de la solution

Le data Center FlexPod intégré à NetApp Cloud Volumes ONTAP offre les avantages suivants pour les charges de travail du secteur de la santé :

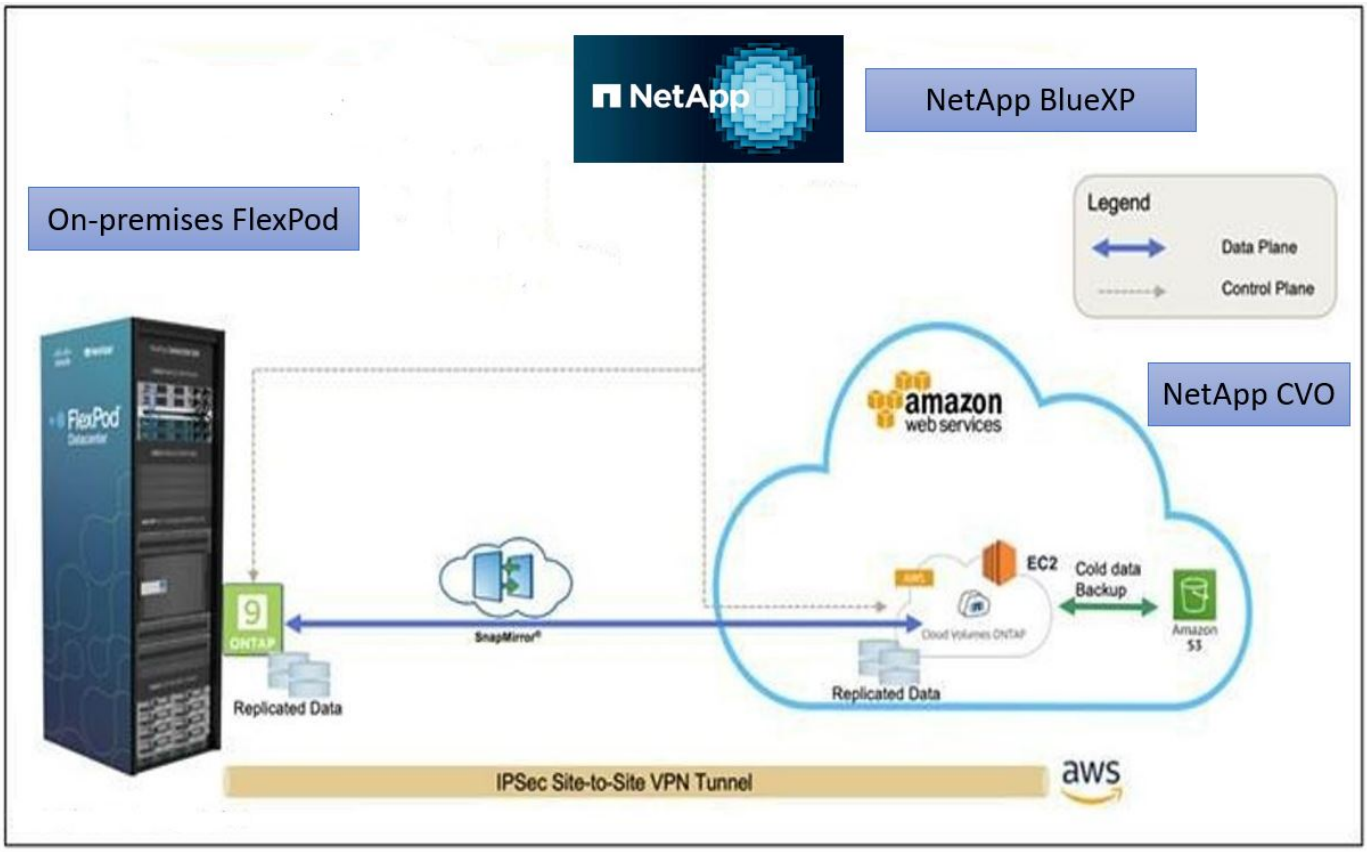
- **Protection personnalisée.** Cloud Volumes ONTAP assure la réplication des données au niveau des blocs de ONTAP vers le cloud afin de maintenir la destination à jour grâce à des mises à jour incrémentielles. Les utilisateurs peuvent spécifier une planification de synchronisation pour déterminer quand les modifications à la source sont transférées. Cela procure une protection personnalisée pour tous les types de données de santé.
- **Basculement et retour arrière.** en cas d'incident, les administrateurs du stockage peuvent rapidement définir le basculement vers les volumes cloud. Une fois le site primaire restauré, les nouvelles données créées dans l'environnement de reprise sont synchronisées avec les volumes source, ce qui permet de rétablir la réplication des données secondaires. Ainsi, les données de santé peuvent être facilement restaurées sans interrompre l'activité.
- **Efficacité.** l'espace de stockage et les coûts de la copie cloud secondaire sont optimisés grâce à la compression des données, au provisionnement fin et à la déduplication. Les données de santé sont transférées au niveau des blocs sous forme compressée et dédupliquée, ce qui accélère les transferts. Ainsi, les données sont automatiquement transférées vers un stockage objet à faible coût et sont transférées vers un stockage haute performance uniquement lors des accès, comme dans un scénario de

reprise après incident. Ceci réduit considérablement les coûts réguliers de stockage.

- **Protection contre les ransomware** la protection NetApp BlueXP analyse les sources de données dans les environnements sur site et cloud, détecte les vulnérabilités de sécurité, et fournit leur état de sécurité actuel et l'évaluation des risques. Il fournit ensuite des recommandations exploitables que vous pouvez approfondir l'investigation et le suivi pour remédier à ces problèmes. Ainsi, vous pouvez protéger vos données de santé stratégiques contre les attaques par ransomware.

Topologie de la solution

Cette section décrit la topologie logique de la solution. La figure suivante représente la topologie de la solution composée de l'environnement sur site FlexPod, de NetApp Cloud Volumes ONTAP (CVO) exécuté sur Amazon Web Services (AWS) et de la plateforme SaaS NetApp BlueXP.



Les plans de contrôle et les plans de données sont clairement indiqués entre les points d'extrémité. Le plan de données s'exécute entre l'instance ONTAP s'exécutant sur un système FAS 100 % Flash dans FlexPod et l'instance NetApp CVO dans AWS grâce à une connexion VPN sécurisée de site à site. La réplication des données de charge de travail liée au secteur de la santé depuis le data Center FlexPod sur site vers NetApp Cloud Volumes ONTAP est gérée par NetApp SnapMirror. Cette solution prend également en charge une sauvegarde et un Tiering facultatifs des données inactives résidant dans l'instance NetApp CVO vers AWS S3.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, la mise en réseau Cisco Nexus, la mise en réseau de stockage Cisco MDS et Cisco Unified Computing System (Cisco UCS).

Les établissements de santé recherchent une solution pour faciliter leur transformation digitale et améliorer l'expérience et les résultats des patients. Avec FlexPod, vous bénéficiez d'une plateforme sécurisée et évolutive qui améliore l'efficacité et permet à votre personnel de prendre plus rapidement des décisions avisées afin de meilleurs soins aux patients.

FlexPod est la plateforme idéale pour répondre aux besoins des workloads dans le domaine de la santé, car elle offre les avantages suivants :

- Optimisation des opérations pour obtenir plus rapidement des informations et améliorer la qualité des soins
- Rationalisation des applications d'imagerie grâce à une infrastructure évolutive et fiable.
- Déploiement rapide et efficace, avec une approche éprouvée pour les applications dédiées au domaine de la santé telles que les DME.

EHR

Electronic Health Records (DSE) est un logiciel destiné aux moyennes et grandes organisations médicales, aux hôpitaux et aux organismes de santé intégrés. Les clients comprennent également des hôpitaux communautaires, des établissements universitaires, des organisations pour enfants, des fournisseurs de filet de sécurité et des systèmes multi-hospitaliers. Les logiciels intégrés aux DME couvrent les fonctions cliniques, d'accès et de revenus, et s'étendent à la maison.

Les prestataires de soins de santé restent sous pression pour maximiser les avantages de leurs investissements substantiels dans les systèmes de santé électroniques de pointe. Lorsque les clients conçoivent leurs data centers pour des solutions EHR et des applications stratégiques, ils identifient souvent les objectifs suivants pour l'architecture de leur data Center :

- Haute disponibilité des applications EHR
- Hautes performances
- Facilité de mise en œuvre de dossiers médicaux électroniques dans le data Center
- Agilité et évolutivité pour soutenir la croissance avec de nouvelles versions ou applications de dossiers médicaux électroniques
- Aspect économique
- Facilité de gestion, stabilité et support
- Protection robuste des données, sauvegarde, restauration et continuité de l'activité

FlexPod est validé pour les DME et prend en charge une plateforme contenant Cisco UCS avec processeurs Intel Xeon, Red Hat Enterprise Linux (RHEL) et la virtualisation avec VMware ESXi. Cette plateforme, associée au classement « High Comfort » de EHR pour le stockage NetApp exécutant ONTAP, permet aux clients d'exécuter leurs applications de santé en toute confiance dans un cloud privé entièrement géré via FlexPod, qui peut également être connecté à n'importe quel fournisseur de cloud public.

NetApp BlueXP

BlueXP (anciennement NetApp Cloud Manager) est une plateforme de gestion SaaS haute performance qui permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud

hybride à l'aide des solutions cloud NetApp. Cette solution offre un système centralisé pour afficher et gérer vos environnements de stockage sur site et cloud, prenant en charge des environnements de cloud hybride de plusieurs fournisseurs et comptes. Pour plus d'informations, voir "BlueXP".

Connecteur

Une instance de connecteur permet à BlueXP de gérer les ressources et les processus dans un environnement de cloud public. Le connecteur est requis pour la plupart des fonctionnalités fournies par BlueXP, et peut être déployé dans le cloud ou sur le réseau sur site.

Le connecteur est pris en charge aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Sur site

Pour en savoir plus sur le connecteur, reportez-vous au "Page connecteur".

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP est une offre de stockage Software-defined qui exécute le logiciel de gestion des données ONTAP dans le cloud afin d'optimiser la gestion des données pour les workloads en mode bloc ou fichier. Avec Cloud Volumes ONTAP, vous pouvez optimiser vos coûts de stockage cloud et augmenter les performances de vos applications tout en améliorant la protection des données, la sécurité et la conformité.

Principaux avantages :

- **Efficacité du stockage.** tirer parti de la déduplication intégrée des données, de la compression des données, du provisionnement fin et du clonage instantané pour réduire les coûts de stockage.
- **Haute disponibilité.** assurer la fiabilité et la continuité de l'activité en cas de défaillances dans votre environnement cloud.
- **Protection des données.** Cloud Volumes ONTAP utilise SnapMirror, la technologie de réplication leader du secteur NetApp, pour répliquer les données sur site vers le cloud afin de disposer facilement de copies secondaires pour de multiples utilisations. Cloud Volumes ONTAP s'intègre également à Cloud Backup pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.
- **Tiering des données.** basculer entre des pools de stockage hautes et basses performances à la demande sans mettre les applications hors ligne.
- **Cohérence des applications.** fournir la cohérence des copies NetApp Snapshot avec la technologie NetApp SnapCenter.
- **Sécurité des données.** Cloud Volumes ONTAP prend en charge le chiffrement des données et offre une protection contre les virus et les ransomware.
- **Contrôles de conformité en matière de confidentialité.** l'intégration à Cloud Data Sense vous aide à comprendre le contexte des données et à identifier les données sensibles.

Pour plus d'informations, reportez-vous à la section "Cloud Volumes ONTAP".

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager permet de surveiller vos clusters de stockage ONTAP à partir d'une interface unique, remaniée et intuitive qui fournit des informations exploitables au savoir de la communauté et à l'analytique IA. Il fournit des informations opérationnelles, performantes et proactives sur l'environnement de stockage et les machines virtuelles qui s'exécutent dessus. Lorsqu'un problème se produit avec l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre un aperçu des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte vSphere vers le réseau, et enfin vers le stockage.

Certains événements fournissent également des mesures correctives qui peuvent être prises pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et des interruptions SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en prévoyant la capacité et les tendances d'utilisation afin d'anticiper les problèmes et d'éviter les décisions réactives à court terme susceptibles d'engendrer d'autres problèmes à long terme.

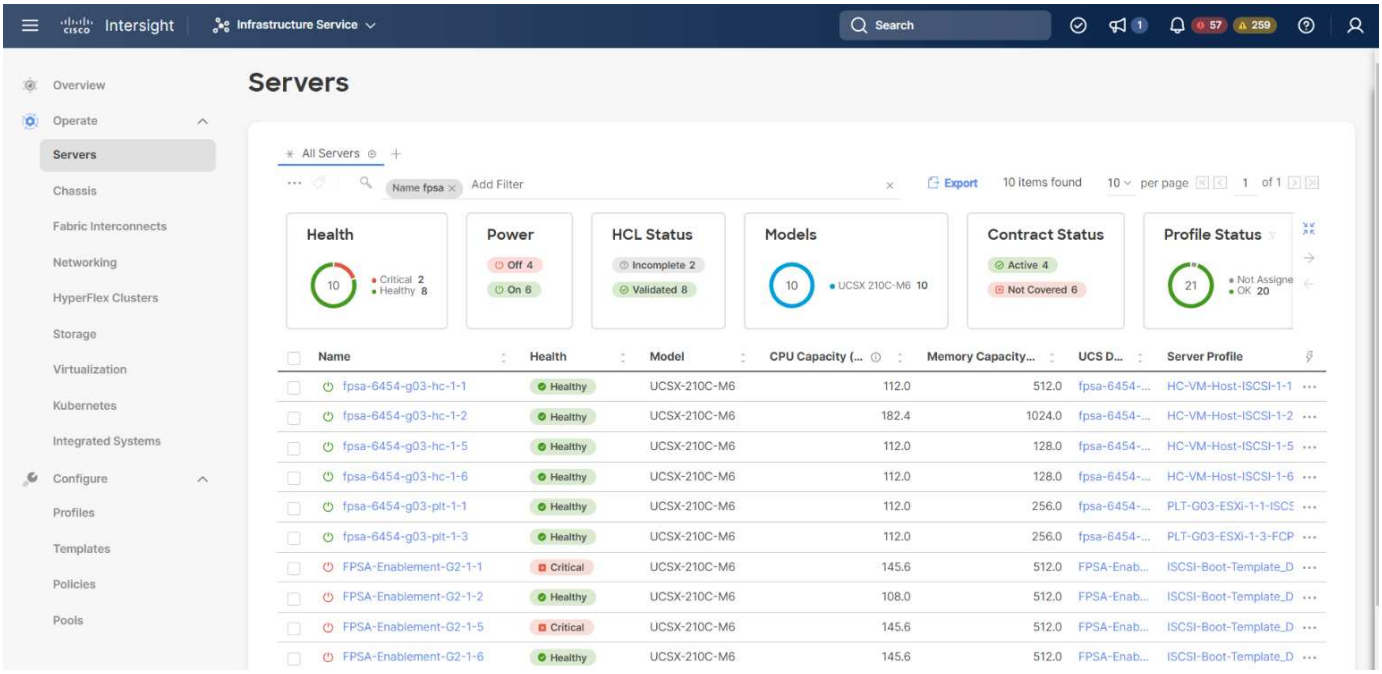
Pour plus d'informations, voir "Active IQ Unified Manager".

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme permet de stimuler les évolutions avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride. Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** Intersight est fourni en tant que service à partir du cloud ou dans le data Center du client avec des mises à jour fréquentes et une innovation continue grâce à un modèle de développement logiciel agile. Ainsi, le client peut se concentrer sur la prise en charge des besoins stratégiques de l'entreprise.
- **Opérations simplifiées.** Intersight simplifie les opérations en utilisant un outil SaaS unique et sécurisé avec un inventaire, une authentification et des API communs pour fonctionner sur l'ensemble de la pile et sur tous les emplacements, éliminant ainsi les silos entre les équipes. Vous pouvez ainsi gérer les serveurs physiques et les hyperviseurs sur site, sur les machines virtuelles, K8s, sans serveur, l'automatisation, d'optimisation et de contrôle des coûts à la fois sur site et dans les clouds publics.
- **Optimisation continue.** vous pouvez optimiser en continu votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur toutes les couches, ainsi que par Cisco TAC. Ces informations sont converties en actions recommandées et automatisables, qui vous permettent de vous adapter en temps réel à toutes les modifications, allant du déplacement des workloads au contrôle de l'état des serveurs physiques en passant par des recommandations de réduction des coûts pour les clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner le mode UCSM géré natif (UMM) ou le mode géré Intersight pour les systèmes FAS Cisco UCS lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'IMM native est utilisé. La figure suivante présente le tableau de bord de Cisco Intersight.



VMware vSphere 7.0

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière globale de vastes ensembles d'infrastructures (notamment les processeurs, le stockage et la mise en réseau) dans un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation classiques qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un datacenter entier afin de créer une centrale unique avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application dans le besoin.

Pour plus d'informations sur VMware vSphere et ses composants, voir "VMware vSphere".

Serveur VMware vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Pour plus d'informations, reportez-vous à la section "VMware vCenter".

Révisions matérielles et logicielles

Cette solution de cloud hybride peut être étendue à tout environnement FlexPod exécutant les versions logicielles, matérielles et firmware prises en charge, comme défini dans le "Matrice d'interopérabilité NetApp", "Compatibilité matérielle et logicielle UCS", et "Guide de compatibilité VMware".

Le tableau suivant présente les révisions matérielles et logicielles FlexPod sur site.

Composant	Solution NetApp	Version
Calcul	Cisco UCS X210c M6	5.0(1b)

Composant	Solution NetApp	Version
	Cisco UCS Fabric Interconnect 6454	4.2(2a)
Le réseau	Cisco Nexus 9336C-FX2 NX-OS	9.3(9)
Stockage	NetApp AFF A400	ONTAP 9.11.1P2
	Outils NetApp ONTAP pour VMware vSphere	9.11
	Plug-in NetApp NFS pour VMware VAAI	2.0
	NetApp Active IQ Unified Manager	9.11P1
Logiciel	VMware vSphere	7.0(U3)
	Pilote Ethernet nenic VMware ESXi	1.0.35.0
	Appliance VMware vCenter	7.0.3
	Appliance virtuelle Cisco InterSight Assist	1.0.9-342

Le tableau suivant présente les versions de NetApp BlueXP et Cloud Volumes ONTAP.

Fournisseur	Solution NetApp	Version
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"Suivant : installation et configuration."

Installation et configuration

"Précédent : composants de la solution."

Déploiement de NetApp Cloud Volumes ONTAP

Pour configurer votre instance Cloud Volumes ONTAP, procédez comme suit :

1. Préparez l'environnement du fournisseur de services clouds publics.

   Pour la configuration de la solution, vous devez capturer les détails de l'environnement de votre fournisseur de services de cloud public. Par exemple, pour la préparation de l'environnement Amazon Web Services (AWS), vous avez besoin de la clé d'accès AWS, de la clé secrète AWS et d'autres détails du réseau tels que la région, le VPC, le sous-réseau, etc.

2. Configurez la passerelle de point de terminaison VPC.

   Une passerelle de terminal VPC est nécessaire pour activer la connexion entre le VPC et le service AWS S3. Elle permet d'activer la sauvegarde sur CVO, un terminal de type passerelle.

3. Accédez à NetApp BlueXP.

   Pour accéder à NetApp BlueXP et à d'autres services cloud, vous devez vous inscrire sur "NetApp

BlueXP". Pour configurer des espaces de travail et des utilisateurs dans le compte BlueXP, cliquez sur "ici". Vous avez besoin d'un compte autorisé à déployer le connecteur dans votre fournisseur cloud directement à partir de BlueXP. Vous pouvez télécharger la règle BlueXP depuis le site "ici".

4. Déployez le connecteur.

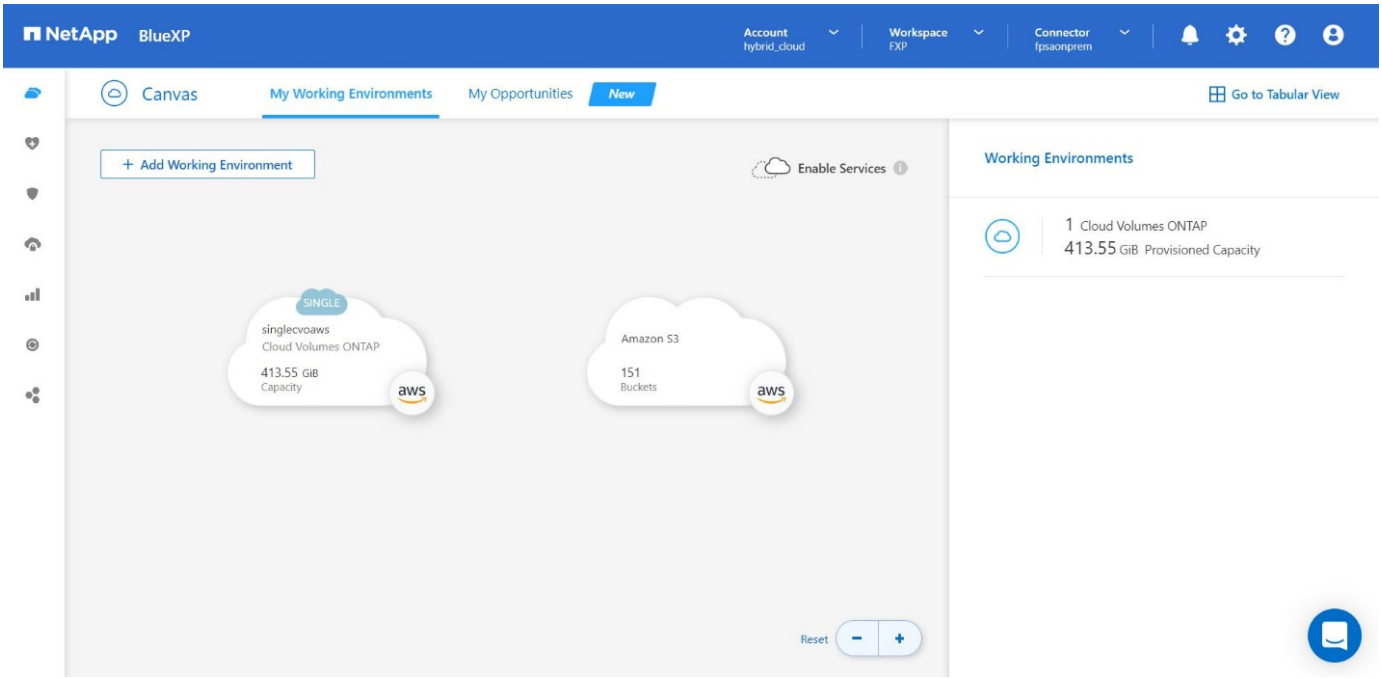
   Avant d'ajouter un environnement de travail Cloud volumes ONTAP, vous devez déployer Connector. BlueXP vous invite si vous essayez de créer votre premier environnement de travail Cloud Volumes ONTAP sans connecteur. Pour déployer Connector dans AWS à partir de BlueXP, consultez cette page "lien".

5. Lancez Cloud Volumes ONTAP dans AWS.

   Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à système unique ou en tant que paire haute disponibilité dans AWS. "Lisez les instructions détaillées".

   Pour plus d'informations sur ces étapes, reportez-vous au "Guide de démarrage rapide de Cloud Volumes ONTAP dans AWS".

   Dans cette solution, nous avons déployé un système Cloud Volumes ONTAP à un seul nœud dans AWS. La figure suivante présente le tableau de bord NetApp BlueXP avec une instance CVO à un seul nœud.



Déploiement FlexPod sur site

Pour en savoir plus sur la conception de FlexPod avec UCS X-Series, VMware et NetApp ONTAP, consultez le "FlexPod Datacenter avec Cisco UCS X-Series" guide de conception. Ce document fournit des conseils de conception pour l'intégration de la plateforme UCS X-Series gérée par Cisco Intersight à l'infrastructure FlexPod Datacenter.

Pour déployer l'instance FlexPod sur site, reportez-vous à la section "ce guide de déploiement".

Ce document apporte des conseils de déploiement pour intégrer la plateforme UCS X-Series gérée par Cisco Intersight à une infrastructure FlexPod Datacenter. Il aborde à la fois les configurations et les meilleures pratiques pour un déploiement réussi.

FlexPod peut être déployé en mode géré UCS et en mode géré Cisco Intersight (IMM). Si vous déployez FlexPod en mode géré UCS, reportez-vous à cette section "guide de conception" et ceci "guide de déploiement".

Le déploiement de FlexPod peut être automatisé avec une infrastructure basée sur le code grâce à Ansible. Vous trouverez ci-dessous des liens vers les référentiels GitHub pour un déploiement FlexPod de bout en bout :

- Vous pouvez voir la configuration Ansible d'FlexPod avec Cisco UCS en mode géré, NetApp ONTAP et VMware vSphere "ici".
- Vous pouvez voir la configuration Ansible d'FlexPod avec Cisco UCS dans IMM, NetApp ONTAP et VMware vSphere "ici".

Configuration du stockage ONTAP sur site

Cette section décrit certaines des importantes étapes de configuration de ONTAP spécifiques à cette solution.

1. Configurez un SVM avec le service iSCSI en cours d'exécution.

```
1. vserver create –vserver Healthcare_SVM –rootvolume
Healthcare_SVM_root –aggregate aggr1_A400_G0312_01 –rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   Si la licence iSCSI n'a pas été installée lors de la configuration du cluster, assurez-vous d'installer la licence avant de créer le service iSCSI.

2. Créer un volume FlexVol.

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. Ajoutez des interfaces pour l'accès iSCSI.

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> –status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
```

Dans cette solution, nous avons créé quatre interfaces logiques iSCSI, deux sur chaque nœud.

Une fois l'instance FlexPod opérationnelle avec vCenter déployée et tous les hôtes ESXi ajoutés, nous devons déployer une VM Linux qui agit comme un serveur qui se connecte au stockage NetApp ONTAP et y accède. Dans cette solution, nous avons installé une instance CentOS 8 dans vCenter.

4. Créer une LUN.

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

Pour une base de données opérationnelle EHR (ODB), un journal et des charges de travail applicatives, EHR recommande de présenter le stockage aux serveurs comme des LUN iSCSI. NetApp prend également en charge l'utilisation de FCP et NVMe/FC si certaines versions d'AIX et de systèmes d'exploitation RHEL sont compatibles, ce qui améliore les performances. FCP et NVMe/FC peuvent coexister sur la même structure.

5. Créer un groupe initiateur.

```
1. igroup create –vserver Healthcare_SVM –igroup ehr –protocol iscsi
–ostype linux –initiator iqn.1994-05.com.redhat:8e91e9769336
```

Les iGroups permettent au serveur d'accéder aux LUN, Pour l'hôte Linux, l'IQN du serveur se trouve dans le fichier `/etc/iscsi/initiatorname.iscsi`.

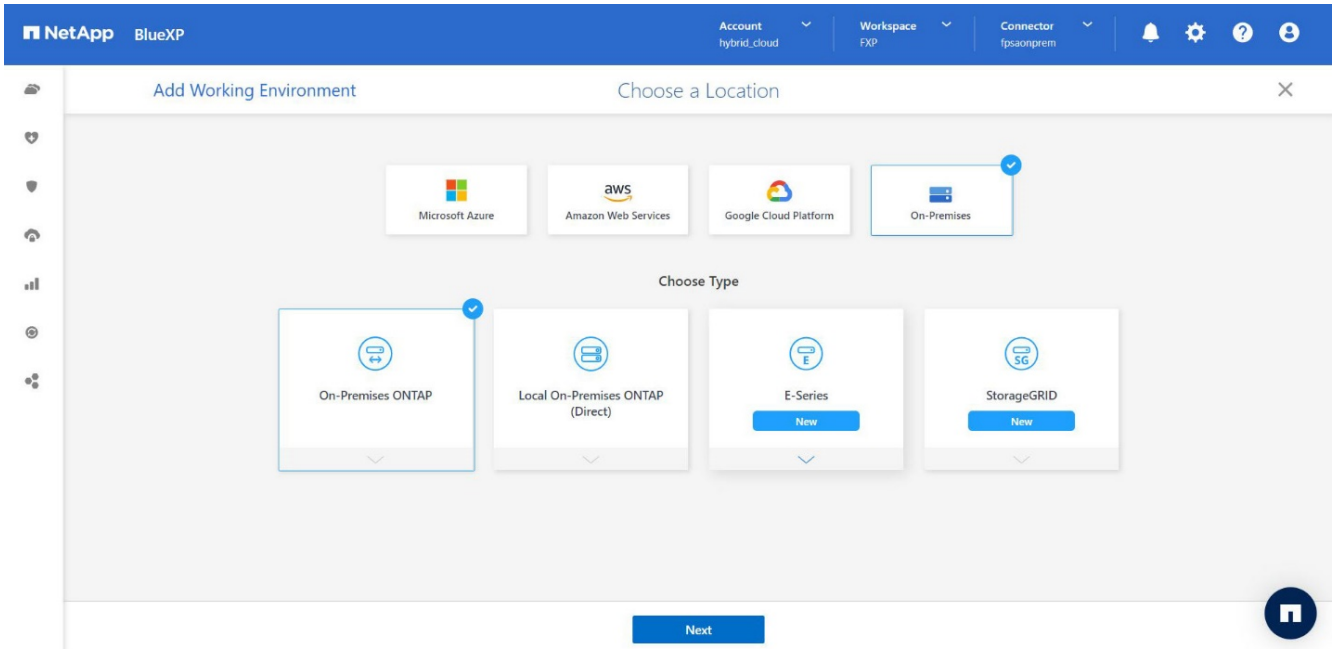
6. Mappez la LUN sur le groupe initiateur.

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

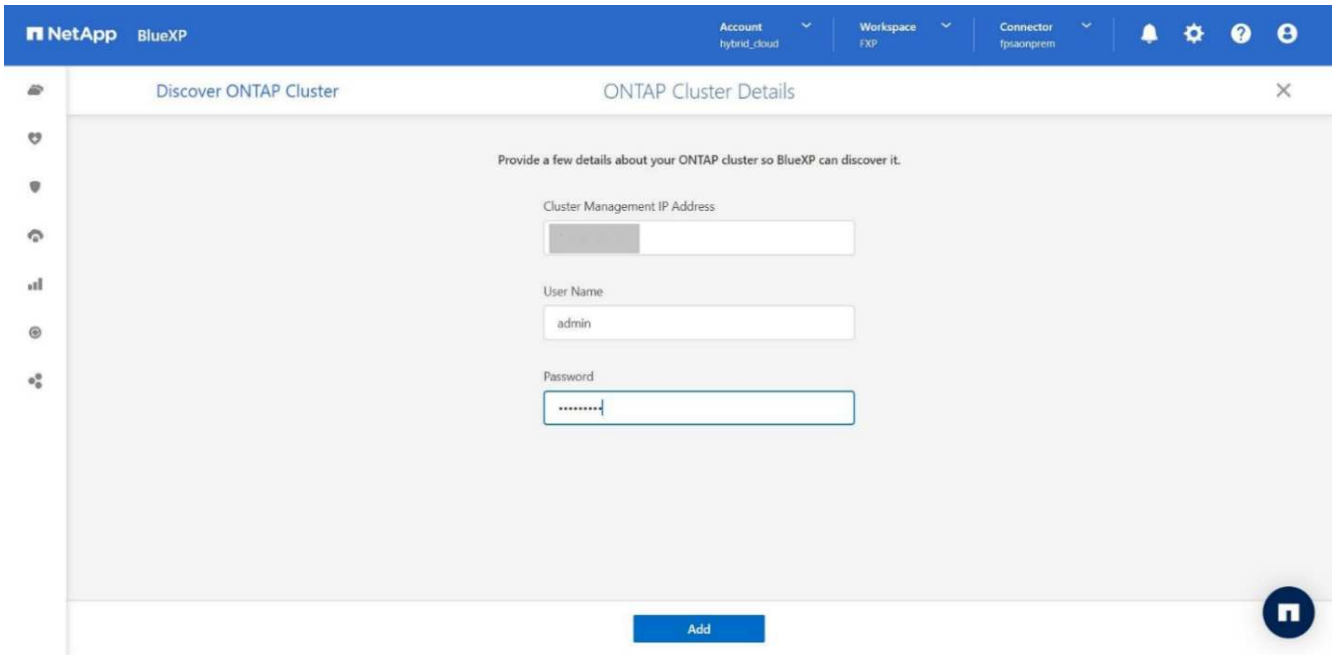
Ajoutez le stockage FlexPod sur site à BlueXP

Procédez comme suit pour ajouter votre stockage FlexPod à l'environnement de travail à l'aide de NetApp BlueXP.

1. Dans le menu de navigation, sélectionnez **stockage** > **Canvas**.
2. Sur la page Canevas, cliquez sur **Ajouter un environnement de travail** et sélectionnez **sur site**.
3. Sélectionnez **ONTAP sur site**. Cliquez sur **Suivant**.

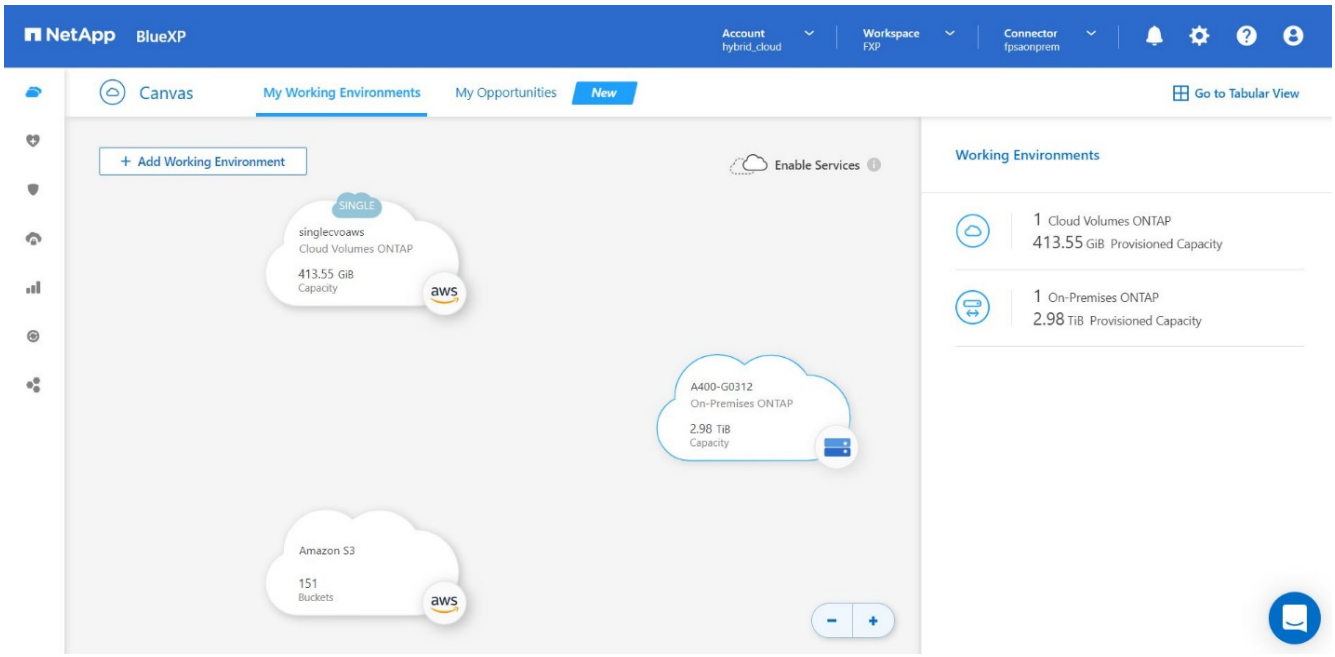


4. Sur la page ONTAP Cluster Details (Détails du cluster ONTAP), entrez l'adresse IP de gestion du cluster et le mot de passe du compte d'utilisateur admin. Cliquez ensuite sur **Ajouter**.



5. Sur la page Détails et informations d'identification, entrez un nom et une description pour l'environnement de travail, puis cliquez sur **Go**.

   BlueXP découvre le cluster ONTAP et l'ajoute en tant qu'environnement de travail sur la zone de travail.



Pour plus d'informations, reportez-vous à la page "Découvrez les clusters ONTAP sur site".

"Ensuite : configuration SAN."

Configuration SAN

"Précédent : installation et configuration."

Cette section décrit la configuration côté hôte requise par le dossier EHR pour permettre

au logiciel d'intégrer au mieux le stockage NetApp. Dans ce segment, nous discutons plus particulièrement de l'intégration de l'hôte pour les systèmes d'exploitation Linux. Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour valider toutes les versions des logiciels et des firmwares.

Les étapes de configuration suivantes sont spécifiques à l'hôte CentOS 8 qui a été utilisé dans cette solution.

Kit d'utilitaire hôte NetApp

NetApp recommande d'installer NetApp Host Utility Kit (Host Utilities Kit) sur les systèmes d'exploitation d'hôtes connectés aux systèmes de stockage NetApp et accédant à ces derniers. Les E/S multichemins Microsoft natives (MPIO) sont prises en charge. Le système d'exploitation doit être compatible ALUA (Asymmetric Logical Unit Access) pour les chemins d'accès multiples. L'installation des utilitaires d'hôtes configure les paramètres de l'adaptateur de bus hôte (HBA) pour le stockage NetApp.

Les utilitaires d'hôte NetApp peuvent être téléchargés "ici". Dans cette solution, nous avons installé Linux Host Utilities 7.1 sur l'hôte.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

Découvrez le stockage ONTAP

Assurez-vous que le service iSCSI est en cours d'exécution lorsque les connexions sont supposées se produire. Pour définir le mode de connexion pour un portail spécifique sur une cible ou pour tous les portails sur une cible, utilisez le `iscsiadm` commande.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

Vous pouvez maintenant utiliser `sanlun` Pour afficher des informations sur les LUN connectées à l'hôte. Assurez-vous d'être connecté en tant que root sur l'hôte.

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                      device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
---
Healthcare_SVM                        /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                        /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

Configurer les chemins d'accès multiples

Device Mapper Multipathing (DM-Multipath) est un utilitaire natif de multipathing sous Linux. Il peut être utilisé pour la redondance et pour améliorer les performances. Elle agrège ou combine les chemins d'E/S multiples entre les serveurs et le stockage, afin de créer un périphérique unique au niveau du système d'exploitation.

1. Avant de configurer DM-Multipath sur votre système, assurez-vous que votre système a été mis à jour et inclut le `device-mapper-multipath` création de package.

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. Le fichier de configuration est le `/etc/multipath.conf` fichier. Mettez à jour le fichier de configuration comme indiqué ci-dessous.

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
   path_checker      readsector0
   no_path_retry      fail
}
devices {
   device {
      vendor         "NETAPP  "
      product         "LUN.*"
      no_path_retry     queue
      path_checker      tur
   }
}
```

3. Activez et démarrez les services multivoies.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. Ajoutez le module noyau chargeable `dm-multipath` et redémarrez le service multivoie. Enfin, vérifiez l'état des chemins d'accès multiples.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

Pour plus d'informations sur ces étapes, reportez-vous à la section "ici".

Créer un volume physique

Utilisez le `pvcreate` commande permettant d'initialiser un périphérique de bloc à utiliser comme volume physique. L'initialisation est similaire au formatage d'un système de fichiers.

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

Créer un groupe de volumes

Pour créer un groupe de volumes à partir d'un ou de plusieurs volumes physiques, utilisez `vgcreate` commande. Cette commande crée un nouveau groupe de volumes par son nom et y ajoute au moins un volume physique.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

Le `vgdisplay` peut être utilisé pour afficher les propriétés des groupes de volumes (taille, extensions, nombre

de volumes physiques, etc.) dans un format fixe.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

Créer un volume logique

Lorsque vous créez un volume logique, le volume logique est découpé dans un groupe de volumes à l'aide des extensions libres sur les volumes physiques qui composent le groupe de volumes.

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Cette commande crée un volume logique appelé `datalv` qui utilise tout l'espace non alloué dans le groupe de volumes `datavg`.

Créer un système de fichiers

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Créer un dossier à monter

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

Montez le système de fichiers

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                1K-blocks    Used Available Use% Mounted on
devtmpfs                    8072804       0   8072804   0% /dev
tmpfs                       8103272       0   8103272   0% /dev/shm
tmpfs                       8103272    9404   8093868   1% /run
tmpfs                       8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root        45496624 5642104  39854520  13% /
/dev/sda2                   1038336  258712    779624  25% /boot
/dev/sda1                    613184    7416    605768   2% /boot/efi
tmpfs                       1620652      12   1620640   1% /run/user/42
tmpfs                       1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

Pour plus d'informations sur ces tâches, reportez-vous à la page "Administration LVM avec commandes CLI".

Génération de données

```
`Dgen.pl` Est un générateur de données de script perl pour le simulateur
d'E/S de EHR (GenerateIO). Les données contenues dans les LUN sont
générées avec le DME `Dgen.pl` script. Le script est conçu pour créer des
données similaires à celles qui se trouvent dans une base de données EHR.
```

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

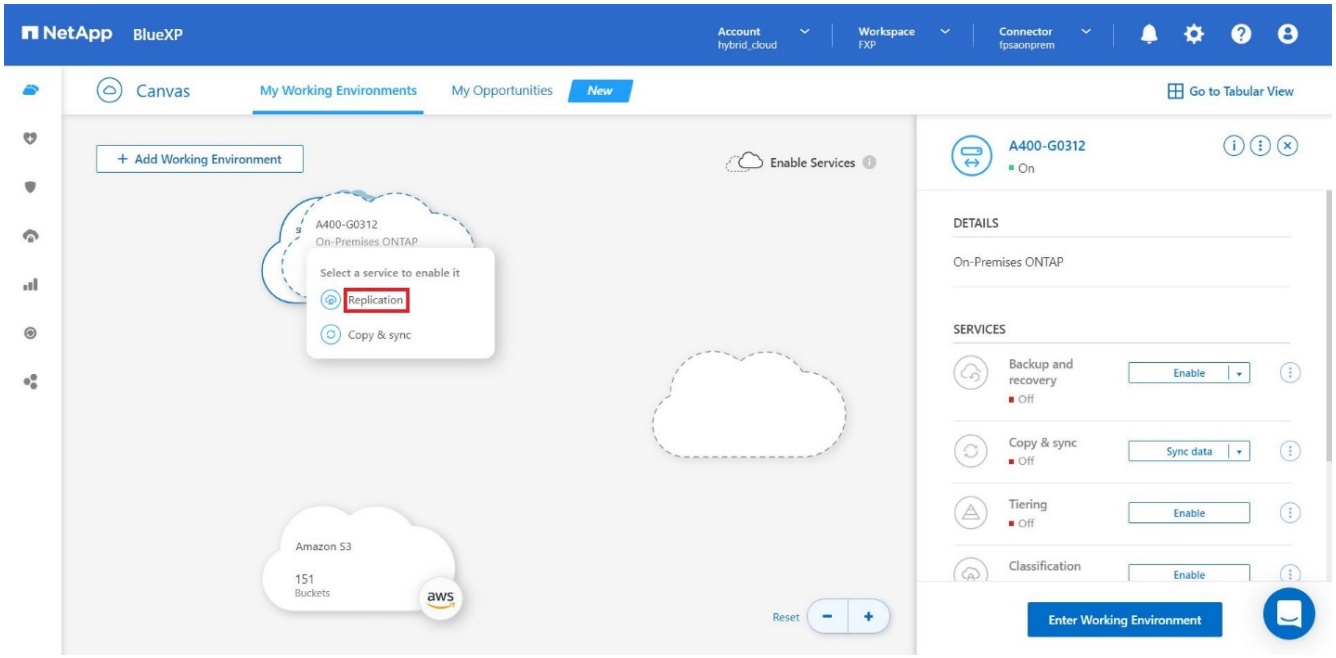
En cours d'exécution, le `Dgen.pl` script utilise 85 % du système de fichiers pour la génération de données par défaut.

Configurez la réplication SnapMirror entre ONTAP et Cloud Volumes ONTAP sur site

NetApp SnapMirror réplique les données à des vitesses élevées sur un réseau LAN ou WAN, vous garantissant ainsi une haute disponibilité et une réplication rapide des données dans les environnements traditionnels et virtualisés. En répliquant vos données sur des systèmes de stockage NetApp, puis en les mettant régulièrement à jour, vous disposez de données actualisées et accessibles dès que vous en avez besoin. Aucun serveur de réplication externe n'est requis.

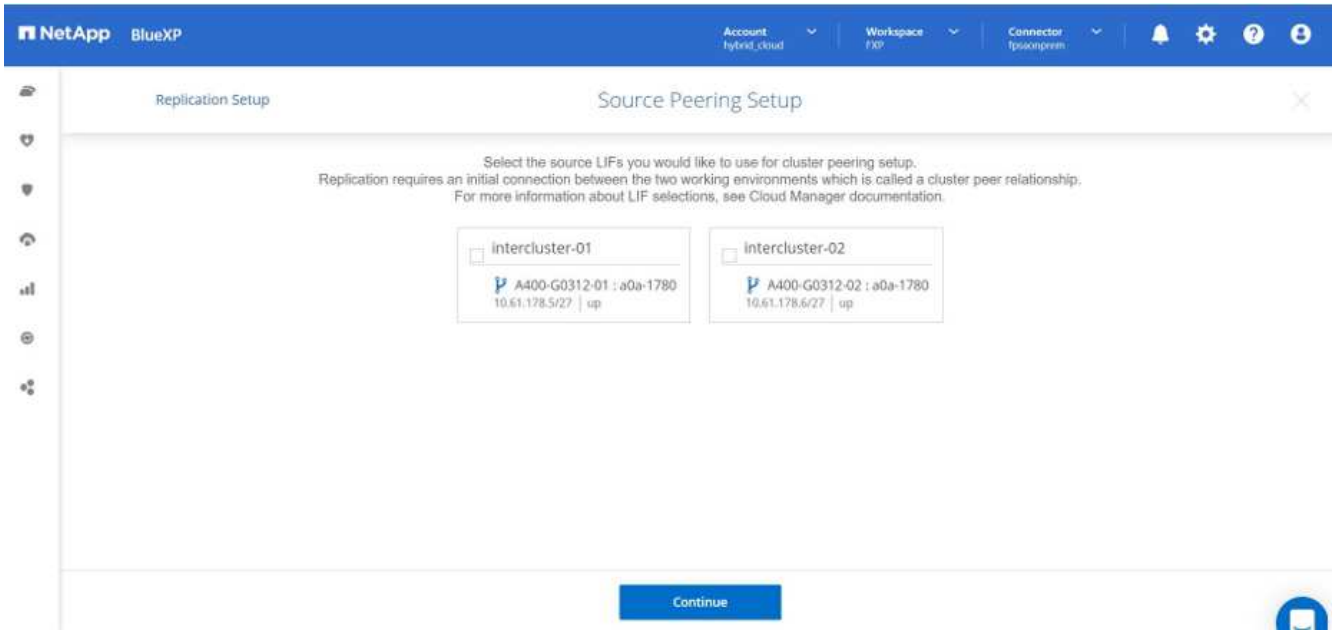
Effectuez les étapes suivantes pour configurer la réplication SnapMirror entre votre système ONTAP sur site et CVO.

1. Dans le menu de navigation, sélectionnez **stockage** > **Canvas**.
2. Dans Canvas, sélectionnez l'environnement de travail qui contient le volume source, faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume, puis sélectionnez **Replication**.

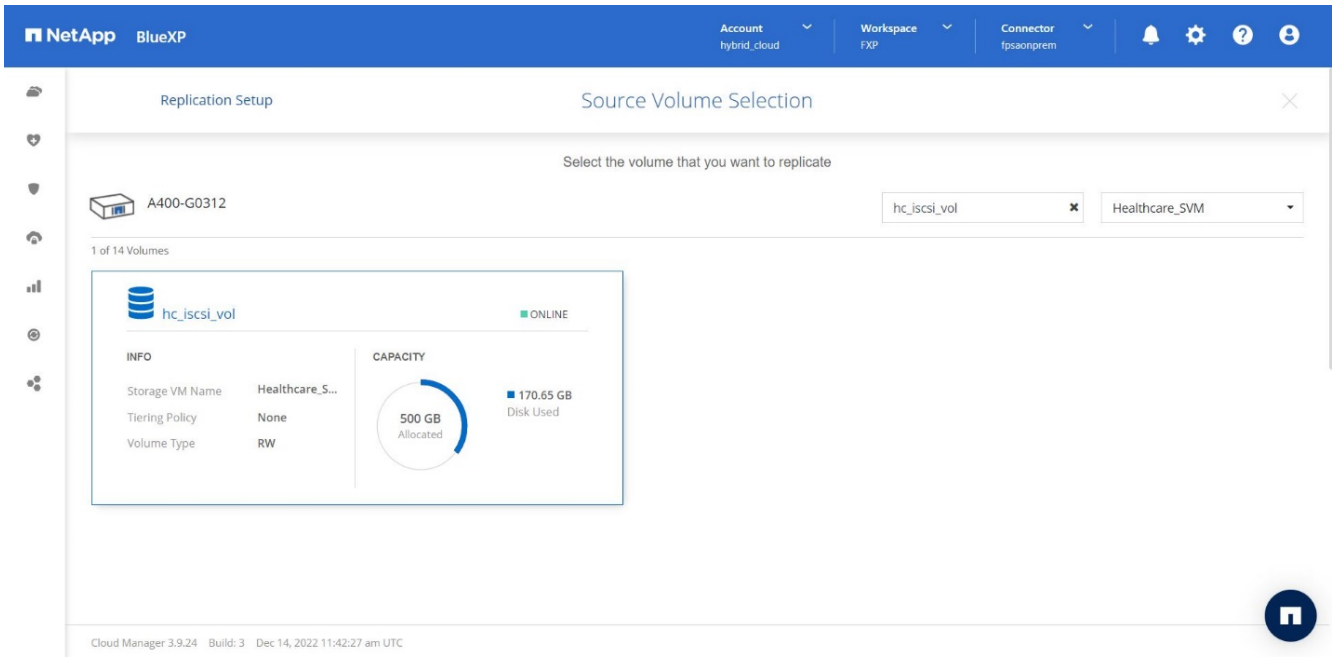


Les autres étapes expliquent comment créer une relation synchrone entre Cloud Volumes ONTAP et les clusters ONTAP sur site.

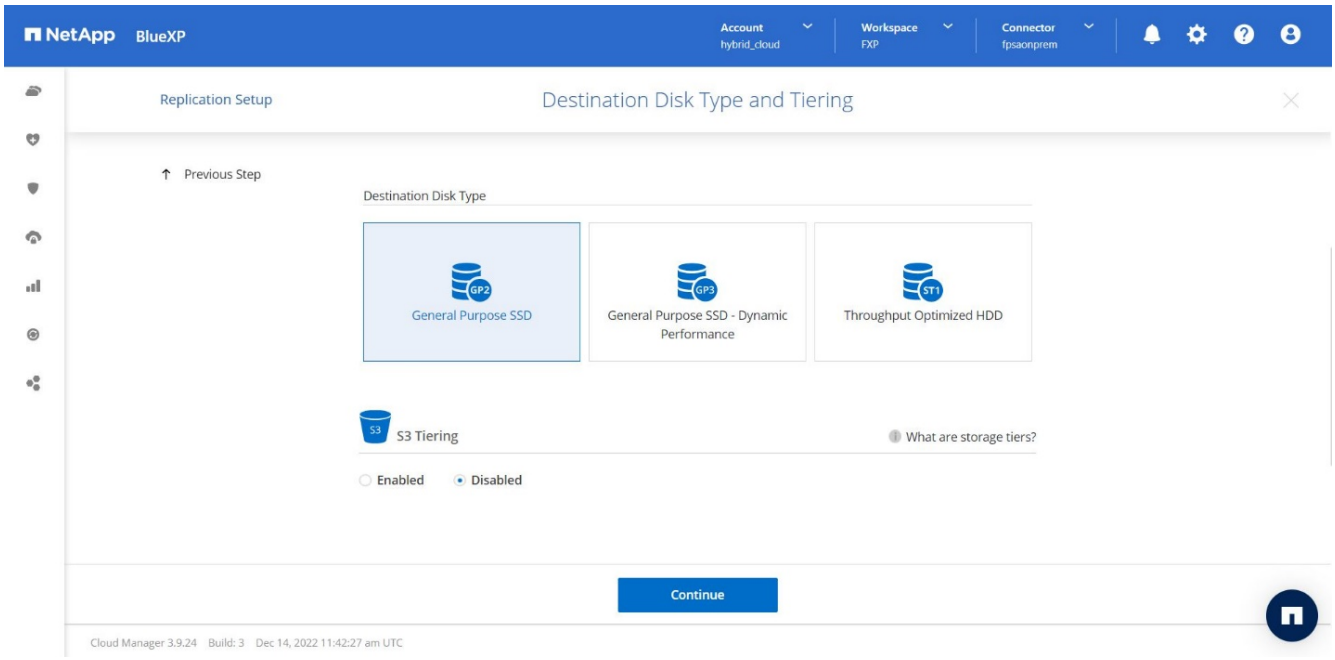
3. **Configuration du peering source et destination.** si cette page s'affiche, sélectionnez toutes les LIFs intercluster pour la relation entre pairs de cluster.



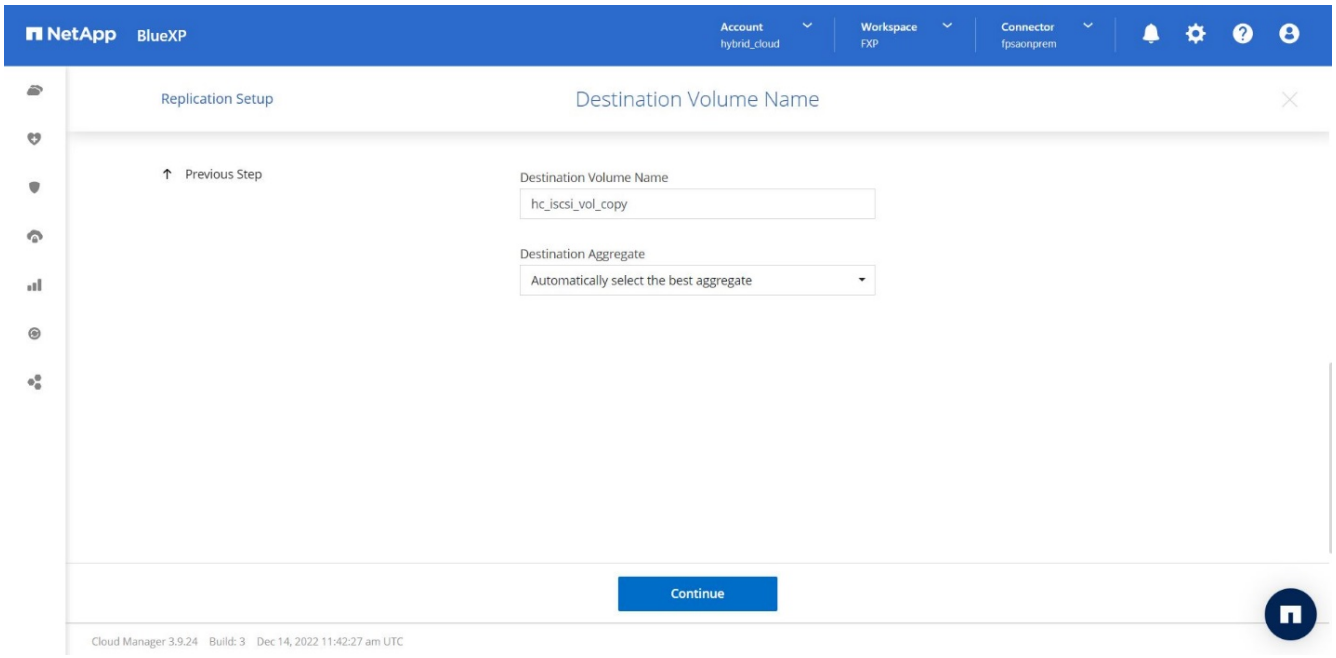
4. **Sélection du volume source.** sélectionnez le volume que vous souhaitez répliquer.



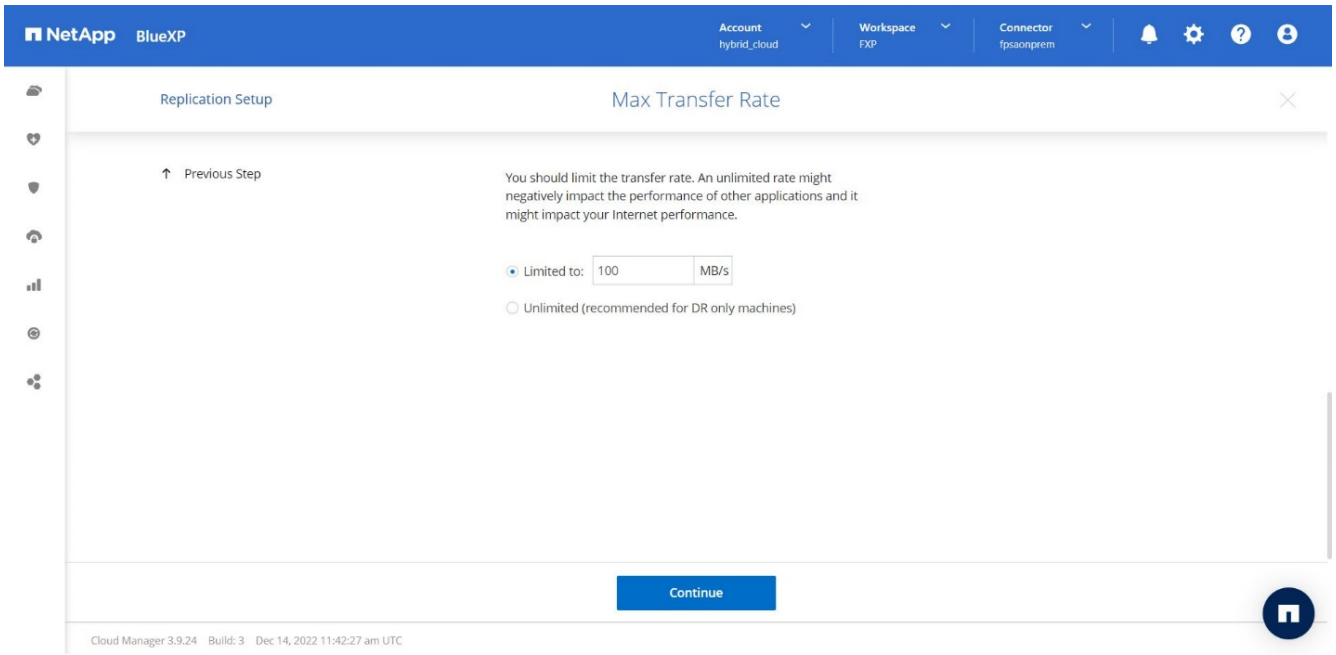
5. **Type de disque de destination et hiérarchisation.** si la cible est un système Cloud Volumes ONTAP, sélectionnez le type de disque de destination et choisissez si vous souhaitez activer la hiérarchisation des données.



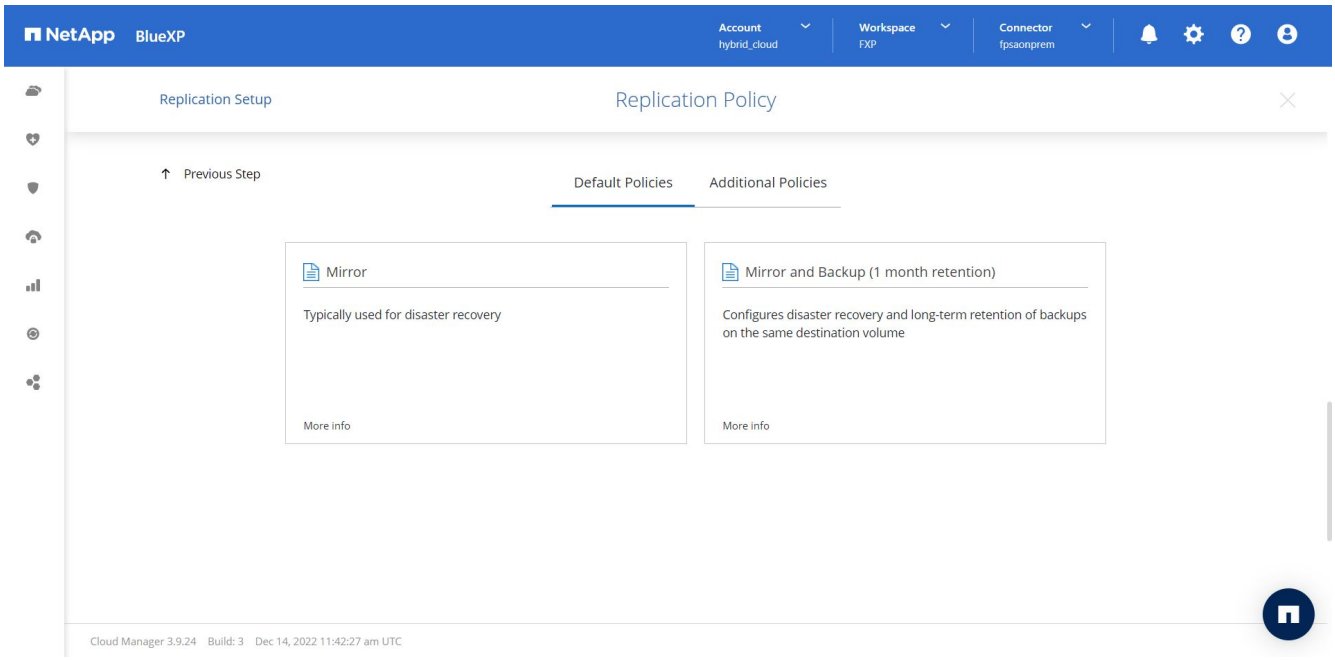
6. **Nom du volume de destination :** Indiquez le nom du volume de destination et choisissez l'agrégat de destination. Si la destination est un cluster ONTAP, vous devez également spécifier la VM de stockage de destination.



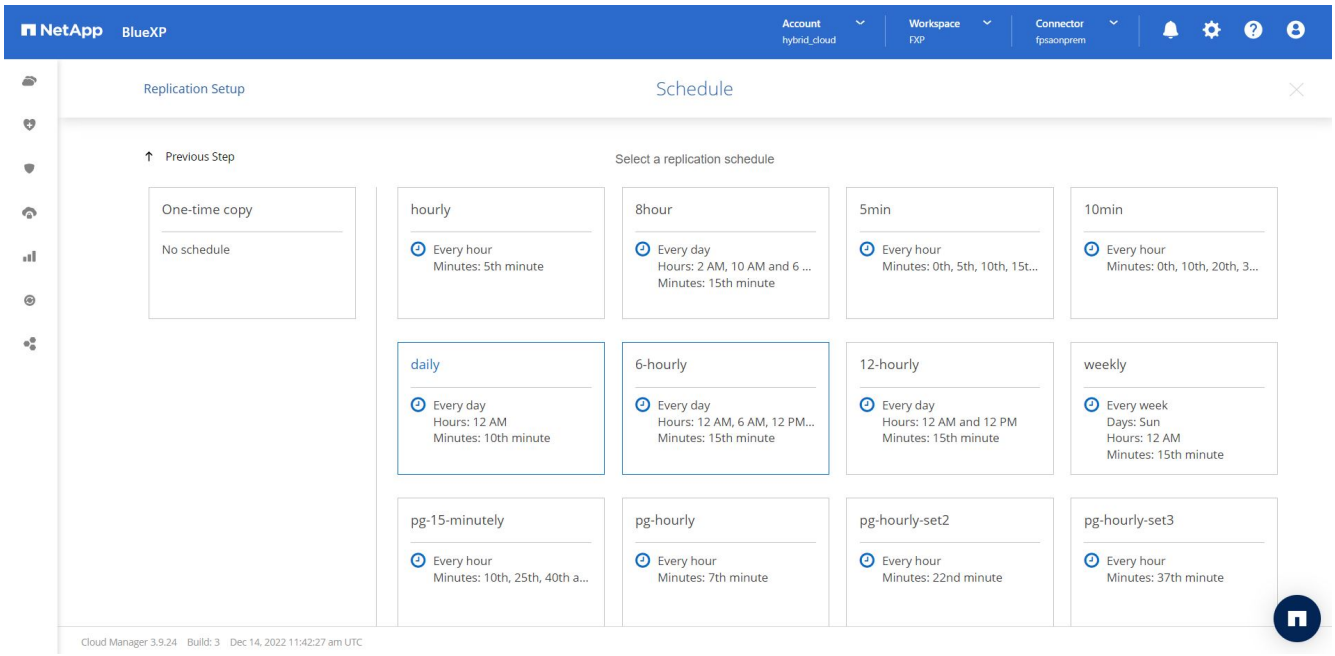
7. **Taux de transfert max.** Indiquez le taux maximal (en mégaoctets par seconde) auquel les données peuvent être transférées.



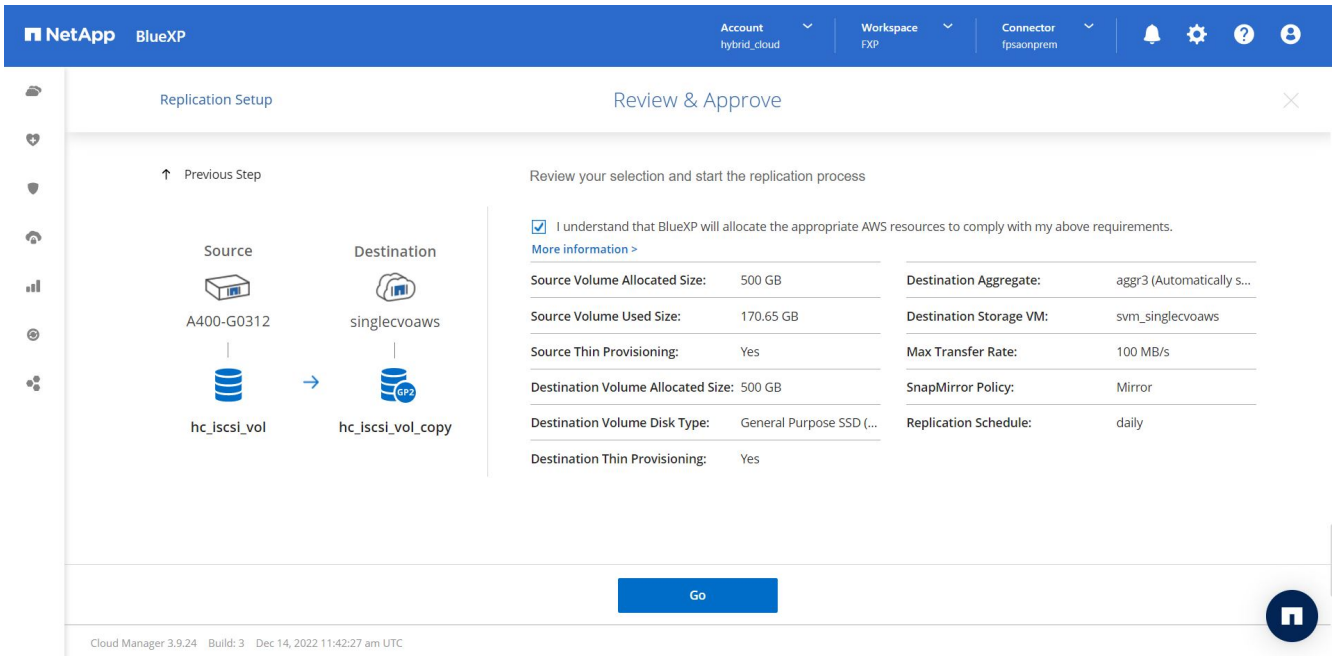
8. **Règle de réplication.** Choisissez une stratégie par défaut ou cliquez sur **règles supplémentaires**, puis sélectionnez l'une des stratégies avancées. Pour obtenir de l'aide, "en savoir plus sur les règles de réplication".



9. **Horaire.** Choisissez une copie ponctuelle ou un horaire récurrent. Plusieurs plannings par défaut sont disponibles. Si vous voulez un autre planning, vous devez créer un nouveau planning sur le `destination cluster` Utiliser System Manager.

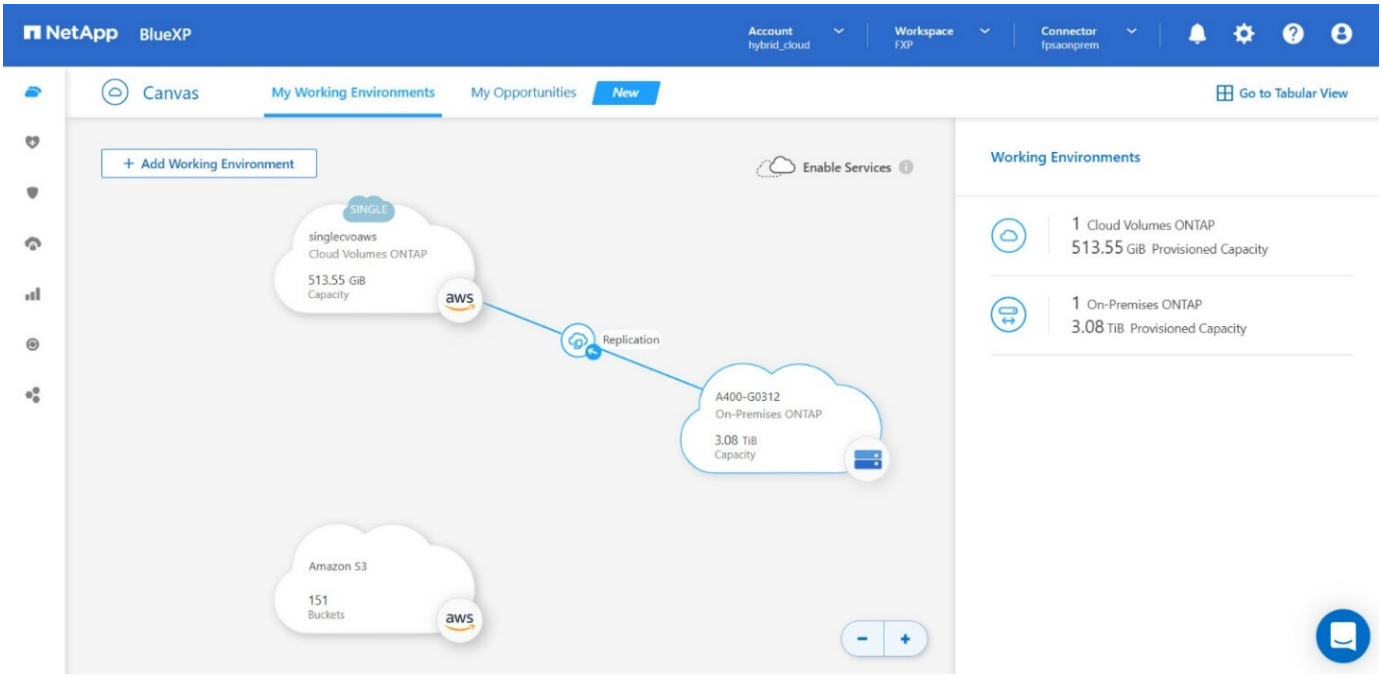


10. **Revoir.** revoir vos sélections et cliquer sur **aller**.

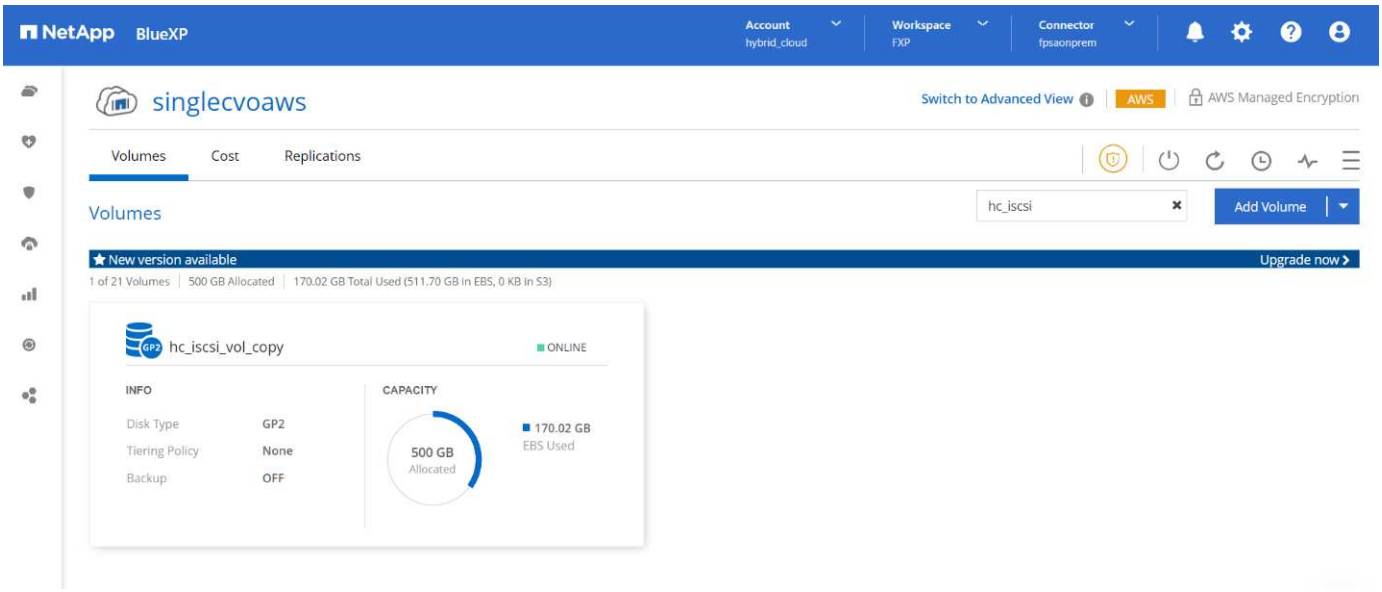


Pour plus d'informations sur ces étapes de configuration, reportez-vous à la section "ici".

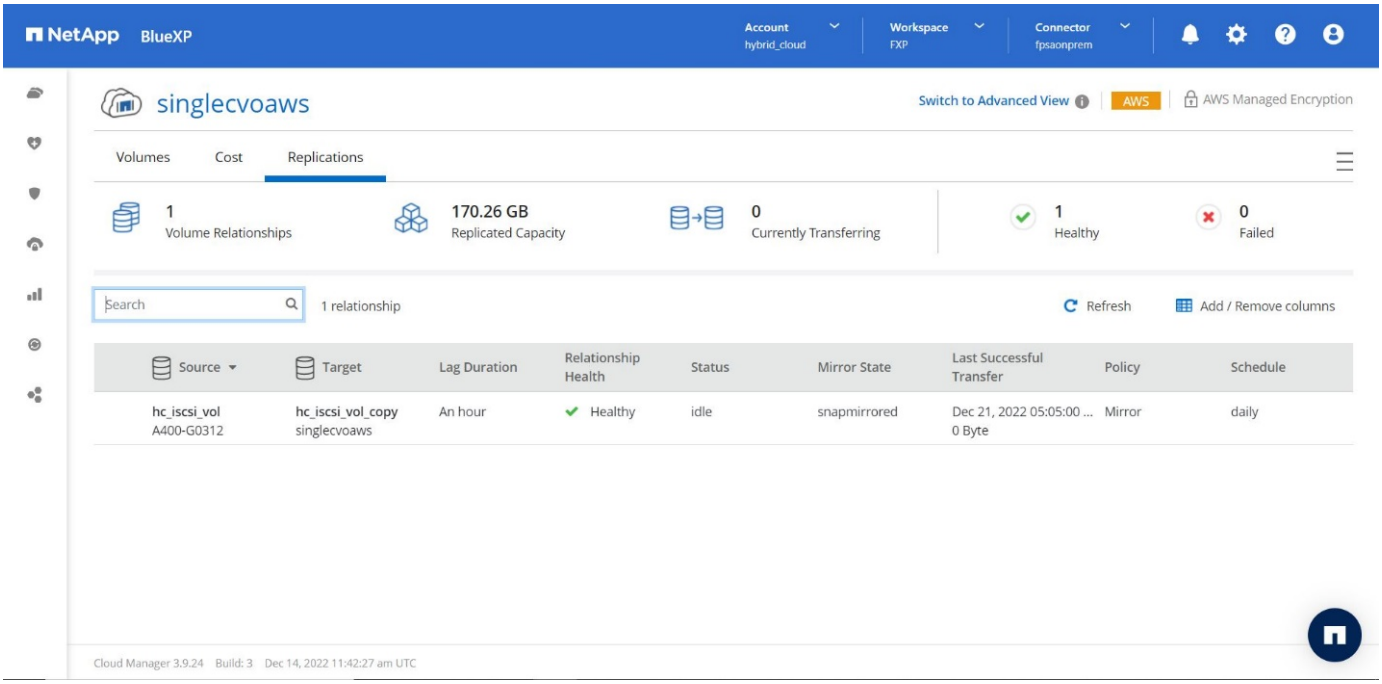
BlueXP démarre le processus de réplication des données. Maintenant, vous pouvez voir le service **Replication** qui a été établi entre votre système ONTAP sur site et Cloud Volumes ONTAP.



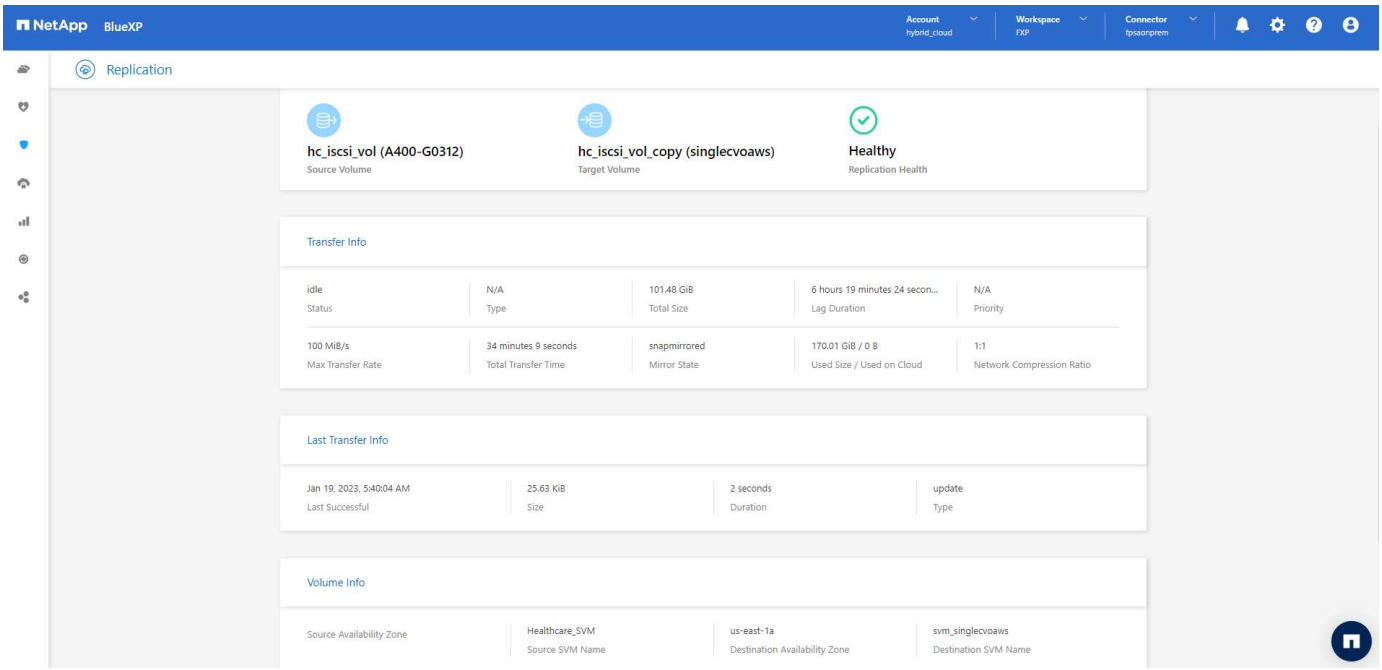
Dans le cluster Cloud Volumes ONTAP, vous pouvez afficher le volume qui vient d'être créé.



Vous pouvez également vérifier que la relation SnapMirror est établie entre le volume sur site et le volume cloud.



Pour plus d'informations sur la tâche de réplication, reportez-vous à l'onglet **Replication**.



"Ensuite, validation de la solution."

Validation des solutions

"Précédent : configuration SAN."

Cette section présente quelques cas d'utilisation de solutions.

- L'une des principales utilisations de SnapMirror est la sauvegarde des données. SnapMirror peut être utilisé en tant qu'outil de sauvegarde principal en répliquant les données au sein d'un même cluster ou vers des cibles distantes.
- Utilisation de l'environnement de reprise d'activité pour exécuter des tests de développement d'applications (développement/test)
- Reprise sur incident en cas d'incident en production.
- Distribution des données et accès aux données à distance.

Toutefois, les rares cas d'utilisation validés dans cette solution ne représentent pas l'intégralité des fonctionnalités de réplication SnapMirror.

Développement et test d'applications (développement/test)

Pour accélérer le développement d'applications, vous pouvez cloner rapidement les données répliquées au niveau du site de reprise après incident et les utiliser pour développer et tester des applications. La colocation des environnements de reprise après incident et de test et développement peut considérablement améliorer l'utilisation des installations de sauvegarde ou de reprise après incident. Les clones à la demande de test et développement fournissent autant de copies que nécessaire pour passer plus rapidement en production.

La technologie NetApp FlexClone permet de créer rapidement une copie en lecture-écriture d'un volume FlexVol de destination SnapMirror si vous souhaitez disposer d'un accès en lecture-écriture à la copie secondaire pour vérifier si toutes les données de production sont disponibles.

Procédez comme suit pour utiliser l'environnement de reprise sur incident afin d'effectuer des opérations de développement/test d'applications :

1. Faire une copie des données de production. Pour ce faire, créez une copie Snapshot d'application d'un volume sur site. La création de snapshots d'applications s'effectue en trois étapes : `Lock`, `Snap`, et `Unlock`.

   a. Mettez le système de fichiers en veille afin que les E/S soient suspendues et que les applications conservent leur cohérence. Toute application qui exécute le système de fichiers reste à l'état d'attente jusqu'à ce que la commande unquiesce soit émise à l'étape c. Les étapes a, b et c sont exécutées via un processus ou un workflow transparent qui n'affecte pas le SLA de l'application.

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
   ```

   Cette option demande que le système de fichiers spécifié soit bloqué à partir de nouvelles modifications. Tout processus tentant d'écrire dans le système de fichiers gelé est bloqué jusqu'à ce que le système de fichiers soit débloqué.

   b. Créez une copie Snapshot du volume sur site.

   ```
   A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
   hc_iscsi_vol -snapshot kamini
   ```

   c. Annulez la mise en veille du système de fichiers pour redémarrer les E/S.

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
   ```

   Cette option est utilisée pour annuler le gel du système de fichiers et permettre aux opérations de continuer. Toutes les modifications du système de fichiers bloquées par le gel sont débloqués et autorisées à se terminer.

   Les copies Snapshot cohérentes au niveau des applications peuvent également être effectuées à l'aide de NetApp SnapCenter, qui dispose de l'orchestration complète du flux de travail décrit ci-dessus dans le cadre de SnapCenter. Pour plus d'informations, reportez-vous à la section "ici".

2. Effectuez une opération de mise à jour de SnapMirror pour maintenir la synchronisation des systèmes de production et de reprise après incident.

   ```
   singlecvoaws::> snapmirror update -destination-path
   svm_singlecvoaws:hc_iscsi_vol_copy -source-path
   Healthcare_SVM:hc_iscsi_vol

   Operation is queued: snapmirror update of destination
   "svm_singlecvoaws:hc_iscsi_vol_copy".
   ```

   Une mise à jour de SnapMirror peut également être effectuée via l'interface graphique BlueXP sous l'onglet **Replication**.

3. Créez une instance FlexClone à partir du snapshot d'application pris précédemment.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

Pour la tâche précédente, un nouvel instantané peut également être créé, mais vous devez suivre les mêmes étapes que ci-dessus pour assurer la cohérence des applications.

4. Activez un volume FlexClone pour afficher l'instance EHR dans le cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. Exécuter les commandes suivantes sur l'instance EHR dans le cloud pour accéder aux données ou au système de fichiers.
   a. Découvrez le stockage ONTAP. Vérifiez l'état des chemins d'accès multiples.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. Activer le groupe de volumes.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. Montez le système de fichiers et affichez le résumé des informations du système de fichiers.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

L’environnement de reprise d’activité est valide pour le développement et les tests d’applications. Les opérations de développement/test d’applications sur votre système de stockage de reprise après incident vous permettent d’exploiter davantage les ressources qui restent inactives la plupart du temps.

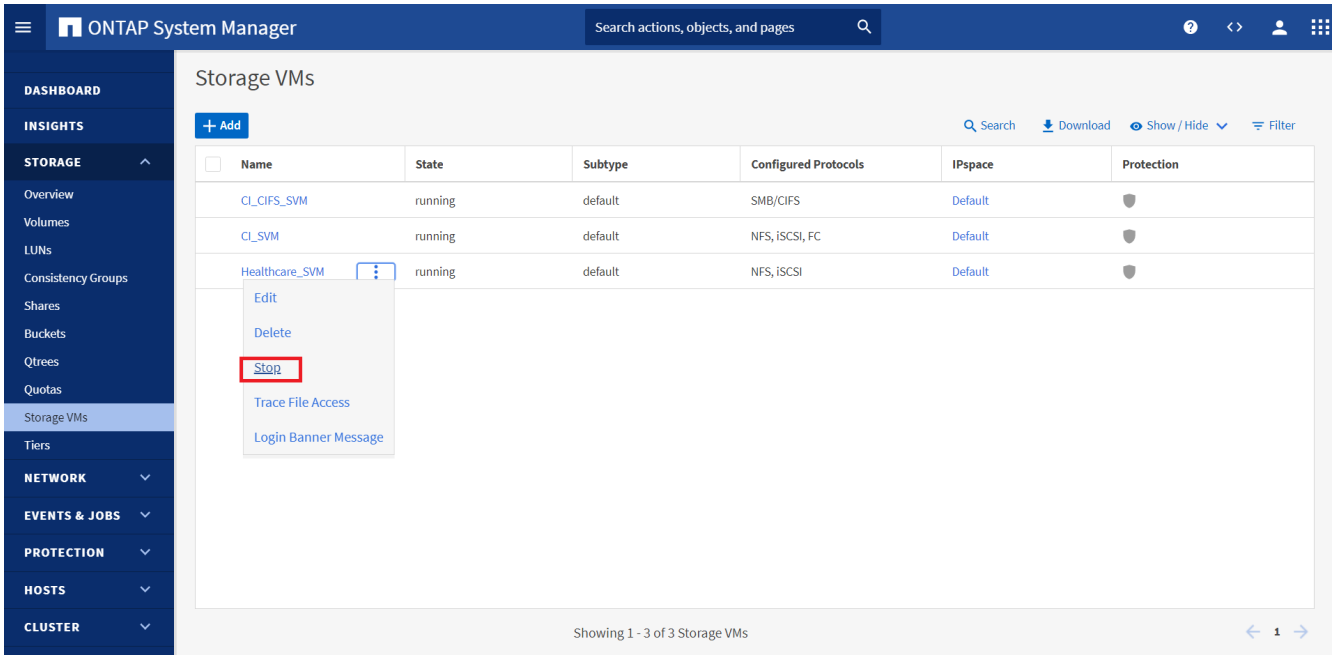
Reprise après incident

La technologie SnapMirror est également utilisée dans le cadre des plans de reprise d'activité. Si les données stratégiques sont répliquées vers un autre emplacement physique, un incident grave n'est pas nécessairement à l'origine de périodes prolongées d'indisponibilité des données pour les applications stratégiques. Les clients peuvent accéder aux données répliquées sur le réseau jusqu'à ce que le site de production soit corrompu, supprimé accidentellement, endommagé, etc.

En cas de restauration sur le site primaire, SnapMirror constitue un moyen efficace de resynchroniser le site de reprise d'activité avec le site primaire, en transférant uniquement les données nouvelles ou modifiées vers le site primaire à partir du site de reprise d'activité, simplement en inversant la relation SnapMirror. Une fois que le site de production principal a repris les opérations normales de l'application, SnapMirror poursuit le transfert vers le site de reprise après incident sans nécessiter un autre transfert de base.

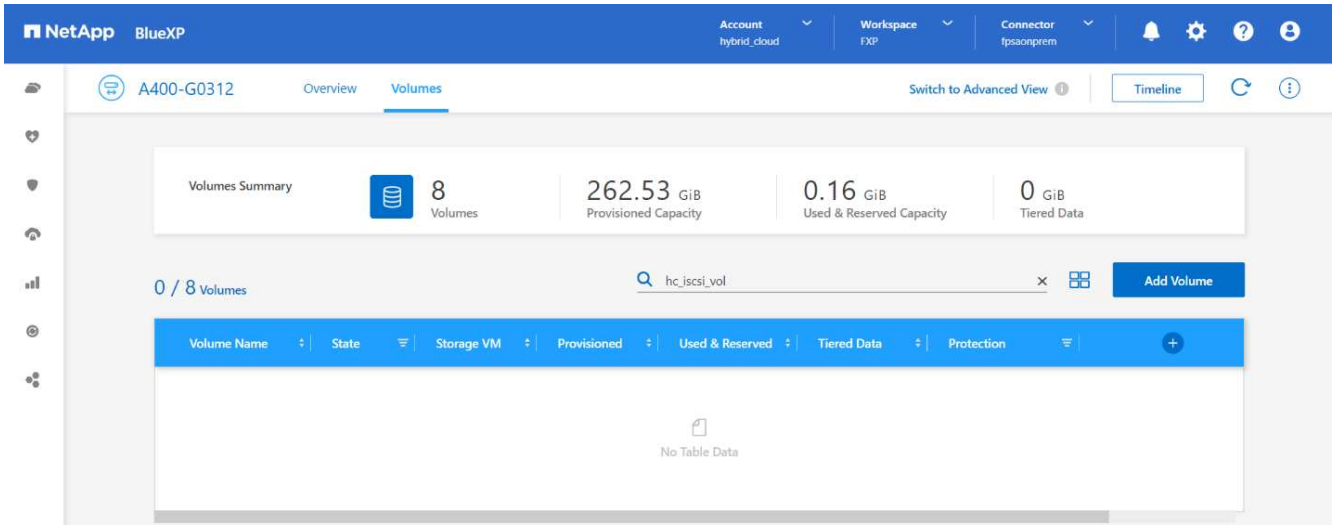
Pour effectuer la validation d'un scénario DR réussi, procédez comme suit :

1. Simuler un incident côté source (production) en arrêtant le SVM qui héberge le volume ONTAP sur site (`hc_iscsi_vol`).



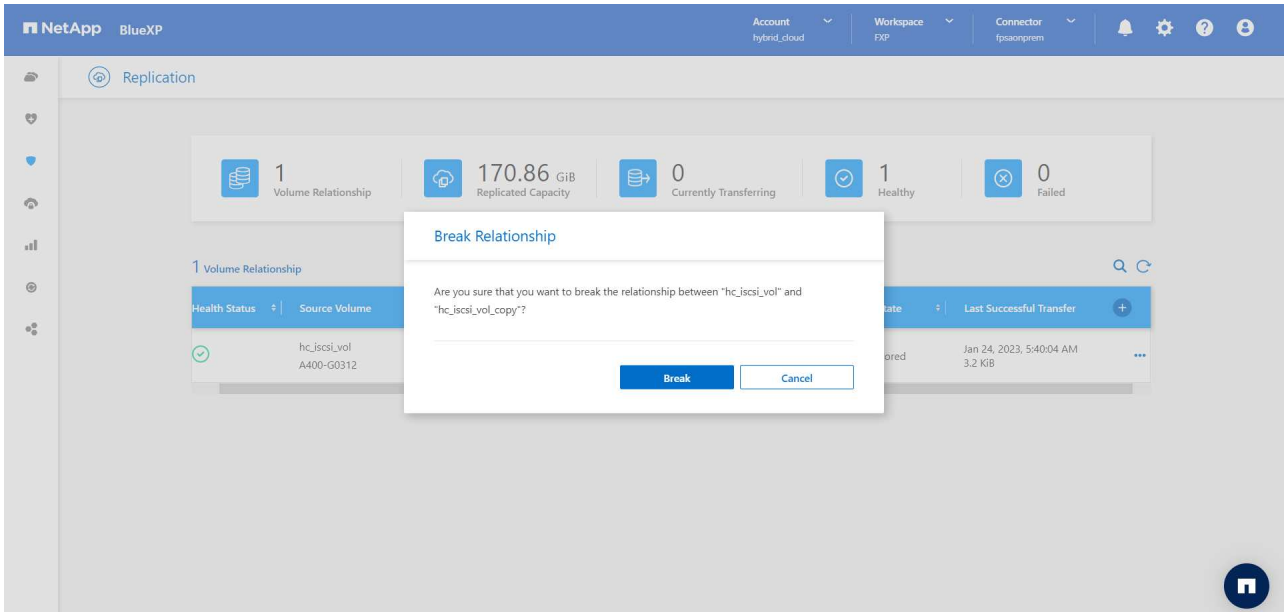
Assurez-vous que la réplication SnapMirror est déjà configurée entre l'ONTAP sur site dans l'instance FlexPod et Cloud Volumes ONTAP dans AWS, afin de pouvoir créer fréquemment des copies Snapshot d'application.

Après l'arrêt du SVM, le `hc_iscsi_vol` Le volume n'est pas visible dans BlueXP.



2. Activer la reprise sur incident dans CVO.

   a. Rompez la relation de réplication SnapMirror entre ONTAP sur site et Cloud Volumes ONTAP et gérez le volume de destination CVO (`hc_iscsi_vol_copy`) à la production.



   Une fois la relation SnapMirror rompue, le type de volume de destination passe de la protection des données (DP) à la lecture/écriture (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume              type
--------------- ------------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Activez le volume de destination dans Cloud Volumes ONTAP pour afficher l'instance EHR sur une instance EC2 dans le cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. Pour accéder aux données et au système de fichiers sur l'instance EHR dans le cloud, commencez par découvrir le stockage ONTAP et vérifiez l'état des chemins d'accès multiples.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. Activez ensuite le groupe de volumes.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

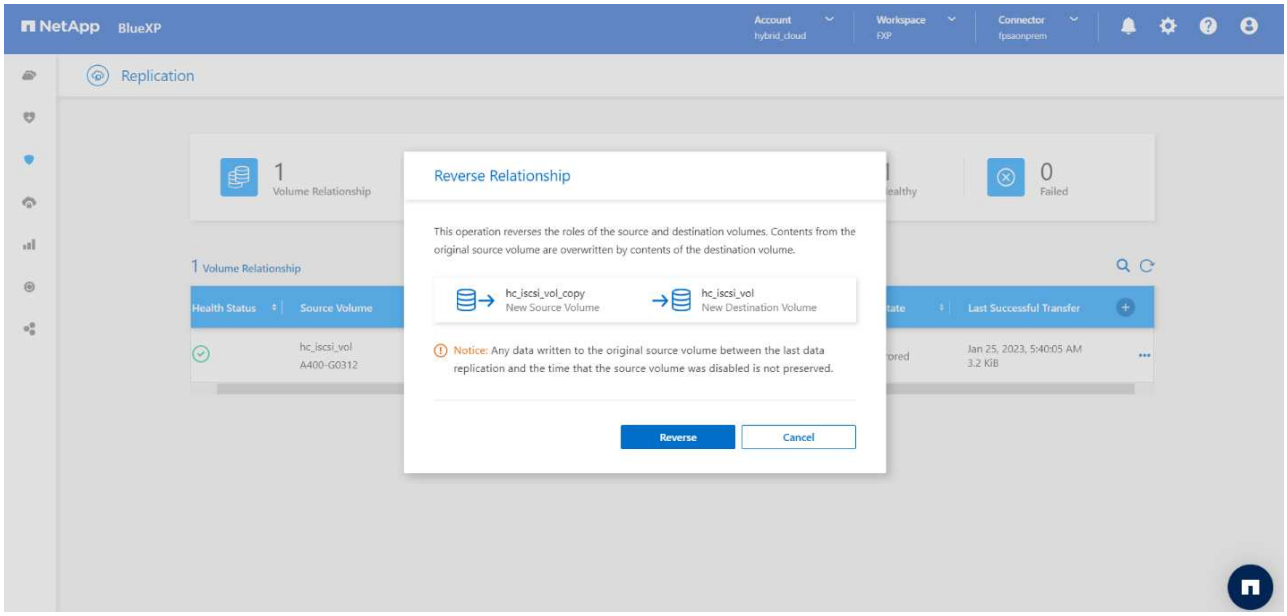
e. Enfin, montez le système de fichiers et affichez les informations sur le système de fichiers.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

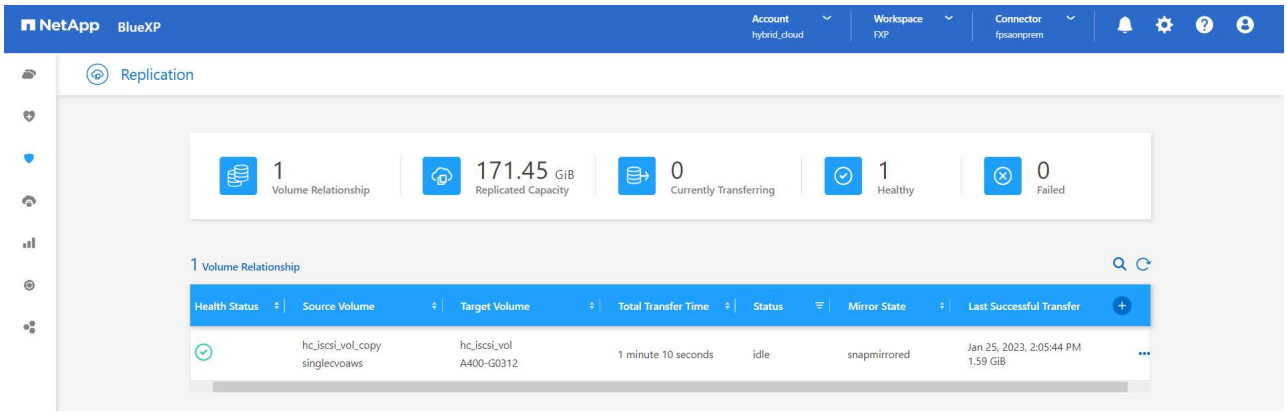
Ce résultat indique que les utilisateurs peuvent accéder aux données répliquées sur le réseau jusqu'à ce que le site de production soit récupéré après sinistre.

f. Inverser la relation SnapMirror. Cette opération inverse les rôles des volumes source et de destination.



Lorsque cette opération est effectuée, le contenu du volume source d'origine est écrasé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne.

Désormais, le volume CVO (`hc_iscsi_vol_copy`) devient le volume source et le volume sur site (`hc_iscsi_vol`) devient le volume de destination.



Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle le volume source a été désactivé ne sont pas conservées.

a. Pour vérifier l'accès en écriture au volume CVO, créez un nouveau fichier sur l'instance EHR dans le cloud.

```
cd /file1/
sudo touch newfile
```

Lorsque le site de production est en panne, les clients peuvent toujours accéder aux données et effectuer des écritures sur le volume Cloud Volumes ONTAP, qui est désormais le volume source.

En cas de restauration sur le site primaire, SnapMirror constitue un moyen efficace de resynchroniser le site de reprise d'activité avec le site primaire, en transférant uniquement les données nouvelles ou modifiées vers le site primaire à partir du site de reprise d'activité, simplement en inversant la relation SnapMirror. Une fois que le site de production principal a repris les opérations normales de l'application, SnapMirror poursuit le transfert vers le site de reprise après incident sans nécessiter un autre transfert de base.

Cette section illustre la résolution d'un scénario de reprise après incident lorsque le site de production est touché par un incident. Les données peuvent désormais être consommées en toute sécurité par des applications qui peuvent désormais servir les clients pendant que le site source effectue une restauration.

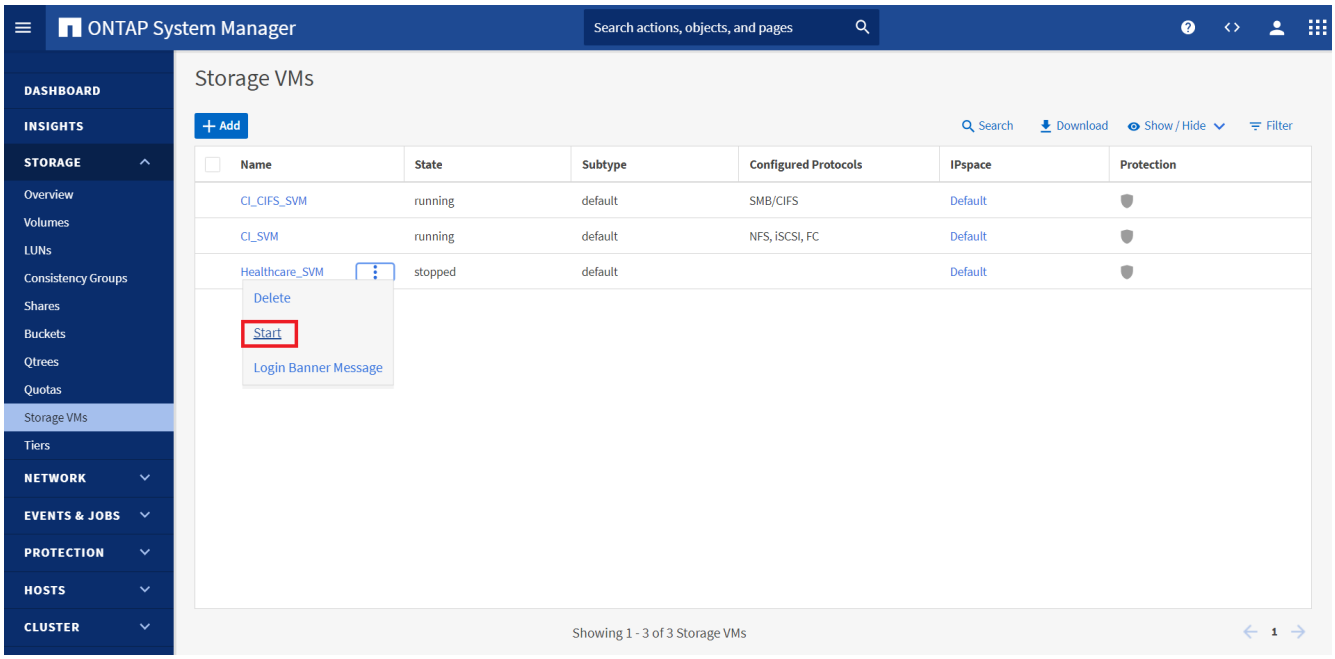
Vérification des données sur le site de production

Une fois le site de production restauré, vous devez vous assurer que la configuration d'origine est restaurée et que les clients peuvent accéder aux données à partir du site source.

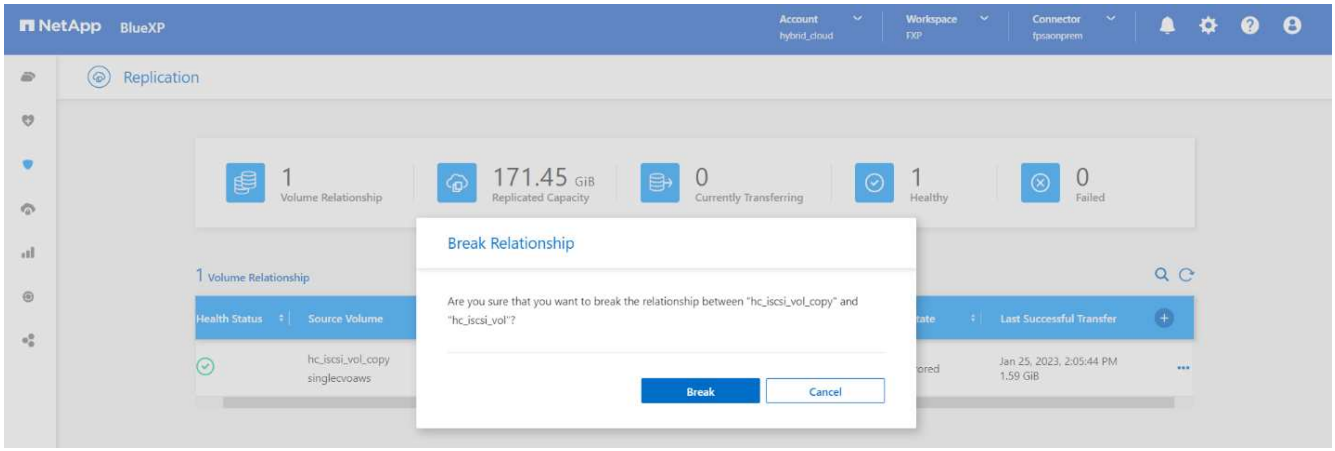
Dans cette section, nous abordons l'accès au site source et la restauration de la relation SnapMirror entre ONTAP sur site et Cloud Volumes ONTAP, puis nous avons enfin effectué un contrôle d'intégrité des données à l'extrémité source

La procédure suivante peut être utilisée pour la vérification des données sur le site de production :

1. Assurez-vous que le site source est maintenant en service. Pour ce faire, démarrer le SVM qui héberge le volume ONTAP sur site (`hc_iscsi_vol`).



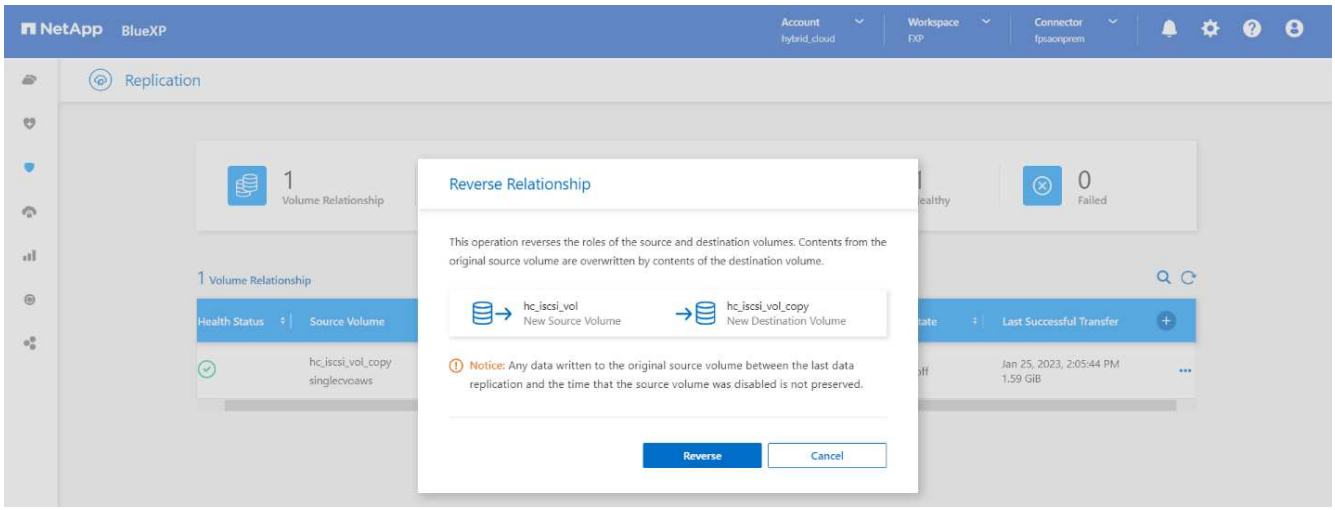
2. Rompre la relation de réplication SnapMirror entre Cloud Volumes ONTAP et ONTAP sur site et promouvoir le volume sur site (`hc_iscsi_vol`) de retour à la production.



Une fois la relation SnapMirror rompue, le type de volume sur site passe de la protection des données (DP) à la lecture/écriture (RW).

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver        volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. Inverser la relation SnapMirror. Désormais, le volume ONTAP sur site (`hc_iscsi_vol`) Devient le volume source tel qu'il était précédemment, et le volume Cloud Volumes ONTAP (`hc_iscsi_vol_copy`) devient le volume de destination.



En suivant ces étapes, nous avons réussi à restaurer la configuration d'origine.

4. Redémarrez l'instance EHR sur site. Montez le système de fichiers et vérifiez que `newfile` Que vous avez créé sur l'instance EHR dans le cloud lorsque la production a été hors service existe également dans ce domaine.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37  dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

Nous pouvons déduire que la réplication des données de la source vers la destination a été effectuée avec succès et que l'intégrité des données a été préservée. La vérification des données sur le site de production est terminée.

"Suivant: Conclusion."

Conclusion

"Précédent : validation de la solution."

La création d'un cloud hybride est un objectif pour la plupart des établissements de santé : garantir la disponibilité des données à tout moment. Dans cette solution, nous avons mis en œuvre une solution de cloud hybride FlexPod avec Cloud Volumes ONTAP, en utilisant la technologie de réplication NetApp SnapMirror pour valider certains cas d'utilisation afin de sauvegarder et de restaurer les applications et les charges de travail de santé.

FlexPod, une infrastructure convergée rigoureusement testée et prévalidée issue d'un partenariat stratégique entre Cisco et NetApp, est conçue pour fournir des performances système prévisibles à faible latence et une haute disponibilité. Cette approche se traduit par des niveaux de confort élevés pour les DME et, à terme, par le meilleur temps de réponse pour les utilisateurs du système EHR.

Avec NetApp, vous pouvez exécuter des opérations de production EHR, de reprise d'activité, de sauvegarde ou de Tiering dans le cloud, comme si vous exécutiez des fonctionnalités de stockage NetApp dans un data Center sur site. Avec NetApp Cloud Volumes ONTAP, NetApp fournit les fonctionnalités de grande qualité et les performances requises pour exécuter efficacement les dossiers EHR dans le cloud. Options cloud de

NetApp pour l'utilisation de blocs sur iSCSI et de fichiers sur NFS ou SMB.

Cette solution répond aux besoins des établissements de santé et leur permet de franchir le pas vers leur transformation digitale. Il peut également les aider à gérer efficacement leurs applications et leurs charges de travail.

"Suivant : où trouver des informations supplémentaires ?"

Où trouver des informations complémentaires

"Précédent: Conclusion."

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

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- Démarrage rapide de Cloud Volumes ONTAP dans AWS

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- Réplication SnapMirror

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- Tr-3928 : meilleures pratiques NetApp pour Epic

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- Tr-4693 : Guide de déploiement du data Center FlexPod pour les DME EPIC

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod pour Epic

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- Matrice d'interopérabilité NetApp

"http://support.netapp.com/matrix/"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Mars 2023	Version initiale

FlexPod Cloud hybride pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

Tr-4939 : Cloud hybride FlexPod pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

Ruchika Lahoti, NetApp

Introduction

L'objectif de protection des données avec reprise après incident est essentiel à la continuité de l'activité. La reprise d'activité permet aux entreprises de basculer leurs opérations sur un emplacement secondaire, puis de restaurer et de rétablir leur fonctionnement vers le site primaire de manière efficace et fiable. Le développement d'une stratégie de reprise après incident est une priorité IT si l'on persiste avec plusieurs problèmes tels que les catastrophes naturelles, les défaillances réseau, les vulnérabilités logicielles et les erreurs humaines.

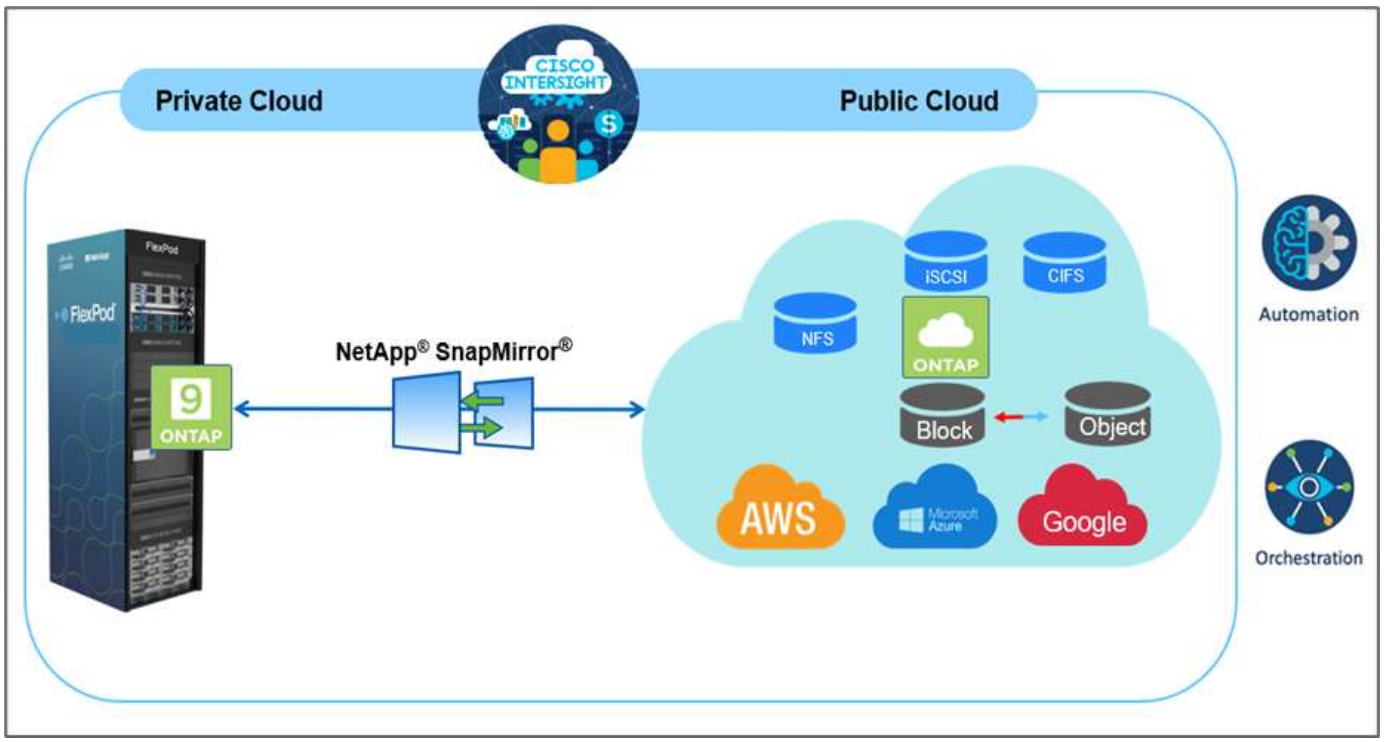
Pour la reprise après incident, toutes les charges de travail exécutées sur le site primaire doivent être fidèlement reproduites sur le site de DR. Une entreprise doit également disposer d'une copie à jour de toutes les données d'entreprise, y compris la base de données, les services de fichiers, le stockage NFS et iSCSI, etc. Comme les données de l'environnement de production sont constamment mises à jour, les modifications doivent être régulièrement transférées vers le site de reprise.

Néanmoins, pour la plupart des entreprises, déployer de tels environnements de reprise est difficile à concilier avec les exigences d'indépendance de l'infrastructure et du site. Le nombre de ressources requises et les coûts de configuration, de test et de maintenance d'un data Center secondaire peuvent être très élevés, ce qui approche généralement du coût de l'ensemble de l'environnement de production. Il est difficile de minimiser l'empreinte des données avec une protection adéquate, tout en synchronisant les données en continu et en établissant des basculements et des rétablissements transparents. Une fois le site de reprise créé, un autre défi se présente : répliquer les données depuis l'environnement de production et les synchroniser dans la suite.

Ce rapport technique rassemble la solution d'infrastructure convergée FlexPod, NetApp Cloud Volumes ONTAP sur Google Cloud et Cisco Intersight pour former un data Center dans le cloud hybride pour la reprise après incident. Dans cette solution, nous abordons la conception et l'exécution d'un workflow ONTAP sur site à l'aide de Cisco Intersight Cloud Orchestrator. Nous discutons également du déploiement de NetApp Cloud

Volumes ONTAP et de l'orchestration et l'automatisation de la réplication et de la reprise après incident des données entre FlexPod et Cloud Volumes ONTAP à l'aide du service Cisco Intersight pour HashiCorp Terraform.

Le schéma suivant fournit une présentation de la solution.



Cette solution offre de nombreux avantages, notamment :

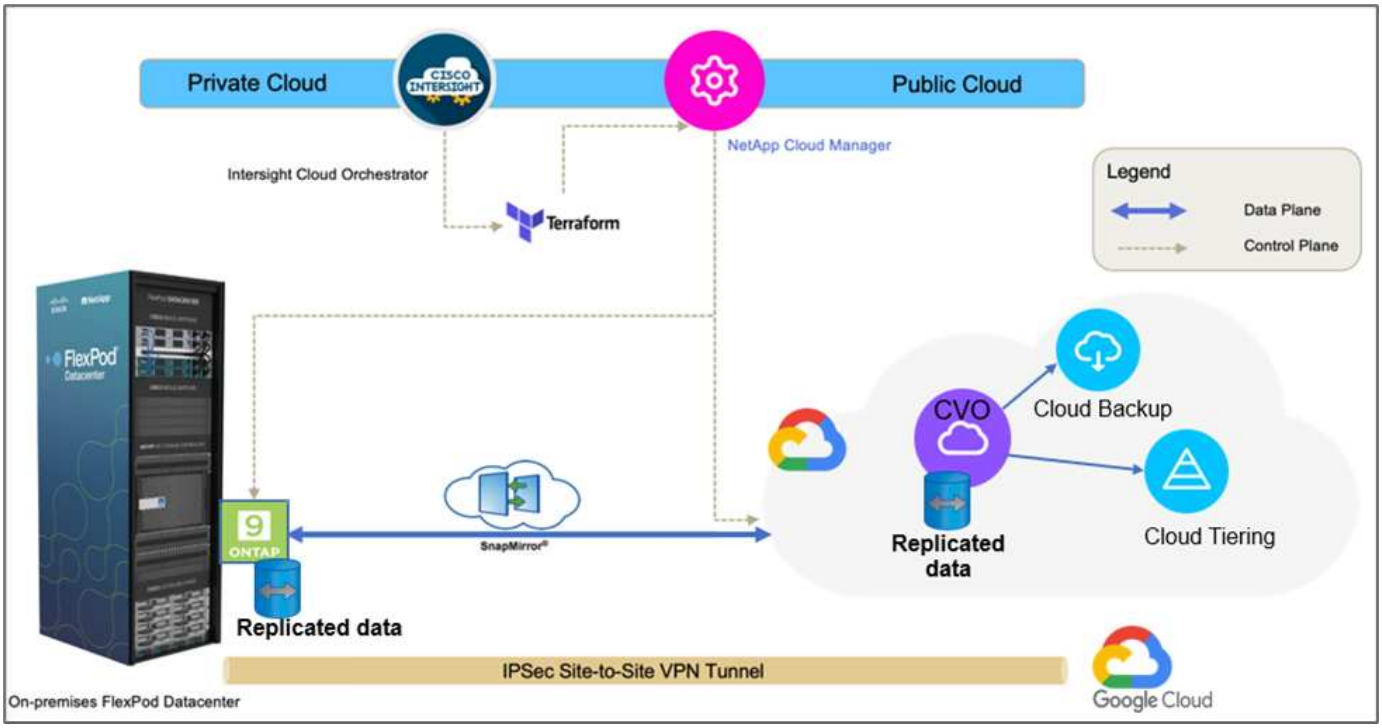
- **Orchestration et automatisation.** Cisco Intersight simplifie les opérations quotidiennes de l'infrastructure de cloud hybride FlexPod en fournissant des frameworks d'orchestration cohérents qui sont proposés via l'automatisation.
- **Protection personnalisée.** Cloud Volumes ONTAP assure la réplication des données au niveau des blocs depuis ONTAP vers le cloud afin de maintenir la destination à jour grâce à des mises à jour incrémentielles. Les utilisateurs peuvent spécifier une planification de synchronisation toutes les 5 minutes ou toutes les heures, par exemple, en fonction des modifications de la source qui sont transférées.
- **Basculement et retour arrière transparents** en cas d'incident, les administrateurs du stockage peuvent rapidement basculer vers les volumes cloud. Lorsque le site primaire est restauré, les nouvelles données créées dans l'environnement de reprise sont resynchronisées sur les volumes source et re-établissent la réplication secondaire.
- **Efficacité :** l'espace de stockage et les coûts pour la copie cloud secondaire sont optimisés grâce à la compression des données, au provisionnement fin et à la déduplication. Les données sont transférées au niveau du bloc sous forme compressée et dédupliquée, ce qui accélère le transfert. Ainsi, les données sont automatiquement transférées vers un stockage objet à faible coût et sont transférées vers un stockage haute performance uniquement lors des accès, comme dans un scénario de reprise après incident. Ceci réduit considérablement les coûts réguliers de stockage.
- * Augmentation de la productivité INFORMATIQUE.* l'utilisation d'Intersight comme plate-forme d'entreprise unique et sécurisée pour la gestion du cycle de vie de l'infrastructure et des applications simplifie la gestion de la configuration et l'automatisation des tâches manuelles à grande échelle pour la solution.

Public

Le public visé peut inclure, sans s'y limiter, les ingénieurs commerciaux, les consultants sur le terrain, les services professionnels, les responsables INFORMATIQUES, Ingénieurs partenaires, ingénieurs de fiabilité des sites, architectes cloud, ingénieurs cloud et clients qui souhaitent exploiter une infrastructure conçue pour optimiser l'efficacité IT et favoriser l'innovation IT.

Topologie de la solution

Cette section décrit la topologie logique de la solution. La figure ci-dessous illustre la topologie de la solution de l'environnement FlexPod sur site, de NetApp Cloud Volumes ONTAP exécuté sur Google Cloud, Cisco Intersight et NetApp Cloud Manager.



Les plans de contrôle et les plans de données sont clairement indiqués entre les points d'extrémité. Le plan de données utilise une connexion VPN site à site sécurisée pour connecter l'instance ONTAP exécutée sur FlexPod FAS 100 % Flash à l'instance NetApp Cloud Volumes ONTAP sur Google Cloud.

La réplication des données de charge de travail de FlexPod vers NetApp Cloud Volumes ONTAP est gérée par NetApp SnapMirror. Le processus global est orchestré à l'aide de Cisco Intersight Cloud Orchestrator pour les environnements sur site et cloud. Cisco Intersight Cloud Orchestrator utilise les fournisseurs de ressources Terraform pour NetApp Cloud Manager pour effectuer des opérations liées au déploiement de NetApp Cloud Volumes ONTAP et établir des relations de réplication des données.

Cette solution prend également en charge la sauvegarde et le Tiering des données inactives résidant dans l'instance NetApp Cloud Volumes ONTAP vers Google Cloud Storage.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS et Cisco Unified Computing System (Cisco UCS). La conception est suffisamment flexible pour que le réseau, le calcul et le stockage puissent s'intégrer dans un seul rack de data Center ou être déployés selon la conception du centre de données du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme permet de stimuler les évolutions avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride. Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** livraison en tant que service depuis le cloud ou dans le centre de données du client avec des mises à jour fréquentes et une innovation continue, grâce à un modèle de développement logiciel agile. Le client peut ainsi se concentrer sur l'accélération de la livraison pour le secteur d'activité.
- **Opérations simplifiées.** simplifier les opérations en utilisant un seul outil SaaS sécurisé avec inventaire, authentification et API communs pour travailler sur l'ensemble de la pile et tous les emplacements, éliminant ainsi les silos entre les équipes. De la gestion des serveurs physiques et des hyperviseurs sur site aux machines virtuelles, K8s, sans serveur, automatisation, l'optimisation et le contrôle des coûts à la fois sur site et dans les clouds publics.
- **Optimisation continue.** optimisation continue de votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur chaque couche, ainsi que Cisco TAC. Cette intelligence est convertie en actions recommandées et automatisés, qui vous permettent de vous adapter en temps réel à chaque changement : du déplacement des charges de travail et du contrôle de l'état des serveurs physiques aux recommandations de réduction des coûts des clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner UMM natif ou IMM pour les systèmes Cisco UCS rattachés au fabric lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'IMM native est utilisé.

Licences Cisco Intersight

Cisco Intersight utilise une licence basée sur un abonnement avec plusieurs niveaux.

Les niveaux de licence Cisco Intersight sont les suivants :

- **Cisco Intersight Essentials.** inclut toutes les fonctionnalités de base ainsi que les fonctionnalités suivantes :
  - Cisco UCS Central
  - Droit Cisco IMC Supervisor
  - Configuration basée sur des règles avec profils de serveur
  - Gestion du firmware
  - Évaluation de la compatibilité avec la liste de compatibilité matérielle (HCL)
- **Cisco Intersight Advantage.** comprend les fonctionnalités du niveau Essentials ainsi que les fonctionnalités suivantes :
  - Widgets, inventaire, capacité, fonctionnalités d'utilisation et corrélation des inventaires interdomaines

sur l'ensemble des ressources de calcul physique, réseau, stockage, virtualisation VMware et cloud public AWS.

    - Service de conseil de sécurité Cisco où les clients peuvent recevoir d'importantes alertes de sécurité et des notifications sur site sur les périphériques de point final affectés.

- **Cisco Intersight Premier.** en plus des capacités offertes par le niveau avantage, Cisco Intersight Premier propose les éléments suivants :
    - Intersight Cloud Orchestrator (ICO) pour les ressources de calcul, de réseau, de stockage, de systèmes intégrés, de virtualisation, des plateformes de conteneur et de cloud public
    - Droit d'abonnement complet pour Cisco UCS Director sans frais supplémentaires.

Vous trouverez plus d'informations sur les licences Intersight et les fonctionnalités prises en charge dans chaque licence "ici".

Dans cette solution, nous utilisons Intersight Cloud Orchestrator et Intersight Service pour HashiCorp Terraform. Ces fonctionnalités sont disponibles pour les utilisateurs disposant de la licence Intersight Premier. Par conséquent, ce niveau de licence doit être activé.

Intégration du cloud Terraform avec ICO

Vous pouvez utiliser Cisco Intersight Cloud Orchestrator (ICO) pour créer et exécuter des workflows qui appellent les API Terraform Cloud (TFC). La tâche Invoke Web API Request prend en charge Terraform Cloud comme cible et peut être configurée avec les API Terraform Cloud via des méthodes HTTP. Le workflow peut donc avoir une combinaison de tâches qui appellent plusieurs API Terraform Cloud à l'aide de tâches API génériques et d'autres opérations. Vous devez disposer d'une licence Premier pour utiliser la fonction ICO.

Assistance Cisco Intersight

Cisco Intersight aide à ajouter des périphériques de terminaison à Cisco Intersight. Un centre de données peut avoir plusieurs périphériques qui ne se connectent pas directement à Cisco Intersight. Tout périphérique pris en charge par Cisco Intersight mais qui ne se connecte pas directement à celui-ci nécessite un mécanisme de connexion. Cisco Intersight fournit ce mécanisme de connexion et vous aide à ajouter des périphériques à Cisco Intersight.

Cisco Intersight Assist est disponible au sein de Cisco Intersight Virtual Appliance, qui est distribué sous la forme d'une machine virtuelle déployable contenue dans un format de fichier OVA (Open Virtual Appliance). Vous pouvez installer l'appliance sur un serveur ESXi. Pour plus d'informations, reportez-vous à la section "Guide de mise en route de Cisco Intersight Virtual Appliance".

Après avoir réclamé Intersight Assist dans Intersight, vous pouvez demander des périphériques de terminaison à l'aide de l'option réclamation via Intersight Assist. Pour plus d'informations, voir "Mise en route".

NetApp Cloud Volumes ONTAP

- Exploitation de la déduplication intégrée et de la compression des données, du provisionnement fin et du clonage pour réduire les coûts de stockage.
- Nous garantissons une fiabilité exceptionnelle et la continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Cloud Volumes ONTAP utilise la technologie de réplication leader de NetApp SnapMirror pour répliquer les données sur site vers le cloud. Les copies secondaires sont ainsi disponibles dans différents cas d'utilisation.
- Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de

sauvegarde et de restauration pour une protection et un archivage à long terme de vos données cloud.

- Basculer à la demande entre des pools de stockage hautes performances et faibles performances, sans mettre les applications hors ligne.
- Cohérence des copies Snapshot avec NetApp SnapCenter.
- Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.
- L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

Cloud Central

Cloud Central est une plateforme centralisée qui permet d'accéder aux services de données cloud NetApp et de les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites de reprise après incident automatisés, de sauvegarder vos données SaaS et de migrer et contrôler efficacement les données sur plusieurs clouds. Pour plus d'informations, voir "Cloud Central".

Le gestionnaire Cloud

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions cloud NetApp. Elle offre un système centralisé pour afficher et gérer vos ressources de stockage sur site et cloud afin de prendre en charge plusieurs fournisseurs et comptes de cloud hybride. Pour plus d'informations, voir "Le gestionnaire Cloud".

Connecteur

Connector permet à Cloud Manager de gérer les ressources et les processus dans un environnement de cloud public. Une instance de connecteur est requise pour utiliser de nombreuses fonctionnalités fournies par Cloud Manager et peut être déployée dans le réseau dans le cloud ou sur site. Le connecteur est pris en charge aux emplacements suivants :

- AWS
- Microsoft Azure
- Google Cloud
- Sur site

NetApp Active IQ Unified Manager

Avec NetApp Active IQ Unified Manager, vous pouvez contrôler vos clusters de stockage ONTAP à partir d'une interface intuitive unique, reconçue pour l'intelligence artificielle et les connaissances de la communauté. Il offre des informations complètes sur les opérations, les performances et le mode proactif de l'environnement de stockage et des machines virtuelles qui s'exécutent sur celui-ci. Lorsqu'un problème se produit avec l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre un aperçu des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte vSphere vers le réseau, et enfin vers le stockage.

Certains événements fournissent également des mesures correctives que vous pouvez prendre pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et des interruptions SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en anticipant les besoins en stockage et

en vous permettant d'anticiper les problèmes, ce qui évite de prendre des décisions réactives à court terme et même d'engendrer des problèmes supplémentaires à long terme.

VMware vSphere

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière holistique de vastes ensembles d'infrastructures (ressources notamment les processeurs, le stockage et le réseau), sous la forme d'un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation traditionnels qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un data Center dans son ensemble pour créer une seule puissance avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application, selon les besoins.

Pour plus d'informations sur VMware vSphere, veuillez suivre "ce lien".

VMware vSphere vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Versions matérielles et logicielles

Cette solution de cloud hybride peut être étendue à tout environnement FlexPod qui exécute des versions logicielles, matérielles et de firmware prises en charge telles que définies dans la matrice d'interopérabilité NetApp et dans la liste de compatibilité matérielle Cisco UCS.

La solution FlexPod utilisée comme plateforme de base dans notre environnement sur site a été déployée selon les instructions et les spécifications décrites "ici".

Le réseau au sein de cet environnement est basé sur l'ACI. Pour plus d'informations, voir "ici".

- Consultez les liens suivants pour plus d'informations :
- "Matrice d'interopérabilité NetApp"
- "Guide de compatibilité VMware"
- "Outil d'interopérabilité matérielle et logicielle Cisco UCS"

Le tableau suivant présente les révisions matérielles et logicielles de FlexPod.

Composant	Solution NetApp	Version
Calcul	CISCO UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric Interconnect 6454	4.2(2a)
Le réseau	Cisco Nexus 9332C (Rachis)	14.2(7)
	Cisco Nexus 9336C-FX2 (feuille)	14.2(7)
	ACI Cisco	4.2(7)
Stockage	Avec AFF A220	9.11.1

Composant	Solution NetApp	Version
	Outils NetApp ONTAP pour VMware vSphere	9.10
	Plug-in NetApp NFS pour VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
Logiciel	VSphere ESXi	7.0(U3)
	Appliance VMware vCenter	7.0.3
	Appliance virtuelle Cisco InterSight Assist	1.0.11-306

L'exécution des configurations Terraform s'effectue sur le compte Terraform Cloud for Business. La configuration Terraform utilise le fournisseur Terraform pour NetApp Cloud Manager.

Le tableau suivant répertorie les fournisseurs, les produits et les versions.

Composant	Solution NetApp	Version
HashiCorp	Terraform	1.2.7

Le tableau suivant présente les versions de Cloud Manager et de Cloud Volumes ONTAP.

Composant	Solution NetApp	Version
NetApp	Cloud Volumes ONTAP	9.11
	Le gestionnaire Cloud	3.9.21

"Suivant : installation et configuration - déployer FlexPod."

Installation et configuration

Déployez FlexPod

"Précédent : composants de la solution."

Pour comprendre les détails de la conception et du déploiement de FlexPod, notamment la configuration de différents éléments de la conception et des meilleures pratiques associées, consultez la section "Conceptions validées par Cisco pour FlexPod".

FlexPod peut être déployé à la fois en mode géré UCS et en mode géré Cisco InterSight. Si vous déployez FlexPod en mode géré UCS, vous trouverez la dernière conception validée Cisco "ici".

Cisco Unified Computing System (Cisco UCS) X-Series est un tout nouveau système de calcul modulaire, configuré et géré à partir du cloud. Elle est conçue pour répondre aux besoins des applications modernes et pour améliorer l'efficacité opérationnelle, l'agilité et l'évolutivité au travers d'un design modulaire, adaptable et prêt pour le futur. Vous trouverez des conseils de conception concernant l'intégration de la plateforme UCS X-Series gérée par Cisco Intersight dans l'infrastructure FlexPod "ici".

FlexPod avec Cisco ACI est disponible "ici".

"Suivant : configuration Cisco Intersight."

Configuration Cisco Intersight

"Précédent : déployer FlexPod."

Pour configurer Cisco Intersight et Intersight, consultez les conceptions validées par Cisco pour FlexPod trouvées "ici".

"Suivant : intégration du cloud Terraform avec la condition préalable d'ICO."

Terraform intégration au cloud avec une condition préalable de l'ICO

"Précédent : configuration Cisco Intersight."

Procédure 1 : connecter Cisco Intersight et Terraform Cloud

1. Faites une demande de remboursement ou créez une cible cloud Terraform en fournissant les informations pertinentes sur le compte Terraform Cloud.
2. Créez une cible Terraform Cloud Agent pour les clouds privés afin que les clients puissent installer l'agent dans le data Center et activer la communication avec Terraform Cloud.

   Pour plus d'informations, veuillez consulter la section "ce lien".

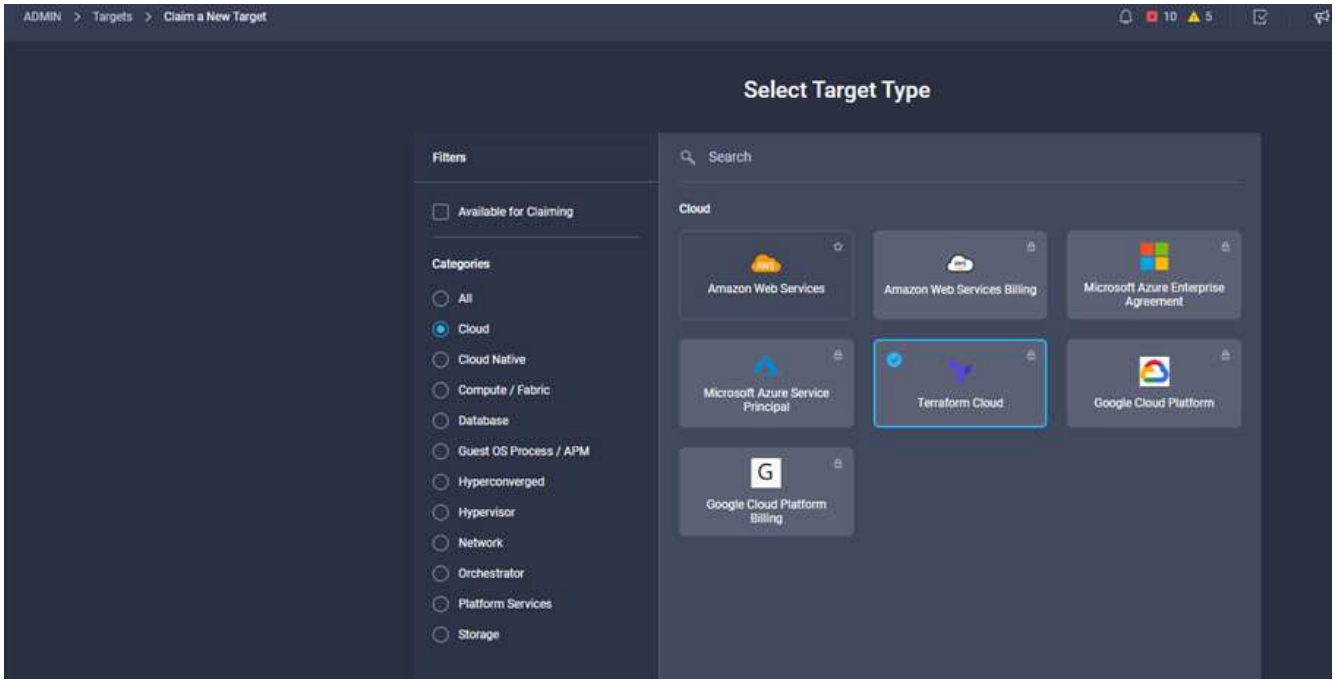
Procédure 2 : générer un jeton utilisateur

Dans le cadre de l'ajout d'une cible pour Terraform Cloud, vous devez fournir le nom d'utilisateur et le jeton d'API à partir de la page des paramètres Terraform Cloud.

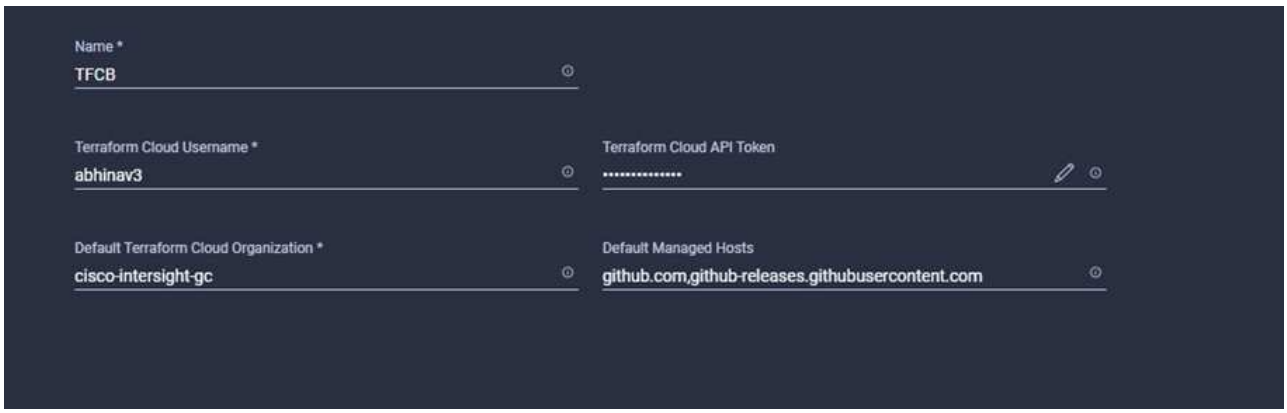
1. Connectez-vous à Terraform Cloud et accédez à **User Tokens** : "https://app.terraform.io/app/settings/tokens".
2. Cliquez sur **Créer un nouveau jeton API**.
3. Attribuez un nom à mémoriser et enregistrez le token dans un endroit sécurisé.

Procédure 3 : cible de cloud de demande Terraform

1. Connectez-vous à Intersight avec les privilèges Administrateur de compte, Administrateur de périphérique ou technicien de périphérique.
2. Accédez à **ADMIN > Targets > Claim a New Target**.
3. Dans **Categories**, cliquez sur **Cloud**.
4. Cliquez sur **Terraform Cloud** et cliquez sur **Start**.



5. Entrez un nom pour la cible, votre nom d'utilisateur pour le Terraform Cloud, le jeton API et une organisation par défaut dans Terraform Cloud comme indiqué dans l'image suivante.
6. Dans le champ **Default Managed Hosts**, assurez-vous d'ajouter les liens suivants avec d'autres hôtes gérés :
   - github.com
   - github-releases.githubusercontent.com



Si tout est correctement saisi, votre cible Terraform Cloud s'affiche dans la section **cibles Intersight**.

Procédure 4 : ajouter des agents Terraform Cloud

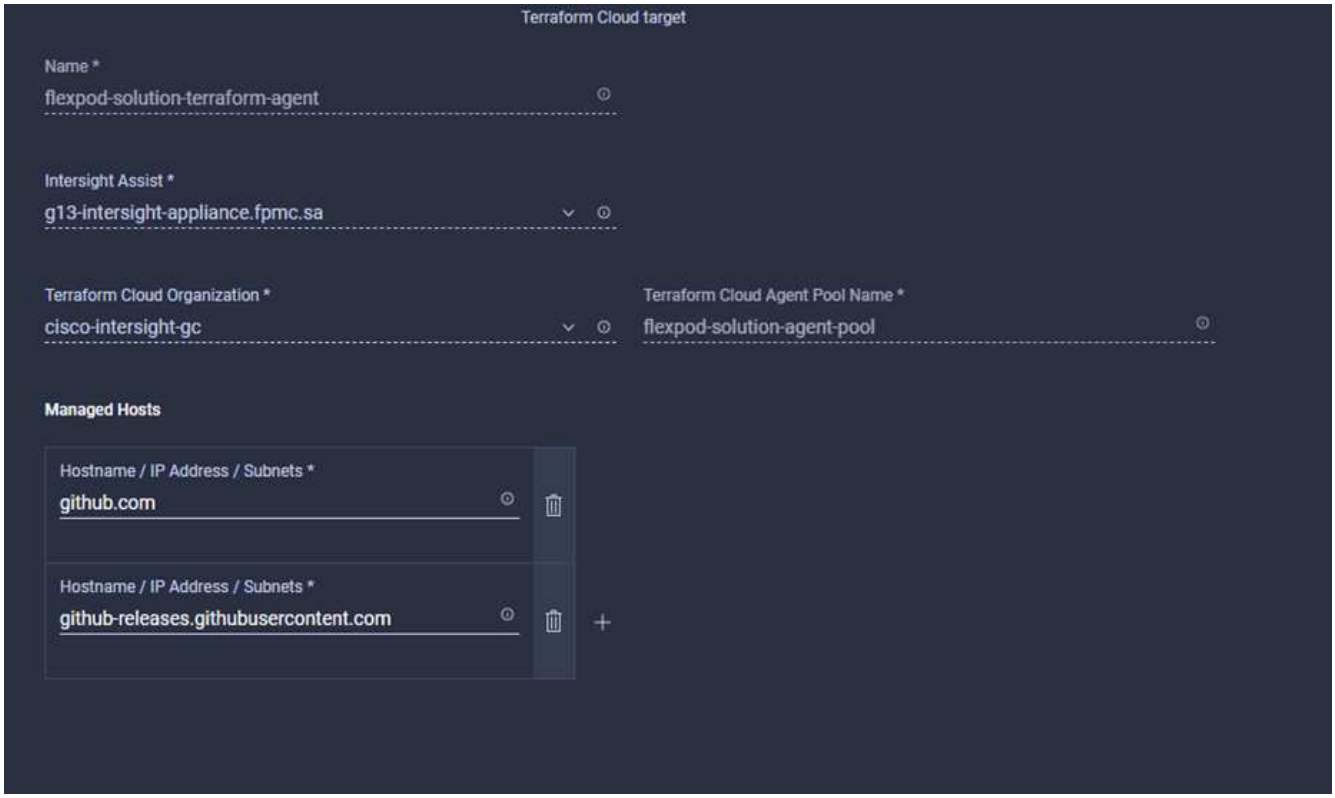
Prérequis :

- Cible Terraform Cloud.
- Demande d'assistance Intersight dans Intersight avant de déployer l'agent Cloud Terraform.

Vous ne pouvez demander que cinq agents pour chaque assistance.

Après avoir créé la connexion à Terraform, vous devez faire tourner un agent Terraform pour exécuter le code Terraform.

1. Cliquez sur **Claim Terraform Cloud Agent** dans la liste déroulante de votre cible Terraform Cloud.
2. Entrez les détails de l'agent Terraform Cloud. La capture d'écran suivante montre les détails de configuration de l'agent Terraform.



Vous pouvez mettre à jour n'importe quelle propriété Terraform Agent. Si la cible est à l'état **non connecté** et n'a jamais été à l'état **connecté**, alors aucun jeton n'a été généré pour l'agent Terraform.

Une fois la validation de l'agent réussie et qu'un jeton d'agent est généré, vous ne pouvez pas reconfigurer l'organisation et/ou le pool d'agents. Le déploiement réussi d'un agent Terraform est indiqué par l'état **Connected**.

Après avoir activé et demandé l'intégration Terraform Cloud, vous pouvez déployer un ou plusieurs agents Terraform Cloud dans Cisco InterSight Assist. L'agent Terraform Cloud est modélisé comme cible enfant de la cible Terraform Cloud. Lorsque vous demandez la cible de l'agent, un message s'affiche pour indiquer que la demande cible est en cours.

Au bout de quelques secondes, la cible est déplacée à l'état **Connected** et la plateforme Intersight achemine les paquets HTTPS de l'agent vers la passerelle Terraform Cloud.

Votre agent Terraform doit être correctement réclamé et s'afficher sous cibles comme **connecté**.

"Configuration du fournisseur de services clouds publics"

Configurez le fournisseur de services clouds publics

"Précédent : intégration du cloud Terraform avec la condition préalable d'ICO."

Procédure 1 : accéder à NetApp Cloud Manager

Pour accéder à NetApp Cloud Manager et aux autres services cloud, vous devez vous inscrire "NetApp Cloud Central".

> Pour configurer des espaces de travail et des utilisateurs sur le compte Cloud Central, cliquez sur "ici".

Procédure 2 : déployer le connecteur

Pour déployer Connector dans Google Cloud, rendez-vous ici "lien".

"Ensuite, déploiement automatisé du stockage NetApp dans le cloud hybride."

Déploiement automatisé du stockage de cloud hybride NetApp

"Précédent : configuration du fournisseur de services clouds publics."

Google Cloud

Vous devez d'abord activer des API et créer un compte de service qui fournit à Cloud Manager des autorisations pour déployer et gérer des systèmes Cloud Volumes ONTAP dans le même projet que celui du connecteur ou dans des projets différents.

Avant de déployer un connecteur dans un projet Google Cloud, vérifiez que ce connecteur ne s'exécute pas sur vos sites ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis Cloud Manager :

- Vous devez déployer Connector à l'aide d'un compte Google qui dispose d'autorisations pour lancer l'instance de VM Connector à partir de Cloud Manager.
- Lors du déploiement de Connector, vous êtes invité à sélectionner l'instance de VM. Cloud Manager obtient les autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.vous devez configurer deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. Découvrez comment utiliser "Les fichiers YAML pour configurer les autorisations" ici.

Voir "cette vidéo détaillée" pour tous les prérequis requis.

Architecture et modes de déploiement Cloud Volumes ONTAP

Cloud Volumes ONTAP est disponible dans Google Cloud sous forme de système à un seul nœud et en tant que paire de nœuds à haute disponibilité. En fonction de ces exigences, nous pouvons choisir le mode de déploiement Cloud Volumes ONTAP. La mise à niveau d'un système à un seul nœud vers une paire haute disponibilité n'est pas prise en charge. Si vous souhaitez passer d'un système à un seul nœud à une paire HA, vous devez déployer un nouveau système et répliquer les données du système existant vers le nouveau.

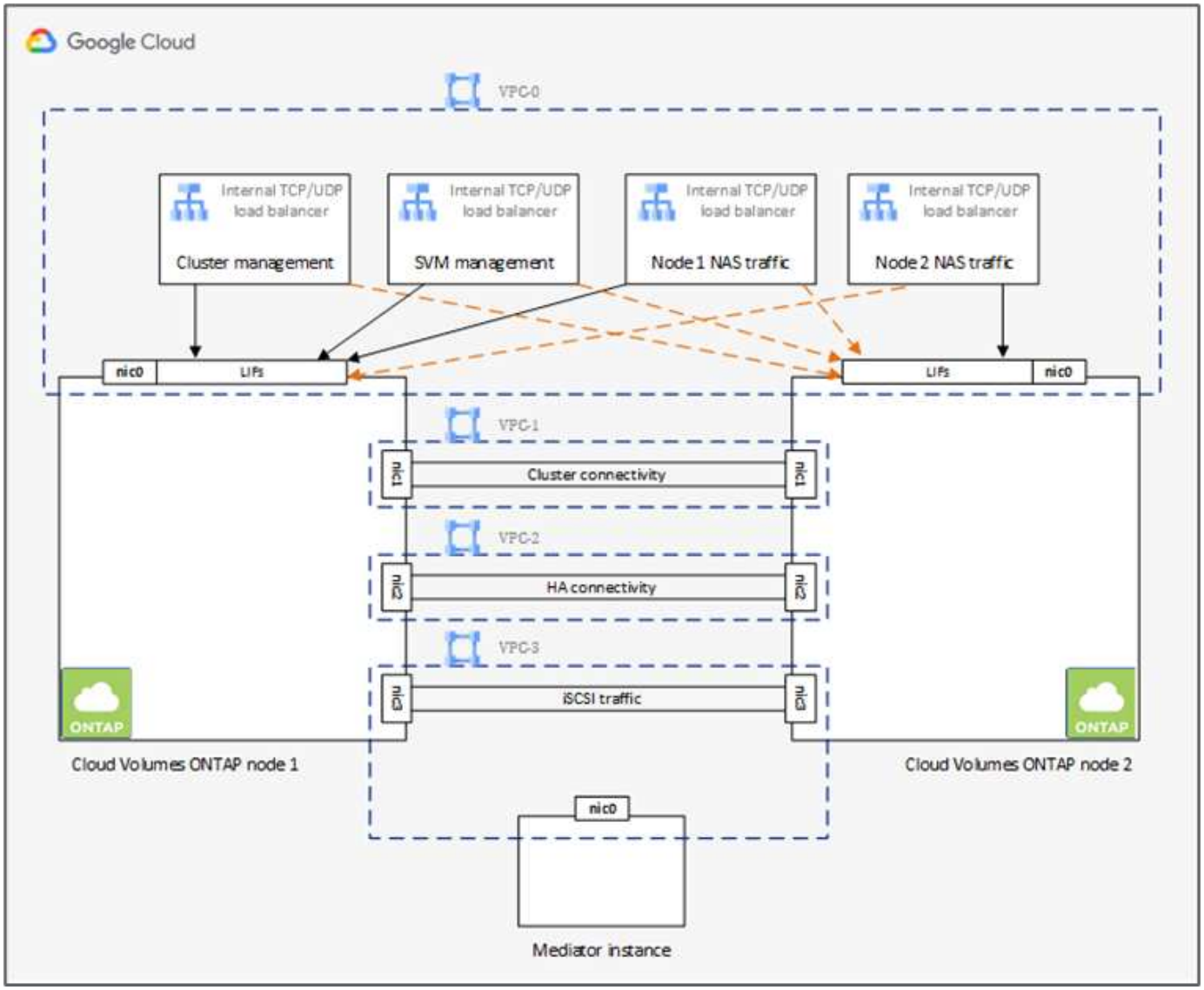
Haute disponibilité de Cloud Volumes ONTAP dans Google Cloud

Google Cloud prend en charge le déploiement de ressources dans plusieurs régions géographiques et zones géographiques. Le déploiement HA comprend deux nœuds ONTAP qui utilisent de puissants types de machines standard n1 ou n2 disponibles dans Google Cloud. Les données sont répliquées de manière synchrone entre les deux nœuds Cloud Volumes ONTAP afin d'assurer la disponibilité en cas de défaillance. Le déploiement HAUTE DISPONIBILITÉ de Cloud Volumes ONTAP requiert quatre VPC et un sous-réseau privé dans chaque VPC. Les sous-réseaux des quatre VPC doivent être configurés avec des plages CIDR non chevauchantes.

Les quatre VPC sont utilisés à des fins suivantes :

- VPC 0 permet la communication entrante aux nœuds de données et Cloud Volumes ONTAP.
- VPC 1 assure la connectivité du cluster entre les nœuds Cloud Volumes ONTAP.
- VPC 2 permet la réplication des RAM non volatiles (NVRAM) entre les nœuds.
- VPC 3 est utilisé pour la connectivité à l'instance de médiateur HA et au trafic de réplication de disque pour les reconstructions de nœuds.

L'image suivante montre un Cloud Volumes ONTAP hautement disponible dans Goggle Cloud.



Pour plus de détails, voir "ce lien".

Pour connaître les exigences de mise en réseau pour Cloud Volumes ONTAP dans Google Cloud, consultez "ce lien".

Pour plus d'informations sur le Tiering des données, voir "ce lien".

Configurez les conditions préalables à l'environnement

La création automatisée de clusters Cloud Volumes ONTAP, la configuration SnapMirror entre un volume sur site et un volume cloud, la création d'un volume cloud, etc., s'effectue à l'aide de la configuration Terraform. Ces configurations Terraform sont hébergées sur un compte Terraform Cloud for Business. Avec Intersight Cloud Orchestrator, vous orchestrez des tâches telles que la création d'un espace de travail dans un compte Terraform Cloud for Business, l'ajout de toutes les variables requises à l'espace de travail, l'exécution d'un plan Terraform, etc.

Pour ces tâches d'automatisation et d'orchestration, quelques exigences et données sont nécessaires, comme décrit dans les sections suivantes.

Référentiel GitHub

Vous avez besoin d'un compte GitHub pour héberger votre code Terraform. Intersight Orchestrator crée un nouvel espace de travail dans le compte Terraform Cloud for Business. Cet espace de travail est configuré avec un workflow de contrôle de version. À cette fin, vous devez conserver la configuration Terraform dans un référentiel GitHub et la fournir comme entrée lors de la création de l'espace de travail.

"Lien GitHub" Fournit la configuration Terraform avec diverses ressources. Vous pouvez forer ce référentiel et en faire une copie dans votre compte GitHub.

Dans ce référentiel, `provider.tf` A la définition du fournisseur Terraform requis. Le fournisseur Terraform pour NetApp Cloud Manager est utilisé.

`variables.tf` dispose de toutes les déclarations de variables. La valeur de ces variables est entrée en tant qu'entrée de workflow d'Intersight Cloud Orchestrator. Cela permet de transmettre des valeurs à un espace de travail et d'exécuter la configuration Terraform.

`resources.tf` Définit les diverses ressources nécessaires pour ajouter un système ONTAP sur site à l'environnement de travail, créer un cluster Cloud Volumes ONTAP à nœud unique sur Google Cloud, établir une relation SnapMirror entre l'infrastructure sur site et Cloud Volumes ONTAP, créer un volume cloud sur Cloud Volumes ONTAP, etc.

Dans ce référentiel :

- `provider.tf` Définit NetApp Cloud Manager comme fournisseur Terraform requis.
- `variables.tf` Dispose des déclarations de variables utilisées comme entrée pour le workflow Intersight Cloud Orchestrator. Cela permet de transmettre des valeurs à l'espace de travail et d'exécuter la configuration Terraform.
- `resources.tf` Définit diverses ressources pour ajouter une ONTAP sur site à l'environnement de travail, créer un cluster Cloud Volumes ONTAP à un seul nœud sur Google Cloud, établir une relation SnapMirror entre l'infrastructure sur site et Cloud Volumes ONTAP, créer un volume cloud sur Cloud Volumes ONTAP, etc.

Vous pouvez ajouter un bloc de ressources supplémentaire pour créer plusieurs volumes sur Cloud Volumes ONTAP, ou utiliser count ou `for_each` Constructions Terraform.

Pour connecter des espaces de travail Terraform, des modules et des jeux de règles aux référentiels git contenant des configurations Terraform, Terraform Cloud doit accéder à votre GitHub repo.

Ajoutez un client et l'ID Token OAuth du client est utilisé comme l'une des entrées de workflow d'InterSight Cloud Orchestrator.

1. Connectez-vous à votre compte Terraform Cloud for Business. Accédez à **Paramètres > fournisseurs**.
2. Cliquez sur **Ajouter un fournisseur VCS**.
3. Sélectionnez votre version.
4. Suivez les étapes de la section **configurer fournisseur**.
5. Vous voyez le client ajouté dans **VCS Providers**. Notez l'ID du token OAuth.

Jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager

En plus de l'interface du navigateur Web, Cloud Manager dispose d'une API REST qui permet aux développeurs de logiciels d'accéder directement à la fonctionnalité Cloud Manager via l'interface SaaS. Le service Cloud Manager comprend plusieurs composants distincts qui forment collectivement une plateforme de développement extensible. Le jeton d'actualisation vous permet de générer des jetons d'accès que vous ajoutez à l'en-tête autorisation pour chaque appel d'API.

Sans appeler directement une API, le fournisseur netapp-cloudManager utilise un jeton d'actualisation et convertit les ressources Terraform en appels d'API correspondants. Vous devez générer un jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager à partir de "NetApp Cloud Central".

Vous devez disposer de l'ID client du connecteur Cloud Manager pour créer des ressources dans Cloud Manager, par exemple pour créer un cluster Cloud Volumes ONTAP, configurer SnapMirror, etc.

1. Connectez-vous à Cloud Manager : "https://cloudmanager.netapp.com/".
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les connecteurs**.
4. Cliquez sur les points de suspension et copiez l'ID du connecteur.

Développez le workflow Cisco Intersight Cloud Orchestrator

Cisco Intersight Cloud Orchestrator est disponible dans Cisco Intersight si :

- Vous avez installé la licence InterSight Premier.
- Vous êtes administrateur de compte, administrateur de stockage, administrateur de virtualisation ou administrateur de serveurs et avez au moins un serveur qui vous est attribué.

Concepteur de flux de travail

Le concepteur de flux de travail vous aide à créer de nouveaux flux de travail (ainsi que des tâches et des types de données) et à modifier des flux de travail existants pour gérer des cibles dans Cisco Intersight.

Pour lancer Workflow Designer, accédez à **orchestration > workflows**. Un tableau de bord affiche les détails suivants sous les onglets **Mes workflows**, **modèles de flux de travail** et **tous les workflows** :

- État de validation
- Statut de la dernière exécution

- Flux de travail par nombre d'exécution
- Principales catégories de flux de travail
- Nombre de flux de travail définis par le système
- Principaux flux de travail par cible

Le tableau de bord vous permet de créer, modifier, cloner ou supprimer un onglet. Pour créer votre propre onglet de vue personnalisée, cliquez sur **+**, spécifiez un nom, puis sélectionnez les paramètres requis à afficher dans les colonnes, les colonnes de balises et les widgets. Vous pouvez renommer un onglet s'il ne possède pas d'icône **Lock**.

Sous le tableau de bord, vous trouverez une liste tabulaire des flux de production affichant les informations suivantes :

- Afficher le nom
- Description
- Défini par le système
- Version par défaut
- Exécutions
- Statut de la dernière exécution
- État de validation
- Dernière mise à jour
- Entreprise

La colonne actions vous permet d'effectuer les actions suivantes :

- **Exécuter.** exécute le flux de travail.
- **Historique.** affiche l'historique d'exécution du flux de travail.
- **Gérer les versions.** Créer et gérer des versions pour les flux de travail.
- **Supprimer.** Supprimer un flux de travail.
- **Réessayer.** Réessayer un flux de travail échoué.

Flux de travail

Créer un flux de travail composé des étapes suivantes :

- **Définition d'un flux de travail.** spécifier le nom d'affichage, la description et d'autres attributs importants.
- **Définir les entrées de flux de travail et les sorties de flux de travail.** spécifier les paramètres d'entrée obligatoires pour l'exécution du flux de travail et les sorties générées lors de l'exécution réussie
- **Ajouter des tâches de flux de travail.** Ajouter une ou plusieurs tâches de flux de travail dans le concepteur de flux de travail qui sont nécessaires pour que le flux de travail puisse exécuter sa fonction.
- *Valider le flux de travail. *Valider un flux de travail pour s'assurer qu'il n'y a pas d'erreurs dans la connexion des entrées et sorties de tâche.

Créez des workflows de stockage FlexPod sur site

Pour configurer un workflow pour le stockage FlexPod sur site, reportez-vous à la section "ce lien".

"Suivant : workflow de reprise après incident."

Workflow de reprise d'activité

"Précédent : déploiement automatisé du stockage NetApp dans le cloud hybride."

Les étapes sont les suivantes :

1. Définir le flux de travail.
   - Créez un nom court et convivial pour le flux de travail, tel que Disaster Recovery Workflow.
2. Définissez l'entrée du flux de travail. Nous utilisons les données d'entrée suivantes pour ce flux de travail :
   - Options de volume (nom du volume, chemin de montage)
   - Capacité du volume
   - Data Center associé au nouveau datastore
   - Cluster sur lequel le datastore est hébergé
   - Nom du nouveau datastore à créer dans vCenter
   - Type et version du nouveau datastore
   - Nom de l'organisation Terraform
   - Espace de travail Terraform
   - Description de l'espace de travail Terraform
   - Variables (sensibles et non sensibles) requises pour exécuter la configuration Terraform
   - Motif du démarrage du plan
3. Ajoutez les tâches du flux de travail.

   Les tâches liées aux opérations dans FlexPod incluent les tâches suivantes :

   - Création de volumes dans FlexPod.
   - Ajout de l'export policy de stockage au volume créé
   - Mappez le nouveau volume sur un datastore dans VMware vCenter.

     Tâches liées à la création d'un cluster Cloud Volumes ONTAP :

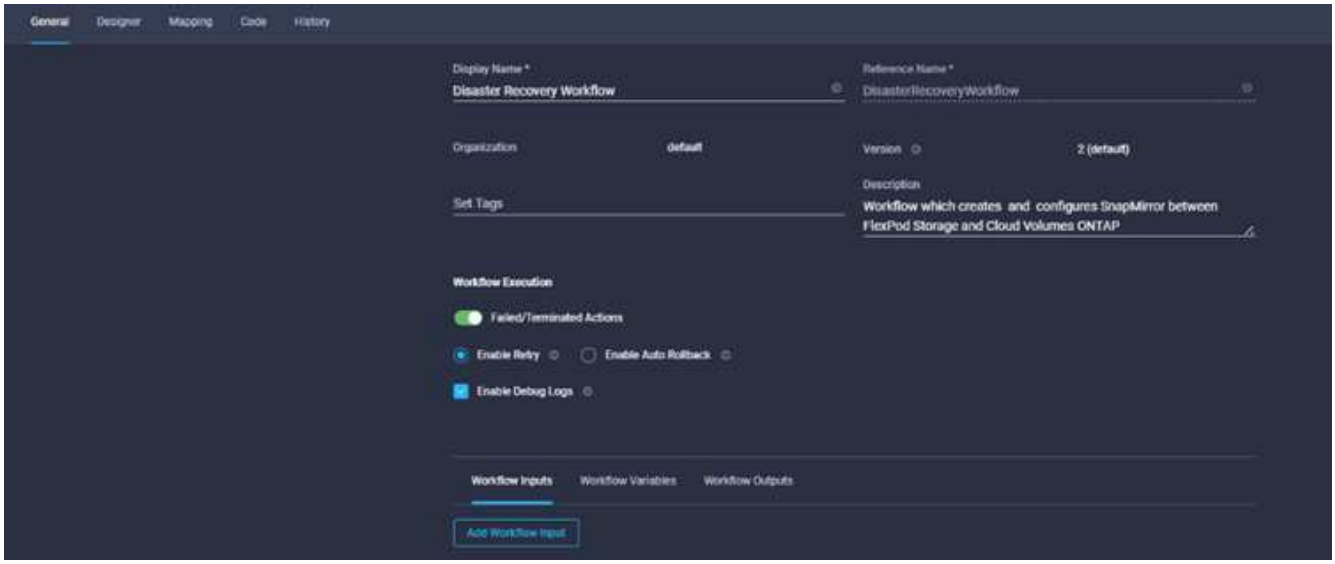
   - Ajouter un espace de travail Terraform
   - Ajouter des variables Terraform
   - Ajoutez des variables sensibles à Terraform
   - Démarrez un nouveau plan Terraform
   - Confirmez l'exécution de Terraform
4. Validation du flux de travail

Procédure 1 : créez le flux de travail

1. Cliquez sur **orchestration** dans le volet de navigation de gauche et cliquez sur **Créer un flux de travail**.
2. Dans l'onglet **général** :
   a. Indiquez le nom d'affichage (flux de travail de reprise après sinistre).

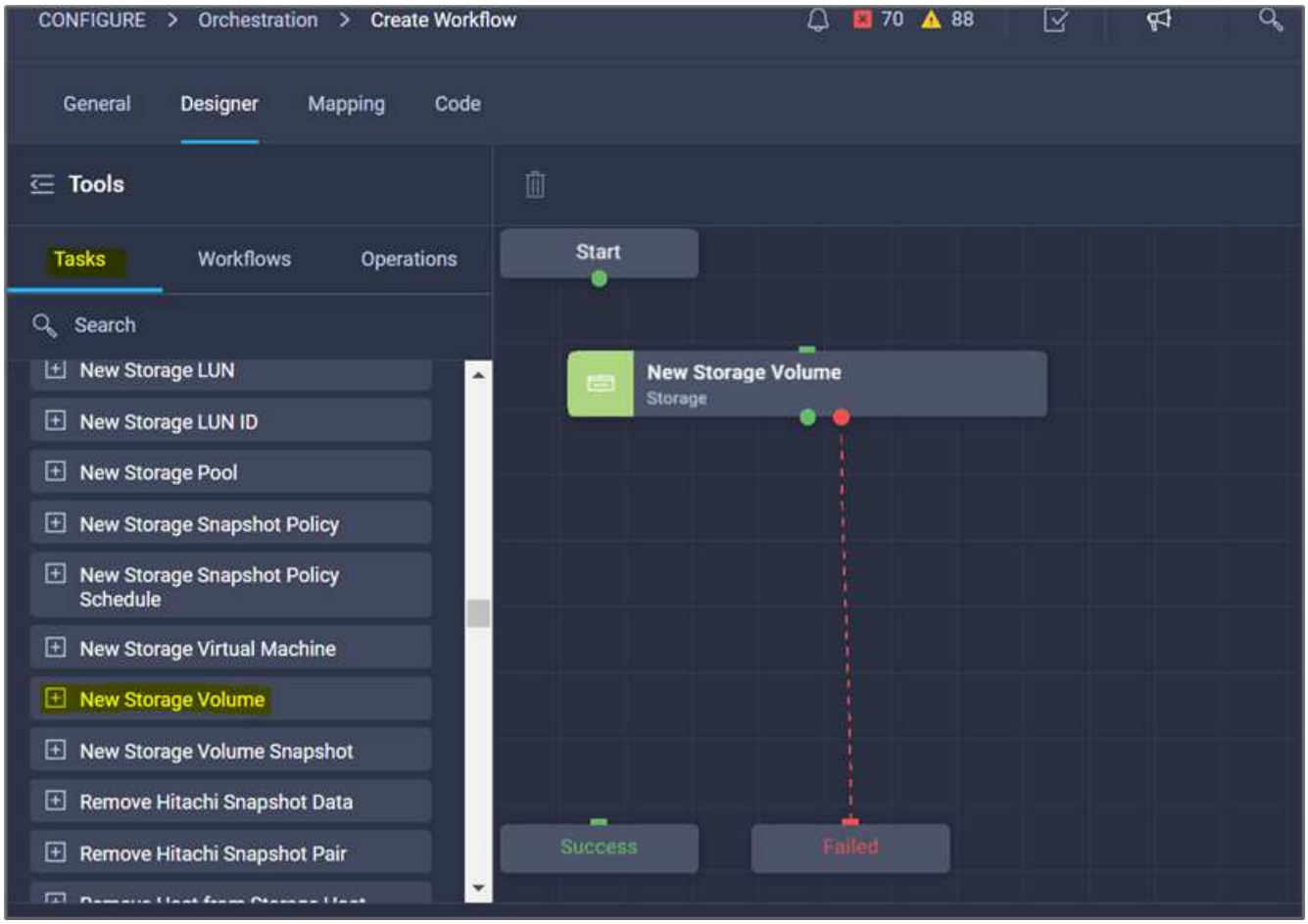
b. Sélectionnez l’organisation, définissez les balises et fournissez une description.

3. Cliquez sur Enregistrer.

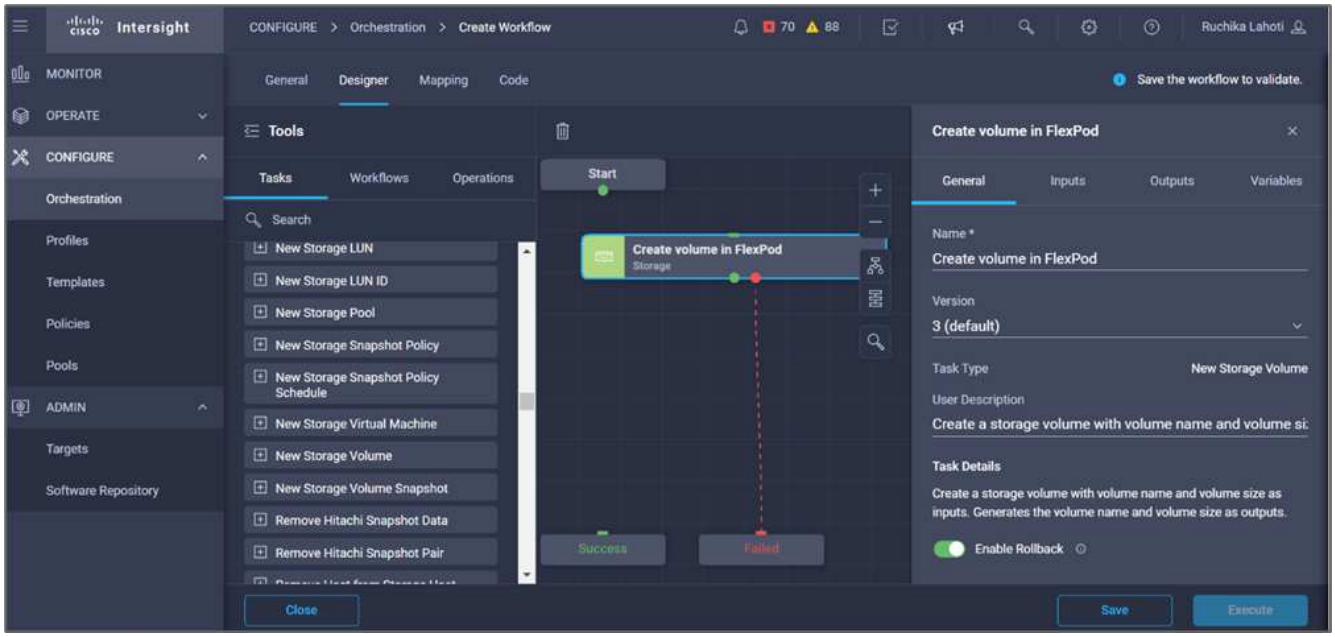


Procédure 2. Créer un nouveau volume dans FlexPod

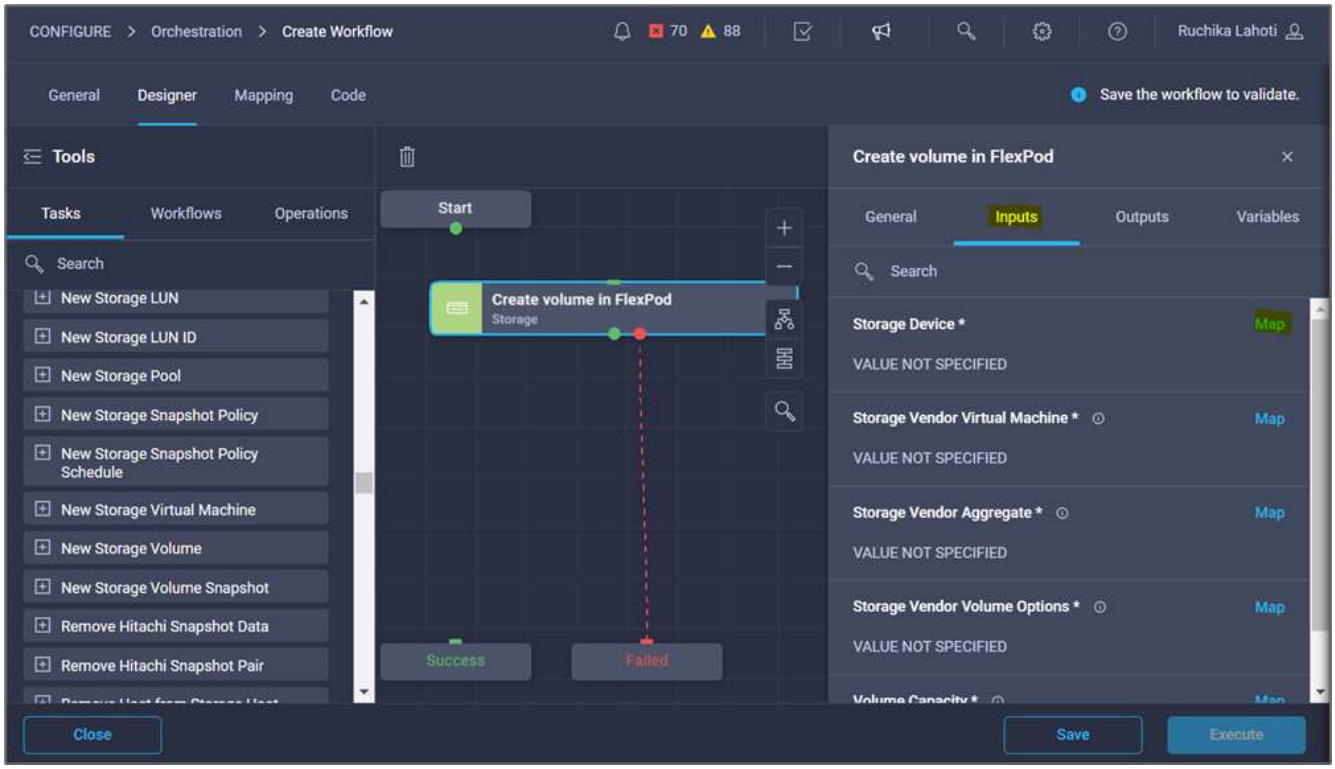
1. Accédez à l’onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **stockage > Nouveau volume de stockage** de la section **Outils** dans la zone **Design**.
3. Cliquez sur **Nouveau volume de stockage**.



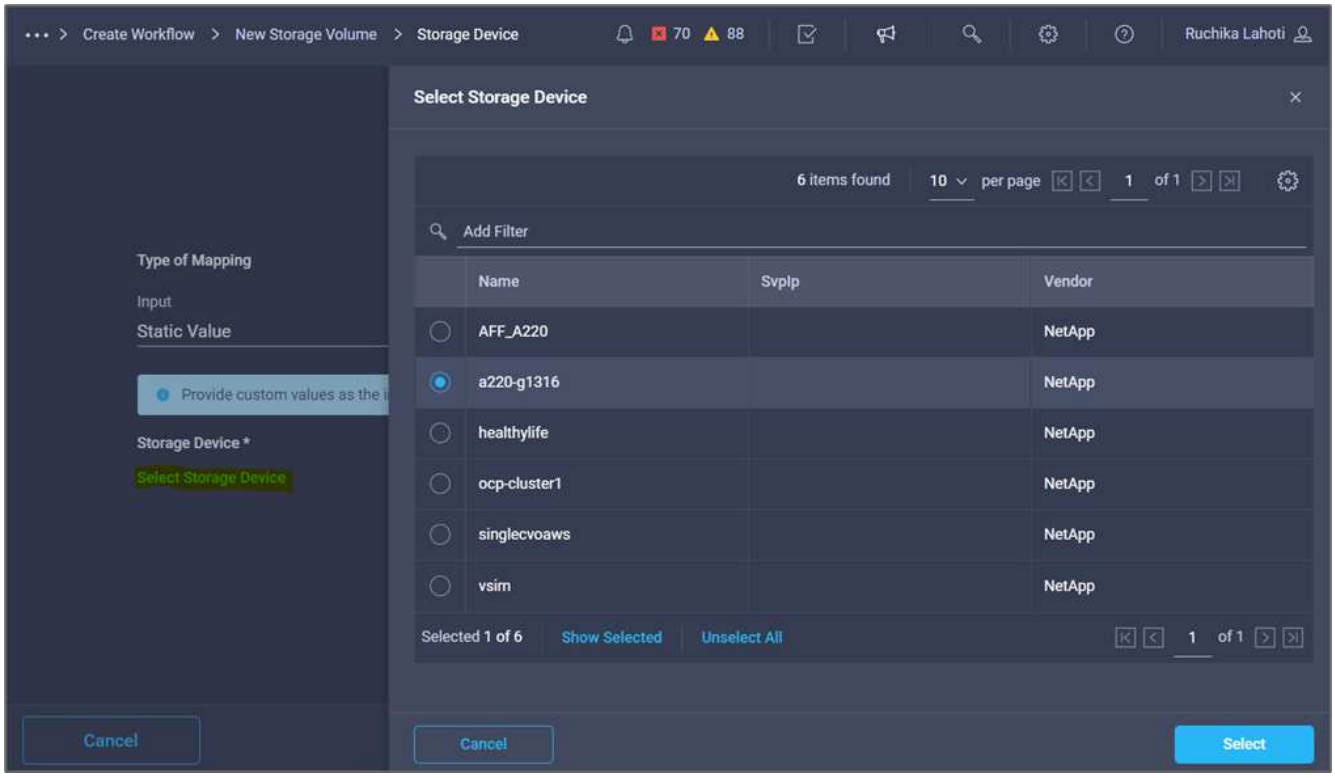
4. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Créer un volume dans FlexPod**.



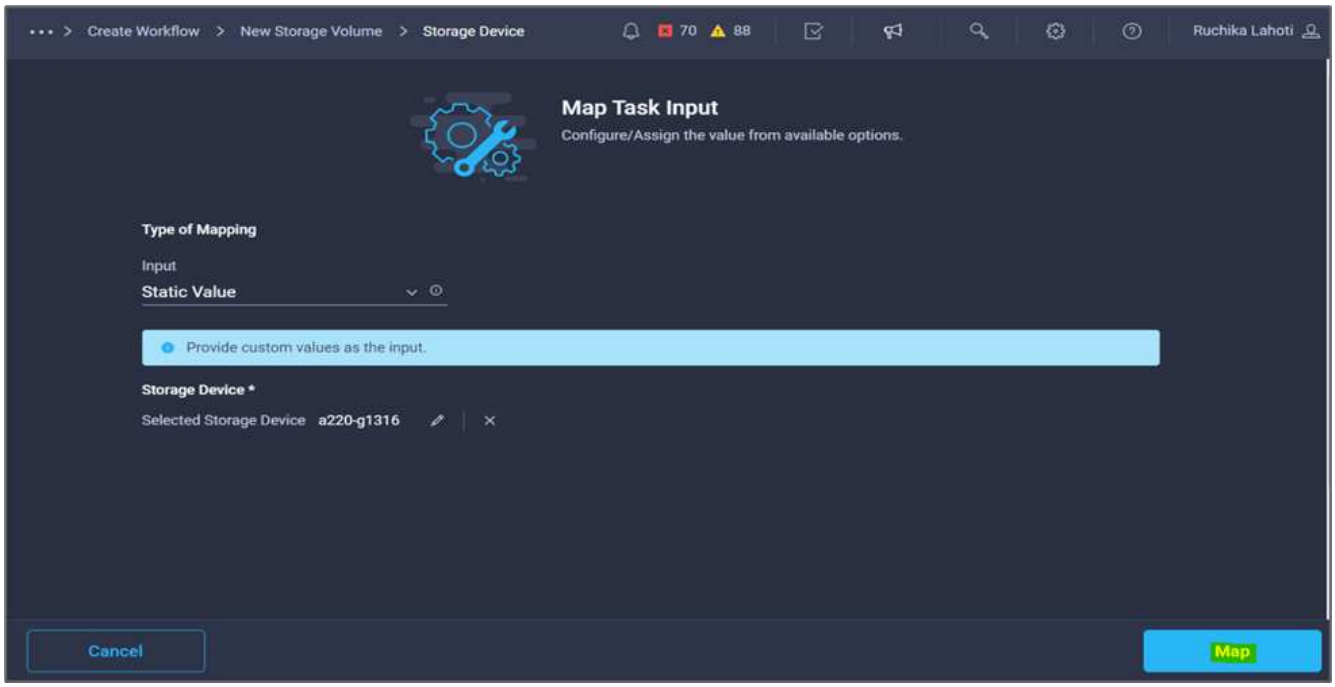
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Storage Device**.



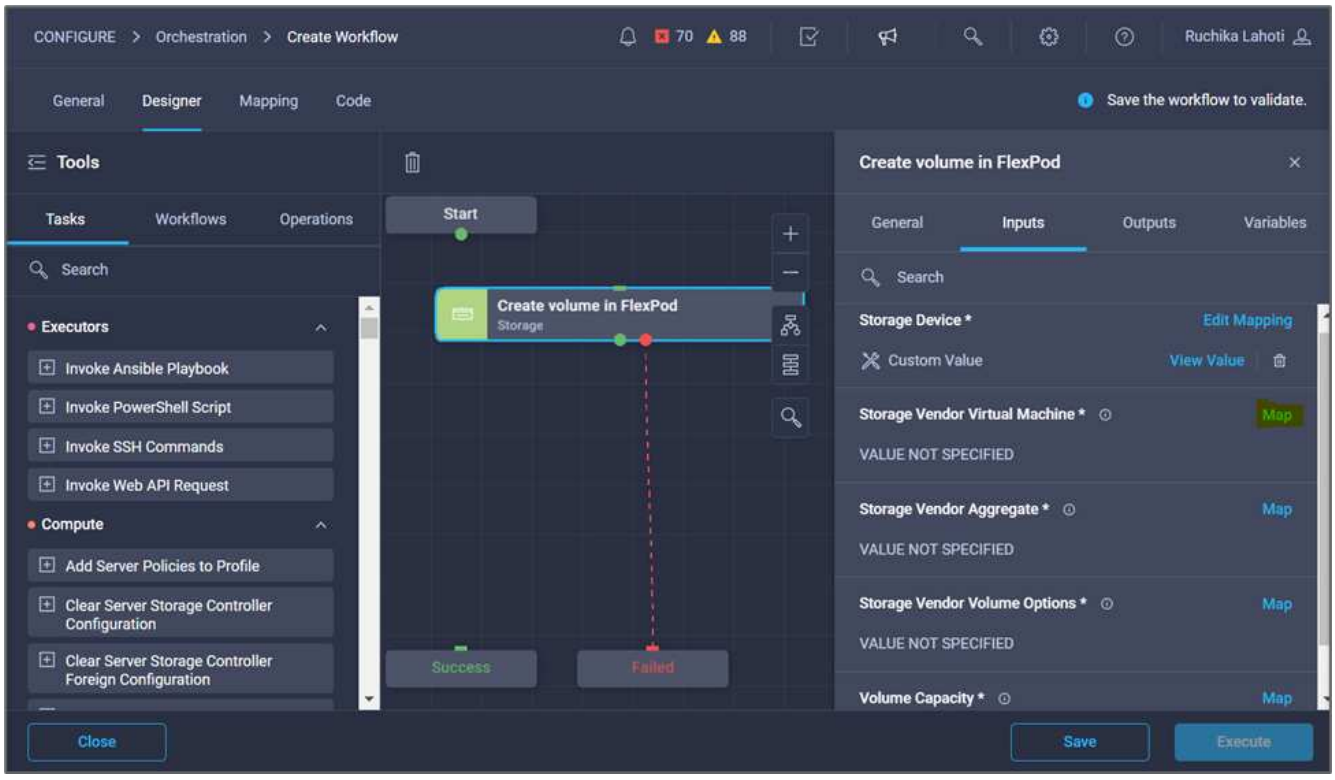
7. Choisissez **valeur statique** et cliquez sur **Sélectionner le périphérique de stockage**.
8. Cliquez sur la cible de stockage ajoutée et cliquez sur **Sélectionner**.



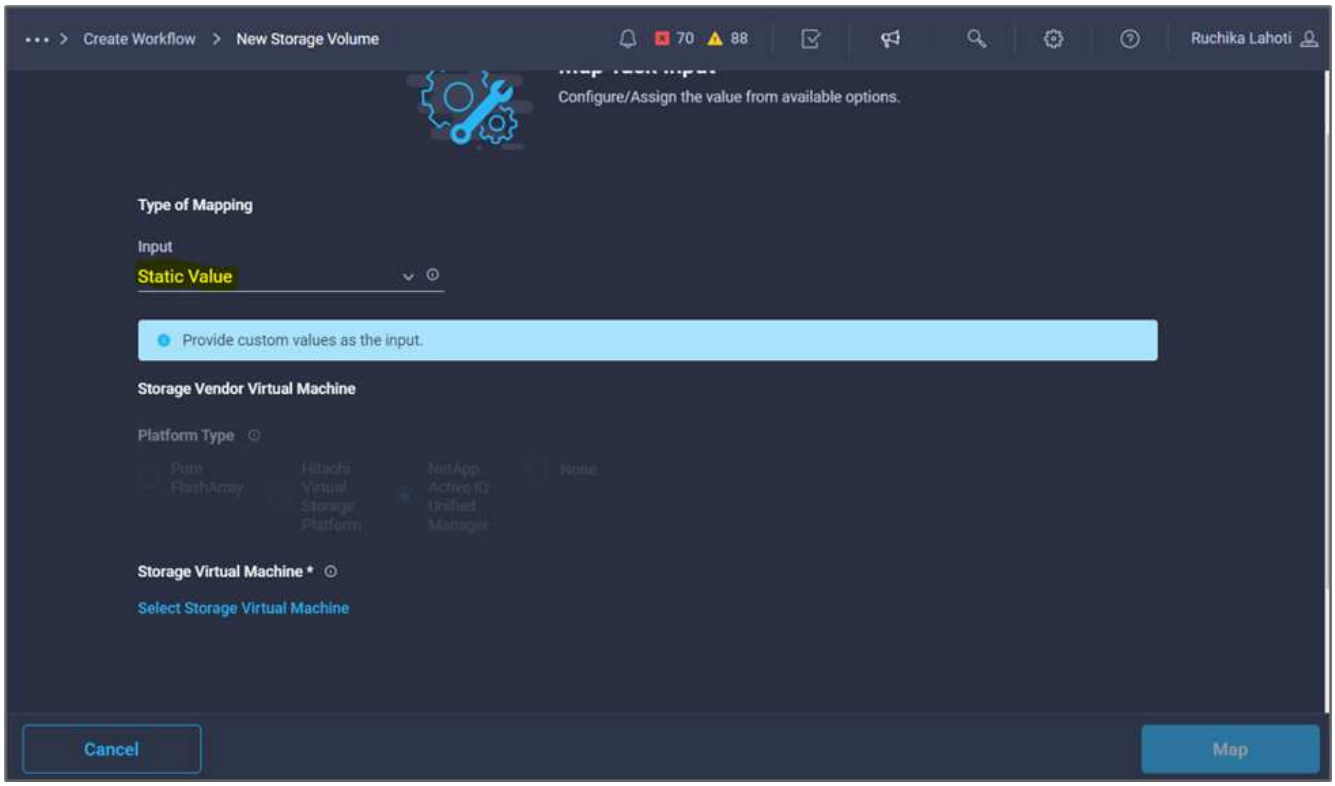
9. Cliquez sur **carte**.



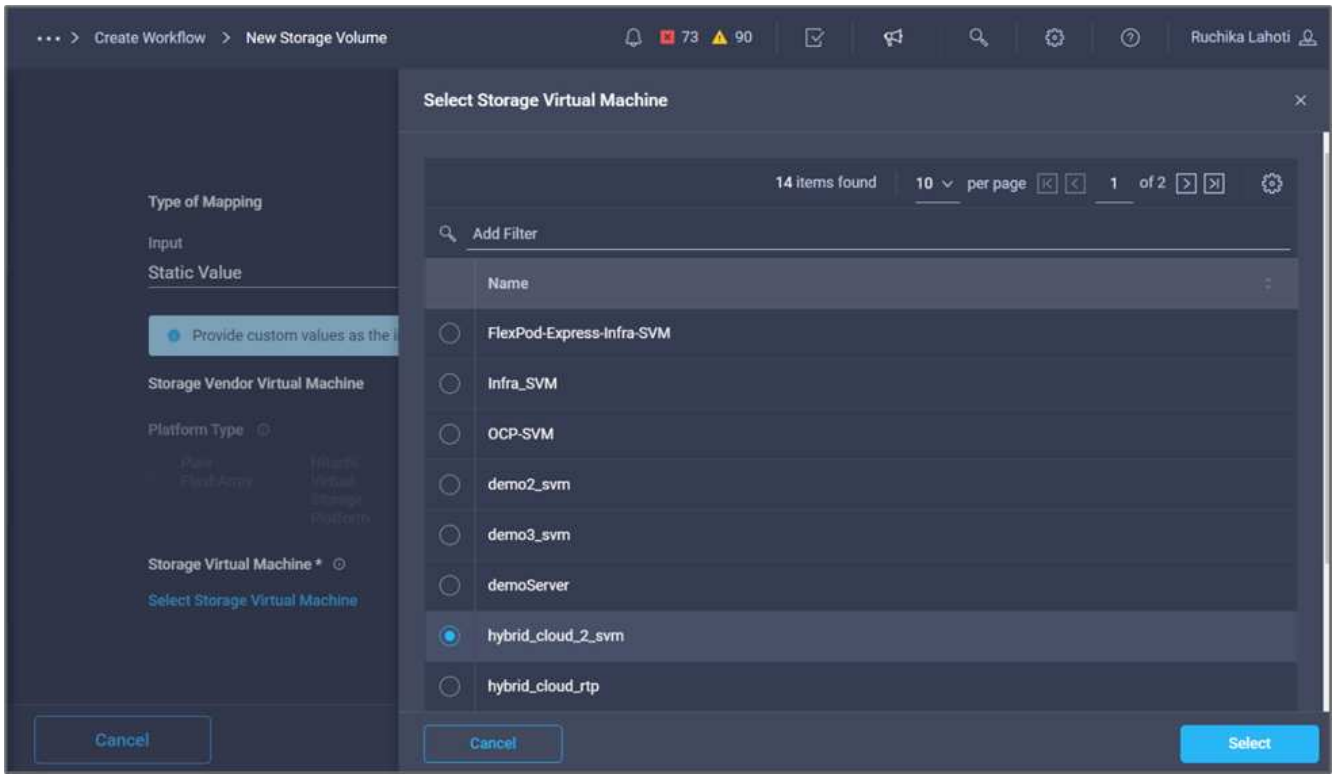
10. Cliquez sur **Map** dans le champ **Storage Vendor Virtual machine**.



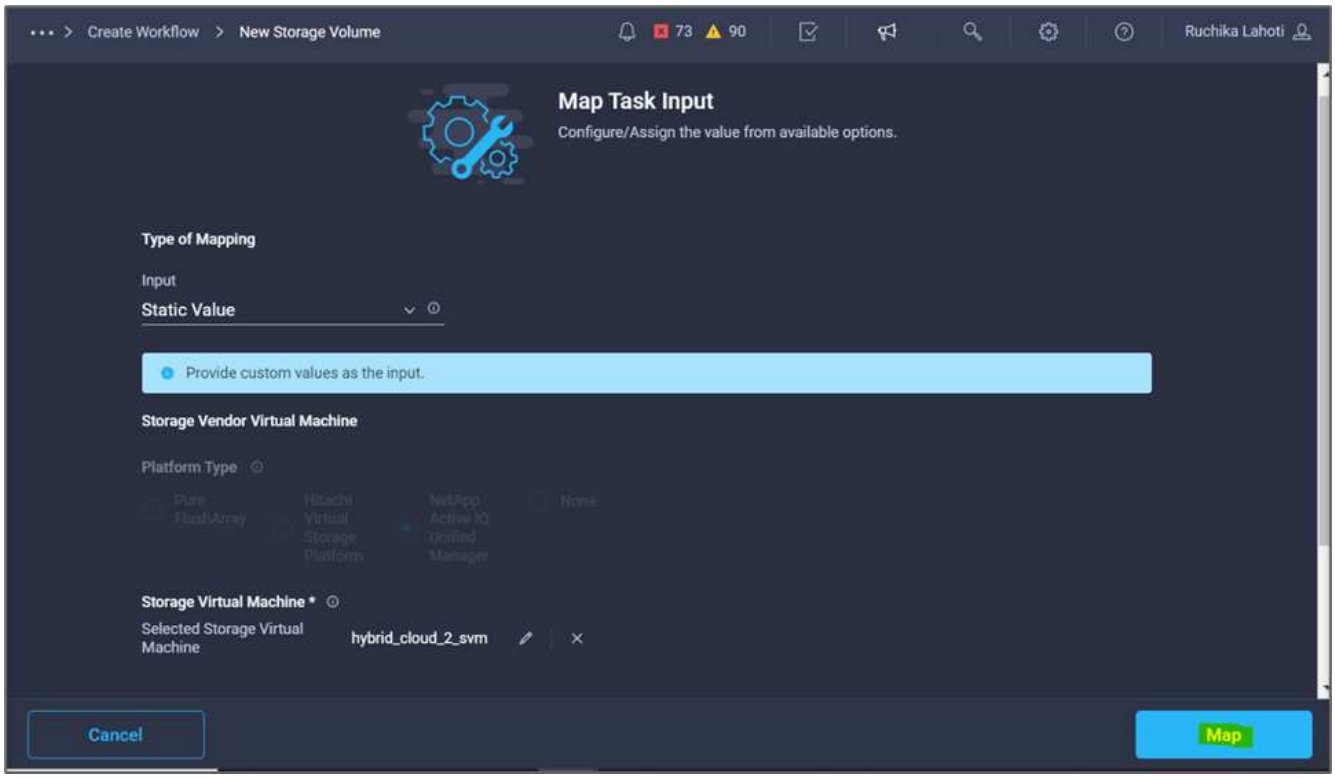
11. Choisissez **valeur statique** et cliquez sur **Sélectionner Storage Virtual machine**.



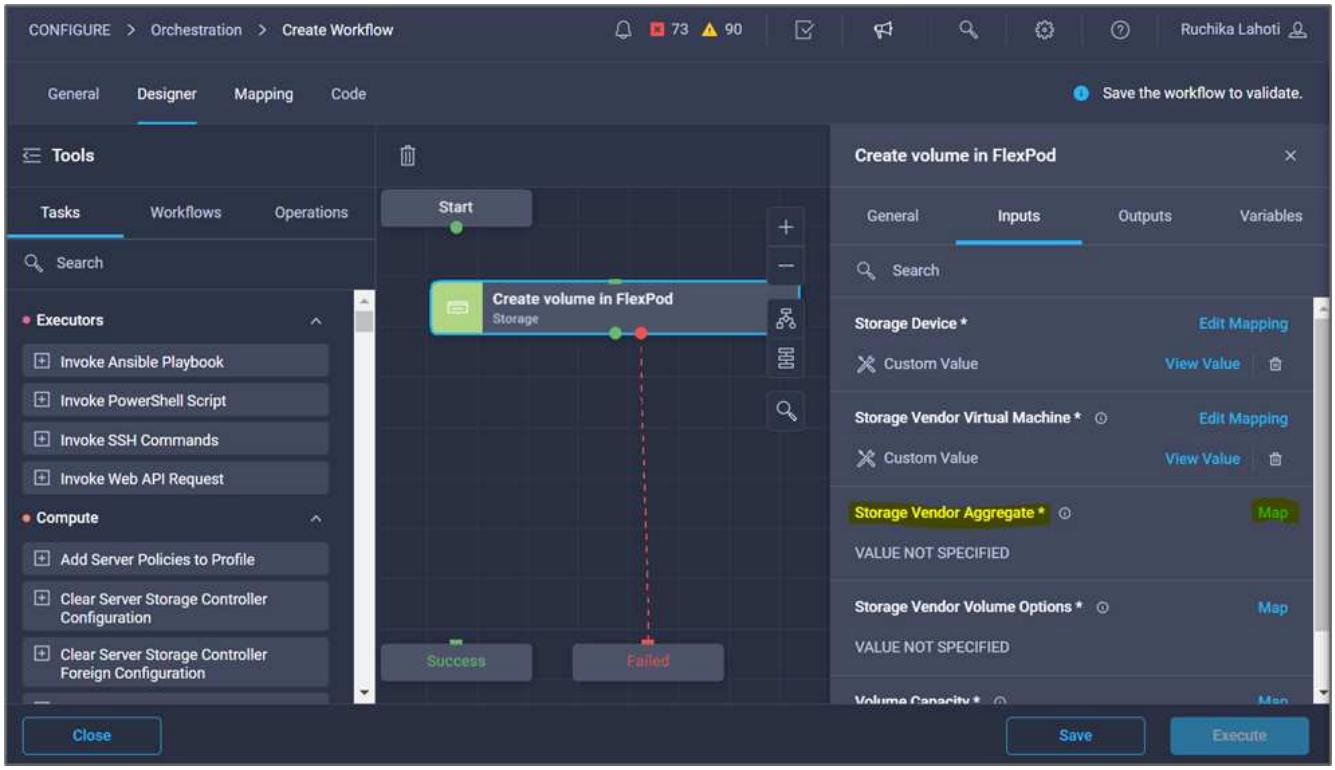
12. Sélectionnez la machine virtuelle de stockage sur laquelle le volume doit être créé et cliquez sur **Sélectionner**.



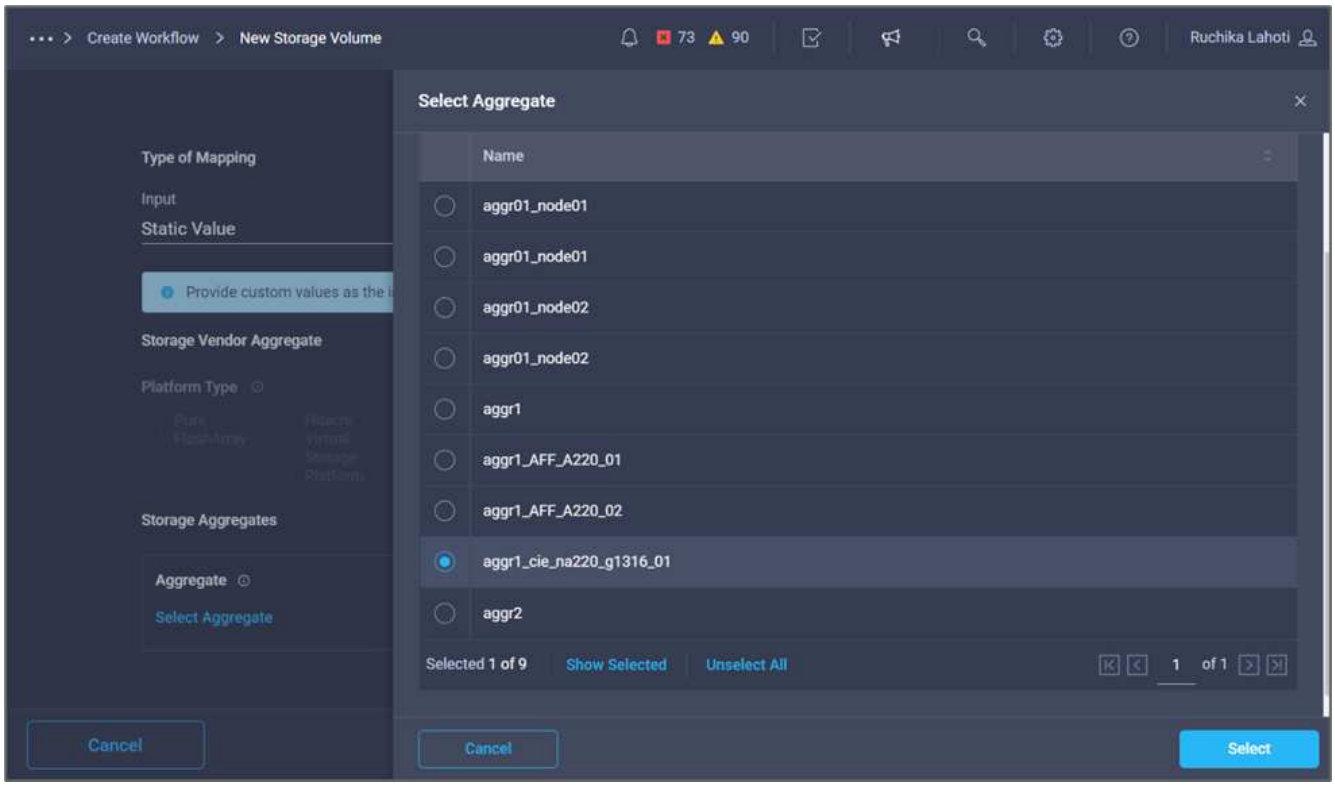
13. Cliquez sur **carte**.



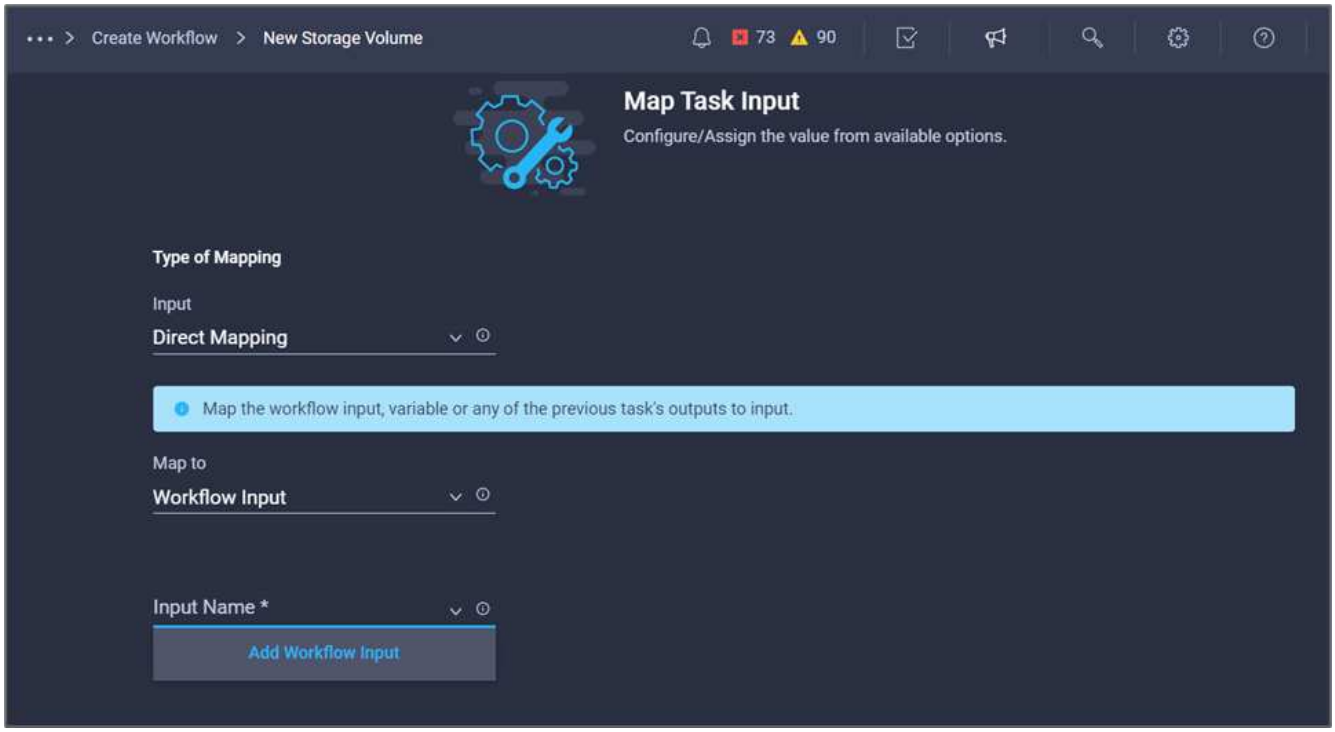
14. Cliquez sur **Map** dans le champ **Storage Vendor Aggregate**.



15. Choisissez **valeur statique** et cliquez sur **Sélectionner l'agrégat de stockage**. Choisissez l'agrégat et cliquez sur **Select**.



16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Storage Vendor Volume Options**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.



19. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous que **Storage Vendor Volume Options** est sélectionné pour **Type**.

c. Cliquez sur **définir la valeur par défaut et remplacer**.

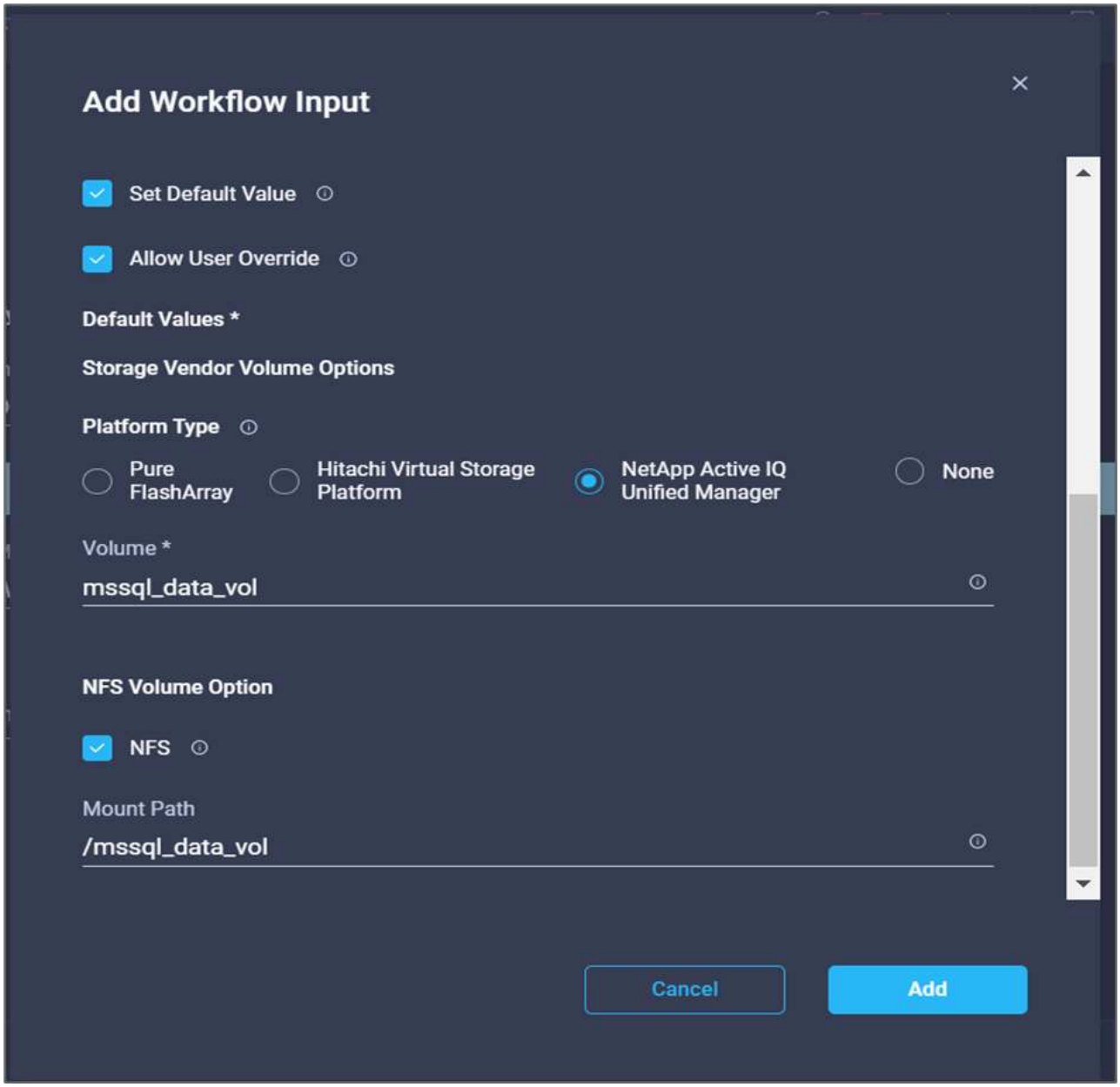
d. Cliquez sur **requis**.

e. Définissez **Type de plateforme** sur **NetApp Active IQ Unified Manager**.

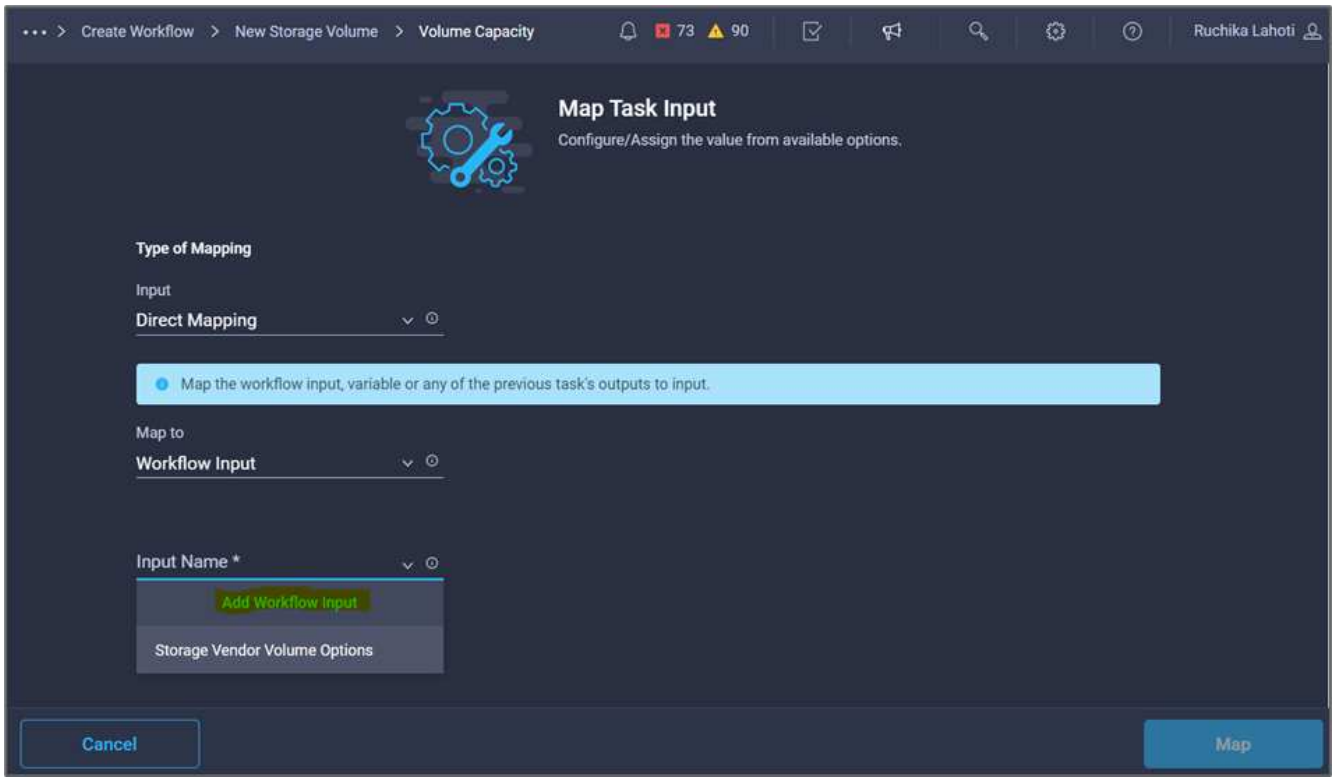
f. Indiquez une valeur par défaut pour le volume créé sous **Volume**.

g. Cliquez sur **NFS**. Si NFS est défini, un volume NFS est créé. Si cette valeur est définie sur FALSE, un volume SAN est créé.

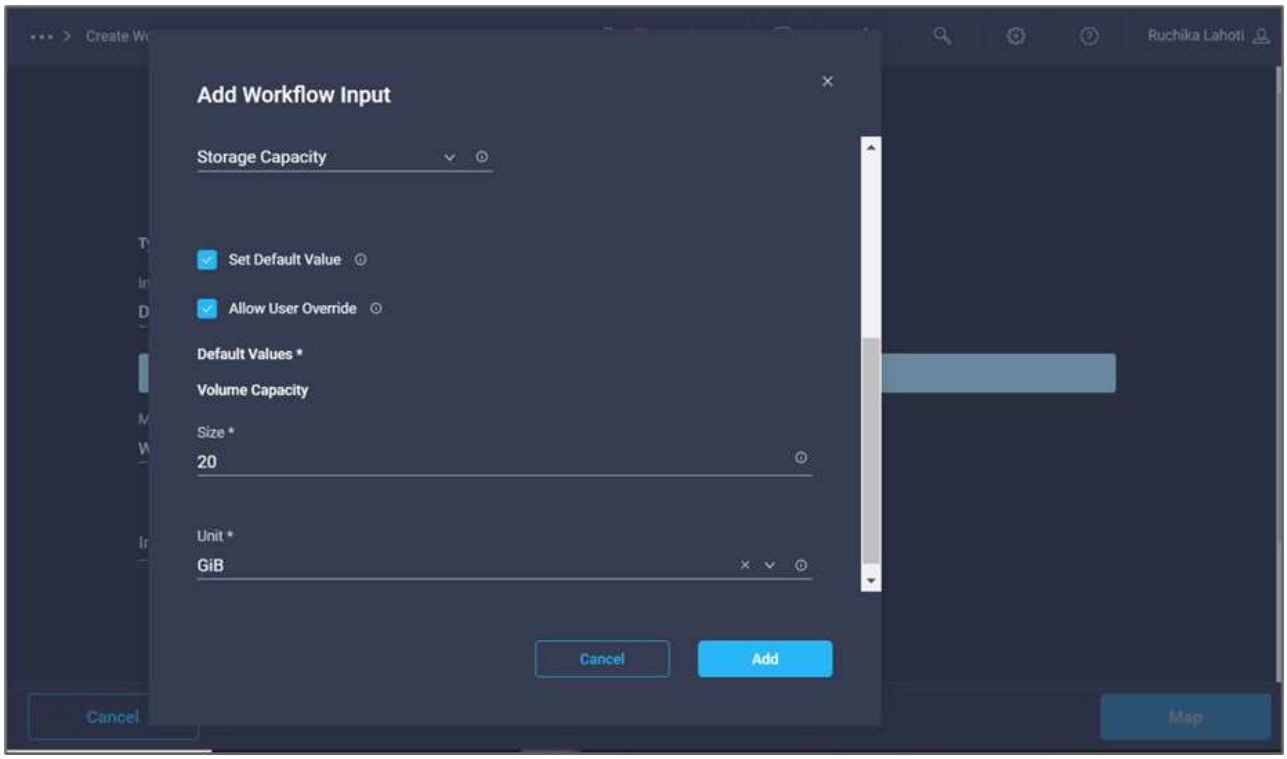
h. Indiquez un chemin de montage et cliquez sur **Ajouter**.



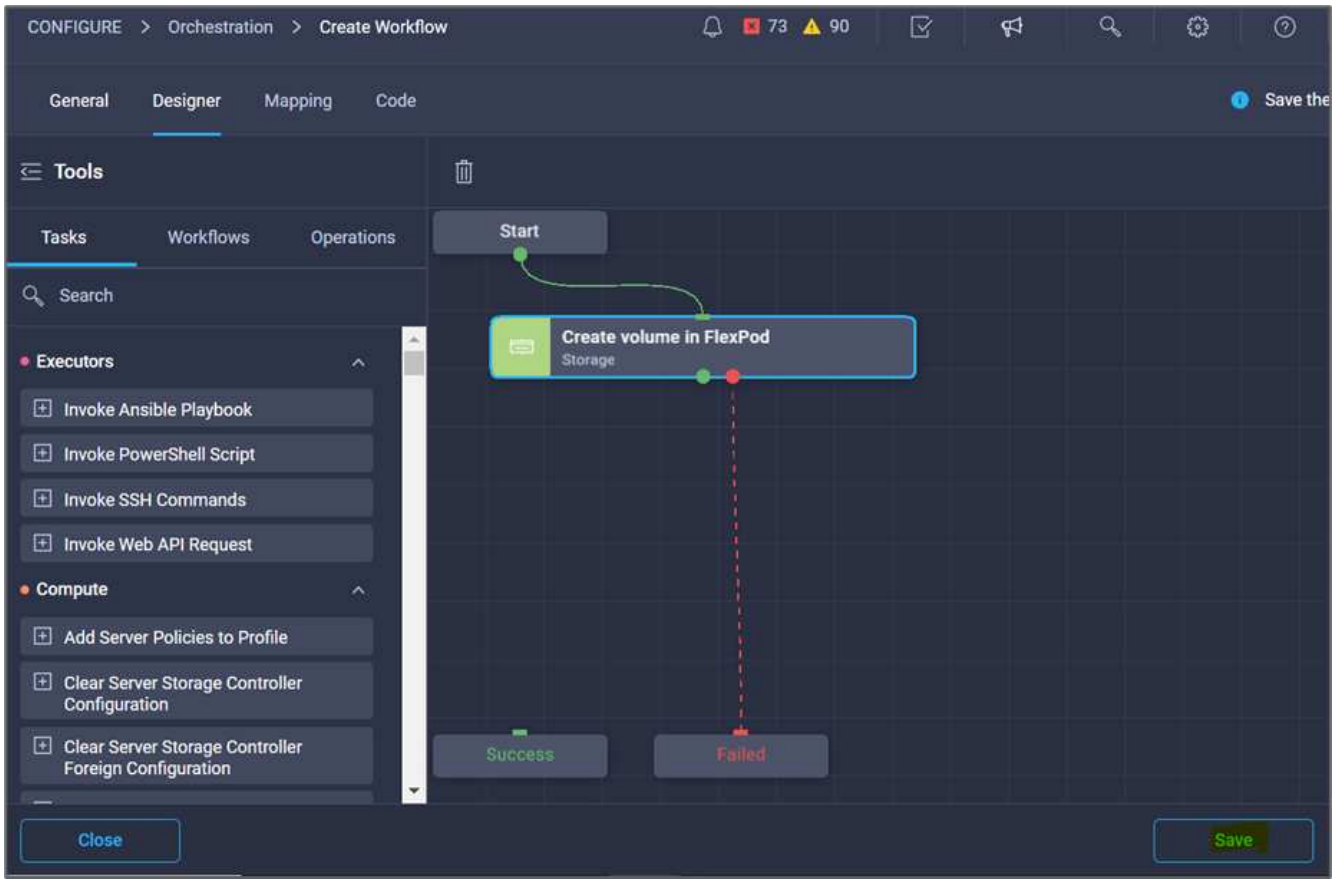
20. Cliquez sur **carte**.
21. Cliquez sur **Map** dans le champ **Volume Capacity**.
22. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
23. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



24. Dans l'assistant Ajouter une entrée :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Pour **Type**, sélectionnez **capacité de stockage**.
    d. Cliquez sur **définir la valeur par défaut et remplacer**.
    e. Indiquez une valeur par défaut pour la taille du volume et l'unité.
    f. Cliquez sur **Ajouter**.



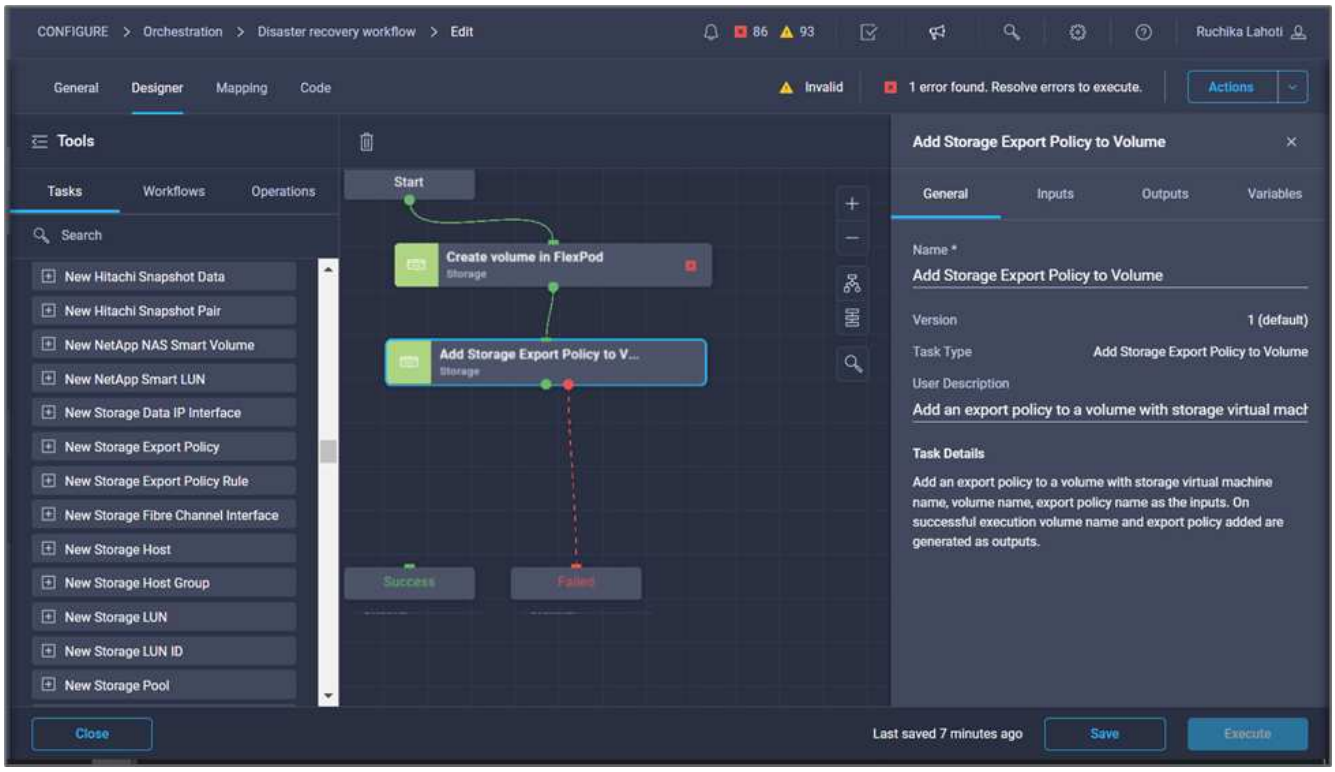
25. Cliquez sur **carte**.
26. Avec Connector, créez une connexion entre les tâches **Démarrer** et **Créer un volume dans FlexPod**, puis cliquez sur **Enregistrer**.



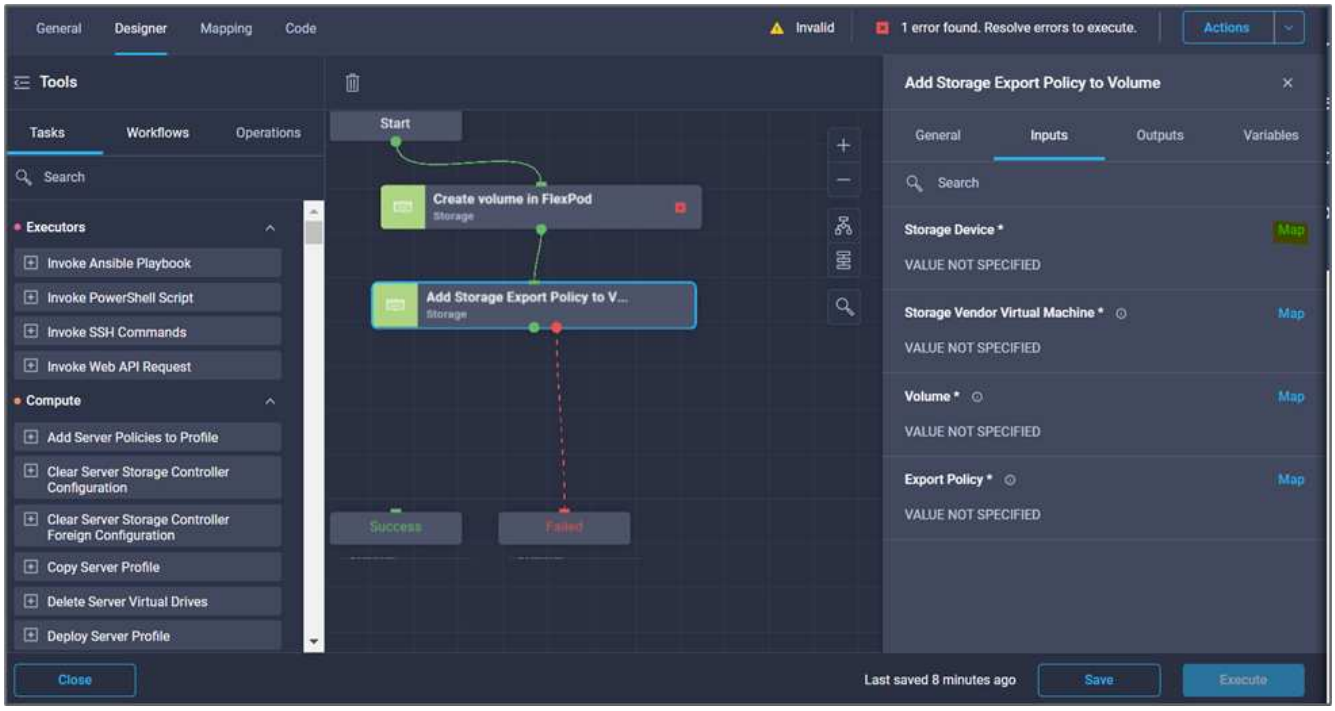
Ignorer l'erreur pour l'instant. Cette erreur s'affiche car il n'y a pas de connectivité entre les tâches **Créer un volume dans FlexPod** et **succès** qui est nécessaire pour spécifier la transition réussie.

Procédure 3 : ajout d'une règle d'exportation de stockage

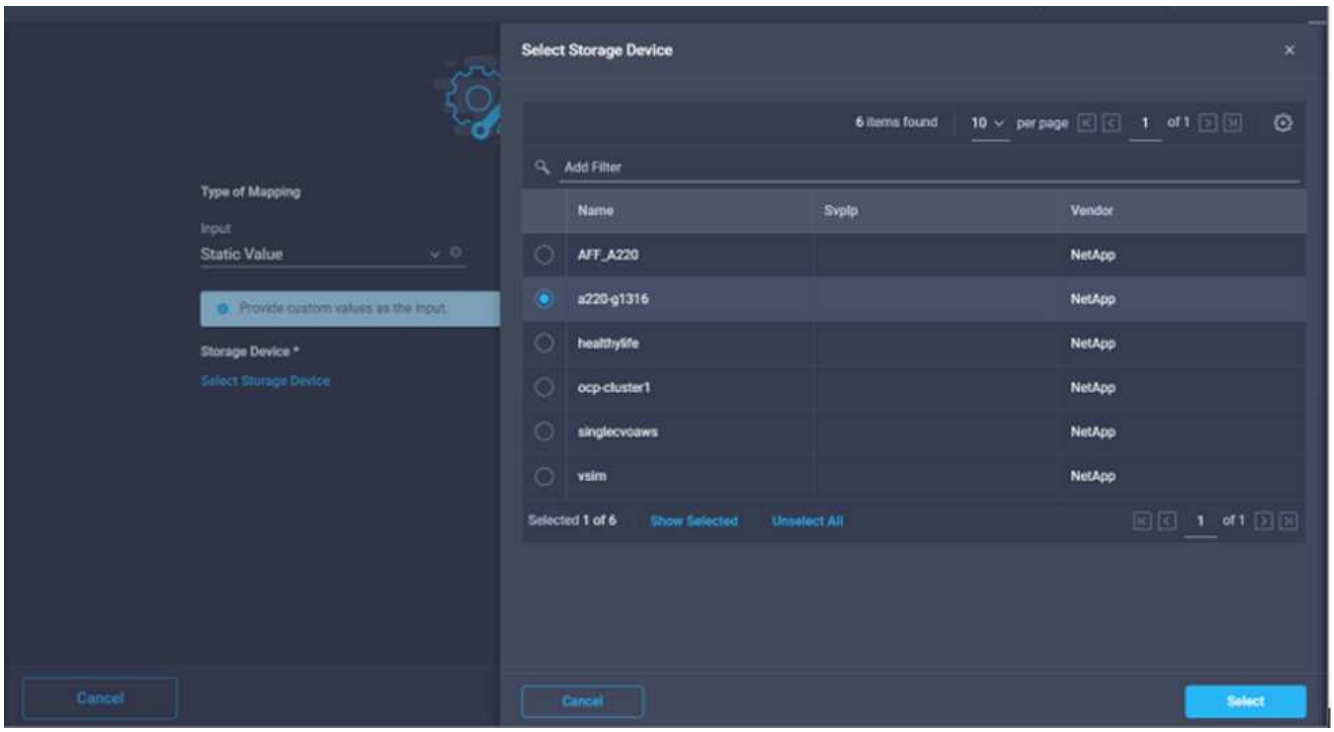
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **stockage > Ajouter une stratégie d'exportation de stockage au volume** à partir de la section **Outils** de la zone **Design**.
3. Cliquez sur **Ajouter une stratégie d'exportation de stockage au volume**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est Ajouter une stratégie d'exportation de stockage.
4. Utilisez Connector pour établir une connexion entre les tâches **Créer un volume dans FlexPod** et **Ajouter une stratégie d'exportation de stockage**. Cliquez sur **Enregistrer**.



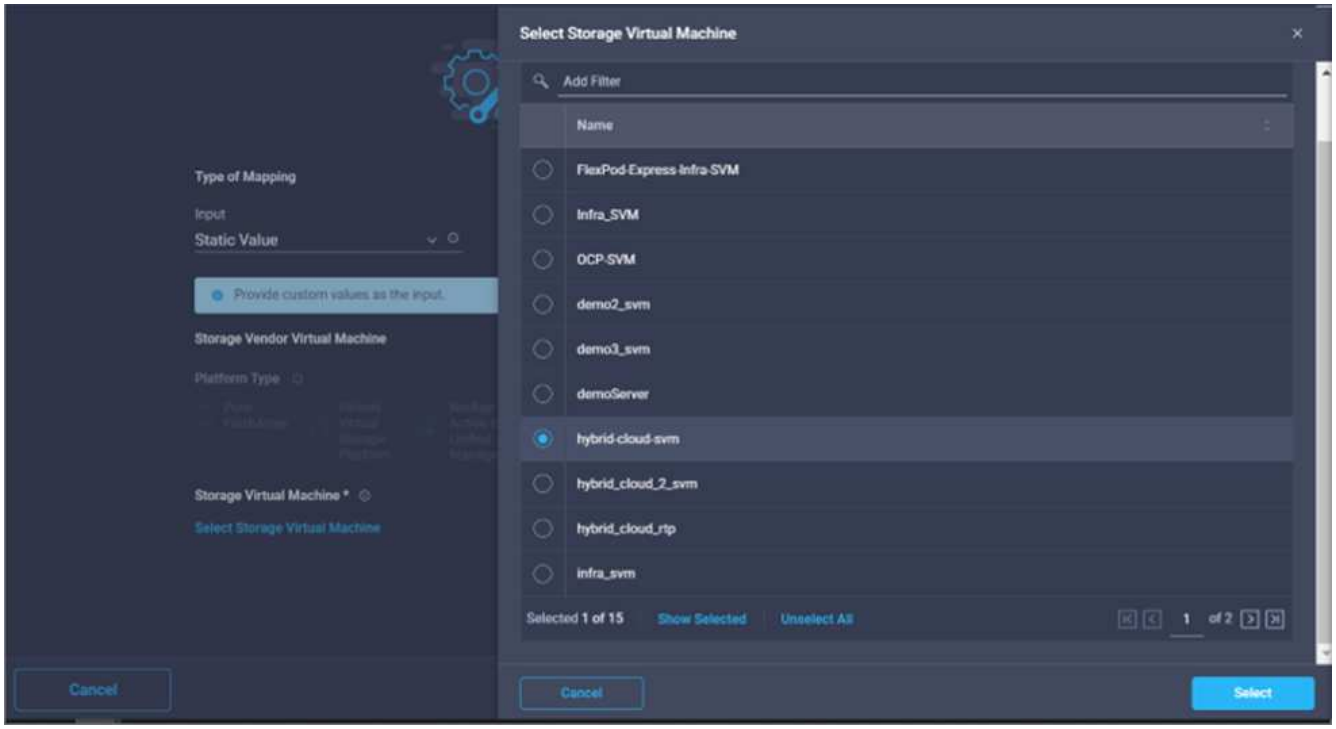
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Storage Device**.



7. Choisissez **valeur statique** et cliquez sur **Sélectionner le périphérique de stockage**. Sélectionnez la même cible de stockage ajoutée lors de la création de la tâche précédente de création d'un volume de stockage.
8. Cliquez sur **carte**.

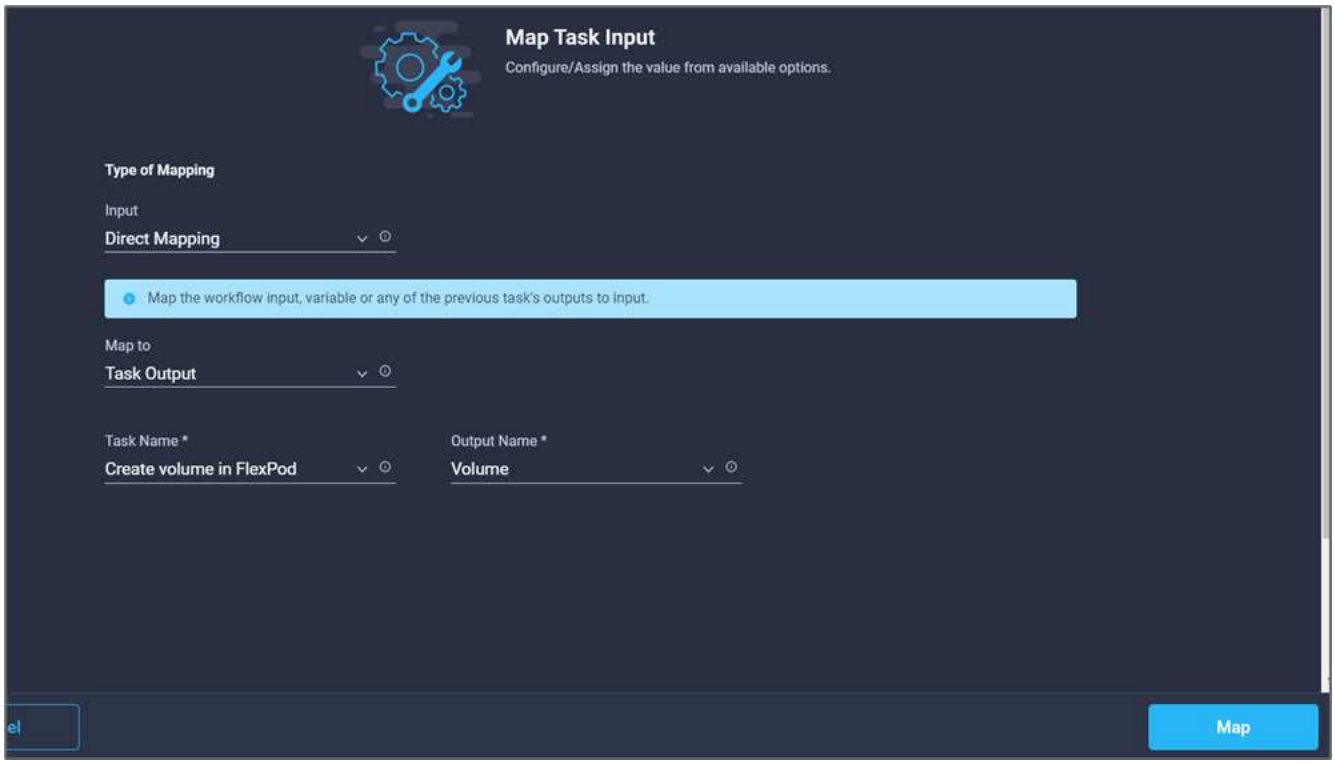


9. Cliquez sur **Map** dans le champ **Storage Vendor Virtual machine**.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner Storage Virtual machine**. Sélectionnez la même machine virtuelle de stockage ajoutée lors de la création de la précédente tâche de création d'un volume de stockage.

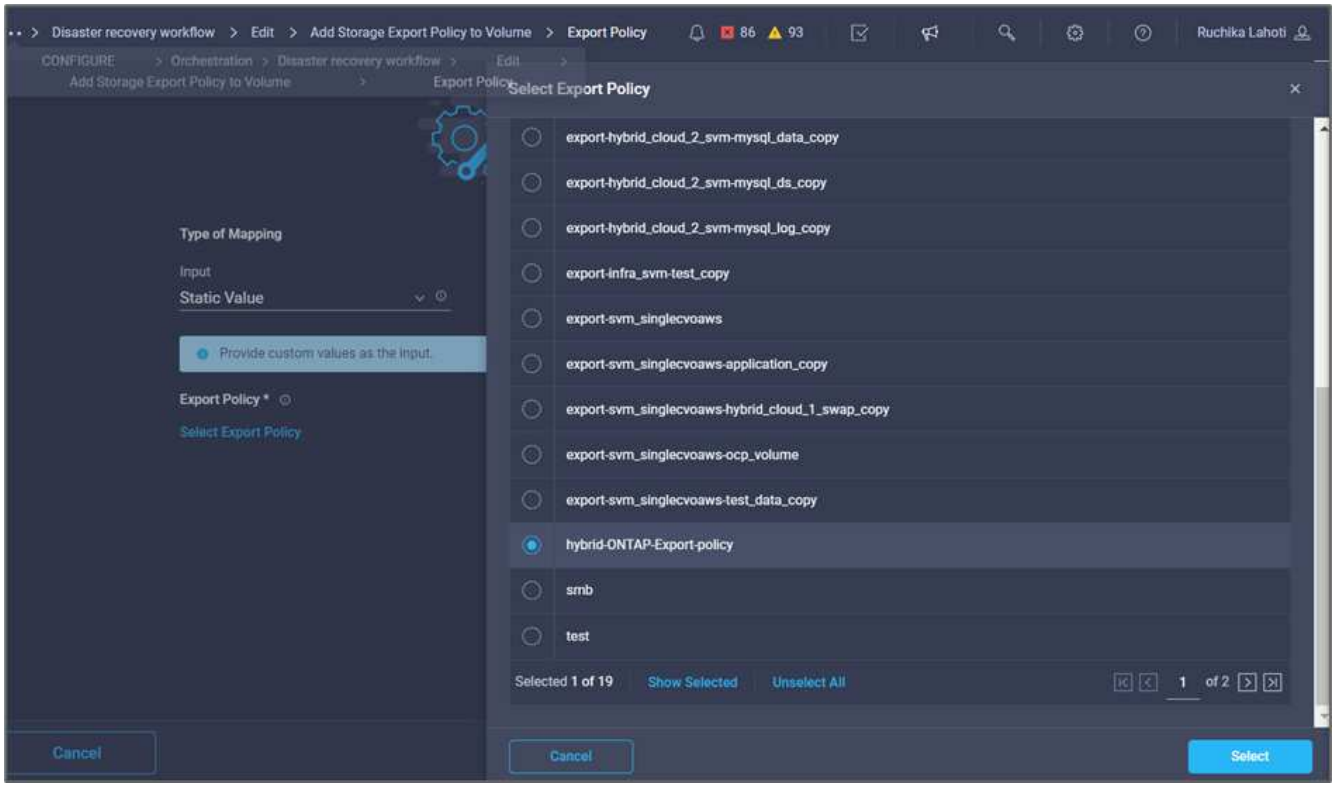


11. Cliquez sur **carte**.
12. Cliquez sur **Map** dans le champ **Volume**.
13. Cliquez sur **Nom de la tâche**, puis sur **Créer un volume dans FlexPod**. Cliquez sur **Nom de sortie**, puis sur **Volume**.

> Dans Cisco Intersight Cloud Orchestrator, vous pouvez fournir la sortie d'une tâche précédente comme entrée pour une nouvelle tâche. Dans cet exemple, les détails **Volume** ont été fournis à partir de la tâche **Créer un volume dans FlexPod** sous forme d'entrée pour la tâche **Ajouter une stratégie d'exportation de stockage**.



14. Cliquez sur **carte**.
15. Cliquez sur **carte** dans le champ **politique d'exportation**.
16. Choisissez **valeur statique** et cliquez sur **Sélectionner stratégie d'exportation**. Sélectionner la export policy créée.

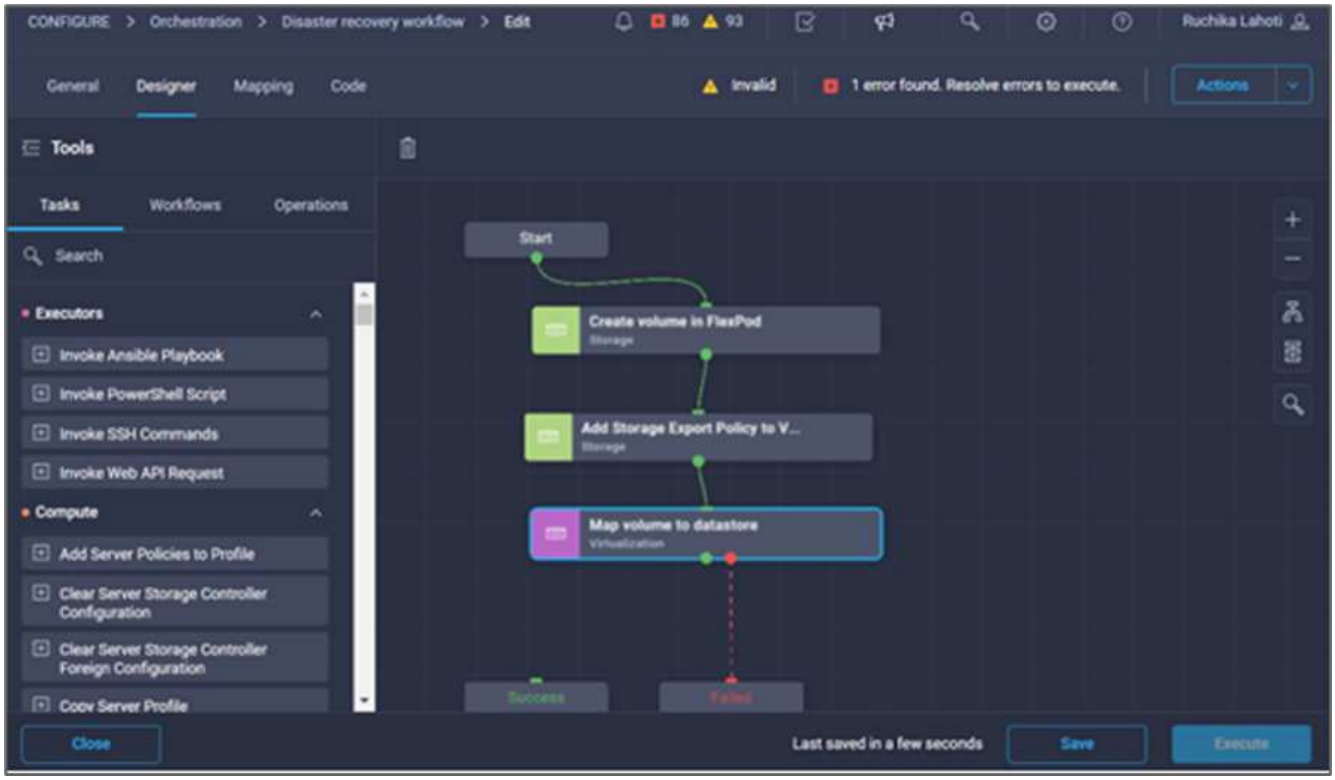


17. Cliquez sur **carte**, puis sur **Enregistrer**.

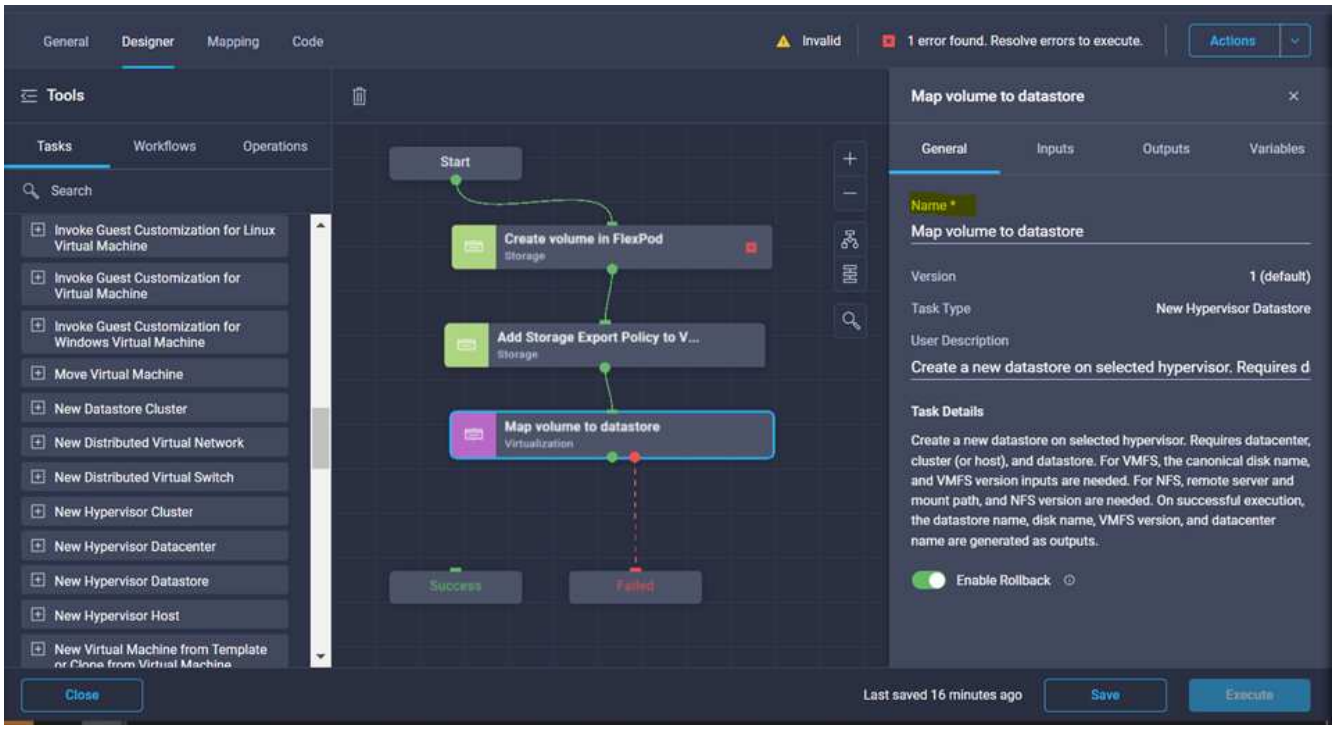
L’ajout d’une export-policy au volume est maintenant terminé. Ensuite, vous créez un nouveau datastore mappant le volume créé.

Procédure 4 : mappe de volumes FlexPod sur le datastore

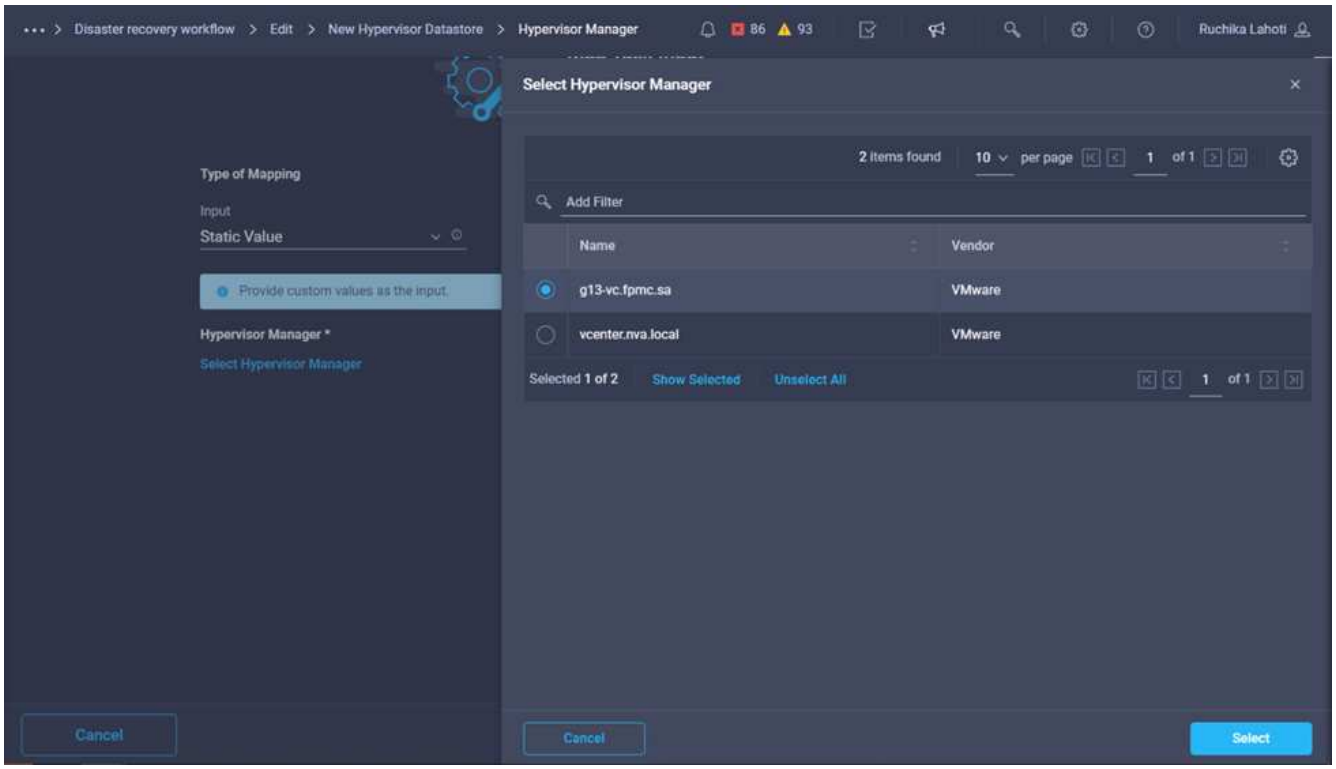
1. Accédez à l’onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **virtualisation > Nouveau datastore d’hyperviseur** de la section **Outils** de la zone **Design**.
3. Utilisez Connector pour établir une connexion entre les tâches **Ajouter stratégie d’exportation de stockage** et **Nouveau datastore d’hyperviseur**. Cliquez sur **Enregistrer**.



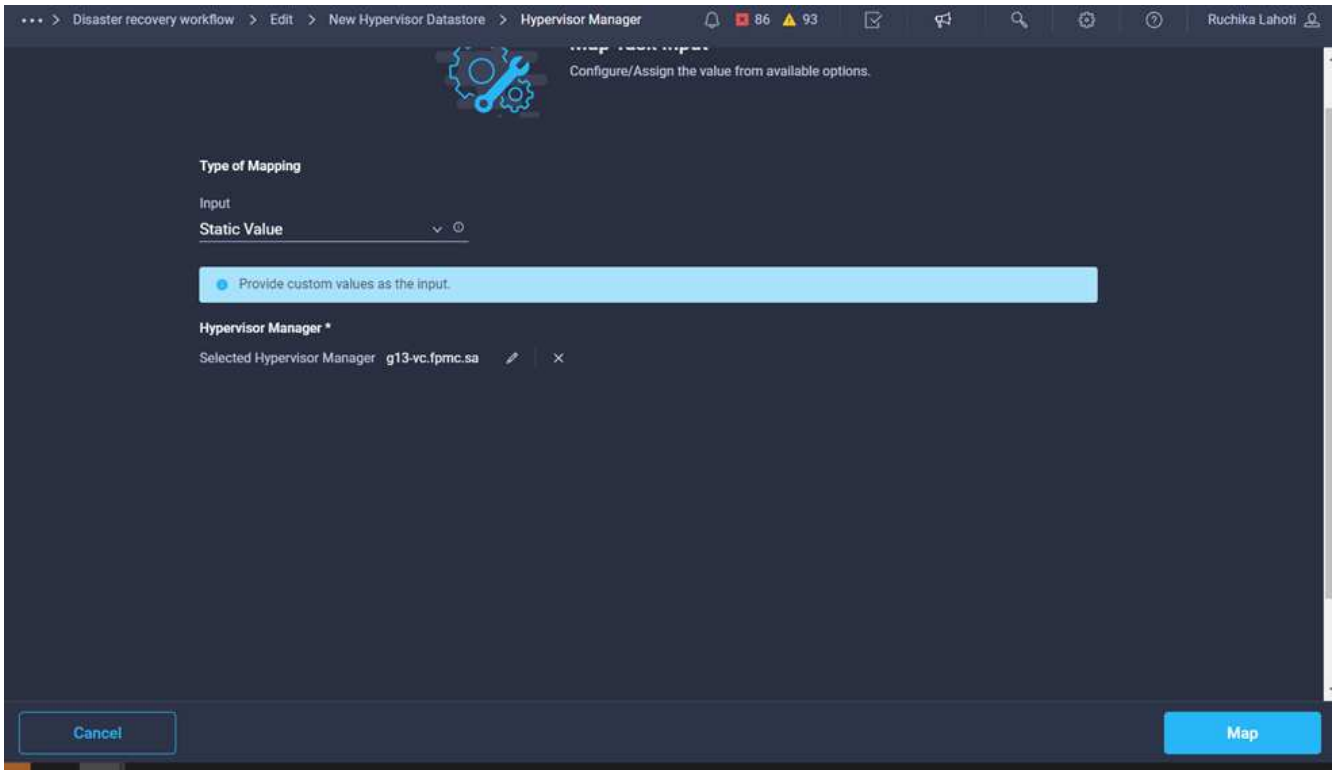
4. Cliquez sur **Nouveau datastore d’hyperviseur**. Dans la zone **Propriétés de tâche**, cliquez sur l’onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **mapper le volume sur le datastore**.



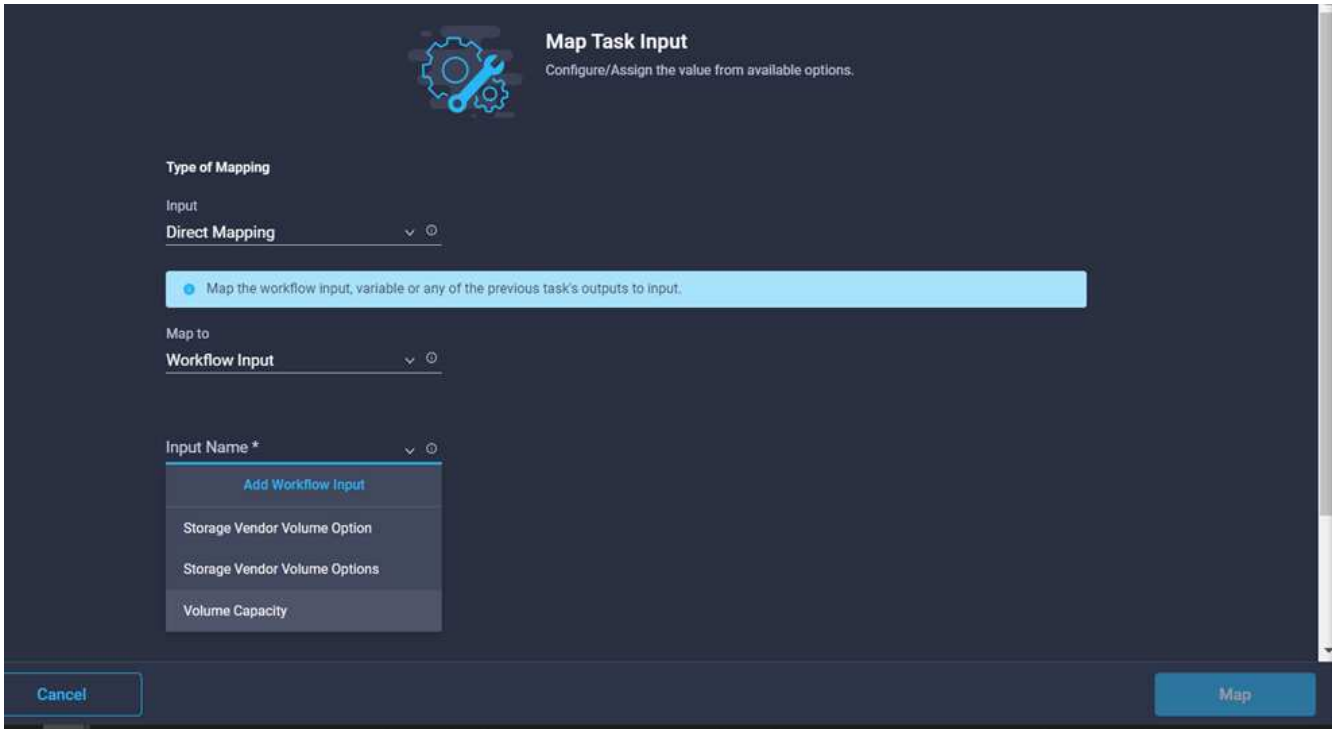
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Hypervisor Manager**.
7. Choisissez **valeur statique** et cliquez sur **Select Hypervisor Manager**. Cliquez sur la cible VMware vCenter.



8. Cliquez sur **carte**.



9. Cliquez sur **carte** dans le champ **Data Center**. Il s'agit du data Center associé au nouveau datastore.
10. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
11. Cliquez sur **Nom d'entrée**, puis sur **Créer entrée de flux de travail**.

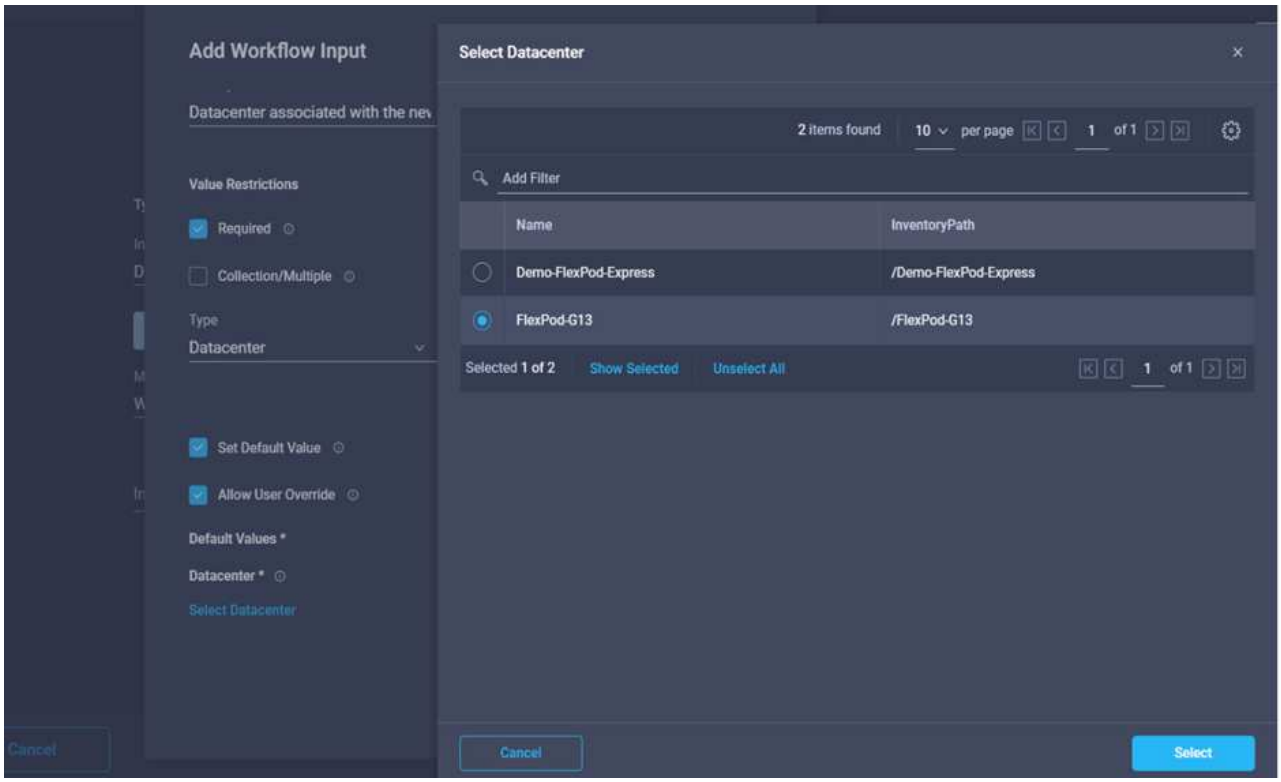


12. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Sélectionnez **Datacenter** comme type.

c. Cliquez sur **définir la valeur par défaut et remplacer**.

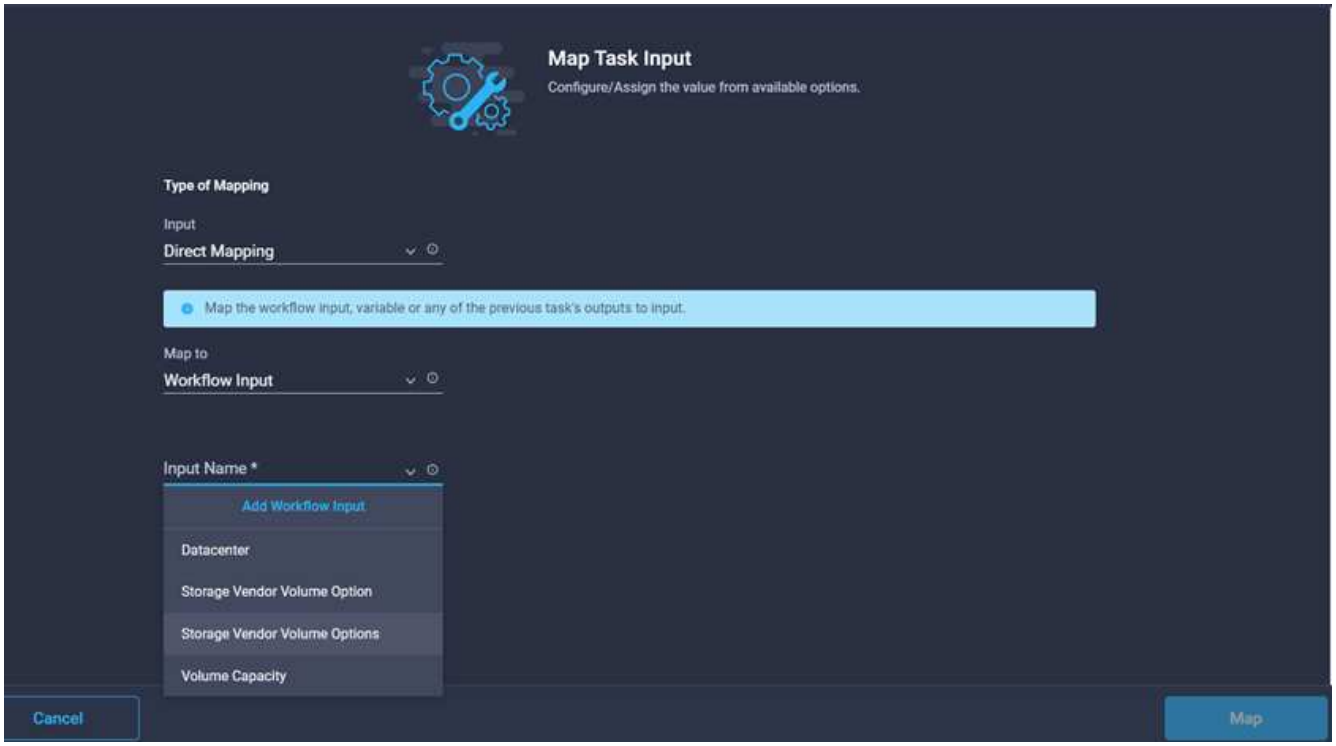
d. Cliquez sur **Select Datacenter**.

e. Cliquez sur le centre de données associé au nouveau datastore, puis sur **Select**.

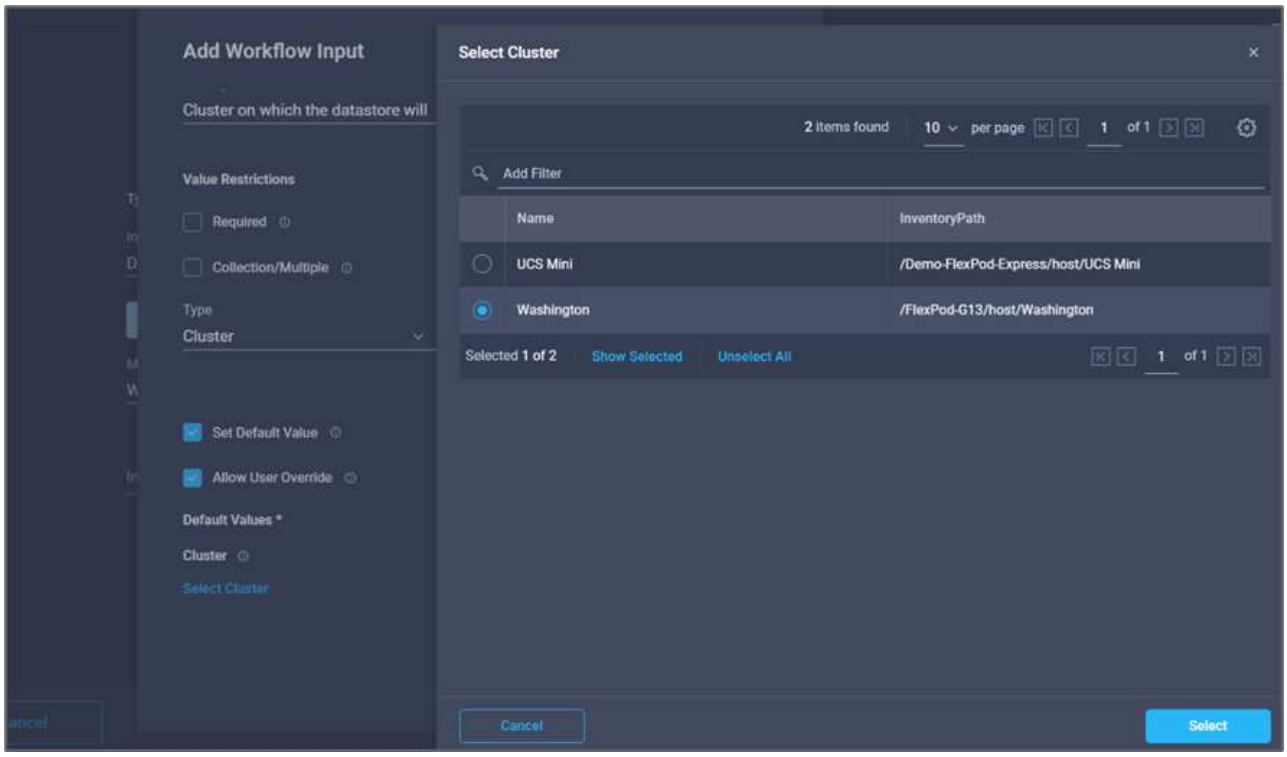


- Cliquez sur **Ajouter**.

13. Cliquez sur **carte**.
14. Cliquez sur **carte** dans le champ **Cluster**.
15. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.

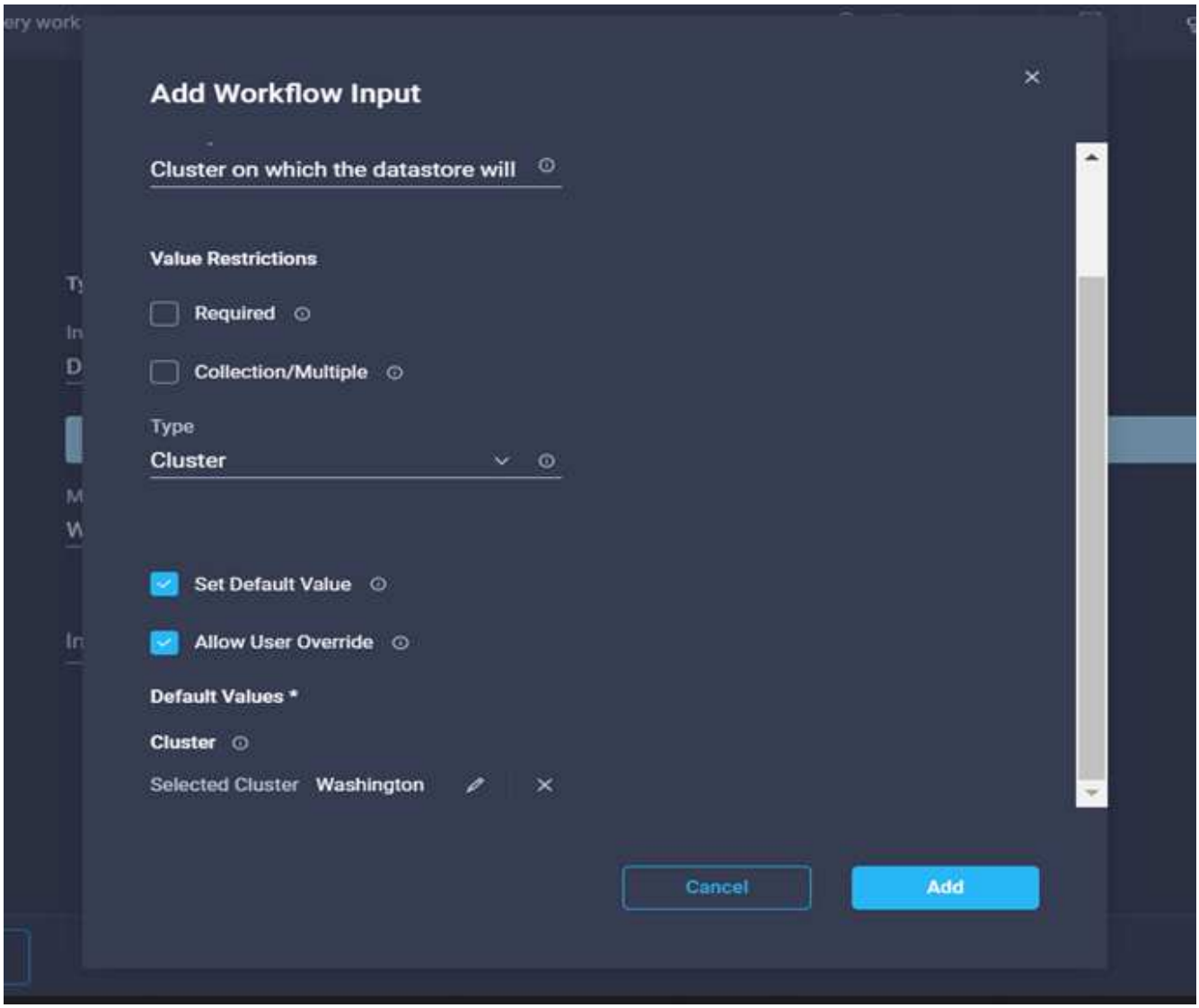


16. Dans l’assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d’affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Sélectionnez Cluster comme type.
    d. Cliquez sur **définir la valeur par défaut et remplacer**.
    e. Cliquez sur **Sélectionner un cluster**.
    f. Cliquez sur le cluster associé au nouveau datastore.
    g. Cliquez sur **Sélectionner**.

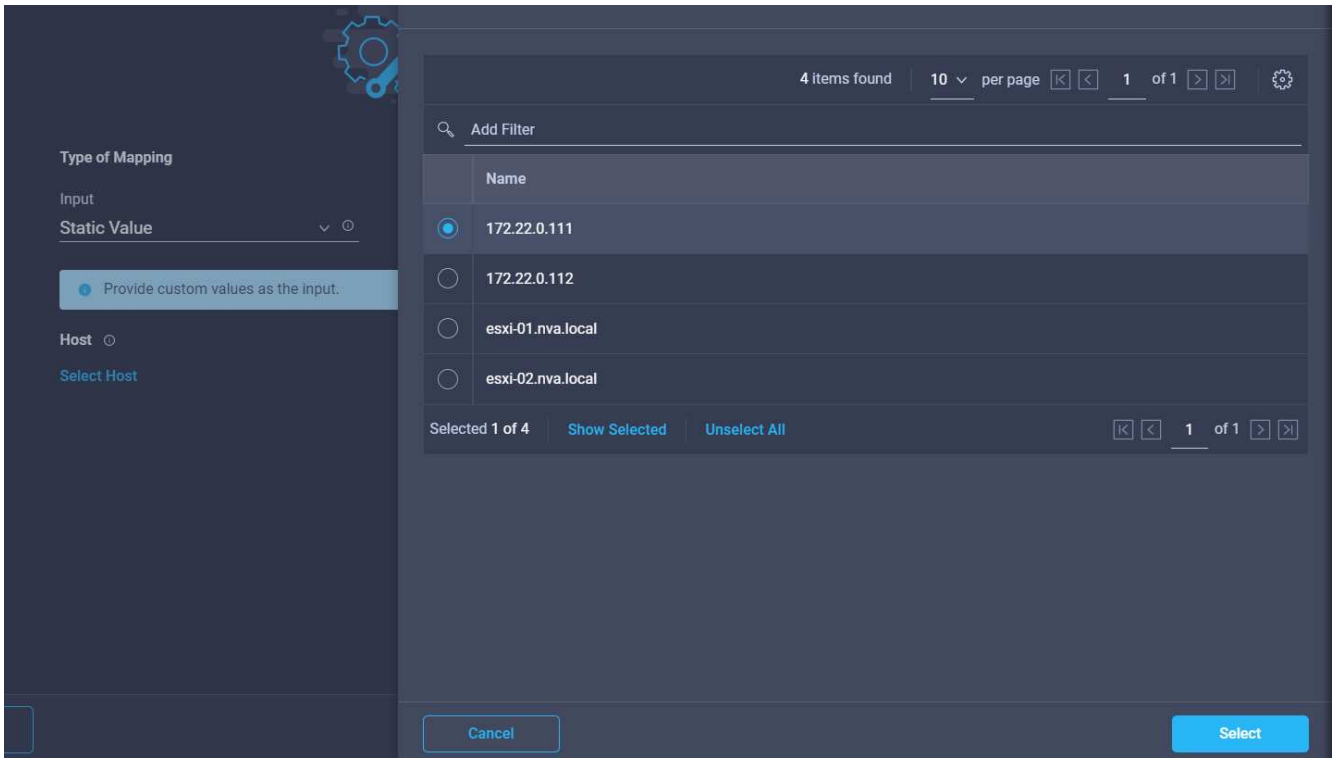


h. Cliquez sur **Ajouter**.

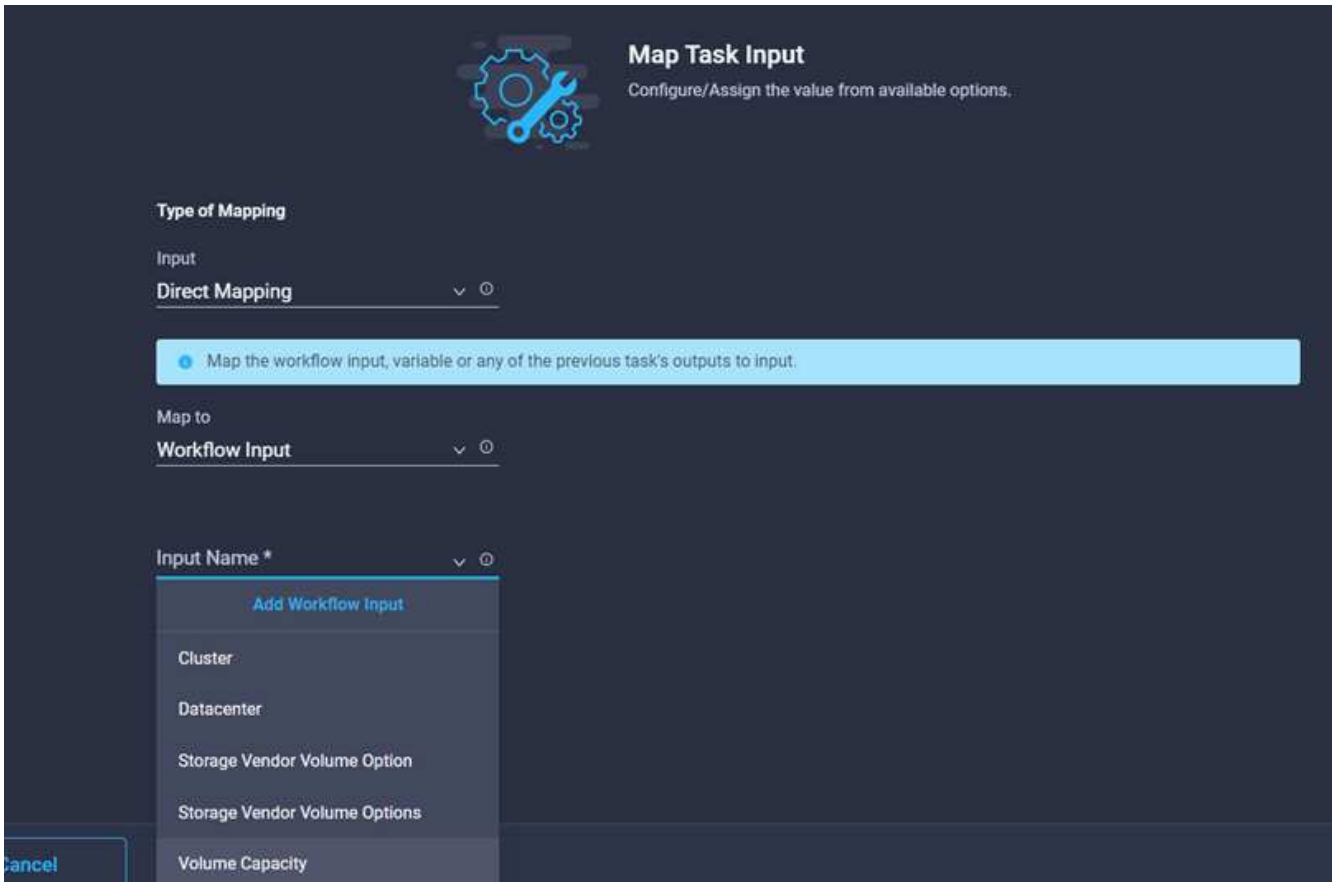
17. Cliquez sur **carte**.
18. Cliquez sur **Map** dans le champ **Host**.



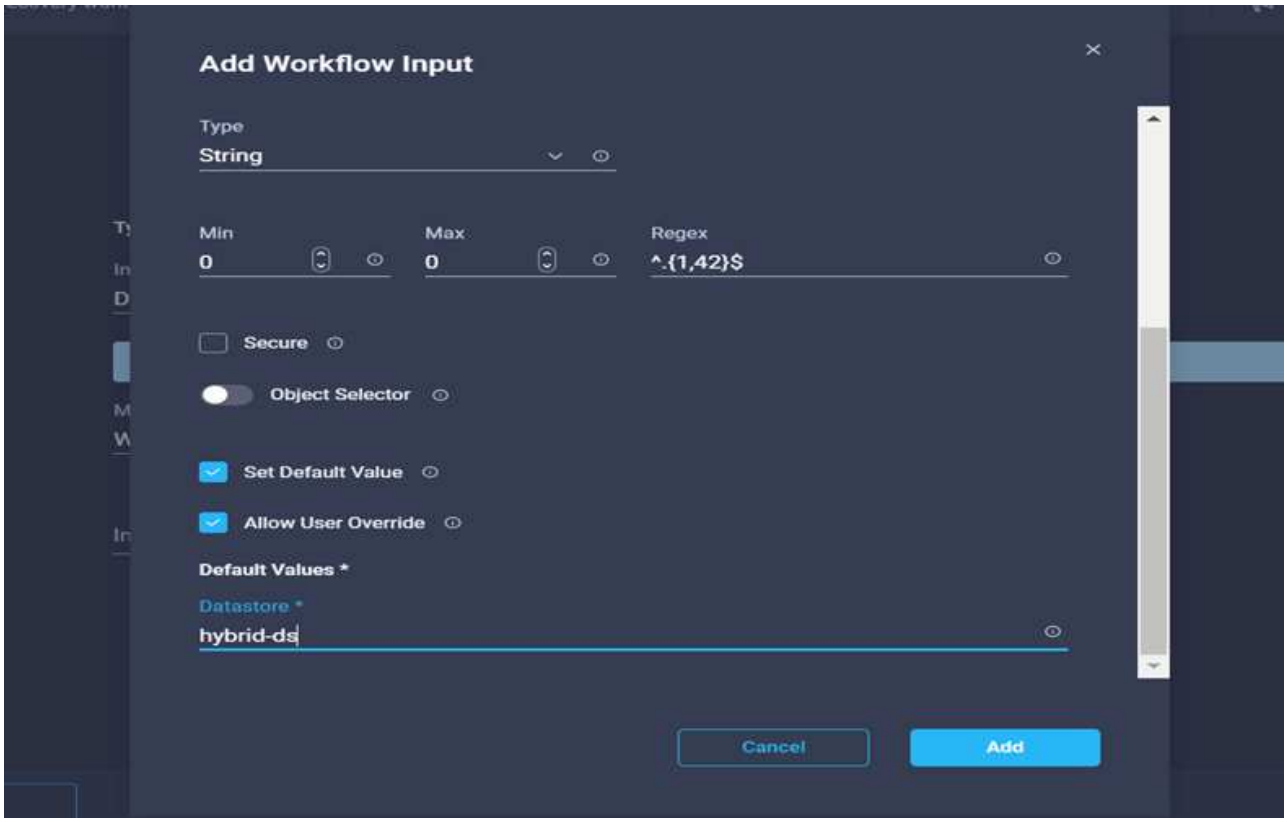
19. Choisissez **valeur statique** et cliquez sur l'hôte sur lequel le datastore sera hébergé. Si un cluster est spécifié, l'hôte est ignoré.



20. Cliquez sur **Sélectionner et carte**.
21. Cliquez sur **Map** dans le champ **datastore**.
22. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
23. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.

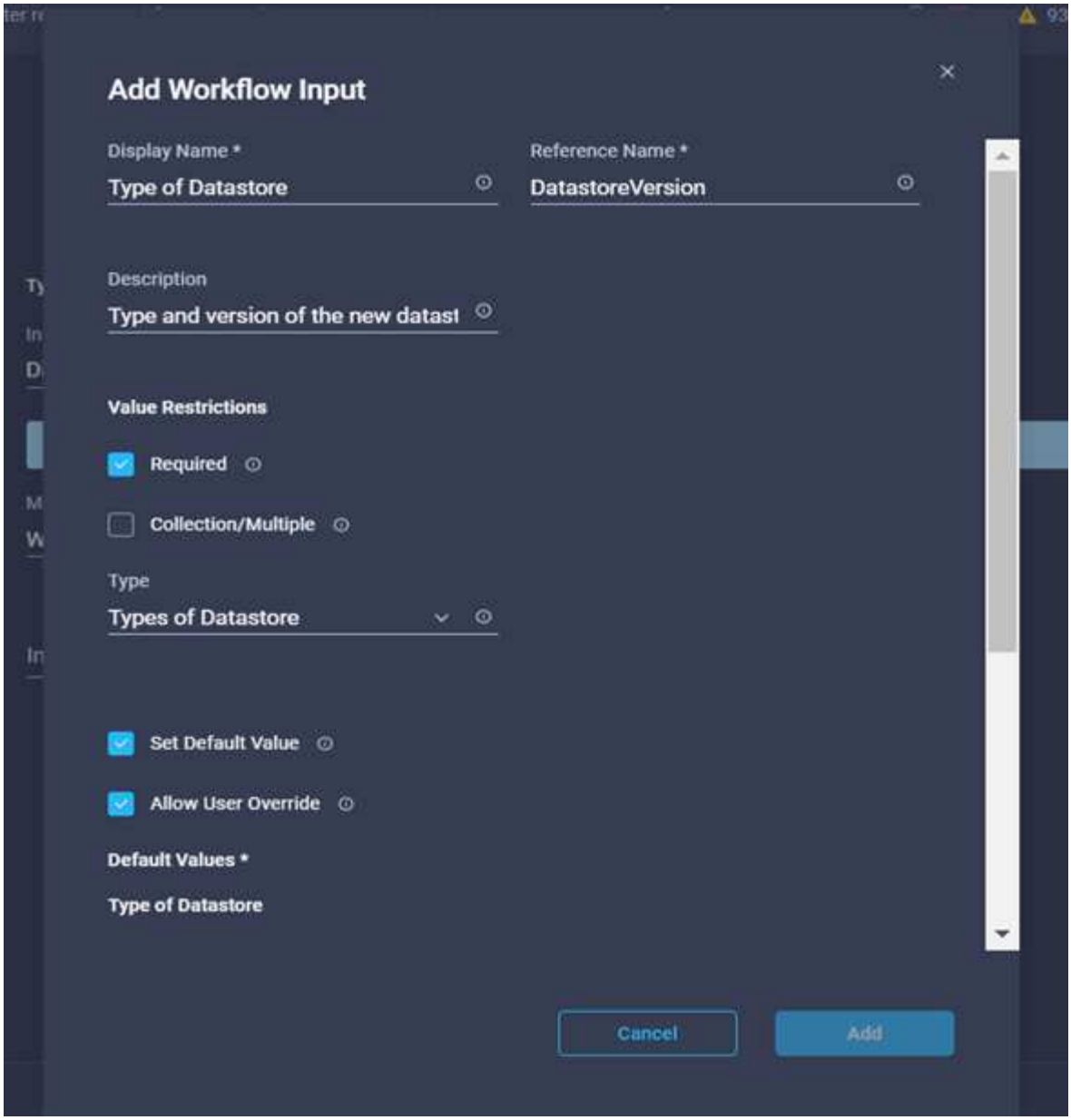


24. Dans l’assistant Ajouter une entrée :
    a. Indiquez un nom d’affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Indiquez une valeur par défaut pour le datastore et cliquez sur **Ajouter**.



25. Cliquez sur **carte**.
26. Cliquez sur **carte** dans le champ de saisie **Type de datastore**.
27. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
28. Cliquez sur **Nom d’entrée** et **Créer une entrée de flux de travail**.

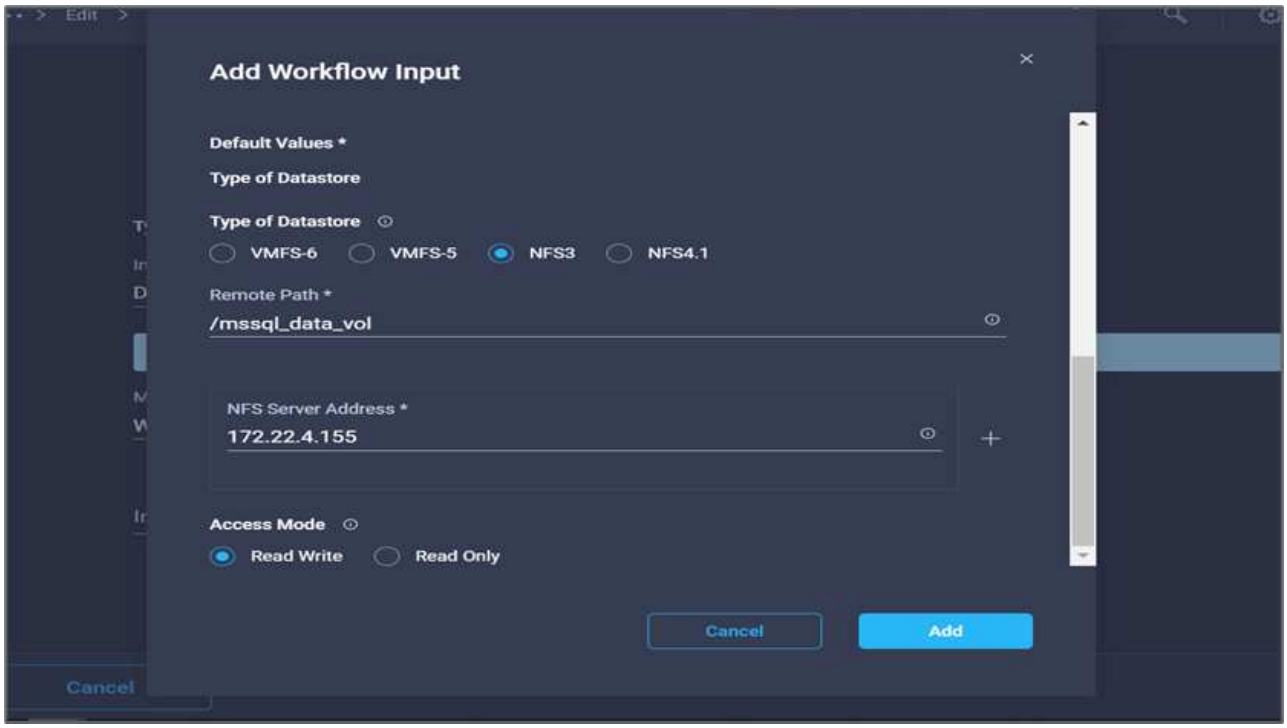
29. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif) et cliquez sur **requis**.
    b. Assurez-vous de sélectionner le type **types de datastore** et cliquez sur **définir la valeur par défaut et remplacer**.



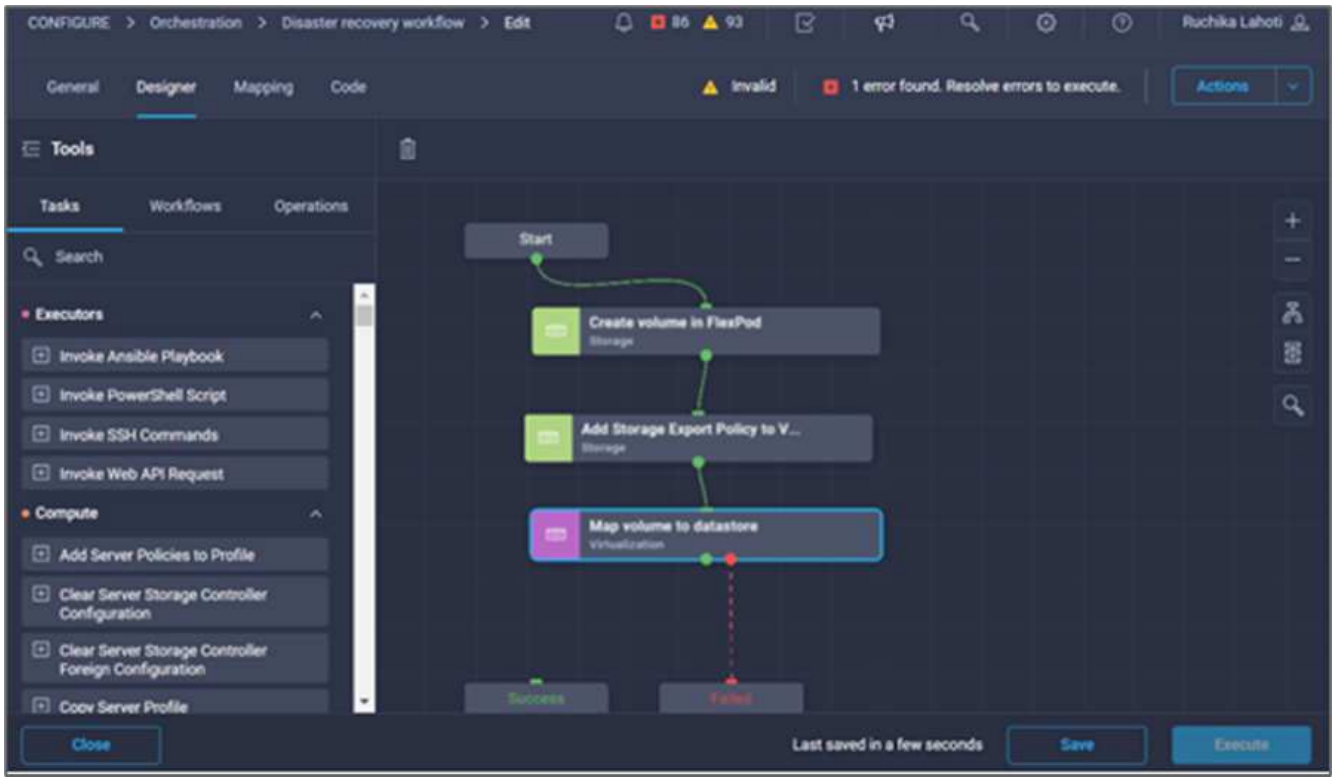
c. Indiquez le chemin distant. Il s'agit du chemin d'accès distant du point de montage NFS.

d. Indiquez les noms d'hôte ou les adresses IP du serveur NFS distant dans l'adresse du serveur NFS.

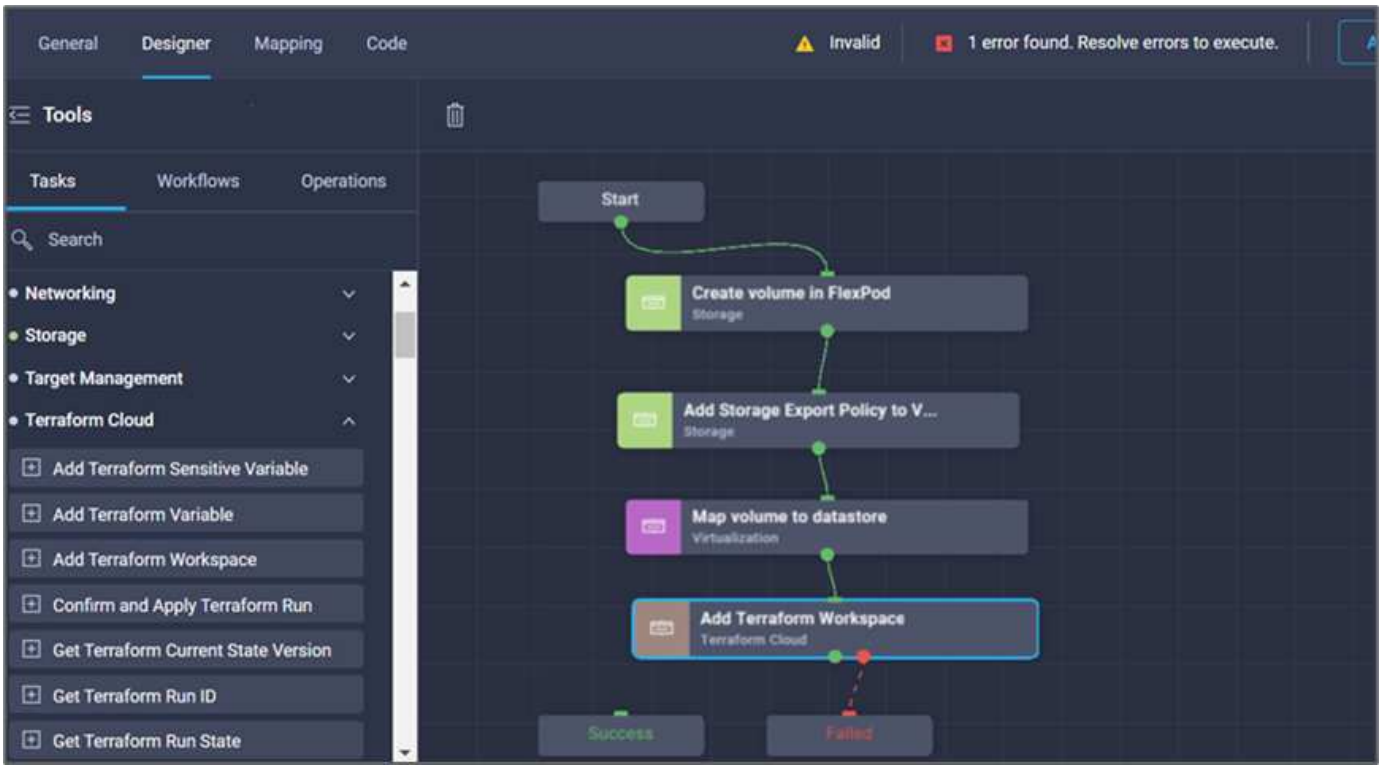
e. Cliquez sur le **mode d'accès**. Le mode d'accès est destiné au serveur NFS. Cliquez sur lecture seule si les volumes sont exportés en lecture seule. Cliquez sur **Ajouter**.



30. Cliquez sur **carte**.
31. Cliquez sur **Enregistrer**.

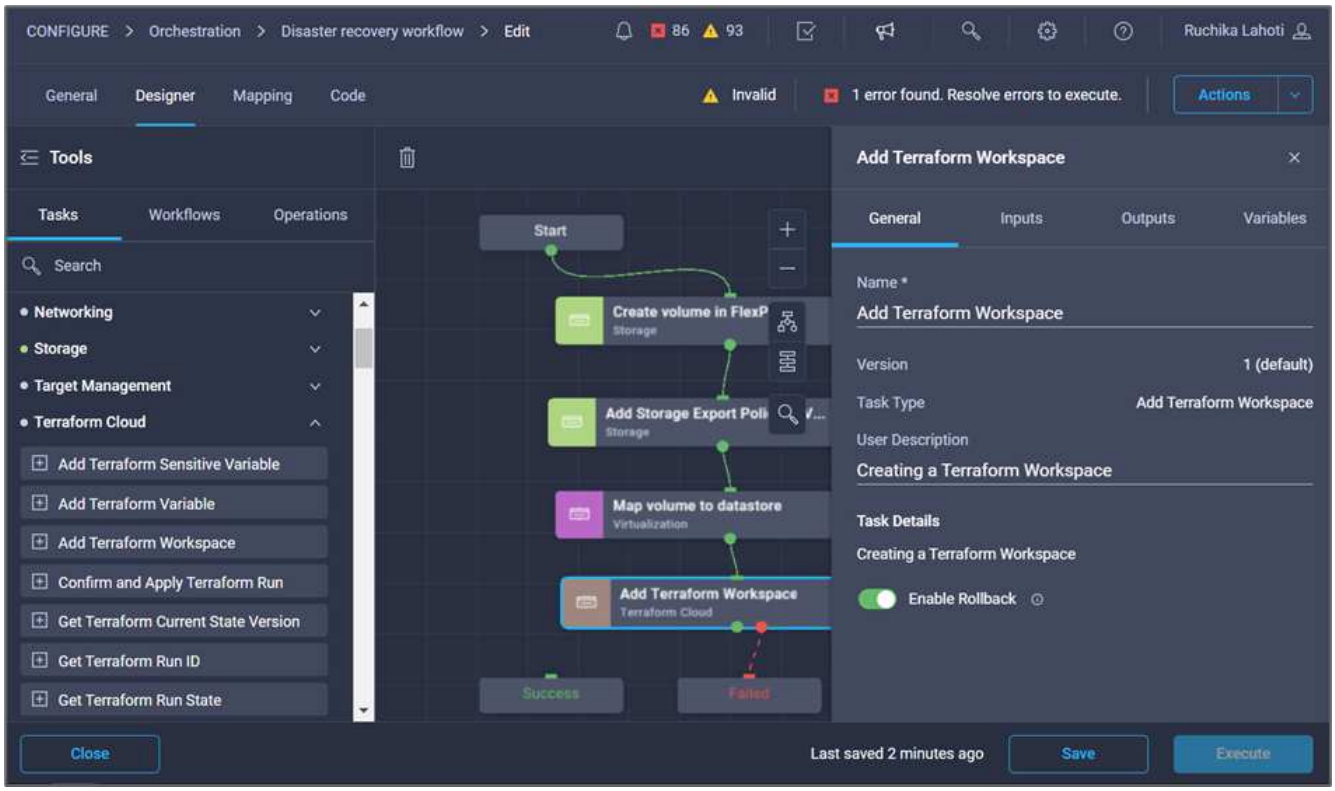


La tâche de création du datastore est terminée. Toutes les tâches effectuées dans le data Center FlexPod sur site sont effectuées.

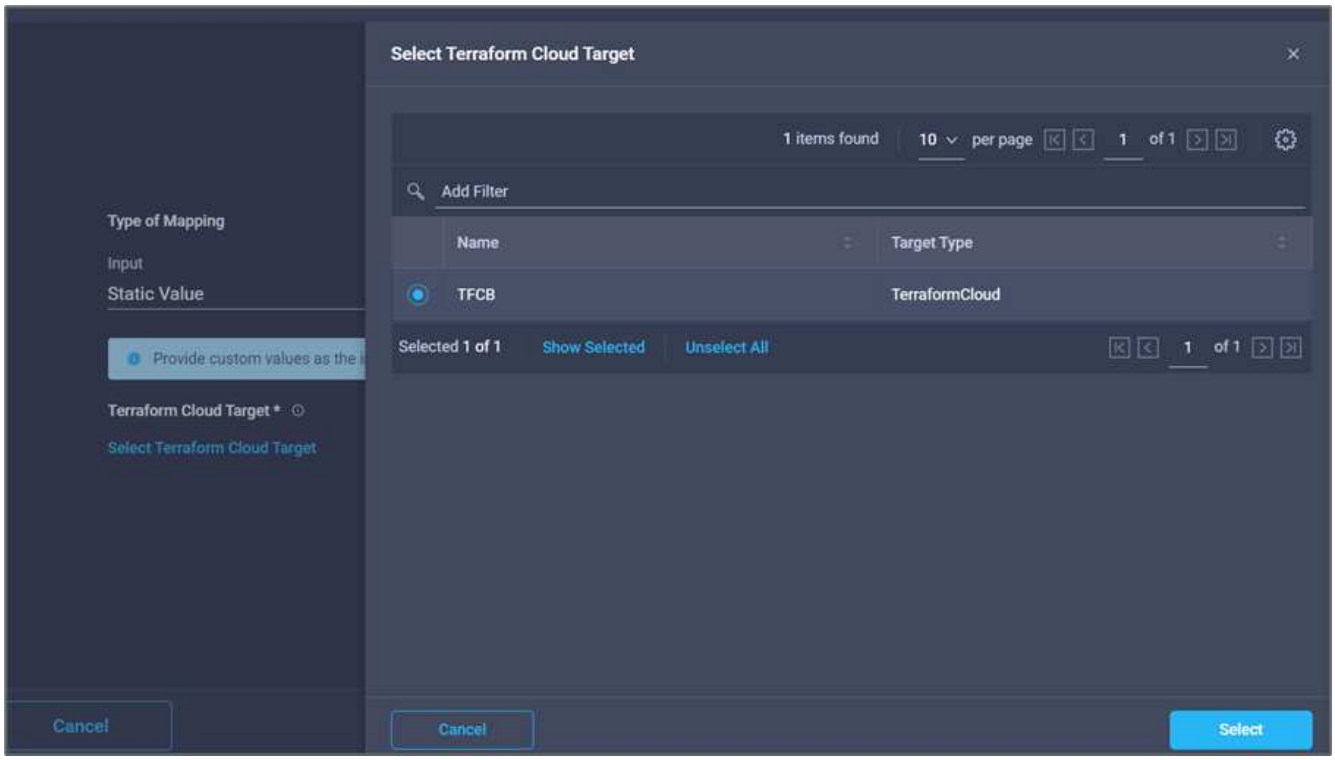


Procédure 5 : Ajout d'un nouvel espace de travail Terraform

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > Ajouter un espace de travail Terraform** dans la section Outils de la zone conception.
3. Utilisez Connector pour connecter les tâches **Map volume au datastore** et **Add Terraform Workspace** et cliquez sur **Save**.
4. Cliquez sur **Ajouter un espace de travail Terraform**. Dans la zone Propriétés de la tâche, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.

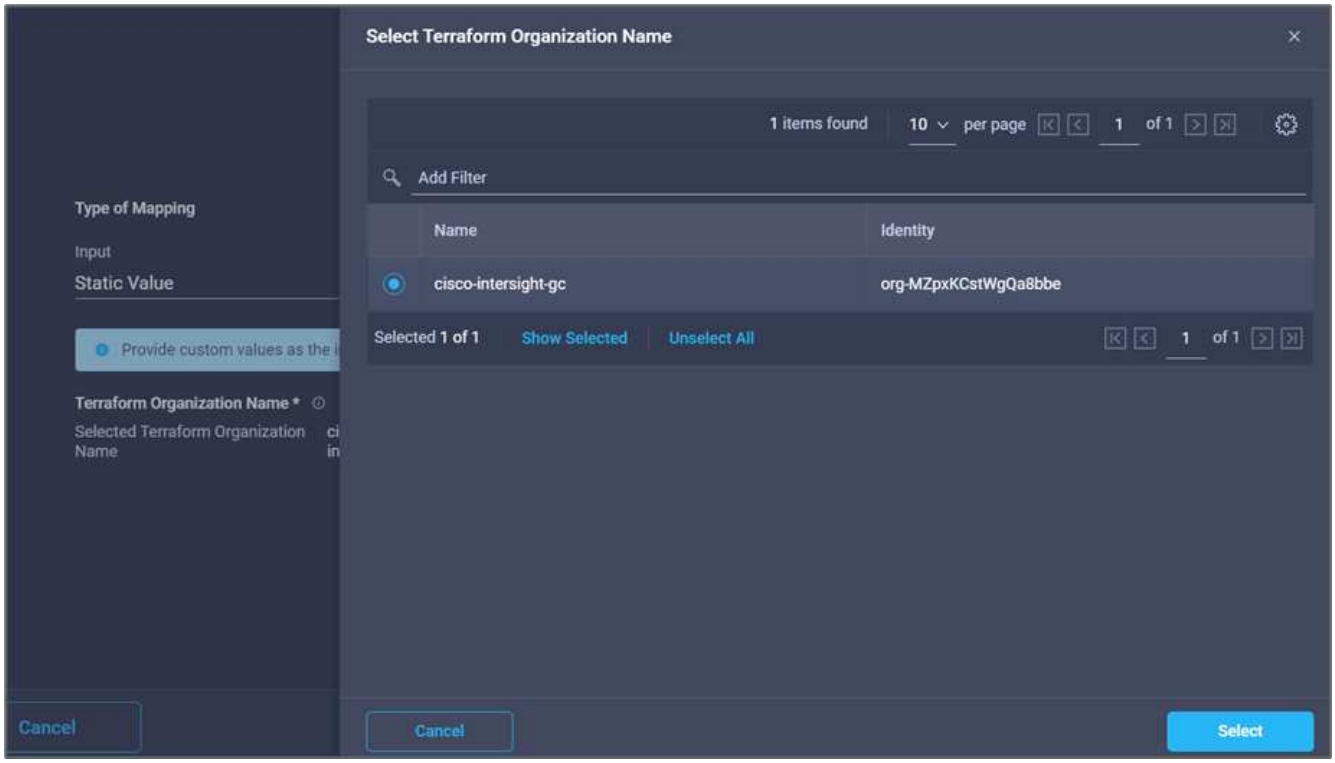


5. Dans la zone Propriétés de la tâche, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ de saisie **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté comme expliqué dans "Configurez Cisco Intersight Service pour HashiCorp Terraform". ».

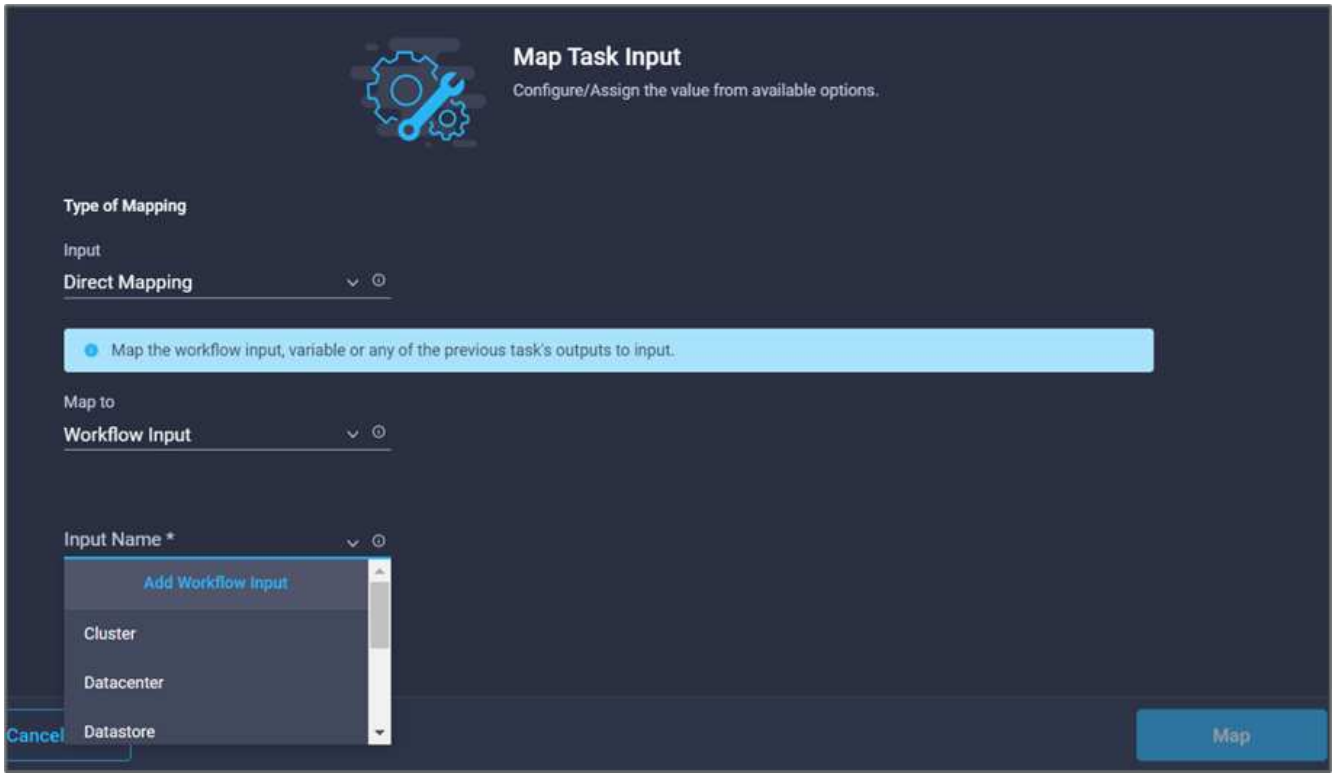


8. Cliquez sur **carte**.

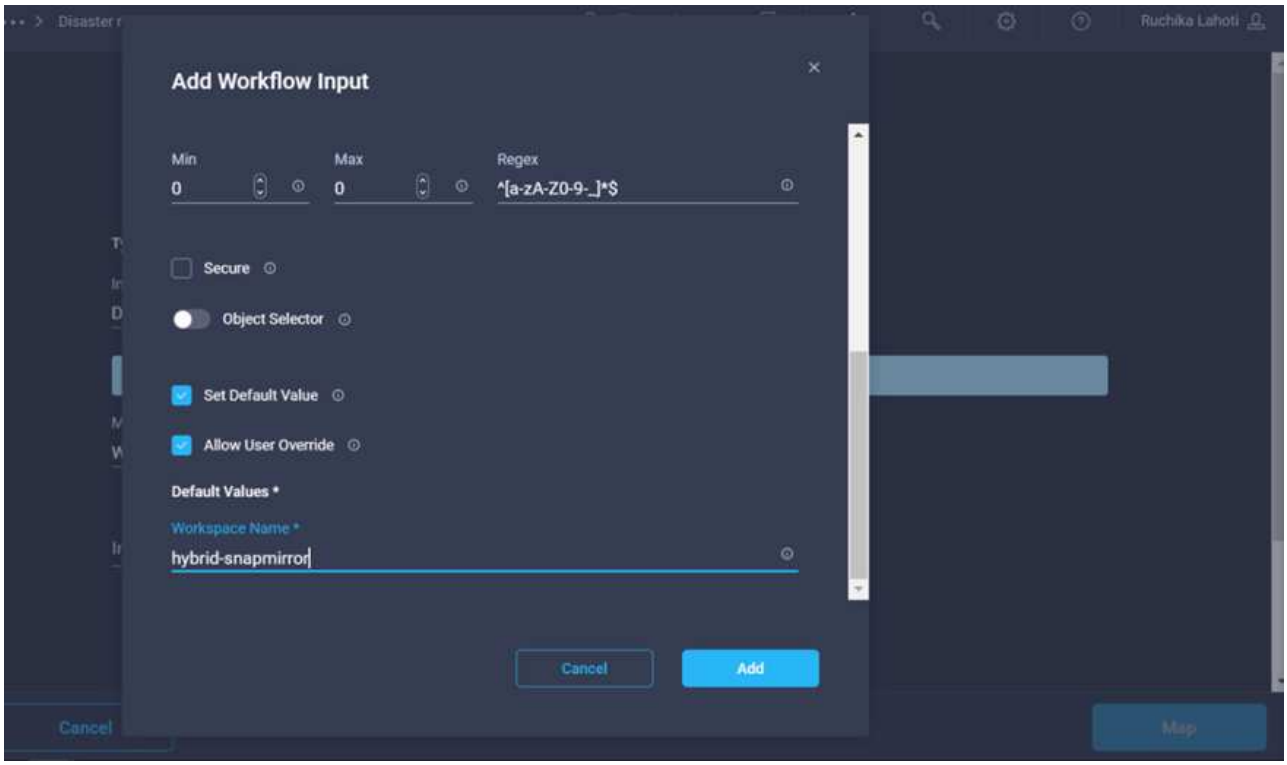
9. Cliquez sur **carte** dans le champ de saisie **Nom de l'organisation Terraform**.
10. Choisissez **valeur statique**, puis cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.



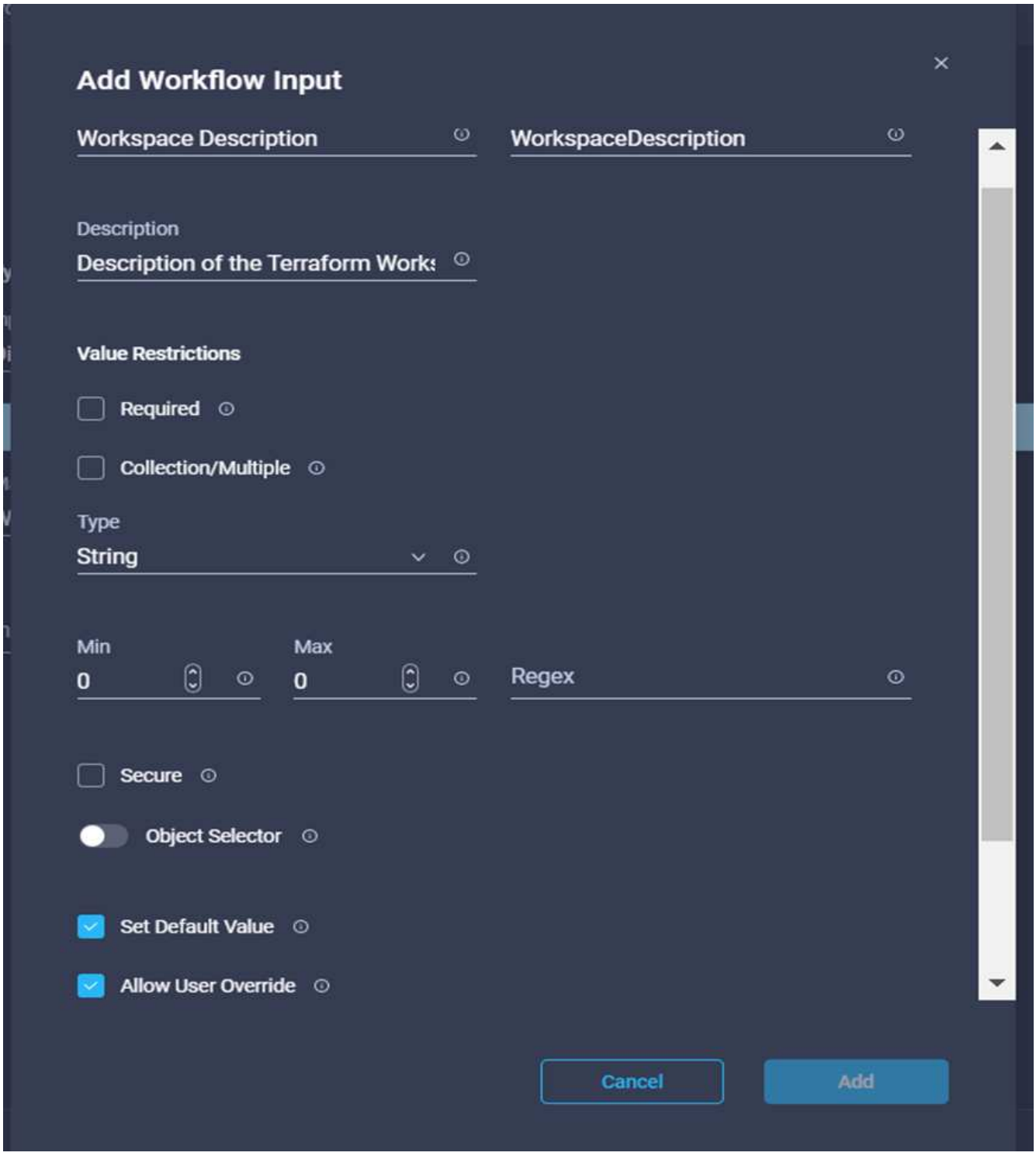
11. Cliquez sur **carte**.
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**. Il s'agit du nouvel espace de travail dans le compte Terraform Cloud for Business.
13. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
14. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



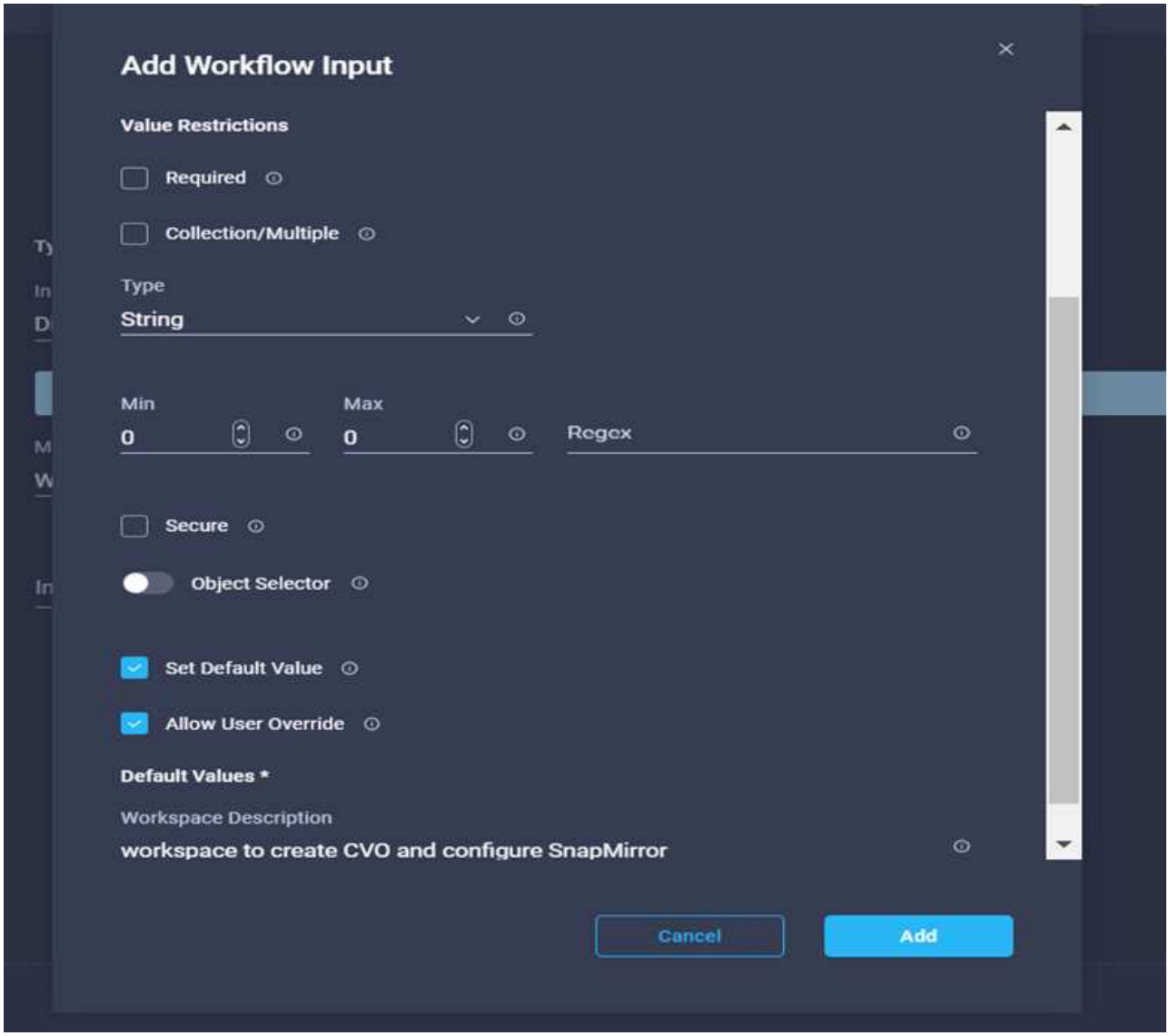
15. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Assurez-vous de sélectionner **String** pour **Type**.
    d. Cliquez sur **définir la valeur par défaut et remplacer**.
    e. Indiquez un nom par défaut pour l'espace de travail.
    f. Cliquez sur **Ajouter**.



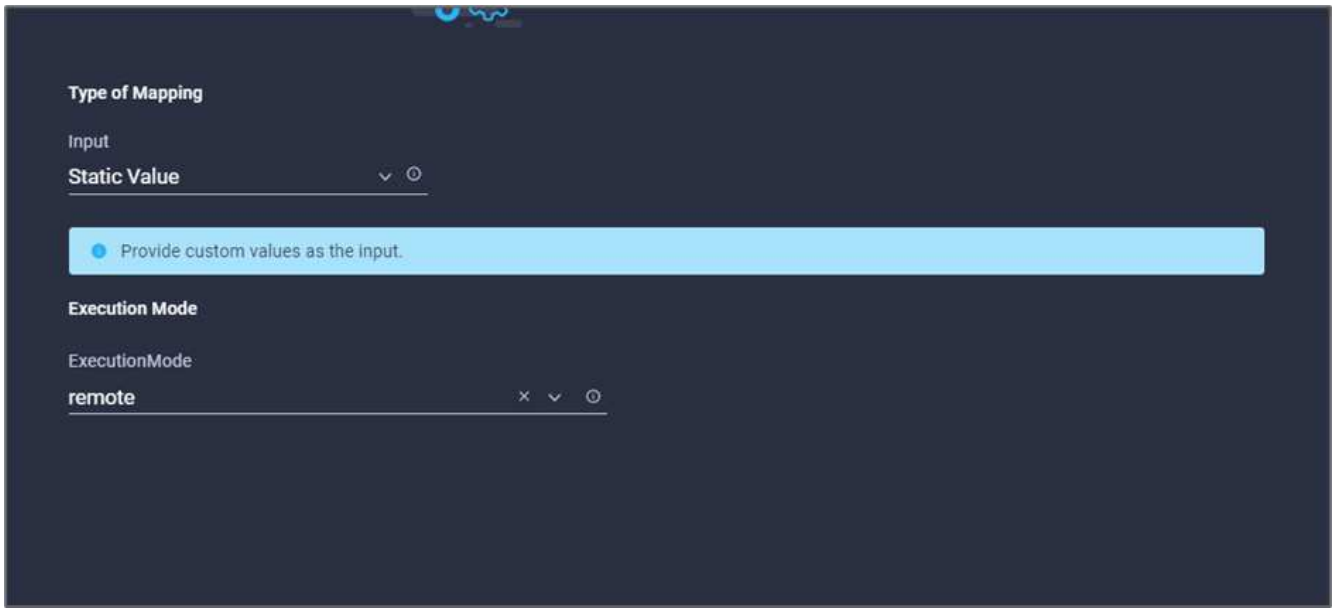
16. Cliquez sur **carte**.
17. Cliquez sur **carte** dans le champ **Description de l'espace de travail**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



20. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **String** pour **Type**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Fournissez une description de l'espace de travail et cliquez sur **Ajouter**.



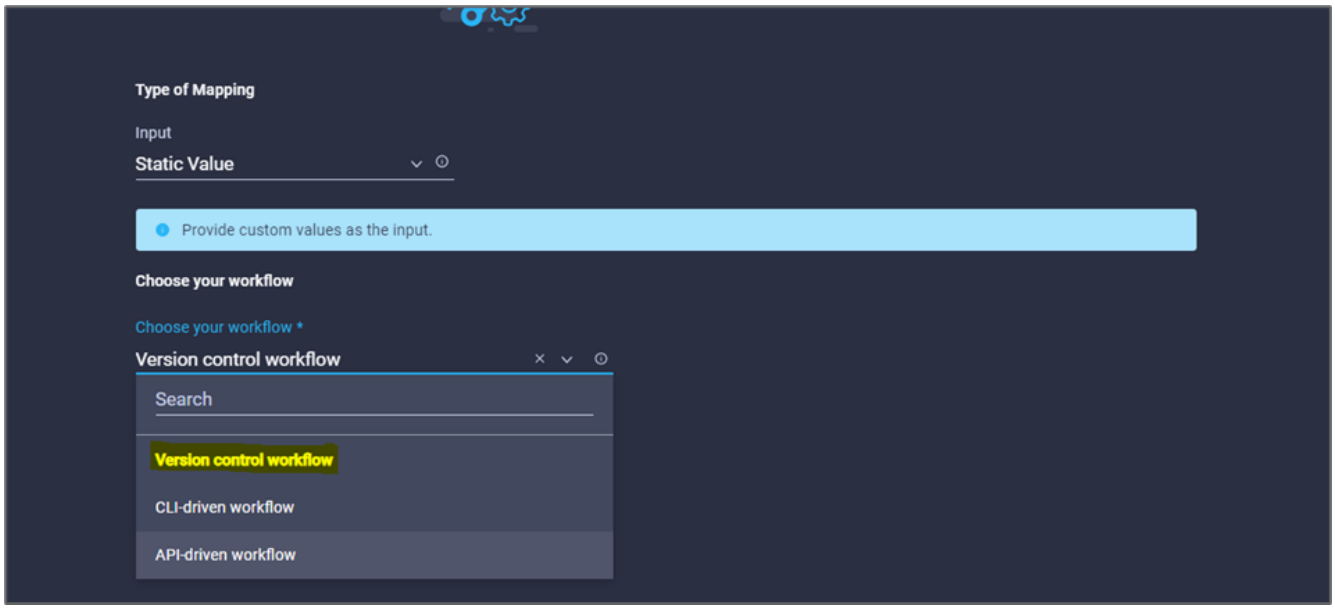
21. Cliquez sur **carte**.
22. Cliquez sur **Map** dans le champ **Execution mode**.
23. Choisissez **valeur statique**, cliquez sur **mode d'exécution**, puis sur **remote**.



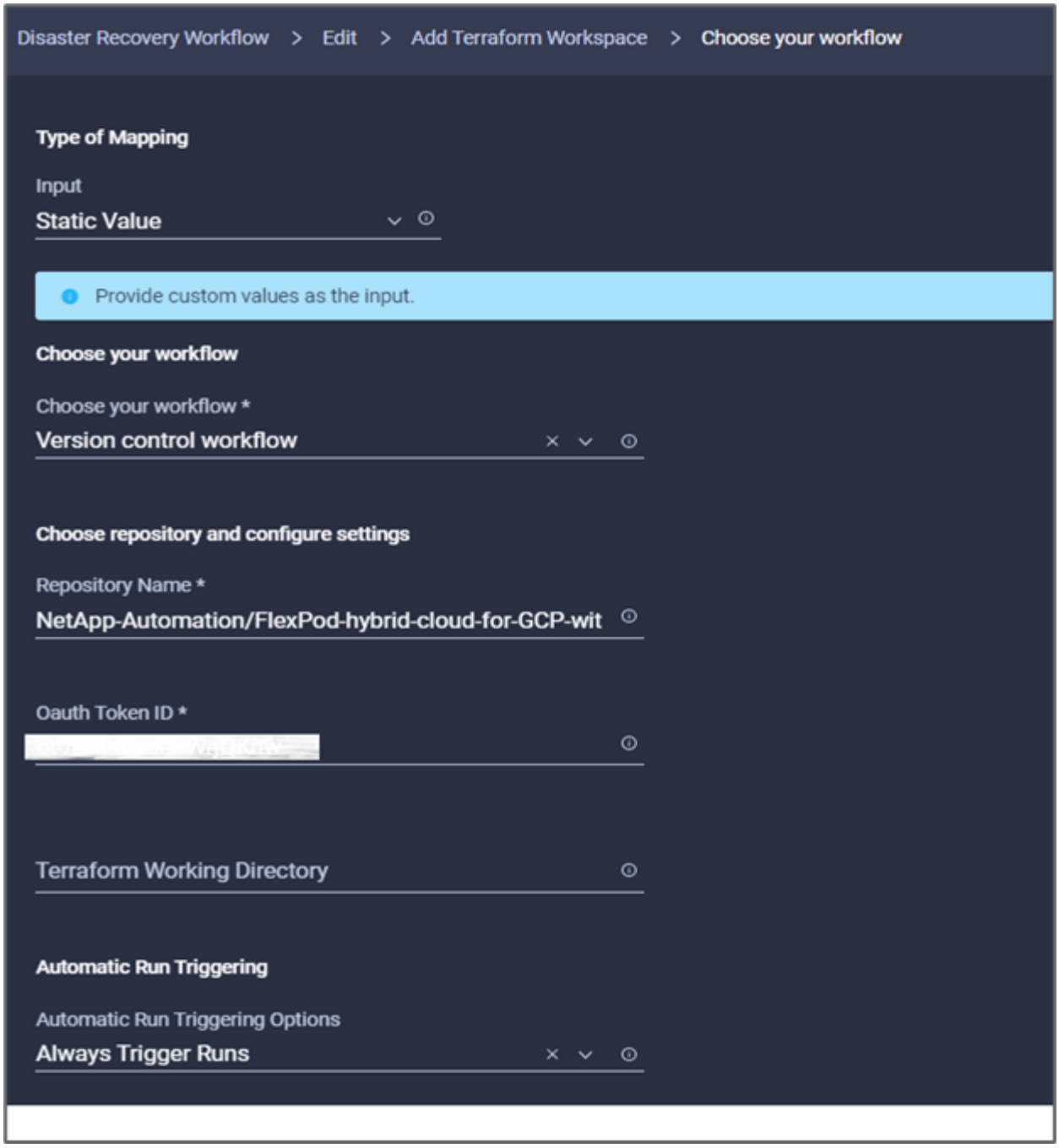
24. Cliquez sur **carte**.
25. Cliquez sur **carte** dans le champ **appliquer méthode**.
26. Choisissez **valeur statique** et cliquez sur **appliquer méthode**. Cliquez sur **application manuelle**.

27. Cliquez sur **carte**.
28. Cliquez sur **Map** dans le champ **User interface**.
29. Choisissez **valeur statique** et cliquez sur **interface utilisateur**. Cliquez sur **interface utilisateur de la console**.

30. Cliquez sur **carte**.
31. Cliquez sur **Map** dans le champ de saisie et sélectionnez votre flux de travail.
32. Sélectionnez **valeur statique**, puis cliquez sur **Choisissez votre flux de travail**. Cliquez sur **version Control Workflow**.



33. Fournissez les informations suivantes sur le référentiel GitHub :
    a. Dans **Nom du référentiel**, entrez le nom du référentiel détaillé dans la section "« Configurer les conditions préalables à l'environnement »".
    b. Indiquez l'ID de token OAuth comme détaillé dans la section "« Configurer les conditions préalables à l'environnement »".
    c. Sélectionnez l'option **déclenchement automatique**.



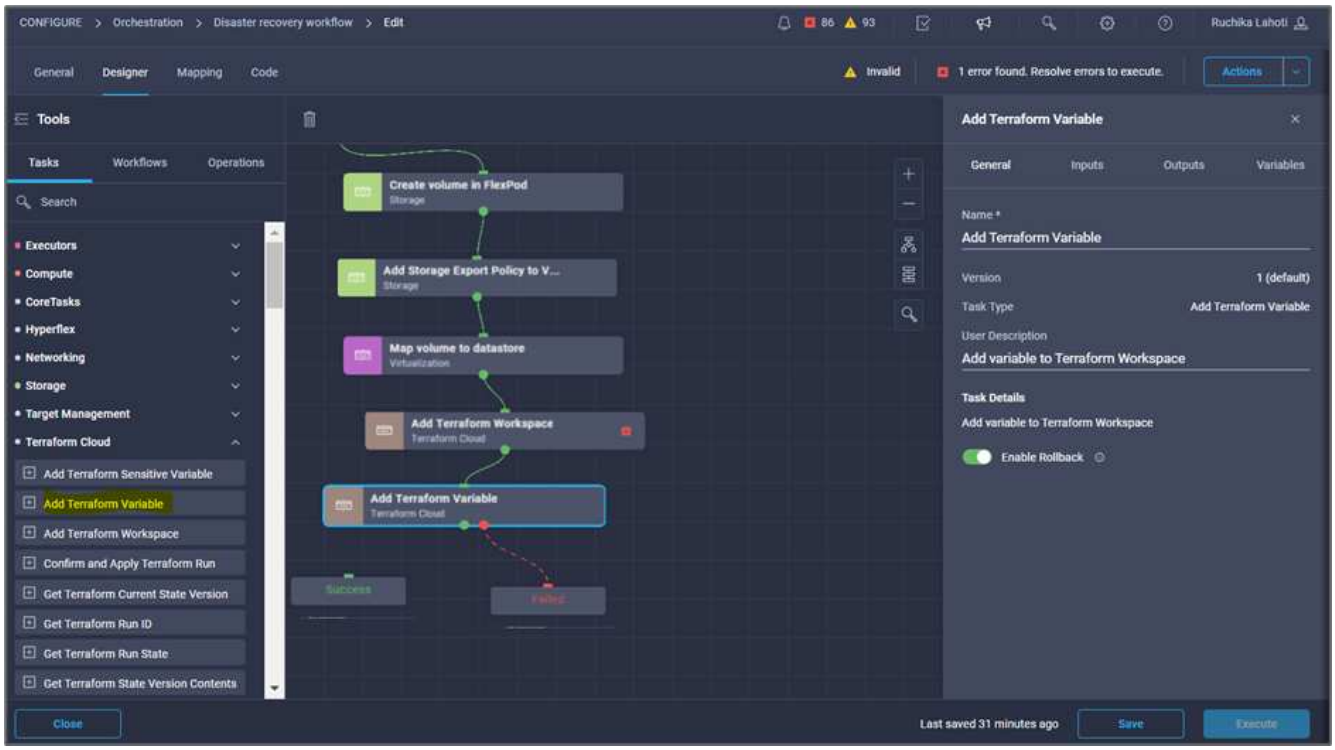
34. Cliquez sur **carte**.
35. Cliquez sur **Enregistrer**.

Cela termine la création d'un espace de travail dans un compte Terraform Cloud for Business.

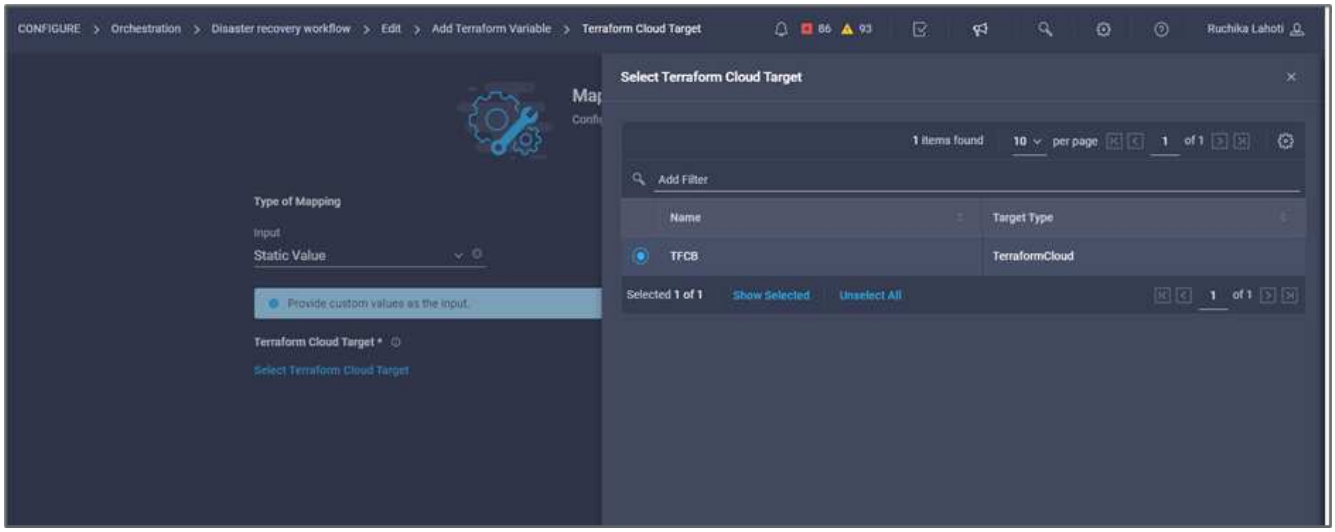
Procédure 6 : ajoutez des variables non sensibles à l'espace de travail

1. Accédez à l'onglet **Designer** et cliquez sur la section **workflows à partir d'Outils**.
2. Faites glisser et déposez le flux de travail **Terraform > Ajouter des variables Terraform** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Add Terraform Workspace** et **Add Terraform variables**. Cliquez sur **Enregistrer**.

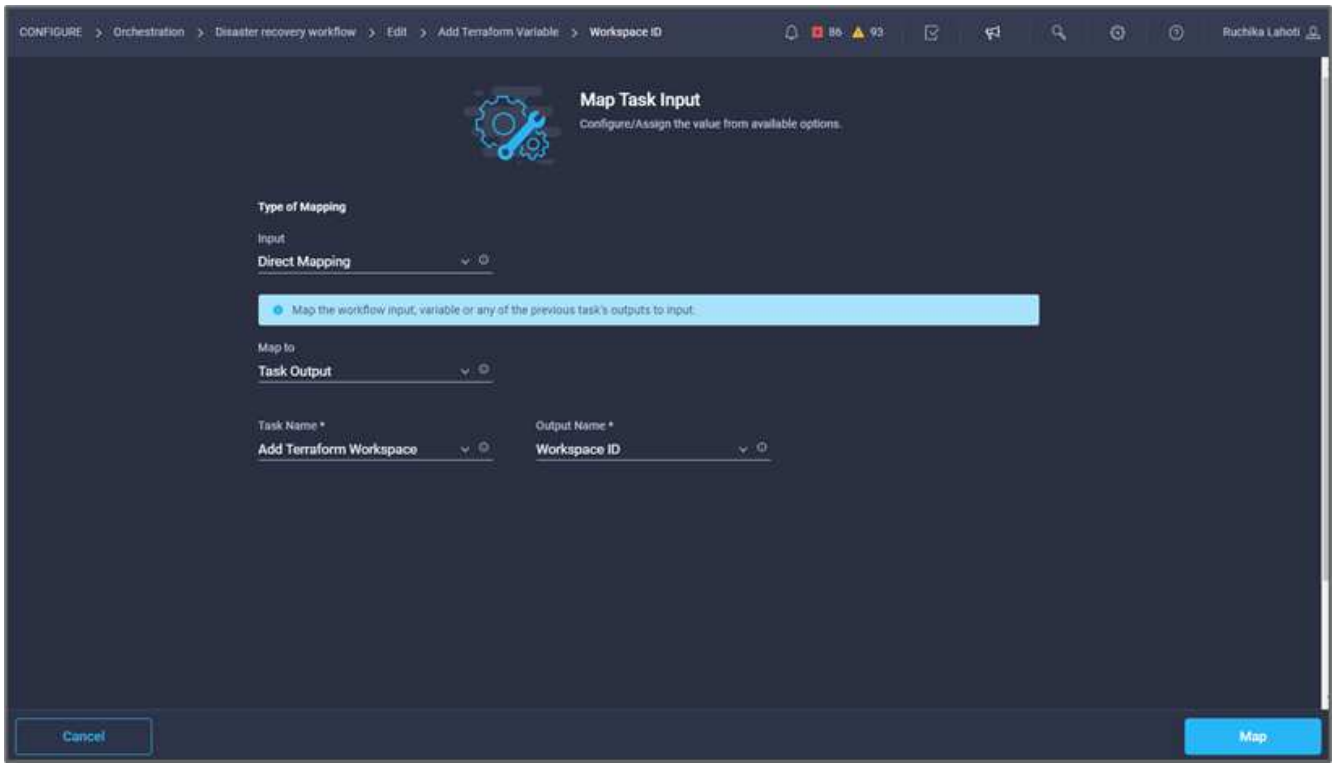
4. Cliquez sur **Ajouter variables Terraform**. Dans la zone **Propriétés du flux de travail**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



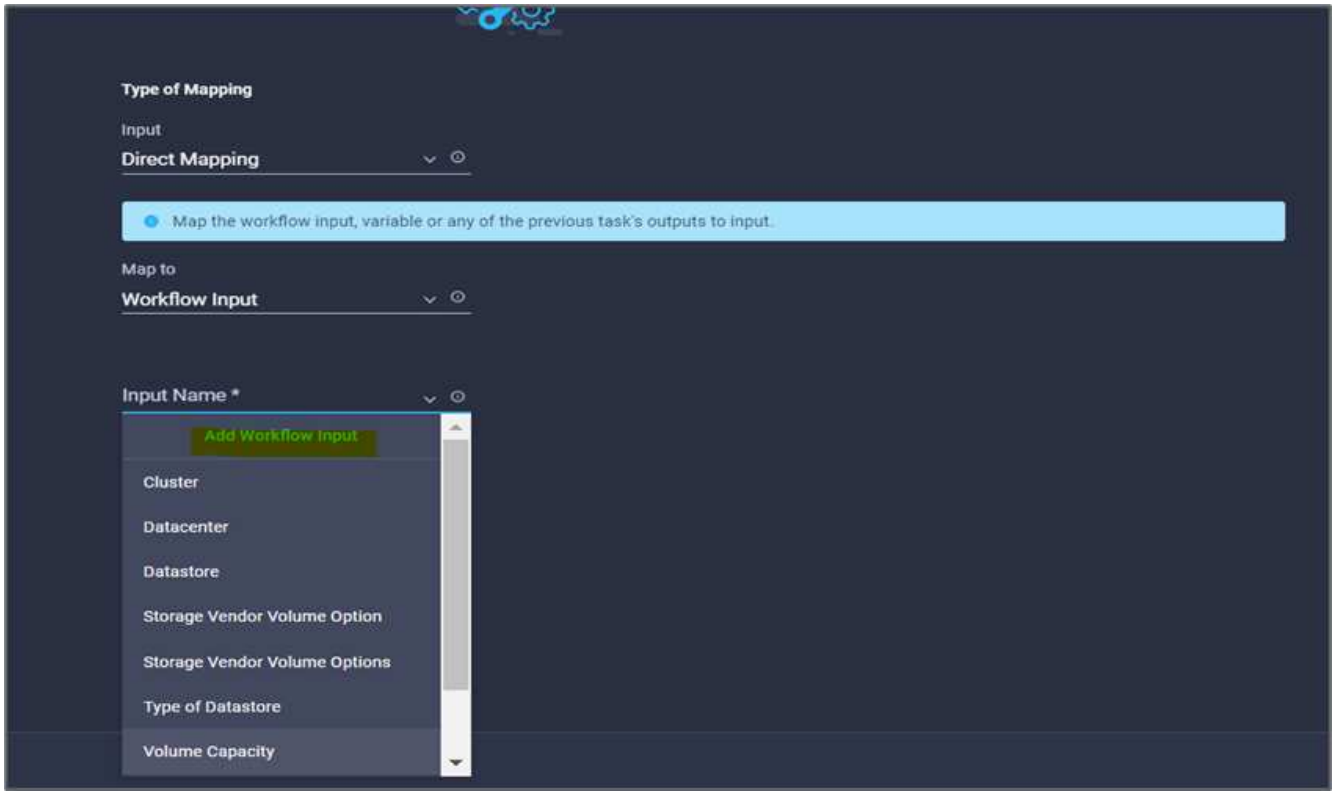
5. Dans la zone **Propriétés du workflow**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté comme expliqué dans "Configurez Cisco Intersight Service pour HashiCorp Terraform". ».



8. Cliquez sur **carte**.
9. Cliquez sur **carte** dans le champ *Nom de l'organisation Terraform *.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.

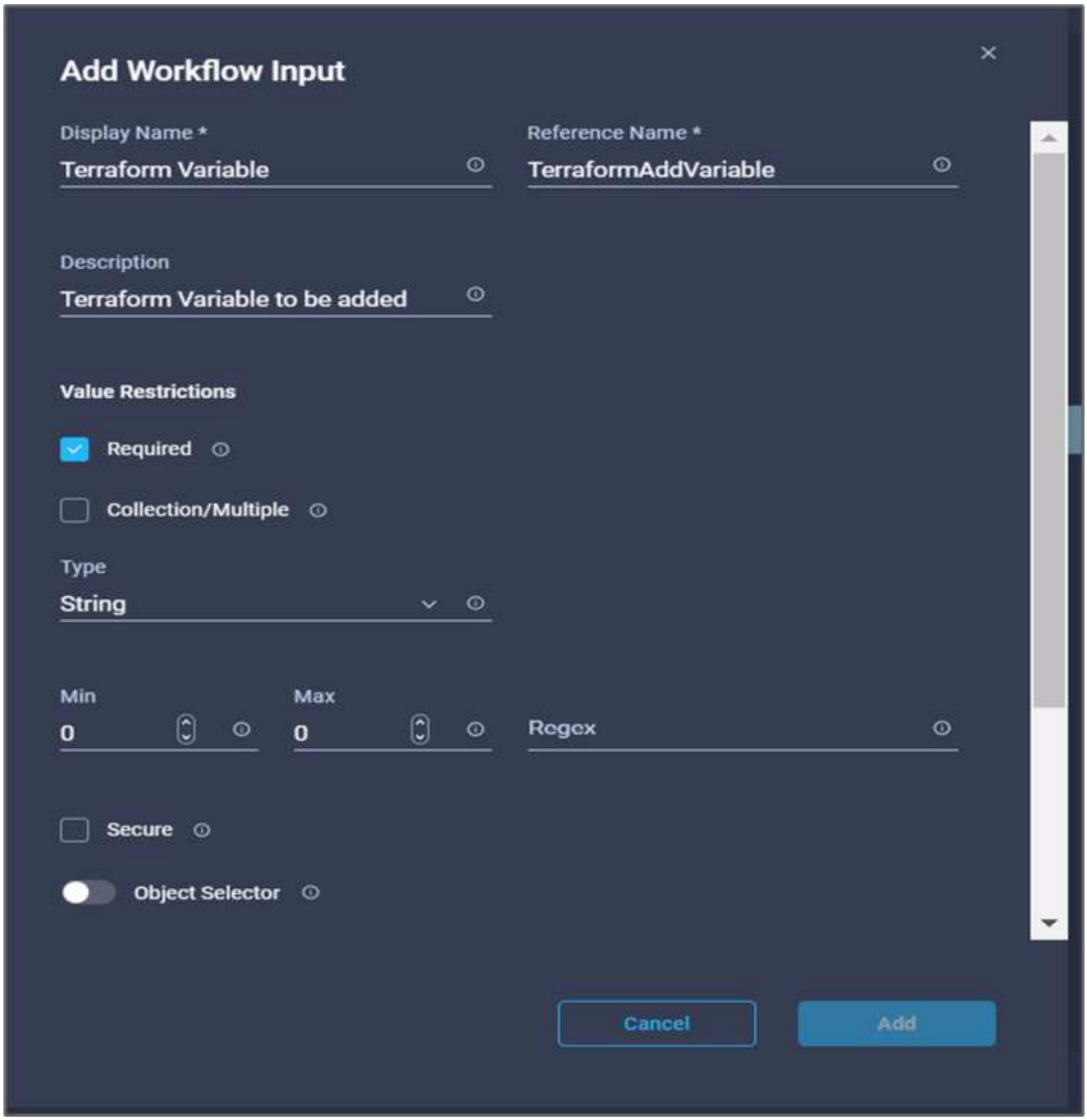


11. Cliquez sur **carte**.
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**.
13. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
14. Cliquez sur **Nom de la tâche** et cliquez sur **Ajouter un espace de travail Terraform**.



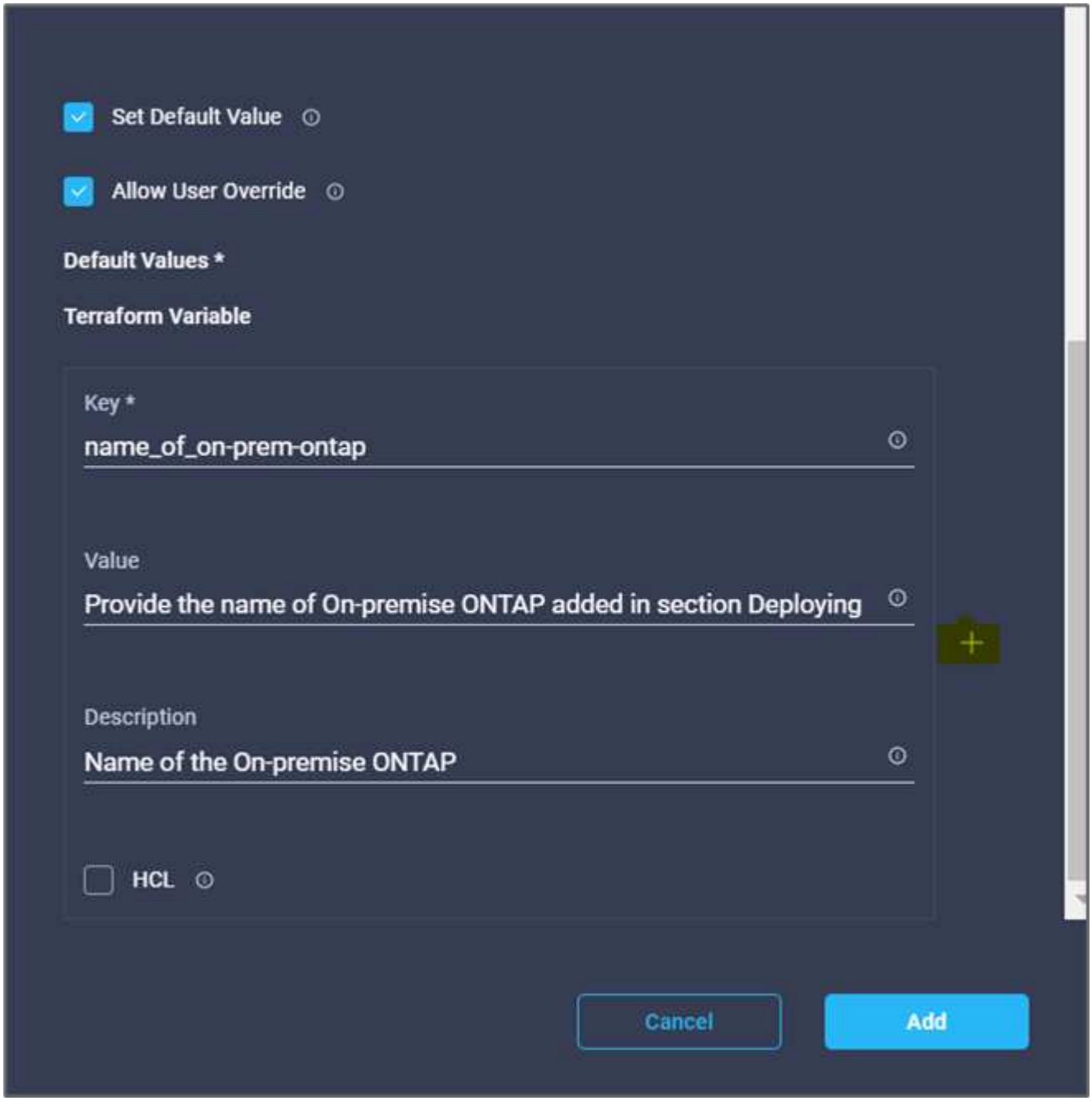
15. Cliquez sur **Nom de sortie** et cliquez sur **Nom d'espace de travail**.

16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Add variables Options**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



20. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **String** pour **Type**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Cliquez sur **Type de variable**, puis sur **variables non sensibles**.

21. Dans la section **Ajouter des variables Terraform**, fournissez les informations suivantes :
    - **Clé.** `name_of_on-prem-ontap`
    - **Valeur.** indiquer le nom de ONTAP sur site.
    - **Description.** Nom du ONTAP sur place.
22. Cliquez sur **+** pour ajouter d'autres variables.

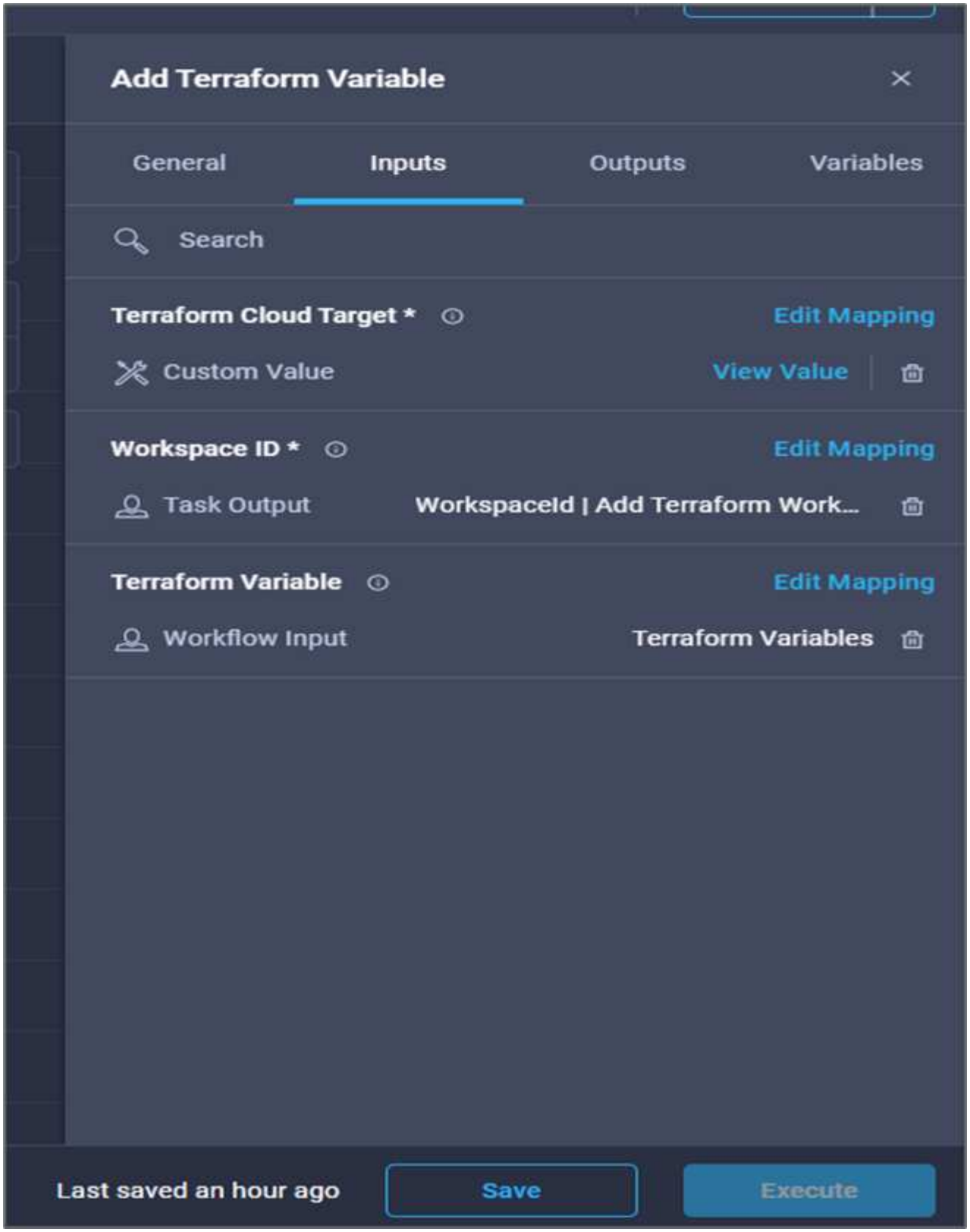


23. Ajoutez toutes les variables Terraform comme indiqué dans le tableau suivant. Vous pouvez également fournir une valeur par défaut.

Nom de la variable Terraform	Description
nom_of_on-ontap sur site	Nom du ONTAP sur site (FlexPod)

Nom de la variable Terraform	Description
ip_cluster_ontap_sur site	L'adresse IP de l'interface de gestion du cluster de stockage
nom_utilisateur_ontap_sur site	Nom d'utilisateur admin pour le cluster de stockage
Zone	Région GCP dans laquelle l'environnement de travail sera créé
id_sous-réseau	ID de sous-réseau GCP dans lequel l'environnement de travail sera créé
id_vpc	ID VPC dans lequel l'environnement de travail sera créé
capacity_package_name	Type de licence à utiliser
volume_source	Nom du volume source
nom_vm_stockage_source	Nom du SVM source
volume_destination	Nom du volume sur Cloud Volumes ONTAP
schedule_of_replication	La valeur par défaut est 1 heure
nom_du_volume_to_create_on_cvo	Nom du volume cloud
id_espace_de_travail	Espace de travail_ID où l'environnement de travail sera créé
ID_projet	ID_projet où l'environnement de travail sera créé
nom_du_cluster_cvo	Nom de l'environnement de travail Cloud Volumes ONTAP
compte_service_gcp	gcp_service_compte de l'environnement de travail Cloud Volumes ONTAP

24. Cliquez sur **carte**, puis sur **Enregistrer**.



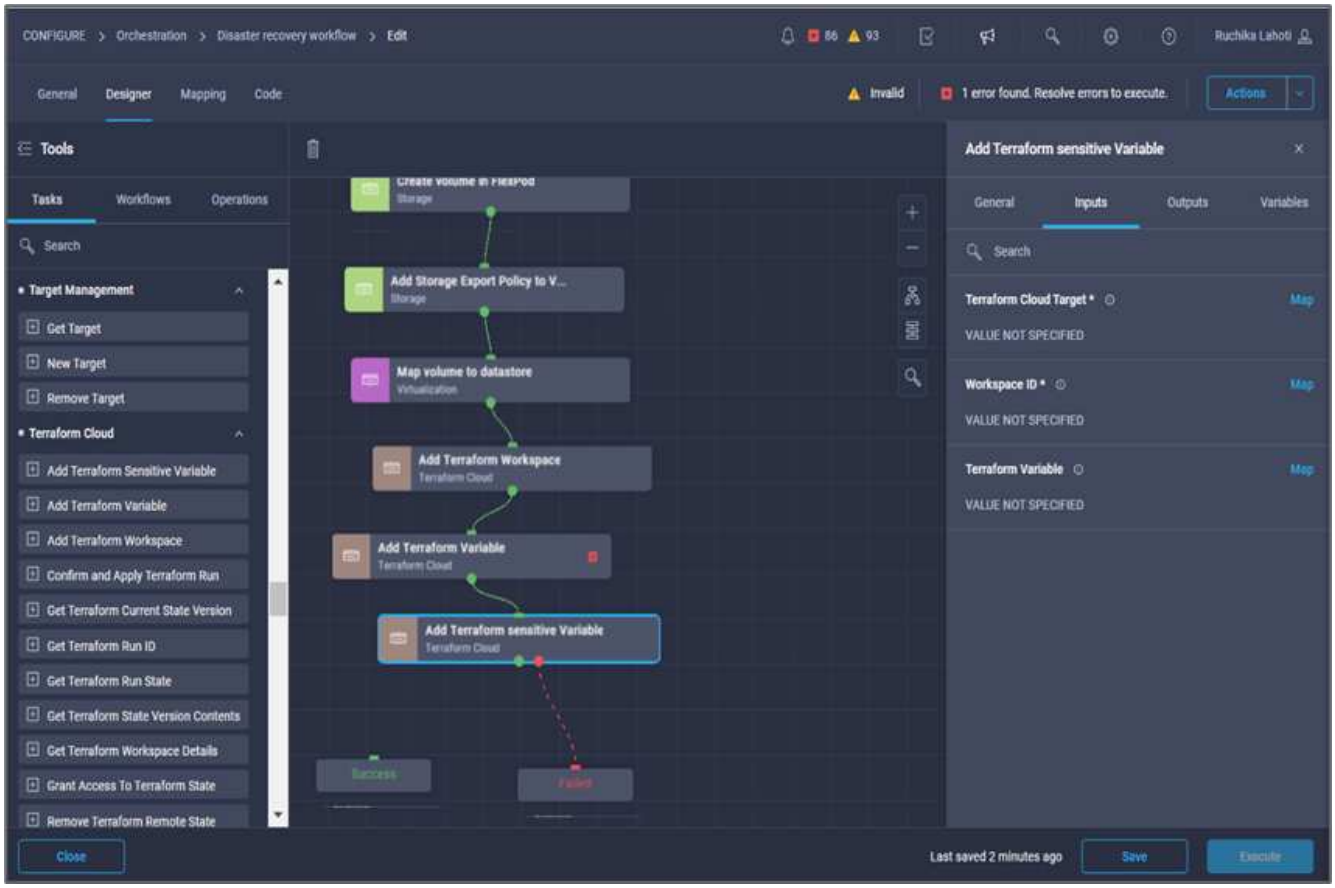
La tâche d'ajout des variables Terraform requises à l'espace de travail est alors terminée. Ajoutez ensuite les variables Terraform sensibles requises à l'espace de travail. Vous pouvez également les combiner en une seule tâche.

Procédure 7 : ajoutez des variables sensibles à un espace de travail

1. Accédez à l'onglet **Designer** et cliquez sur **workflows** dans la section **Outils**.
2. Faites glisser et déposez le flux de travail **Terraform > Ajouter des variables Terraform** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les deux tâches **Ajouter un espace de travail Terraform**. Cliquez sur **Enregistrer**.

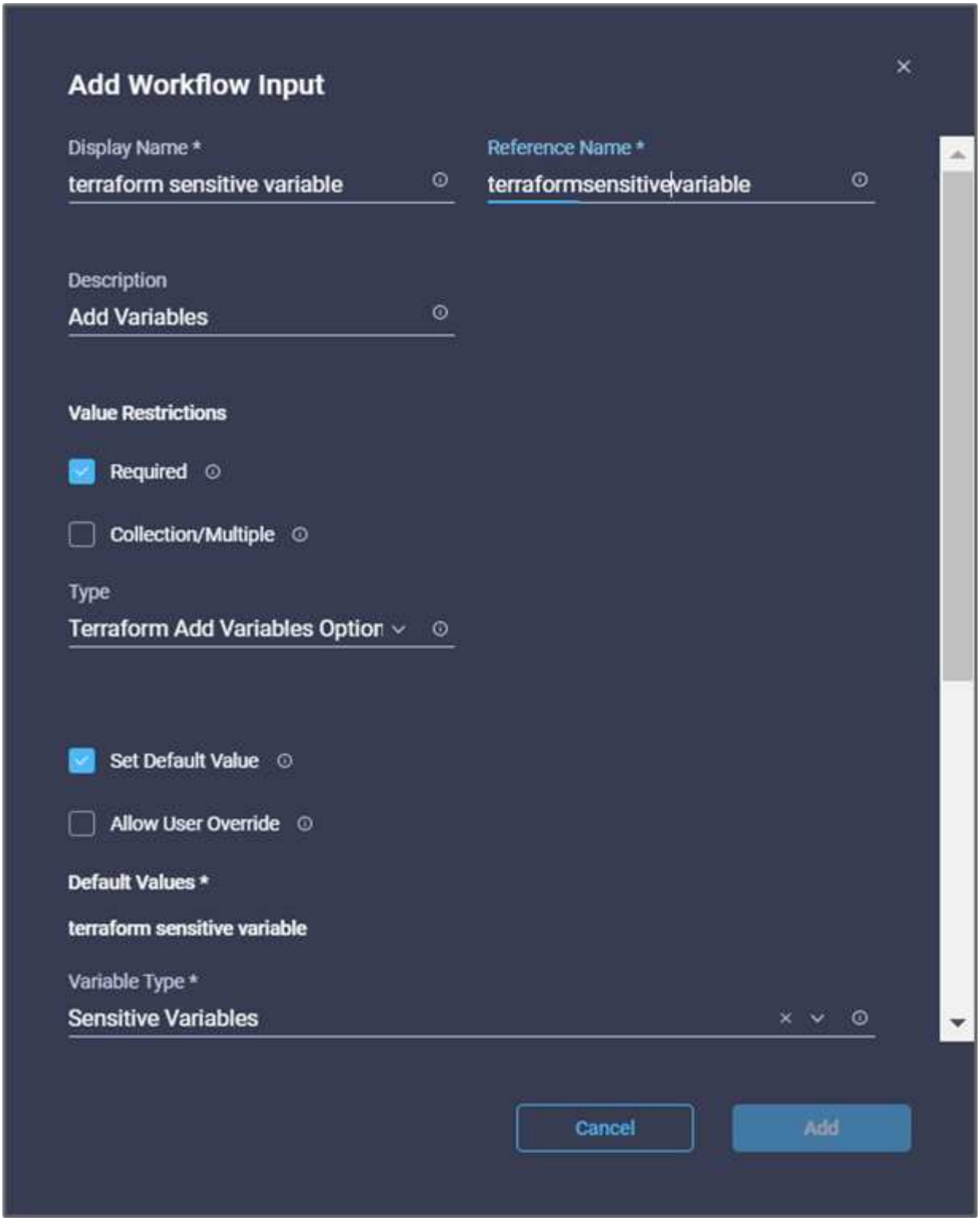
> Un avertissement s'affiche pour indiquer que les deux tâches ont le même nom. Ignorer l'erreur pour l'instant car vous modifiez le nom de la tâche à l'étape suivante.

4. Cliquez sur **Ajouter variables Terraform**. Dans la zone **Propriétés du flux de travail**, cliquez sur l'onglet **général**. Modifiez le nom en **Ajouter des variables sensibles Terraform**.



5. Dans la zone **Propriétés du workflow**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans la section "Configurez Cisco Intersight Service pour HashiCorp Terraform". »
8. Cliquez sur **carte**.
9. Cliquez sur **carte** dans le champ **Nom de l'organisation Terraform**.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.
11. Cliquez sur **carte**.

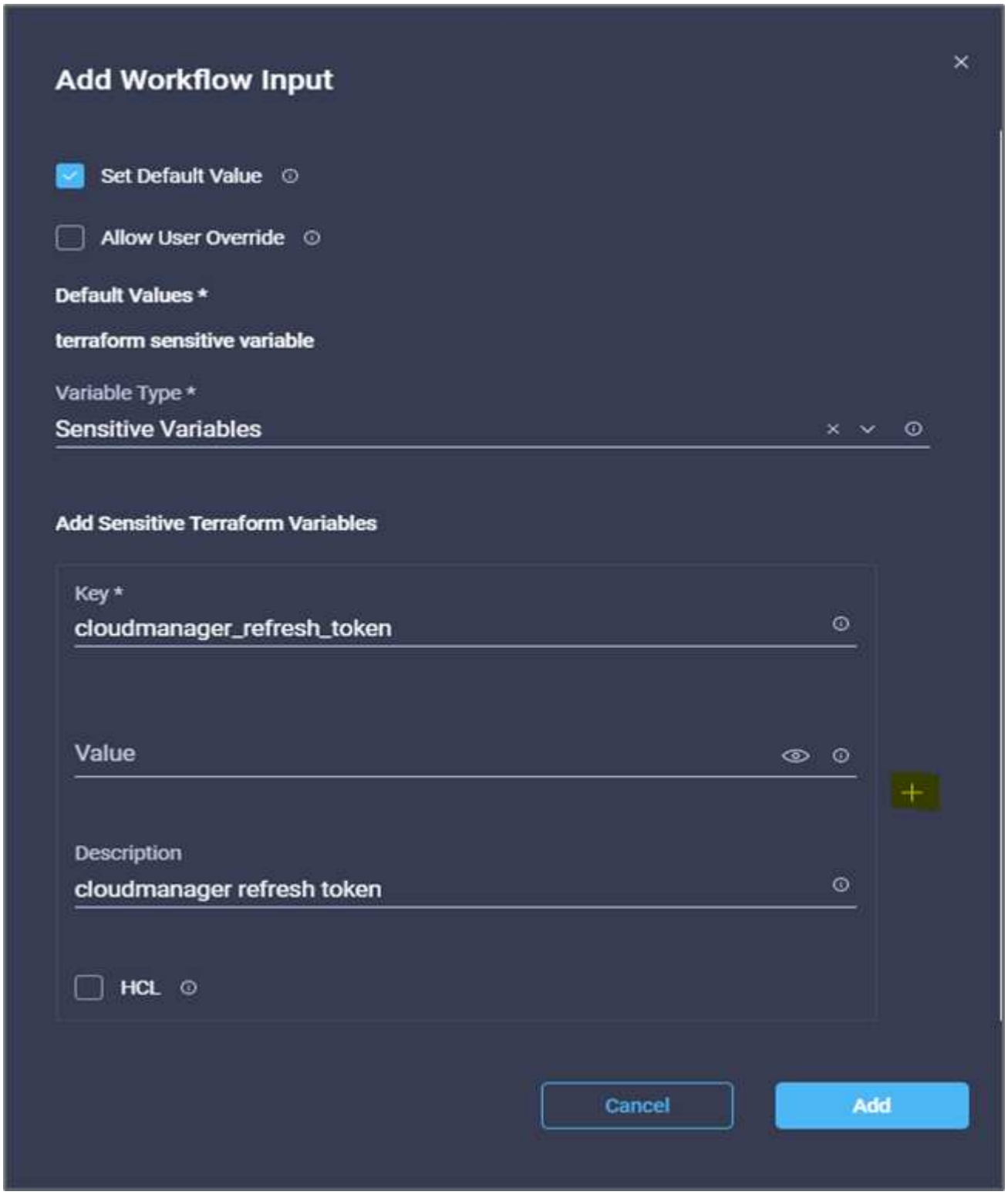
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**.
13. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
14. Cliquez sur **Nom de la tâche**, puis sur **Ajouter un espace de travail Terraform**.
15. Cliquez sur **Nom de sortie** et cliquez sur sortie **Nom d'espace de travail**.
16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Add variables Options**.
18. Choisissez **mappage direct**, puis cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.
20. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **Terraform Ajouter des variables Options** pour le type.
    c. Cliquez sur **définir la valeur par défaut**.
    d. Cliquez sur **Type de variable**, puis sur **variables sensibles**.
    e. Cliquez sur **Ajouter**.



21. Dans la section **Ajouter des variables Terraform**, fournissez les informations suivantes :

    - **Clé.** `cloudmanager_refresh_token`.
    - **Valeur.** saisissez le jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager.
    - **Description.** Actualiser jeton.

Pour en savoir plus sur l'obtention d'un jeton de mise à jour pour les opérations de l'API NetApp Cloud Manager, consultez la section "« Configurer les conditions préalables à l'environnement »."



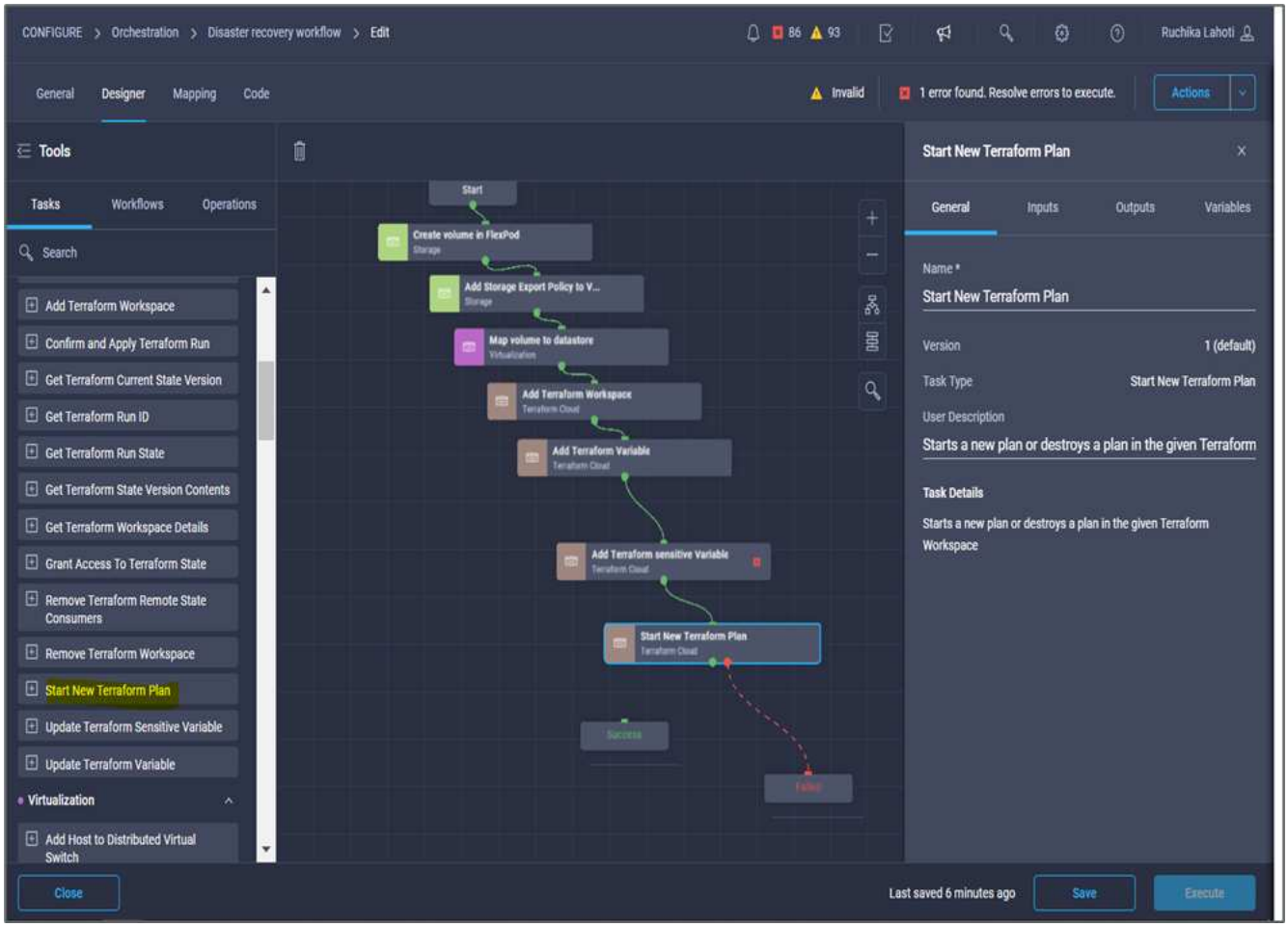
22. Ajoutez toutes les variables sensibles à la Terraform comme indiqué dans le tableau ci-dessous. Vous pouvez également fournir une valeur par défaut.

Nom de variable sensible Terraform	Description
cloudmanager_refresh_token	Actualiser le jeton. Vous pouvez l'obtenir auprès de :
id_connecteur	L'ID client du connecteur Cloud Manager. Obtenez-le à partir de
cvo_admin_password	Mot de passe d'administration pour Cloud Volumes ONTAP
mot_de_passe_utilisateur_ontap_sur site	Mot de passe d'administration pour le cluster de stockage

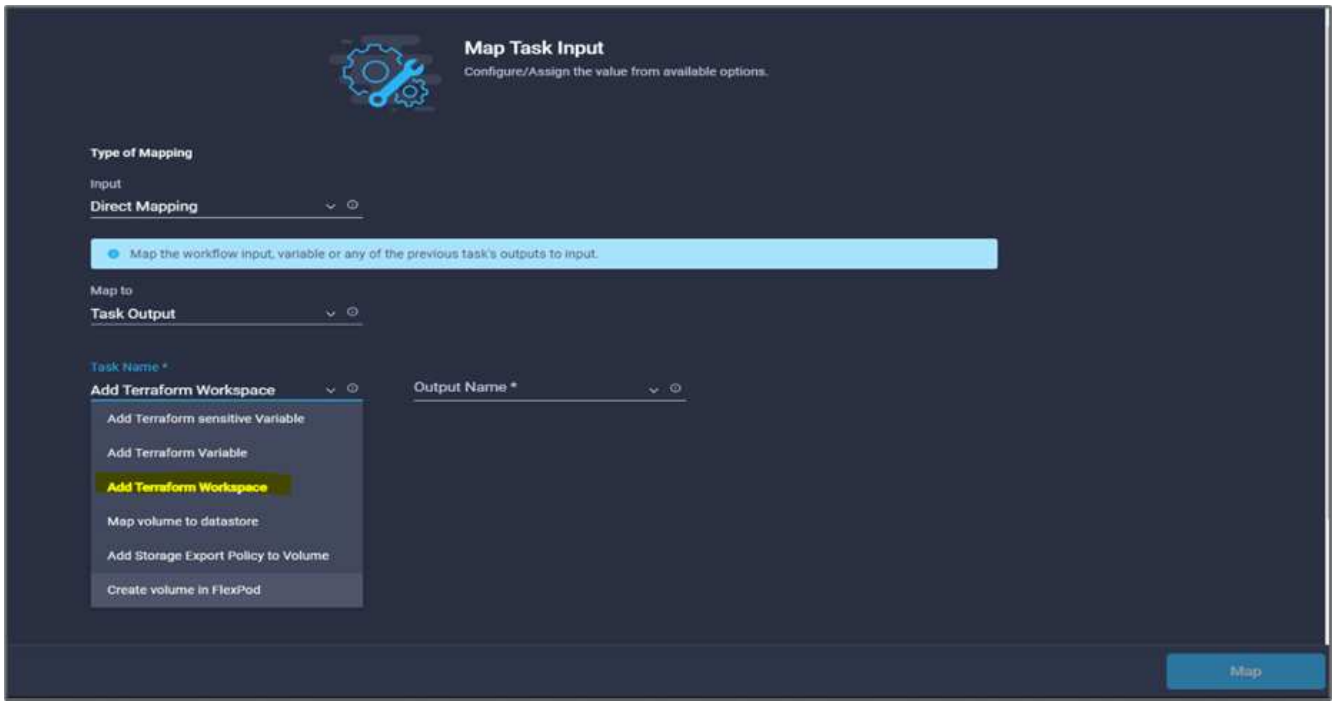
23. Cliquez sur **Map**.cette opération permet d'ajouter les variables sensibles Terraform requises à l'espace de travail. Ensuite, démarrez un nouveau plan Terraform dans l'espace de travail configuré.

Procédure 8 : démarrez un nouveau plan Terraform

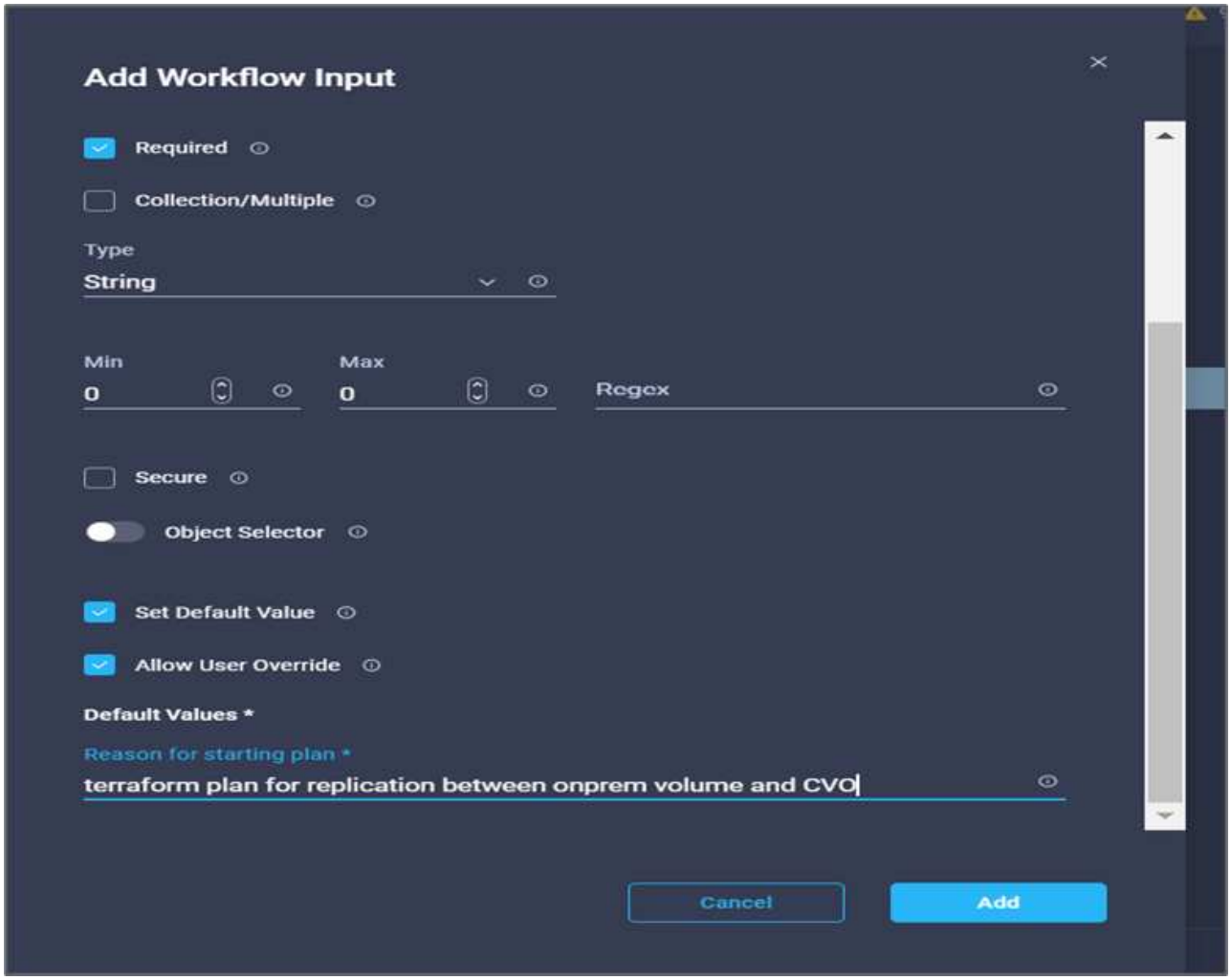
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > Start New Terraform Plan** de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour vous connecter entre les tâches **Ajouter des variables sensibles Terraform** et **Démarrer de nouvelles tâches Terraform Plan**. Cliquez sur **Enregistrer**.
4. Cliquez sur **Démarrer Nouveau plan Terraform**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans la section « Configuration de Cisco Intersight Service for HashiCorp Terraform ».
8. Cliquez sur **carte**.
9. Cliquez sur **Map** dans le champ **Workspace ID**.
10. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
11. Cliquez sur **Nom de la tâche**, puis sur **Ajouter un espace de travail Terraform**.



12. Cliquez sur **Nom de sortie**, **ID d'espace de travail**, puis sur **carte**.
13. Cliquez sur **carte** dans le champ **motif de démarrage du plan**.
14. Choisissez **mappage direct**, puis cliquez sur **entrée de flux de travail**.
15. Cliquez sur **Nom d'entrée**, puis sur **Créer entrée de flux de travail**.
16. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **String** pour **Type**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Entrez une valeur par défaut pour **Reason for Starting plan** et cliquez sur **Add**.



17. Cliquez sur **carte**.
18. Cliquez sur **Map** dans le champ **Plan Operation**.
19. Choisissez **valeur statique** et cliquez sur **opération de plan**. Cliquez sur **New plan**.

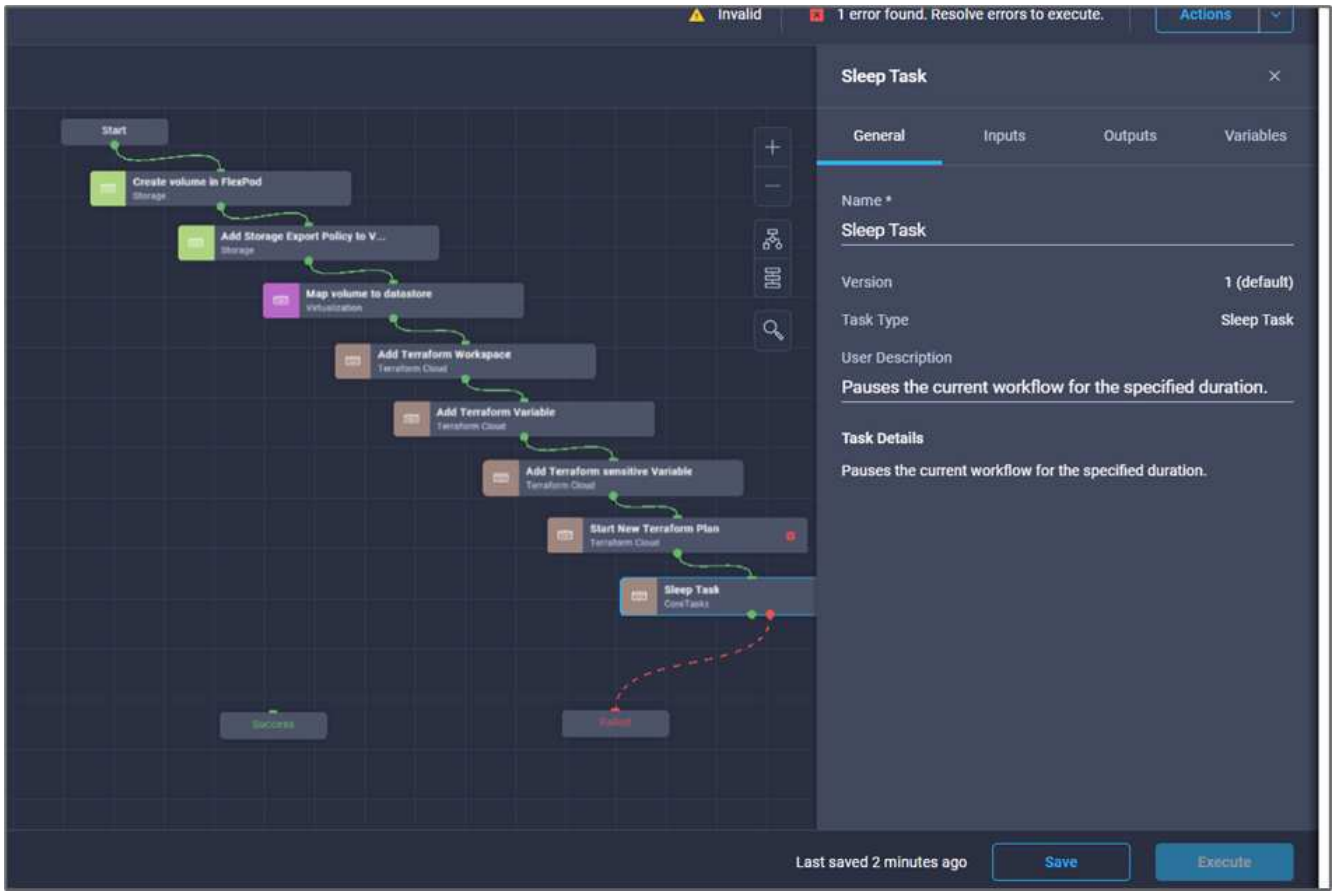
20. Cliquez sur **carte**.
21. Cliquez sur **Enregistrer**.

Cela complète la tâche d'ajout d'un plan Terraform dans le compte Terraform Cloud for Business. Ensuite, créez une tâche de veille pendant quelques secondes.

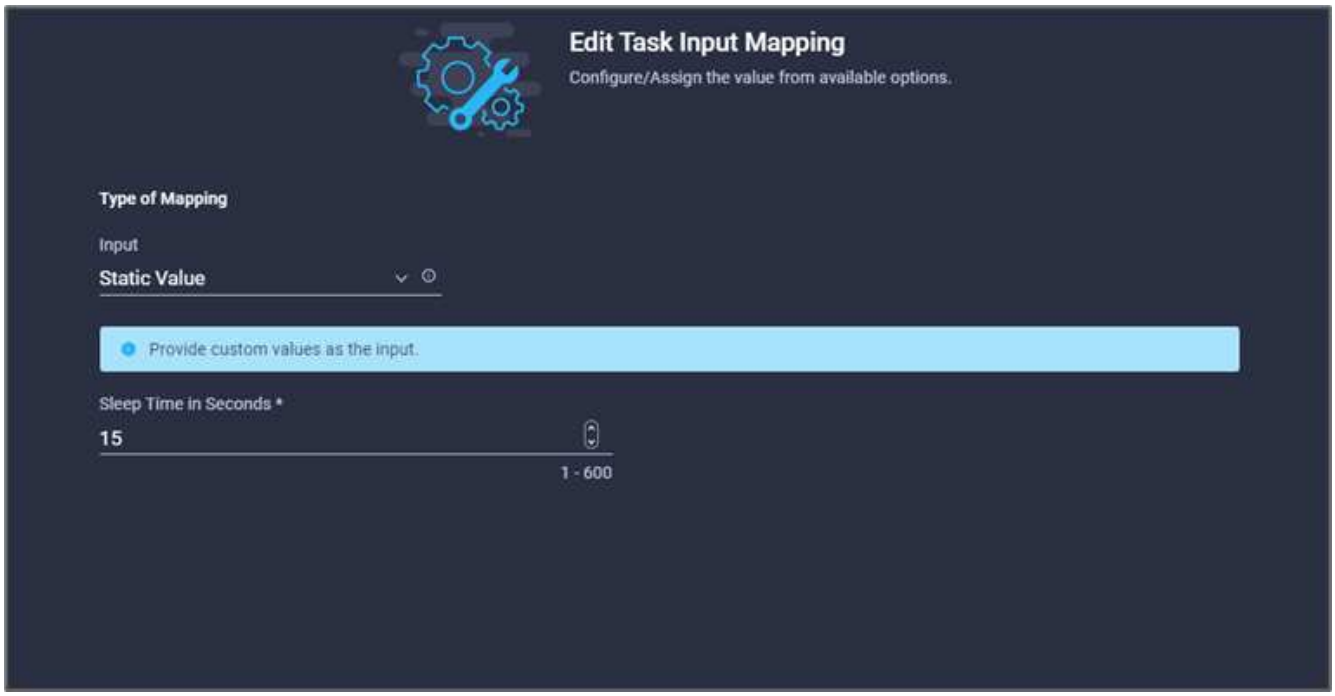
Procédure 9 : tâche de veille pour la synchronisation

Terraform Apply nécessite un runId, qui est généré dans le cadre de la tâche Plan Terraform. L'attente de quelques secondes entre le Plan Terraform et les actions d'application Terraform évite les problèmes de synchronisation.

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Core Tasks > Sleep Task** dans la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Démarrer Nouveau plan Terraform** et **tâche veille**. Cliquez sur **Enregistrer**.



4. Cliquez sur **tâche veille**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Synchroniser**.
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **temps de veille en secondes**.
7. Choisissez **valeur statique** et saisissez **15** dans pour le **temps de veille en secondes**.

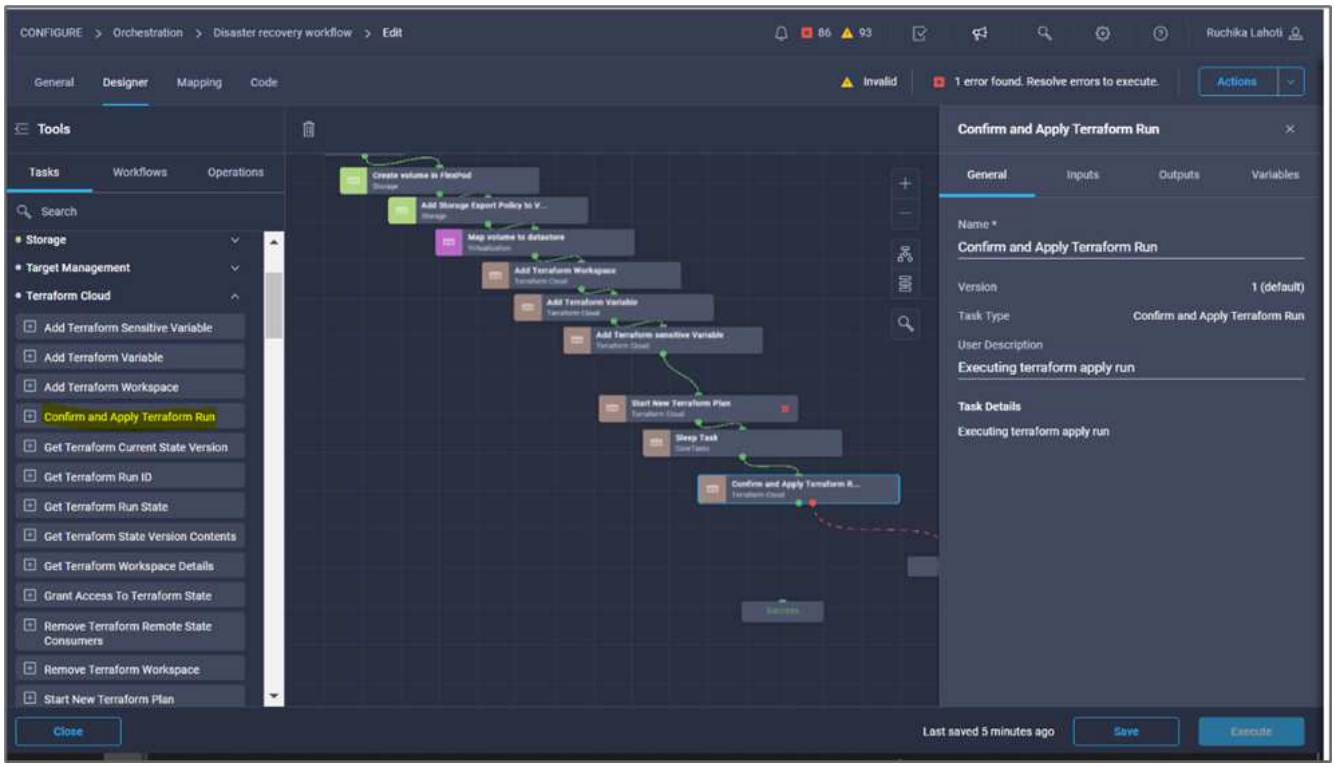


8. Cliquez sur **carte**.
9. Cliquez sur **Enregistrer**.

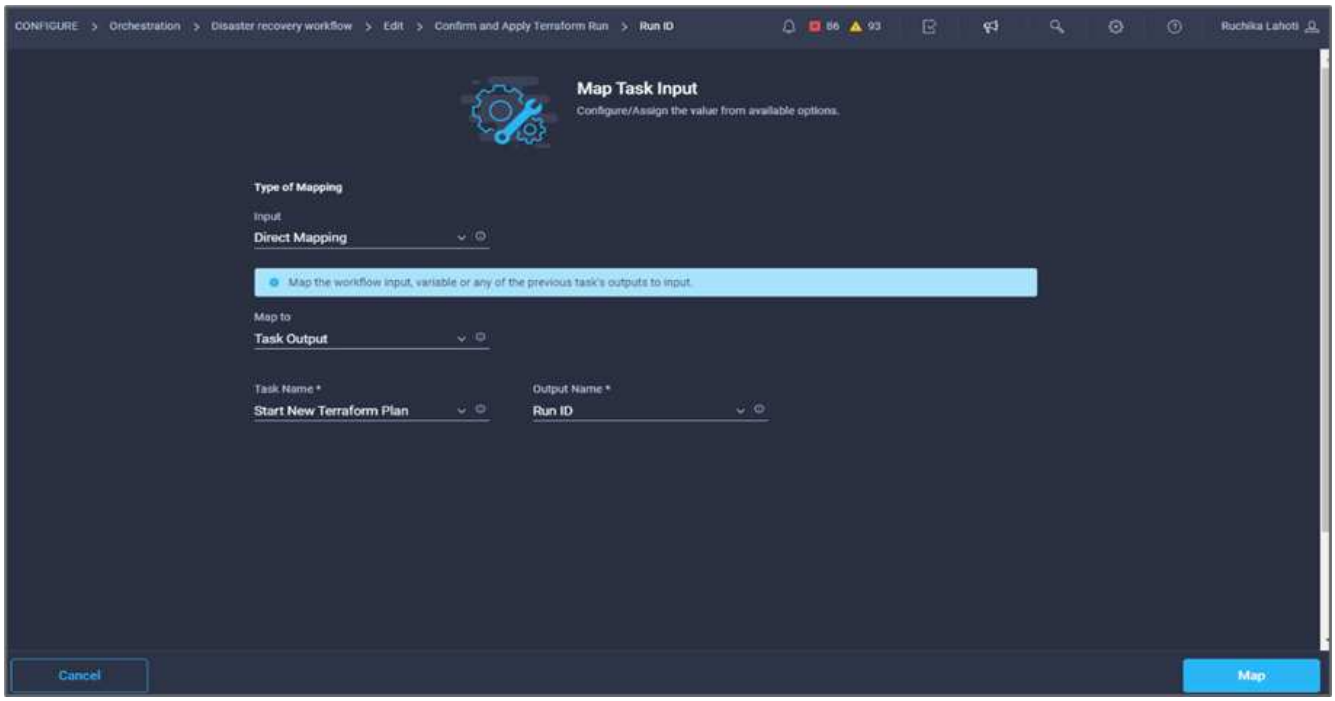
La tâche de veille est terminée. Ensuite, créez la dernière tâche de ce flux de travail, en confirmant et en appliquant l'exécution Terraform.

Procédure 10 : confirmer et appliquer Terraform Run

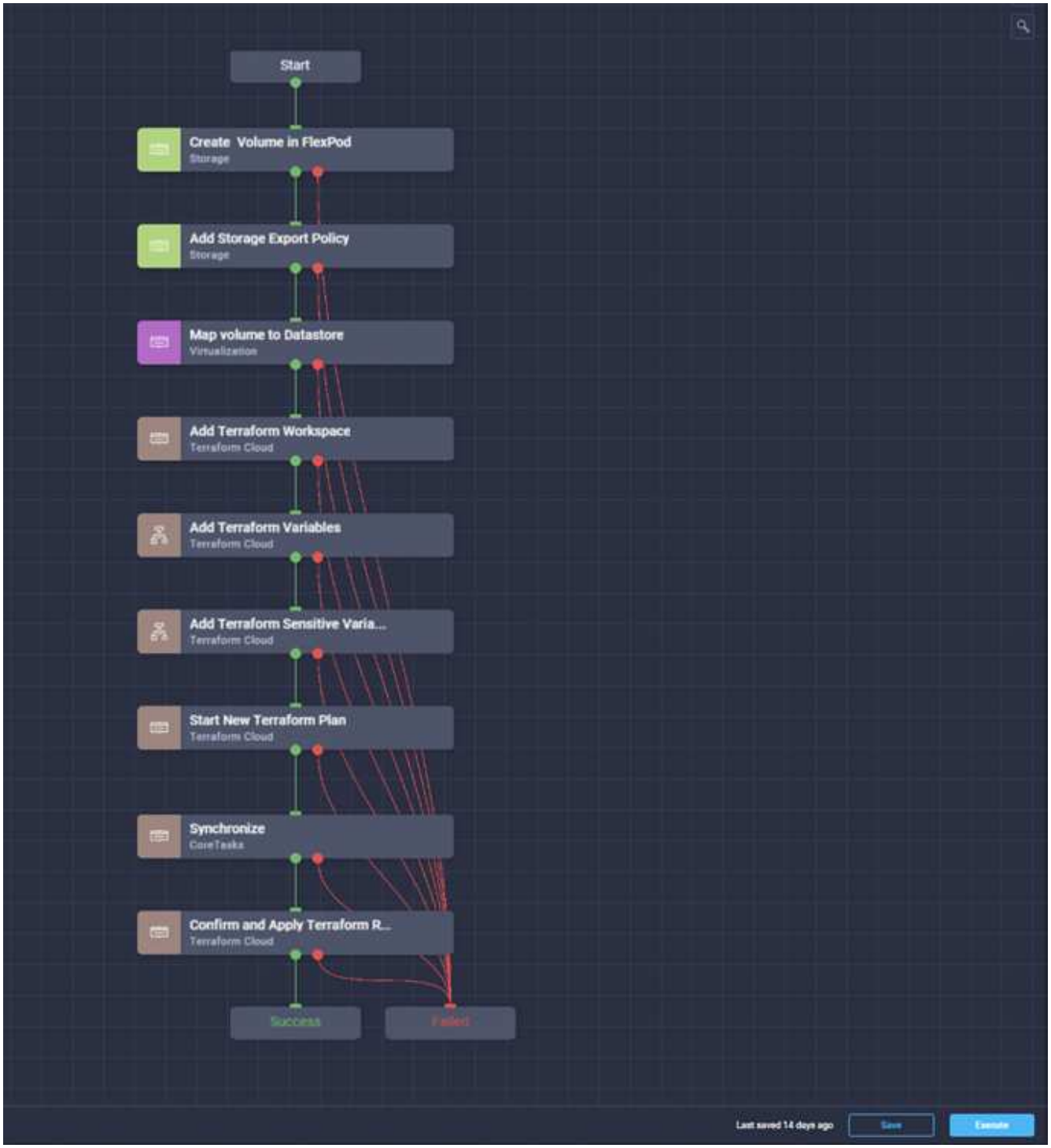
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > confirmer et appliquer Terraform Run** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Synchroniser** et **confirmer et appliquer Terraform Run**. Cliquez sur **Enregistrer**.
4. Cliquez sur **confirmer** et **appliquer Terraform Run**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans "Configurez Cisco Intersight Service pour HashiCorp Terraform". »
8. Cliquez sur **carte**.
9. Cliquez sur **Map** dans le champ **Run ID**.
10. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
11. Cliquez sur **Nom de la tâche** et cliquez sur **Démarrer Nouveau plan Terraform**.
12. Cliquez sur **Nom de sortie**, puis sur **ID d'exécution**.



13. Cliquez sur **carte**.
14. Cliquez sur **Enregistrer**.
15. Cliquez sur **alignement automatique du flux de travail** pour que toutes les tâches soient alignées. Cliquez sur **Enregistrer**.



La tâche confirmer et appliquer Terraform Run est terminée. Utilisez Connector pour vous connecter entre la tâche **confirmer et appliquer Terraform Run** et les tâches **Success** et **failed**.

Procédure 11 : importation d'un flux de travail conçu par Cisco

Cisco Intersight Cloud Orchestrator vous permet d'exporter des workflows d'un compte Cisco Intersight vers votre système, puis de les importer dans un autre compte. Un fichier JSON a été créé en exportant le flux de travail créé qui peut être importé vers votre compte.

Un fichier JSON pour le composant de flux de travail est disponible dans "Référentiel GitHub".

"Next : exécution Terraform à partir du contrôleur."

Exécution Terraform à partir du contrôleur

"Précédent : flux de travail de reprise après incident."

Nous pouvons exécuter le plan Terraform à l'aide d'un contrôleur. Vous pouvez ignorer cette section si vous avez déjà exécuté votre plan Terraform à l'aide d'un flux de travail ICO.

Prérequis

La configuration de la solution commence par une station de travail de gestion qui a accès à Internet et avec une installation de Terraform.

Vous trouverez un guide d'installation de Terraform "ici".

Cloner GitHub

La première étape du processus consiste à cloner le GitHub repo vers un nouveau dossier vide sur la station de travail de gestion. Pour cloner le référentiel GitHub, procédez comme suit :

1. À partir du poste de travail de gestion, créez un nouveau dossier pour le projet. Créez un nouveau dossier dans ce dossier nommé `/root/snapmirror-cvo` Et clonez le référentiel GitHub.
2. Ouvrez une interface de ligne de commande ou de console sur le poste de travail de gestion et modifiez les répertoires dans le nouveau dossier que vous venez de créer.
3. Clonez la collection GitHub à l'aide de la commande suivante :

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Remplacez les répertoires par le nouveau dossier nommé `snapmirror-cvo`.

Exécution Terraform

- **Init.** initialiser l'environnement Terraform (local). Généralement exécuté une seule fois par session.
- **Plan.** Comparez l'état du terraform avec l'état d'entrée dans le nuage et construisez et affichez un plan d'exécution. Cela ne modifie pas le déploiement (lecture seule).
- **Appliquer.** appliquer le plan à partir de la phase du plan. Cela peut potentiellement changer le déploiement (lecture et écriture).
- **Détruire.** toutes les ressources qui sont régies par cet environnement terraform spécifique.

Pour plus de détails, voir "ici".

"Ensuite, validation de la solution."

Validation des solutions

"Précédent : exécution Terraform à partir du contrôleur."

Dans cette section, nous revisitons la solution avec un exemple de workflow de réplication des données et prenons quelques mesures pour vérifier l'intégrité de la réplication des données depuis l'instance NetApp ONTAP exécutée dans FlexPod vers NetApp Cloud Volumes ONTAP s'exécutant sur Google Cloud.

Nous avons utilisé Cisco Intersight workflow orchestrator dans cette solution et nous continuerons à l'utiliser pour notre cas d'utilisation.

De fait, le nombre limité de flux de travail Cisco Intersight utilisés dans cette solution ne représente pas l'ensemble complet des flux de travail utilisés par Cisco Intersight. Vous pouvez créer des flux de travail personnalisés en fonction de vos exigences spécifiques et les avoir déclenchés à partir de Cisco Intersight.

Pour valider un scénario de reprise sur incident réussi, commencez par déplacer les données d'un volume dans ONTAP qui fait partie de FlexPod vers Cloud Volumes ONTAP à l'aide de SnapMirror. Vous pouvez alors tenter d'accéder aux données à partir de l'instance de calcul cloud Google, suivie d'un contrôle de l'intégrité des données.

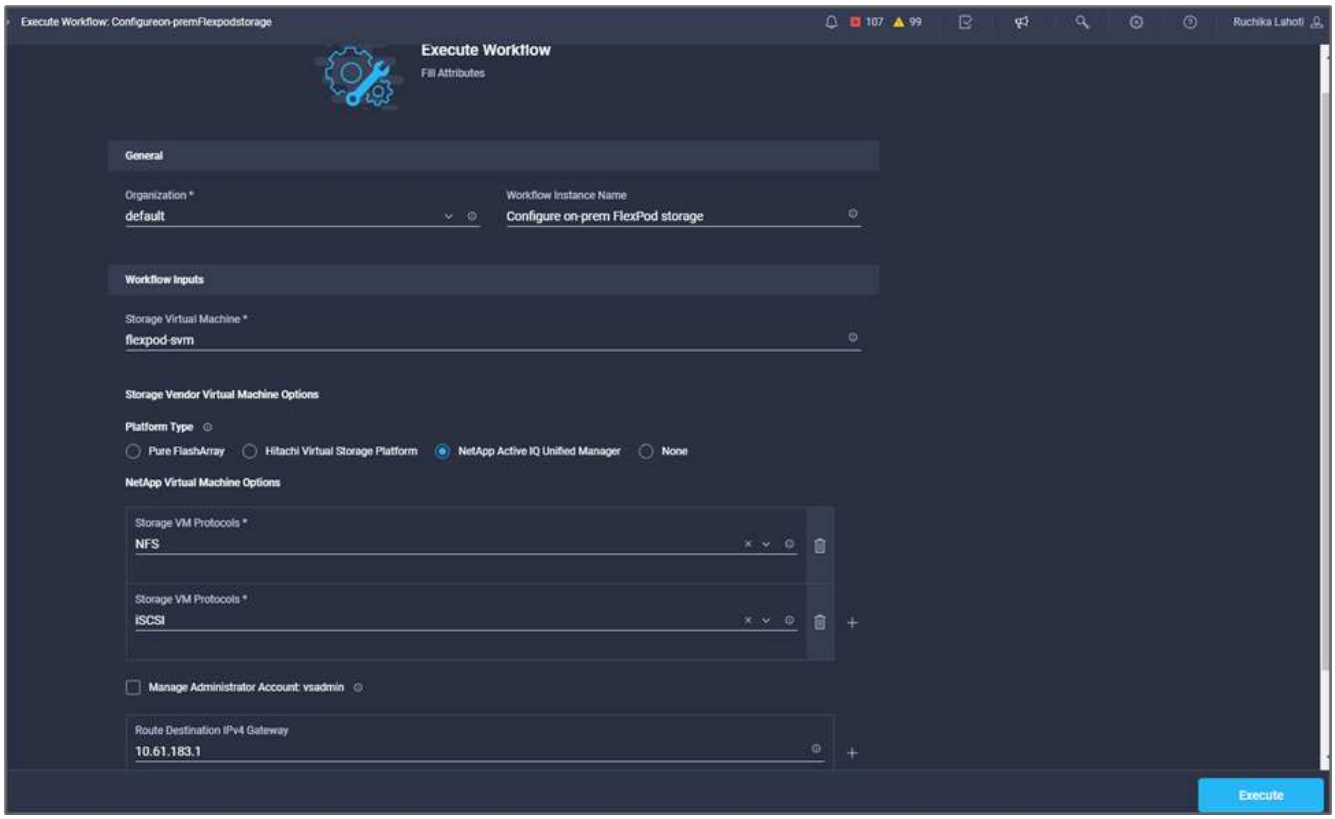
Les étapes générales suivantes permettent de vérifier les critères de réussite de cette solution :

1. Générer un checksum SHA256 sur l'exemple de dataset présent dans un volume ONTAP dans FlexPod.
2. Configurez une relation SnapMirror volume entre ONTAP dans FlexPod et Cloud Volumes ONTAP.
3. Répliquer l'exemple de jeu de données de FlexPod vers Cloud Volumes ONTAP.
4. Interrompre la relation SnapMirror et promouvoir le volume en Cloud Volumes ONTAP vers la production.
5. Mappez le volume Cloud Volumes ONTAP avec le dataset sur une instance de calcul dans Google Cloud.
6. Générer un checksum SHA256 sur l'exemple de dataset dans Cloud Volumes ONTAP.
7. Comparez la somme de contrôle de la source et de la destination, probablement les sommes de contrôle des deux côtés correspondent.

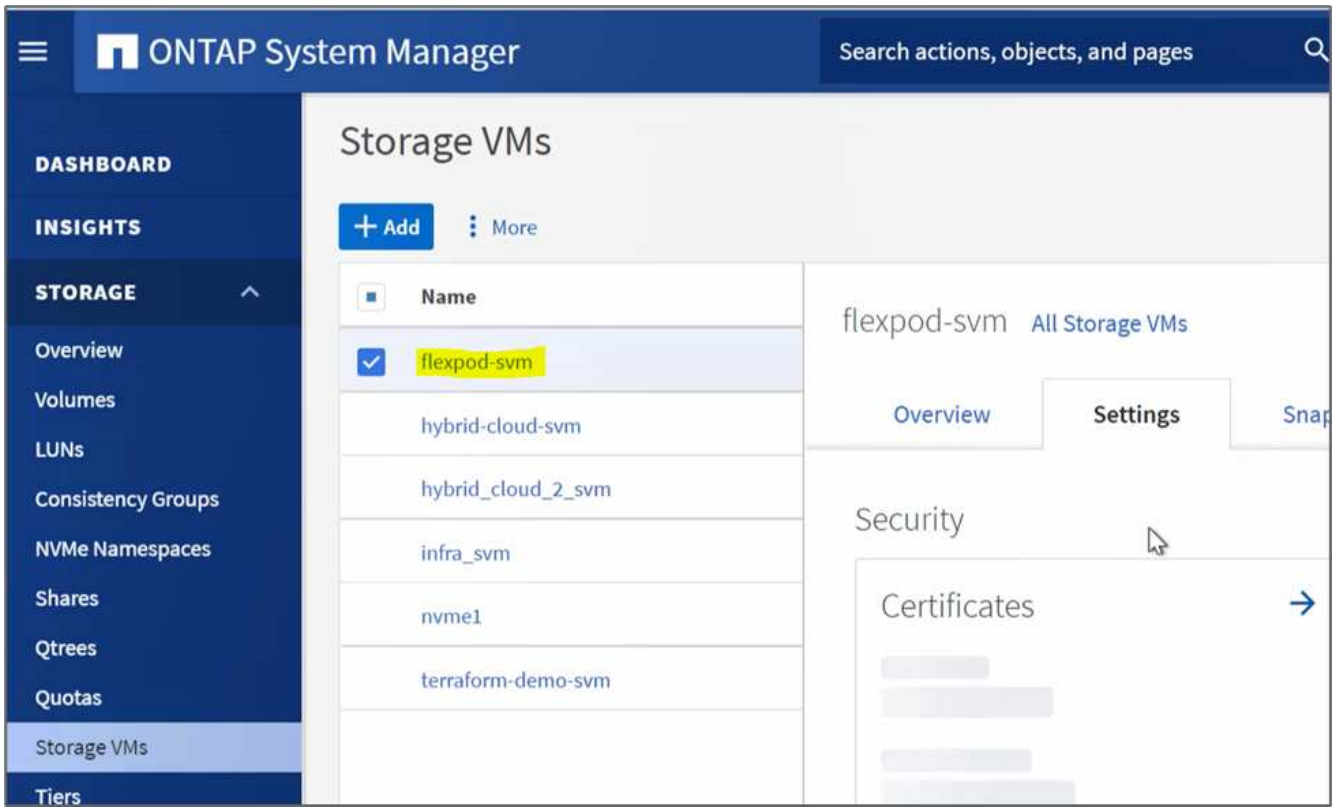
Pour exécuter le workflow sur site, procédez comme suit :

1. Créez un workflow dans InterSight pour les systèmes FlexPod sur site.

2. Fournissez les entrées requises et exécutez le flux de travail.

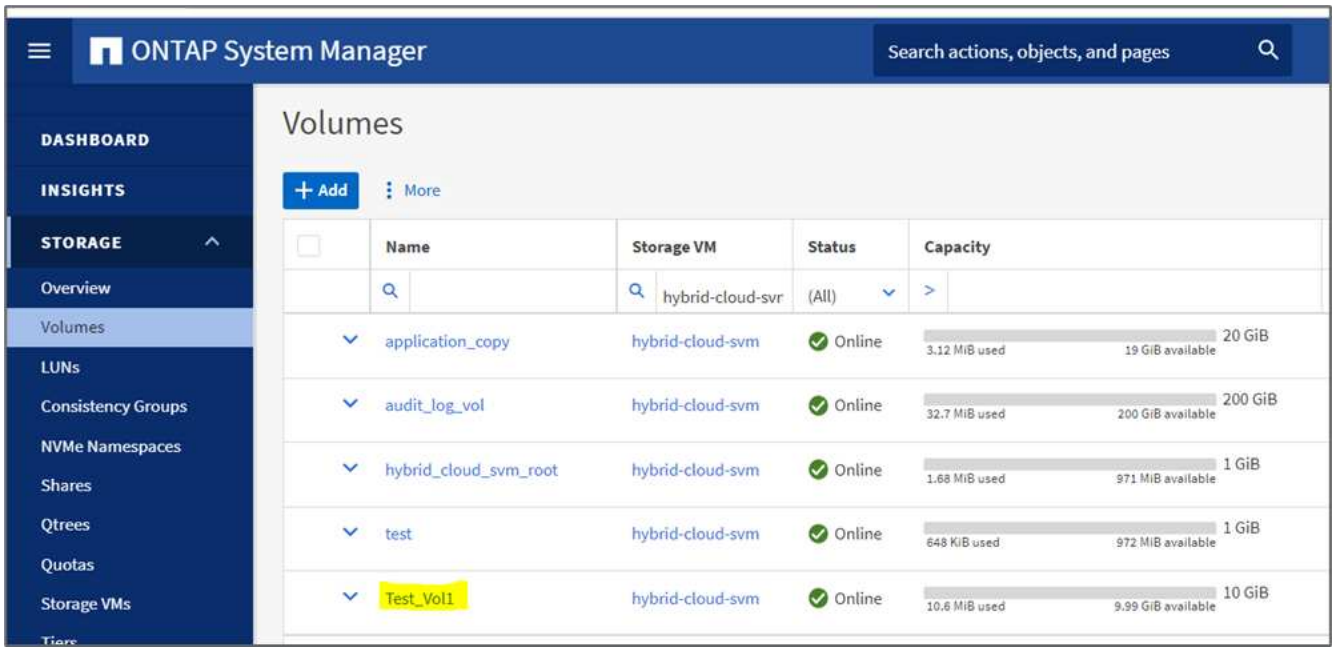


3. Vérifier le nouveau SVM créé dans System Manager



4. Créez et exécutez un autre workflow de reprise d'activité pour créer un volume dans FlexPod sur site et établir une relation SnapMirror entre ce volume dans FlexPod et Cloud Volumes ONTAP.

5. Vérifiez le nouveau volume créé dans ONTAP System Manager.

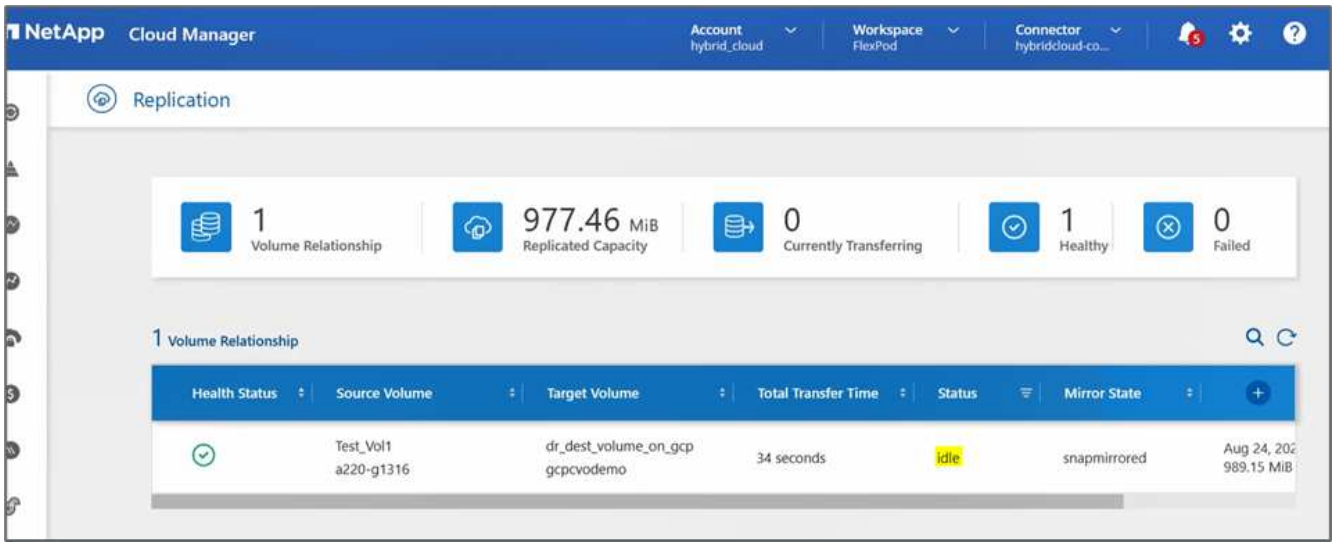


6. Montez le même volume NFS sur une machine virtuelle sur site, puis copiez l'exemple de dataset et exécutez le checksum.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

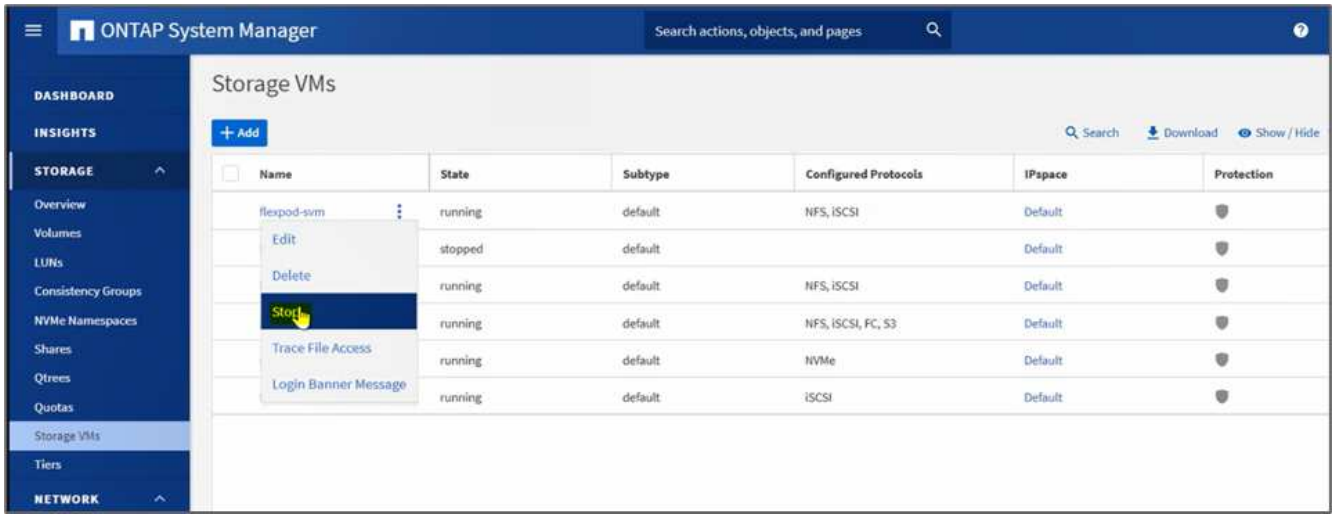
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Vérifiez l'état de la réplication dans Cloud Manager. Le transfert de données peut prendre quelques minutes en fonction de la taille des données. Une fois cette opération terminée, vous pouvez voir l'état de SnapMirror comme **Idle**.

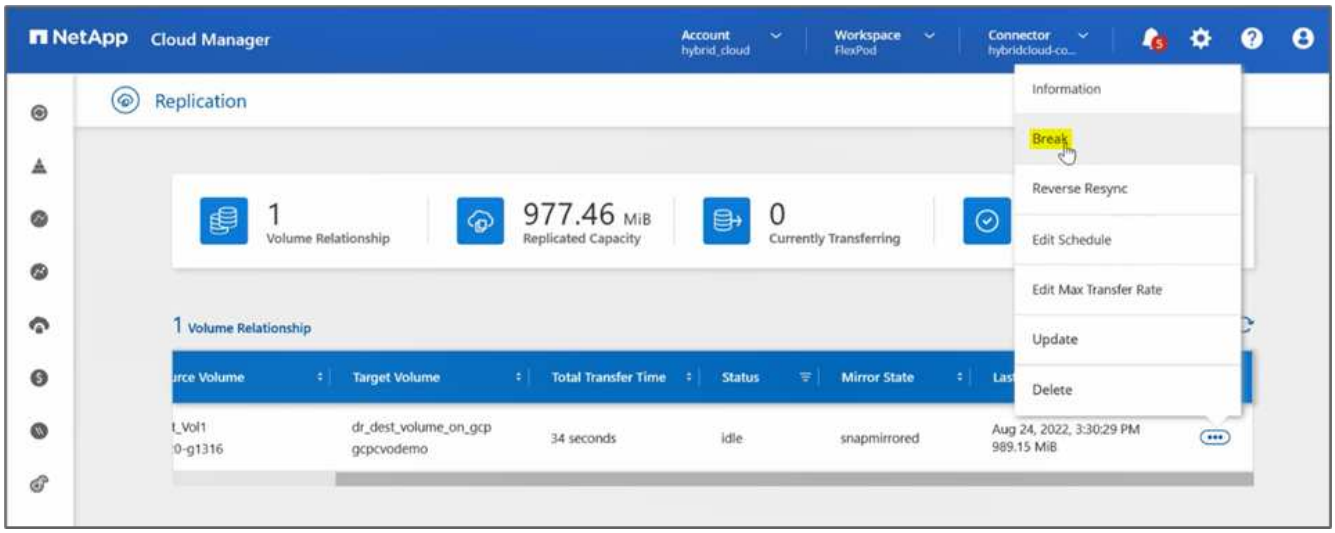


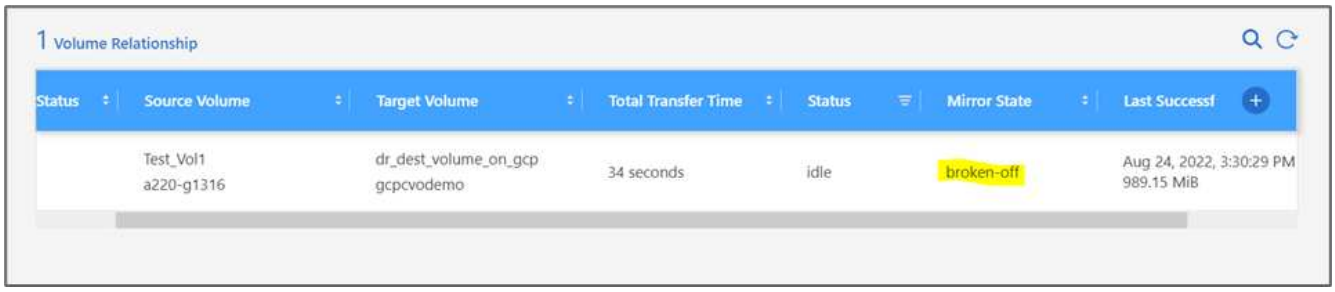
8. Lorsque le transfert de données est terminé, simuler un incident côté source en arrêtant le SVM qui héberge le `Test_vol1` volumétrie.

   Après l'arrêt du SVM, le `Test_vol1` Le volume n'est pas visible dans Cloud Manager.

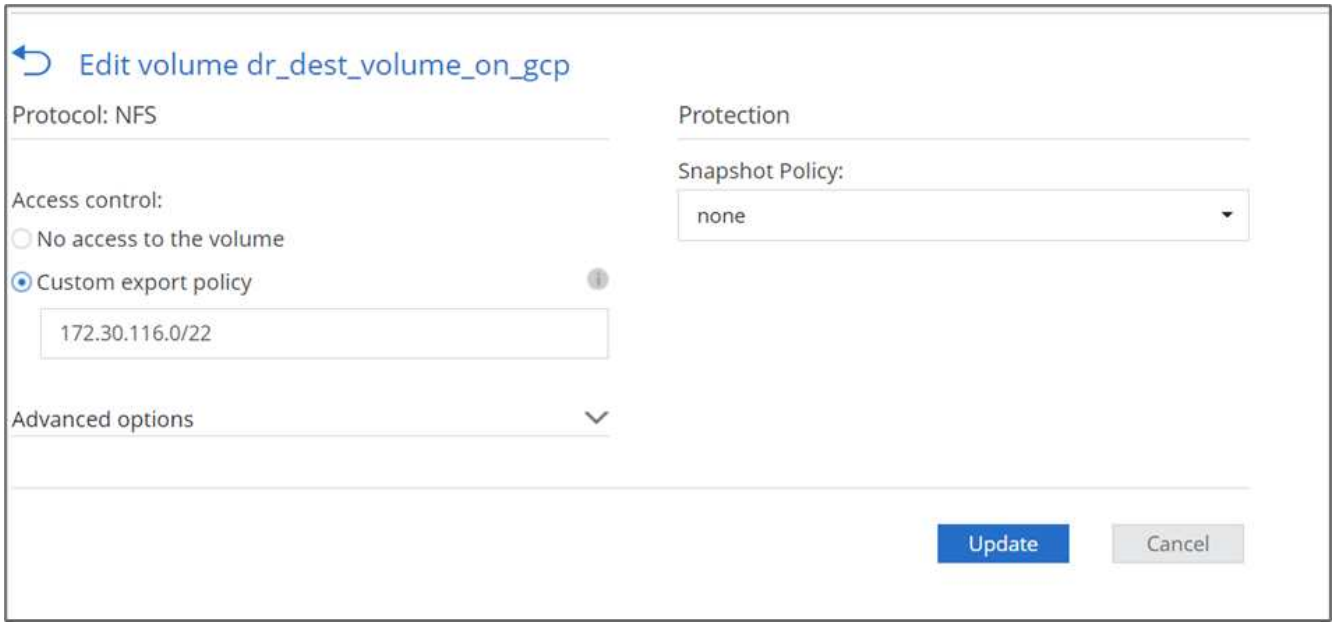


9. Interrompre la relation de réplication et promouvoir le volume de destination Cloud Volumes ONTAP en production.

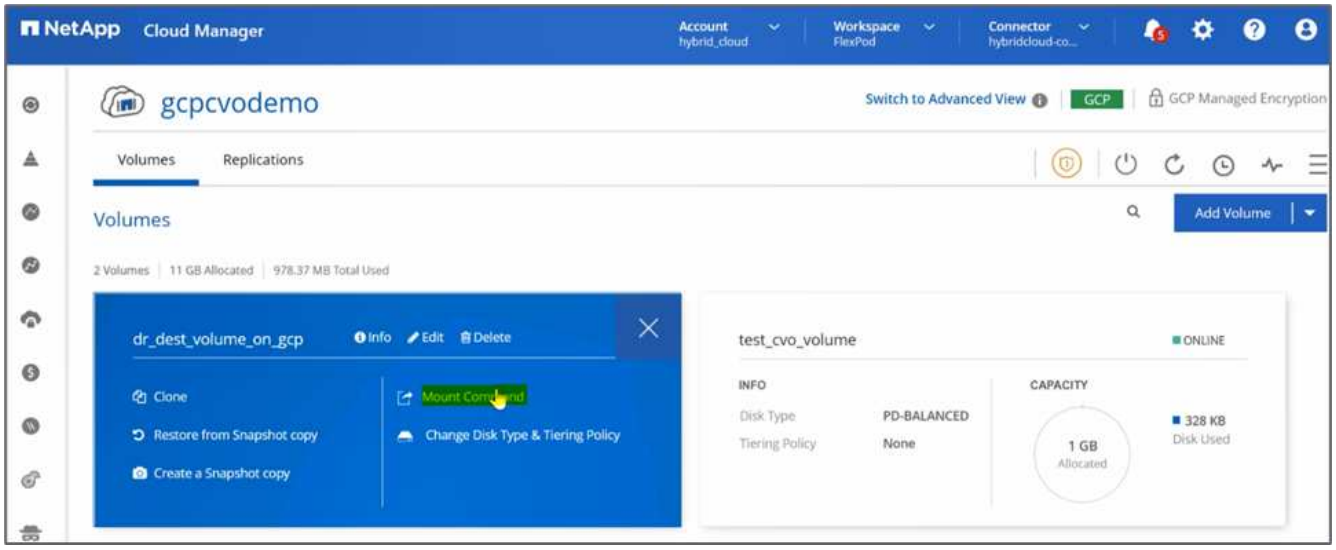




10. Modifiez le volume et activez l'accès client en l'associant à une export policy.



11. Procurez-vous la commande de montage prête à l'emploi pour le volume.



12. Monter le volume sur une instance de calcul, vérifier la présence des données dans le volume de destination et générer le checksum SHA256 du `sample_dataset_2GB` fichier.

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Comparer les valeurs de somme de contrôle à la fois à la source (FlexPod) et à la destination (Cloud Volumes ONTAP).
14. Les checksums correspondent à la source et à la destination.

Vous pouvez confirmer que la réplication des données de la source vers la destination a été correctement effectuée et que l'intégrité des données a été maintenue. Ces données peuvent désormais être consommées en toute sécurité par les applications afin de servir les clients pendant que le site source passe par la restauration.

"Suivant: Conclusion."

Conclusion

"Précédent : validation de la solution."

Dans cette solution, le service de données cloud NetApp, Cloud Volumes ONTAP et l'infrastructure de data Center FlexPod ont été utilisés pour créer une solution de reprise après incident avec un cloud public optimisé par Cisco Intersight Cloud Orchestrator. La solution FlexPod a constamment évolué pour permettre aux clients de moderniser leurs applications et leurs processus de distribution. Avec cette solution, vous pouvez créer un plan de reprise après incident BCDR avec le cloud public, point de passage à un plan de reprise après incident transitoire ou à plein temps, tout en réduisant le coût de la solution de reprise après incident.

La réplication des données entre FlexPod sur site et NetApp Cloud Volumes ONTAP a été gérée par la technologie SnapMirror éprouvée, mais vous pouvez également sélectionner d'autres outils NetApp de transfert et de synchronisation comme Cloud Sync pour vos besoins en termes de mobilité des données. Sécurité des données à la volée assurée par des technologies de chiffrement intégrées basées sur TLS/AES.

Que vous ayez un plan de reprise sur incident temporaire pour une application ou un plan de reprise sur incident à temps plein pour une entreprise, le portefeuille de produits utilisés dans cette solution peut répondre aux deux besoins à grande échelle. Optimisé par Cisco Intersight Workflow Orchestrator, il en va de même pour l'automatisation avec des flux de travail prédéfinis qui éliminent non seulement les processus de reconstruction, mais accélèrent également la mise en œuvre d'un plan de CDR.

Cette solution permet de gérer FlexPod sur site et la réplication des données dans un cloud hybride de manière très simple et pratique, grâce à l'automatisation et à l'orchestration fournies par Cisco Intersight Cloud Orchestrator.

Où trouver des informations complémentaires

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

GitHub

- Toutes les configurations Terraform utilisées

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- Fichiers JSON pour l'importation des flux de production

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Centre d'aide Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentation Cisco Intersight Cloud Orchestrator :

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service pour la documentation Terraform de HashiCorp

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Fiche technique Cisco Intersight

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Fiche technique Cisco Intersight Cloud Orchestrator

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Fiche technique Cisco Intersight Service for HashiCorp Terraform

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "FlexPod Datacenter avec Cisco UCS 4.2(1) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9 : Guide de conception"

- FlexPod Datacenter avec Cisco UCS X-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

Interopérabilité

- Matrice d'interopérabilité NetApp

  "http://support.netapp.com/matrix/"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Documents de référence de NetApp Cloud Volumes ONTAP

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Calculateur de coût total de possession Cloud Volumes ONTAP

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- Outil d'évaluation du cloud

  https://cloud.netapp.com/assessments

- Le cloud hybride NetApp

  https://cloud.netapp.com/hybrid-cloud

- Documentation de l'API Cloud Manager

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Résolution des problèmes

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Terraform Cloud

  "https://www.terraform.io/cloud"

- Documentation Terraform

  "https://www.terraform.io/docs/"

- Registre NetApp Cloud Manager

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- ONTAP haute disponibilité pour GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- Avantages de GCP

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

Cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

Tr-4936 : cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

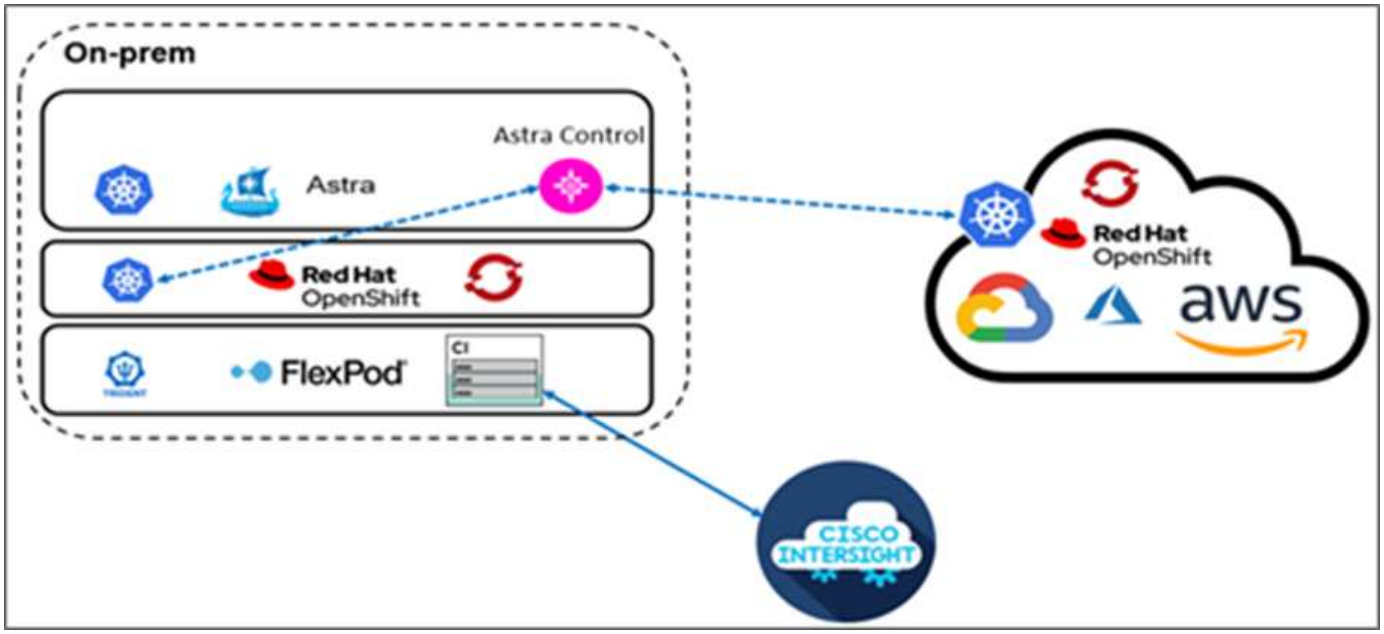
Abhinav Singh

Introduction

Les conteneurs et Kubernetes s'imposent comme la solution idéale pour développer, déployer, exécuter, gérer et faire évoluer les applications conteneurisées, et les entreprises déploient de plus en plus d'applications stratégiques. Les applications stratégiques dépendent fortement de l'état des applications. Une application avec état possède des informations associées à l'état, aux données et à la configuration, et dépend des transactions de données précédentes pour exécuter sa logique applicative. Les applications stratégiques s'exécutant sur Kubernetes continuent de satisfaire aux exigences de disponibilité et de continuité de l'activité telles que les applications classiques. Une panne de service peut avoir des conséquences graves sur la perte de chiffre d'affaires, la productivité et la réputation de l'entreprise. Il est donc essentiel de protéger, restaurer et déplacer les workloads Kubernetes rapidement et facilement dans et entre les clusters, les data centers sur site et les environnements de cloud hybride. Les entreprises ont vu les avantages de basculer leur activité vers un modèle de cloud hybride et de moderniser leurs applications dans un format cloud natif.

Dans ce rapport technique, nous Unis d'un centre de contrôle NetApp Astra avec Red Hat OpenShift Container Platform sur une solution d'infrastructure convergée FlexPod. Il s'étend à Amazon Web Services (AWS) pour former un data Center de cloud hybride. Sur la base de la connaissance "FlexPod et Red Hat OpenShift", Ce document présente NetApp Astra Control Center, qui commence par l'installation, la configuration, les workflows de protection des applications et la migration des applications entre le site et le cloud. Il présente également les avantages des fonctionnalités de gestion des données intégrant la cohérence applicative (notamment la sauvegarde et la restauration, la continuité de l'activité) avec NetApp Astra Control Center pour les applications conteneurisées qui s'exécutent sur Red Hat OpenShift.

La figure suivante illustre la présentation de la solution.



Public

Le public visé est composé de directeurs de la technologie (CTO), de développeurs d'applications, d'architectes de solutions cloud, d'ingénieurs de fiabilité des sites, d'ingénieurs DevOps, d'opérations IT et d'équipes de services professionnels axés sur la conception, l'hébergement et la gestion des applications conteneurisées.

NetApp Astra Control – principales utilisations

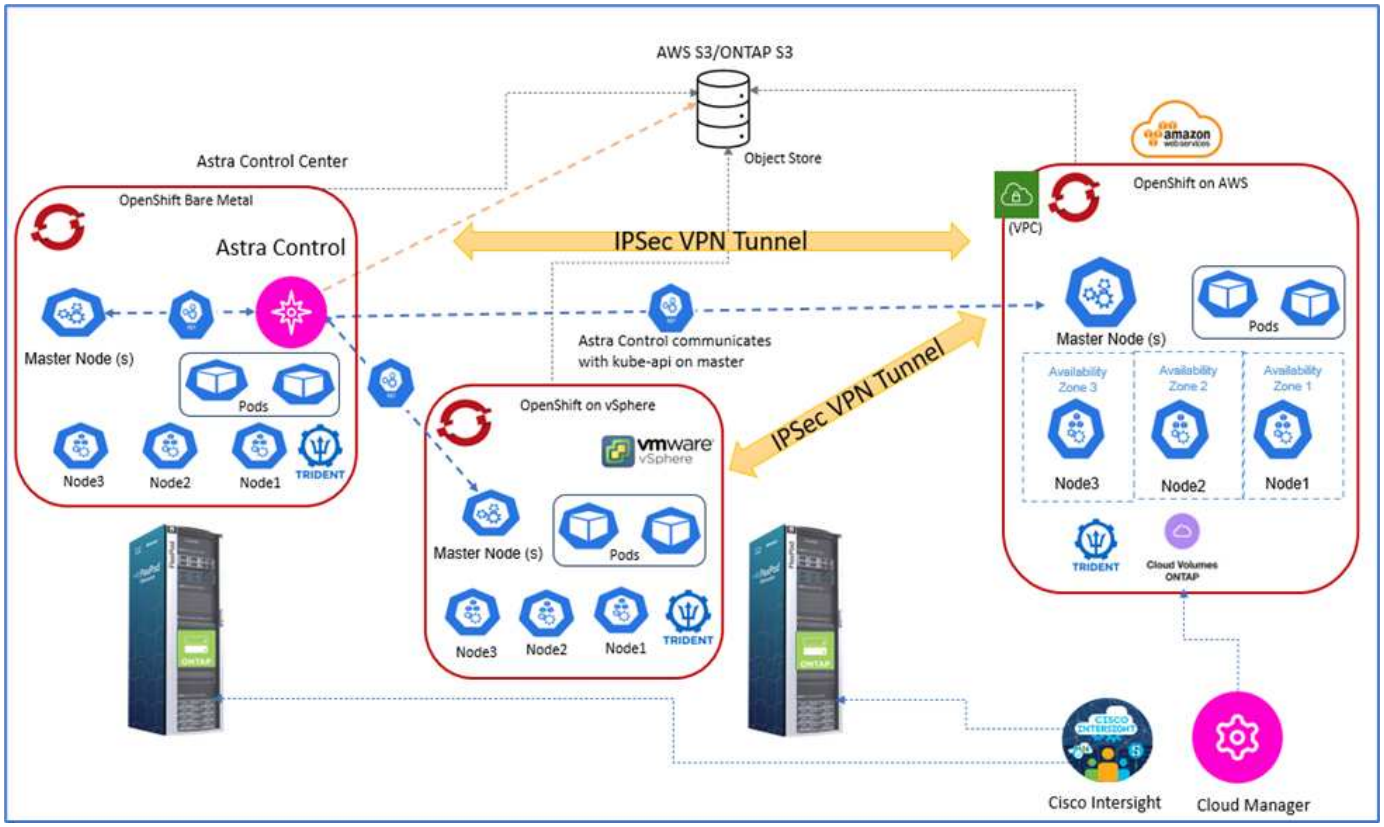
NetApp Astra Control vise à simplifier la protection des applications pour les clients qui gèrent des microservices cloud natifs :

- **Représentation d'application instantanée avec snapshots.** avec Astra Control, vous pouvez effectuer des snapshots de bout en bout de vos applications conteneurisées qui incluent les détails de configuration de l'application exécutée sur Kubernetes et le stockage persistant associé. En cas d'incident, les applications peuvent être restaurées à un état de fonctionnement connu en cliquant sur le bouton.
- **Sauvegarde complète de l'application de copie.** avec Astra Control, vous pouvez effectuer une sauvegarde complète de l'application selon un calendrier prédéfini qui peut être utilisé pour restaurer l'application vers le même cluster K8s ou vers un autre cluster à la demande de façon automatisée.
- **Portabilité des applications et migration avec des clones.** avec Astra Control, vous pouvez cloner une application entière avec ses données d'un cluster Kubernetes vers un autre cluster ou au sein d'un même cluster K8s. Cette fonction contribue également à déplacer ou migrer une application sur les clusters K8s, quel que soit l'emplacement des clusters (il suffit de supprimer l'instance d'application source après le clonage).
- **Personnaliser la cohérence des applications.** avec Astra Control, vous pouvez prendre le contrôle de la définition des États de mise en attente des applications en utilisant les crochets d'exécution. Lorsque vous placez les crochets d'exécution « pré » et « post » dans les flux de travail de snapshot et de sauvegarde, vos applications seront suspendues de votre manière avant qu'un snapshot ou une sauvegarde ne soit créé.
- **Automatisez la reprise après incident au niveau applicatif.** avec Astra Control, vous pouvez configurer un plan de reprise après incident pour la continuité de l'activité pour vos applications conteneurisées. NetApp SnapMirror est utilisé en back-end et la mise en œuvre complète du workflow de reprise après incident est automatisée.

Topologie de la solution

Cette section décrit la topologie logique de la solution.

L'illustration suivante représente la topologie de la solution, constituée de l'environnement FlexPod sur site exécutant des clusters OpenShift Container Platform et d'un cluster OpenShift Container Platform autogéré sur AWS avec NetApp Cloud Volumes ONTAP, Cisco Intersight et la plateforme NetApp Cloud Manager SaaS.



Le premier cluster OpenShift Container Platform est une installation sans système d'exploitation sur FlexPod. Le second cluster OpenShift Container Platform est déployé sur VMware vSphere exécuté sur FlexPod, et le troisième cluster OpenShift Container Platform est déployé en tant que "cluster privé" Dans un cloud privé virtuel (VPC) existant sur AWS en tant qu'infrastructure autonome.

Avec cette solution, FlexPod est connecté à AWS par le biais d'un VPN site à site. Cependant, les clients peuvent également utiliser les implémentations de connexion directe pour s'étendre à un cloud hybride. Cisco Intersight permet de gérer les composants de l'infrastructure FlexPod.

Dans cette solution, Astra Control Center gère l'application conteneurisée hébergée sur le cluster OpenShift Container Platform qui s'exécute sur FlexPod et sur AWS. Astra Control Center est installé sur l'instance OpenShift bare-Metal qui s'exécute sur FlexPod. Astra Control communique avec l'api kube sur le nœud maître et surveille en permanence le cluster Kubernetes pour y apporter des modifications. Toutes les nouvelles applications ajoutées au cluster K8s sont automatiquement découvertes et mises à disposition pour la gestion.

La représentation des applications conteneurisées peut être capturée sous forme de copies Snapshot à l'aide d'Astra Control Center. Les snapshots d'applications peuvent être déclenchés par une stratégie de protection planifiée ou à la demande. Pour les applications prises en charge par Astra, le snapshot est cohérent en cas de panne. Un snapshot d'application constitue un snapshot des données d'application dans les volumes persistants, ainsi que des métadonnées d'application des différentes ressources Kubernetes associées à cette application.

Il est possible de créer une copie de sauvegarde complète d'une application à l'aide d'Astra Control avec un programme de sauvegarde prédéfini ou à la demande. Un stockage objet est utilisé pour stocker la sauvegarde des données d'application. NetApp ONTAP S3, NetApp StorageGRID et toutes les implémentations S3 génériques peuvent être utilisées comme un magasin d'objets.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS, Cisco Unified Computing System (Cisco UCS). La conception est suffisamment flexible pour que le réseau, le calcul et le stockage puissent s'intégrer dans un seul rack de data Center ou être déployés selon la conception du centre de données du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

Contrôle Astra

Astra Control propose des services de protection des données cohérents avec les applications cloud, hébergés dans des clouds publics et sur site. Astra Control assure la protection des données, la reprise d'activité et la migration de vos applications conteneurisées exécutées sur Kubernetes.

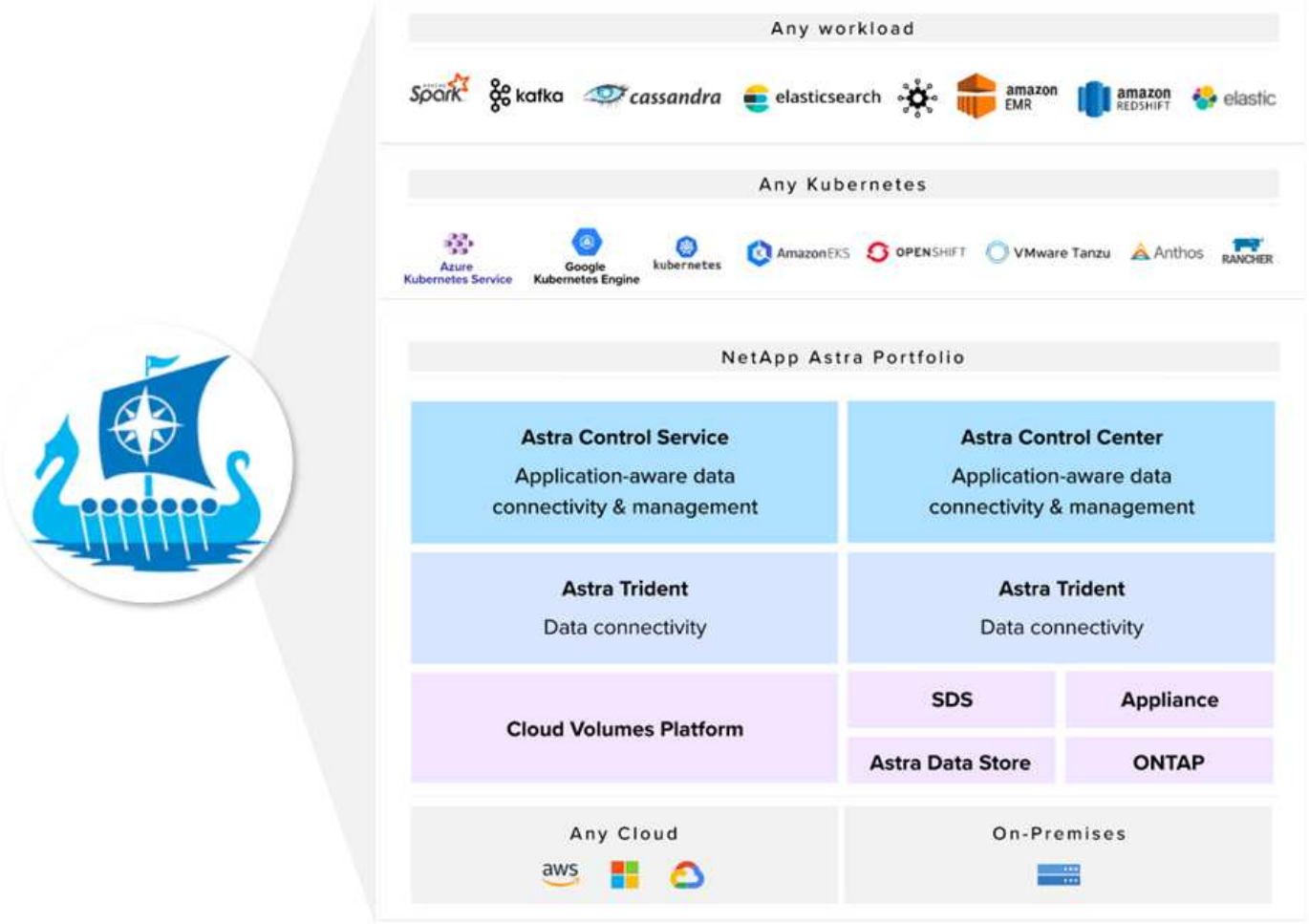
Caractéristiques

Astra Control offre des fonctionnalités stratégiques pour la gestion du cycle de vie des données d'application Kubernetes :

- Gérez automatiquement le stockage persistant
- Création de copies Snapshot et de sauvegardes cohérentes avec les applications à la demande
- Opérations de sauvegarde et de snapshots automatisées basées sur des règles
- Migrez des applications et des données associées d'un cluster Kubernetes vers un autre dans une configuration de cloud hybride
- Clonez une application sur le même cluster K8s ou sur un autre cluster K8s
- Visualisation de l'état de la protection des applications
- Fournit une interface utilisateur graphique et une liste exhaustive d'API REST permettant de mettre en œuvre tous les flux de travail de protection à partir des outils internes existants.

Astra Control offre une visualisation centralisée pour vos applications conteneurisées qui fournit un aperçu des ressources associées créées dans le cluster Kubernetes. Vous pouvez afficher tous vos clusters, toutes vos applications, dans tous les clouds ou dans tous les data centers à partir d'un portail unique. Vous pouvez utiliser les API de contrôle Astra dans tous les environnements (sur site ou dans des clouds publics) pour implémenter vos workflows de gestion des données.

L'image suivante montre les fonctions de contrôle Astra.



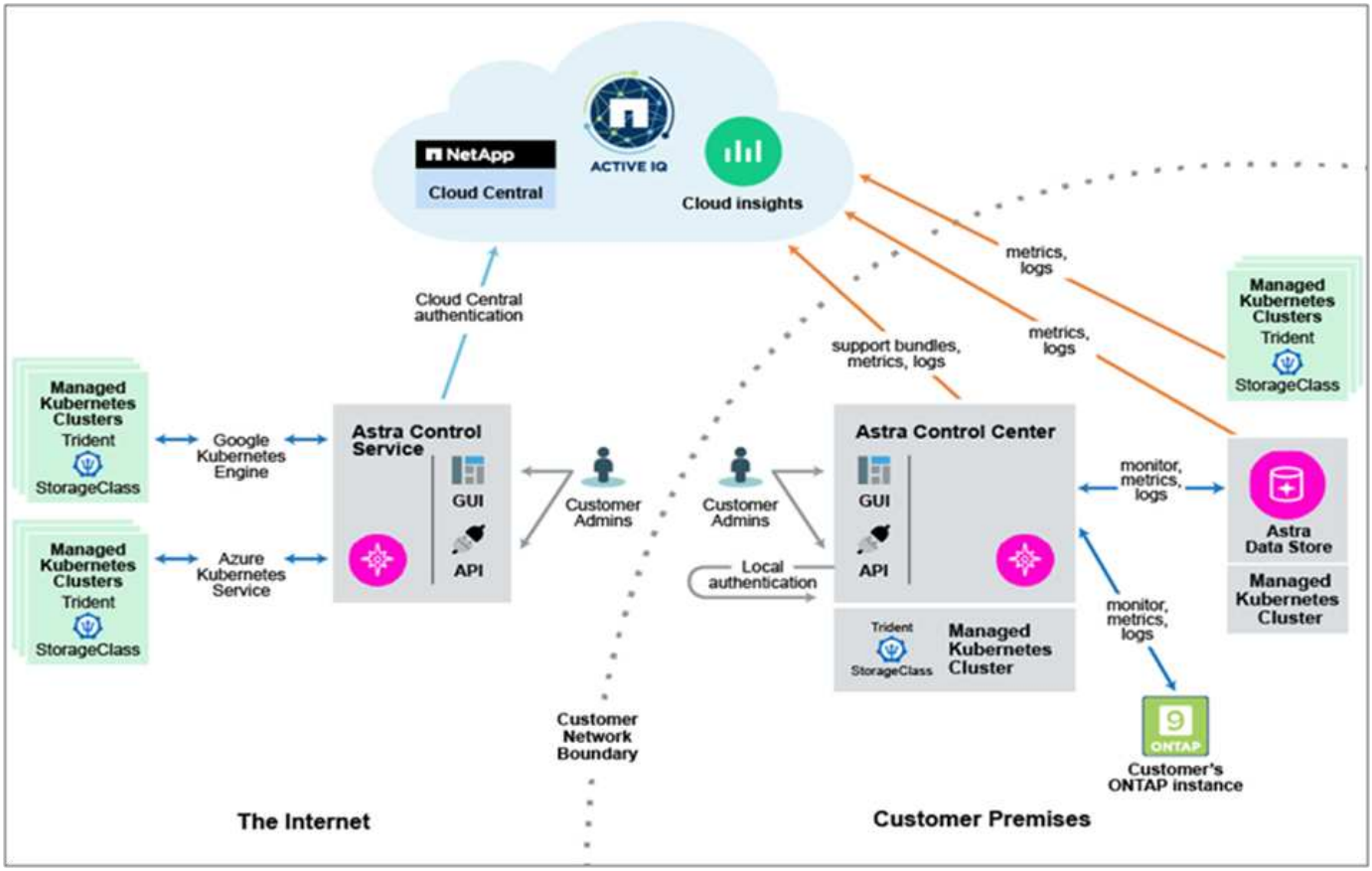
Modèles de consommation Astra Control

Astra Control est disponible en deux modèles de consommation :

- **Astra Control Service.** Un service entièrement géré hébergé par NetApp qui permet la gestion des données intégrant la cohérence applicative des clusters Kubernetes dans Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS).
- **Astra Control Center.** logiciel autogéré qui assure la gestion des données intégrant la cohérence applicative de clusters Kubernetes exécutés dans votre environnement sur site et de cloud hybride.

Dans ce rapport technique, Astra Control Center est utilisé pour la gestion des applications cloud natives qui s'exécutent sur Kubernetes.

L'image suivante montre l'architecture Astra Control.



Astra Trident

Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes. Il a été conçu dès le départ pour vous aider à répondre aux exigences de persistance de vos applications conteneurisées à l'aide d'interfaces standard, telles que le "Interface de stockage de conteneurs (CSI)". Avec Astra Trident, les microservices et les applications conteneurisées peuvent bénéficier des services de stockage haute performance fournis par le portefeuille NetApp de systèmes de stockage.

Astra Trident est déployé sur des clusters Kubernetes en tant que pods et fournit des services d'orchestration du stockage dynamique pour vos workloads Kubernetes. Il permet à vos applications conteneurisées de consommer le stockage persistant rapidement et facilement depuis le vaste portefeuille de NetApp, qui inclut NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, cloud, Et Amazon FSX pour NetApp ONTAP), NetApp Element (NetApp SolidFire), ainsi que le service Azure NetApp Files, Cloud Volume Service sur Google Cloud et Cloud volumes Service sur AWS. Dans un environnement FlexPod, Astra Trident permet de provisionner et de gérer de manière dynamique les volumes persistants pour les conteneurs qui sont sauvegardés par des volumes NetApp FlexVol et des LUN hébergés sur une plateforme de stockage ONTAP, comme les systèmes NetApp AFF, FAS et Cloud Volumes ONTAP. Trident joue également un rôle clé dans la mise en œuvre de systèmes de protection des applications proposés par Astra Control. Pour en savoir plus sur Astra Trident, rendez-vous sur le "Documentation Astra Trident."

Système back-end

Pour utiliser Astra Trident, vous avez besoin d'un système back-end de stockage pris en charge. Un système back-end Trident définit la relation entre Trident et un système de stockage. Il explique à Trident comment communiquer avec ce système de stockage et comment Trident doit provisionner les volumes à partir de celui-ci. Trident va automatiquement proposer des pools de stockage back-end correspondant aux exigences définies par une classe de stockage.

- Système back-end ONTAP AFF et FAS. En tant que plateforme matérielle et logicielle de stockage, ONTAP fournit des services de stockage de base, la prise en charge de plusieurs protocoles d'accès au stockage et des fonctionnalités de gestion du stockage, comme les copies Snapshot et la mise en miroir NetApp.
- Système back-end Cloud Volumes ONTAP
- "Magasin de données Astra" système back-end

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP est une offre de stockage Software-defined qui offre des fonctionnalités avancées de gestion des données pour les workloads de fichiers et de blocs. Avec Cloud Volumes ONTAP, vous pouvez optimiser vos coûts de stockage cloud et augmenter les performances de vos applications tout en améliorant la protection des données, la sécurité et la conformité.

Parmi les principaux avantages :

- Exploitez les fonctionnalités intégrées de déduplication et de compression des données, de provisionnement fin et de clonage pour réduire les coûts de stockage.
- Fiabilité exceptionnelle et continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication leader de NetApp, pour répliquer les données sur site dans le cloud de façon à pouvoir disposer de copies secondaires dans différents cas d'utilisation.
- Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.
- Basculez entre pools de stockage hautes performances et faibles performances à la demande sans interrompre les applications.
- Cohérence des copies Snapshot avec NetApp SnapCenter
- Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.
- L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

Cloud Central

Cloud Central est une plateforme centralisée qui permet d'accéder aux services de données cloud NetApp et de les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites automatisés de reprise d'activité, de sauvegarder les données et de migrer et contrôler efficacement les données entre plusieurs clouds. Pour plus d'informations, voir "Cloud Central."

Le gestionnaire Cloud

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui permet aux experts INFORMATIQUES et aux architectes clouds de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions clouds NetApp. Cette solution offre un système centralisé pour afficher et gérer vos environnements de stockage sur site et cloud, prenant en charge des environnements de cloud hybride de plusieurs fournisseurs et comptes. Pour plus d'informations, voir "Le gestionnaire Cloud".

Connecteur

Connector est une instance qui permet à Cloud Manager de gérer les ressources et les processus dans un

environnement de cloud public. Un connecteur est nécessaire pour utiliser de nombreuses fonctionnalités offertes par Cloud Manager. Un connecteur peut être déployé dans le cloud ou sur site.

Le connecteur est pris en charge aux emplacements suivants :

- AWS
- Microsoft Azure
- Google Cloud
- Sur site

Pour en savoir plus sur le connecteur, voir "ce lien."

NetApp Cloud Insights

Avec l'outil NetApp de surveillance de l'infrastructure cloud, Cloud Insights vous permet de surveiller la performance et l'utilisation de vos clusters Kubernetes gérés par Astra Control Center. Cloud Insights met en corrélation l'utilisation du stockage avec les charges de travail. Lorsque vous activez la connexion Cloud Insights dans le centre de contrôle Astra, les informations de télémétrie s'affichent dans les pages de l'interface utilisateur du centre de contrôle Astra.

NetApp Active IQ Unified Manager

Avec NetApp Active IQ Unified Manager, vous pouvez contrôler vos clusters de stockage ONTAP à partir d'une interface intuitive unique, reconçue pour exploiter les connaissances de la communauté et l'analytique d'IA. Elle fournit des informations opérationnelles, de performance et proactives sur l'environnement de stockage et les machines virtuelles qui s'exécutent sur celui-ci. Lorsqu'un problème survient sur l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre une vue détaillée des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte VMware vSphere, via le réseau et enfin vers le stockage. Certains événements fournissent également des mesures correctives qui peuvent être prises pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et par des traps SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en anticipant les besoins en stockage et en vous permettant d'anticiper les problèmes, ce qui évite de prendre des décisions réactives à court terme et même d'engendrer des problèmes supplémentaires à long terme.

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme contribue aux changements avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride.

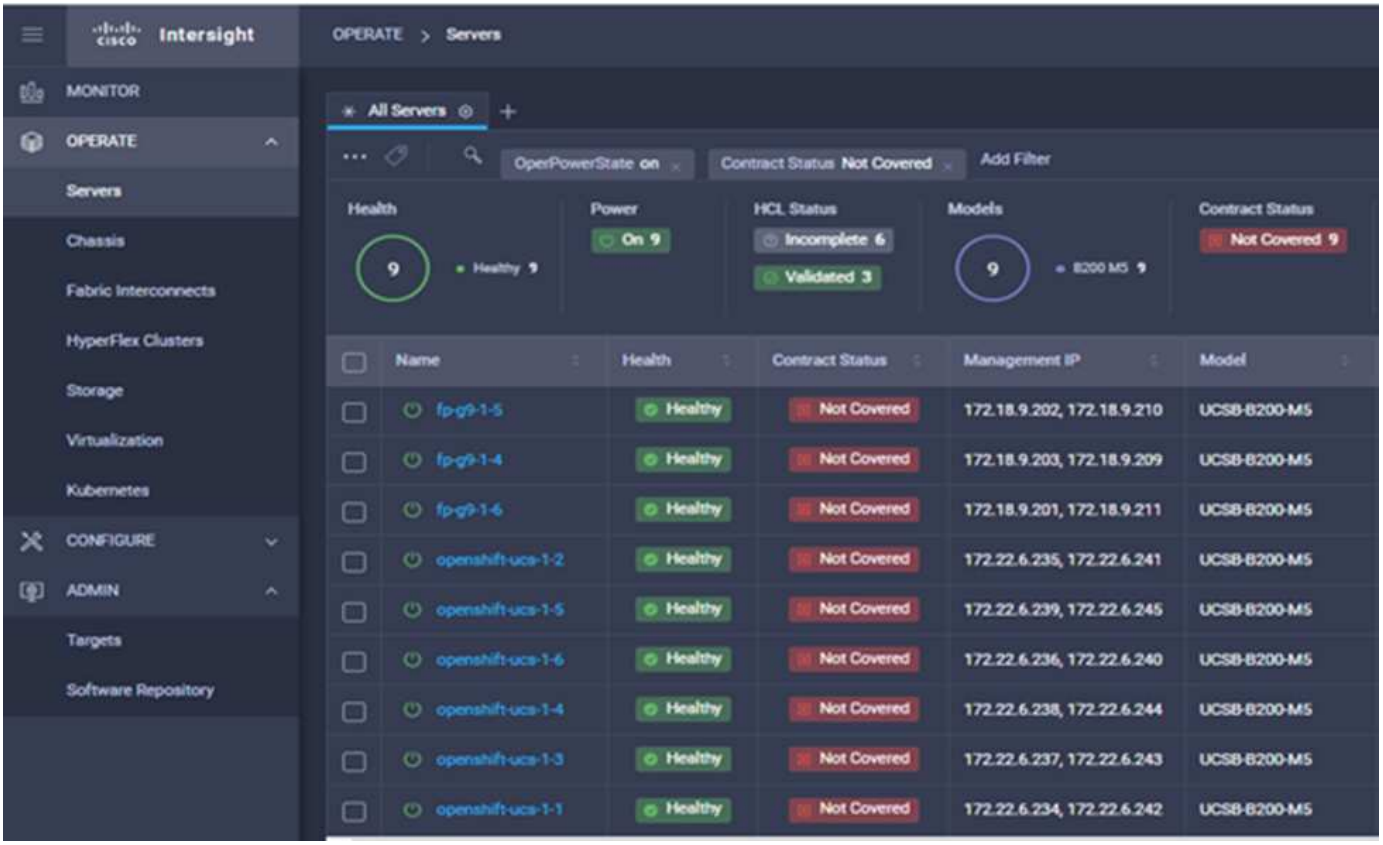
Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** livraison en tant que service depuis le cloud ou dans le centre de données du client avec des mises à jour fréquentes et une innovation continue, grâce à un modèle de développement logiciel agile. De cette façon, le client peut se concentrer sur l'accélération de la livraison pour le secteur d'activité.
- **Opérations simplifiées.** simplifier les opérations en utilisant un seul outil SaaS sécurisé avec inventaire, authentification et API communs pour travailler sur l'ensemble de la pile et tous les emplacements, éliminant ainsi les silos entre les équipes. De la gestion des serveurs physiques et des hyperviseurs sur site aux machines virtuelles, K8s, sans serveur, automatisation, l'optimisation et le contrôle des coûts à la fois sur site et dans les clouds publics.

- **Optimisation continue.** optimisation continue de votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur chaque couche, ainsi que Cisco TAC. Cette intelligence est convertie en actions recommandées et automatisable, ce qui vous permet de vous adapter en temps réel à chaque changement : du déplacement des charges de travail et du contrôle de l'état des serveurs physiques, au dimensionnement automatique des clusters, aux recommandations de réduction des coûts des clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner l'UMM natif ou IMM pour les systèmes Cisco UCS reliés au fabric lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'UMM natif est utilisé.

L'image suivante montre le tableau de bord Cisco Intersight.



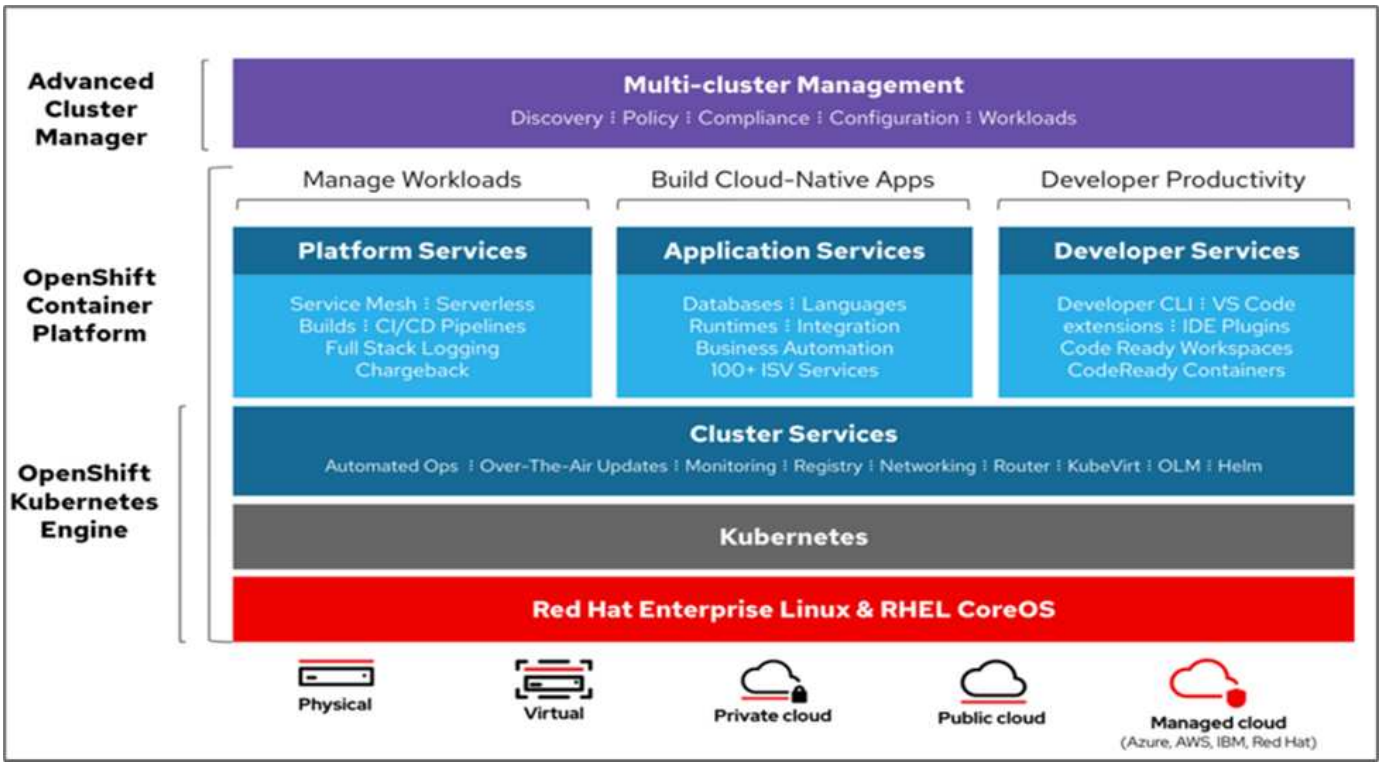
Plateforme de conteneurs Red Hat OpenShift

Red Hat OpenShift Container Platform est une plateforme applicative de conteneurs qui rassemble CRI-O et Kubernetes et qui fournit une API et une interface Web pour gérer ces services. CRI-O est une implémentation de l'interface d'exécution du conteneur Kubernetes (CRI) pour permettre l'utilisation des runtimes compatibles avec l'initiative OCI (Open Container Initiative). Il s'agit d'une alternative légère à l'utilisation de Docker en tant que composant d'exécution pour Kubernetes.

OpenShift Container Platform permet aux clients de créer et de gérer des conteneurs. Les conteneurs sont des processus autonomes qui s'exécutent dans leur propre environnement, indépendamment du système d'exploitation et de l'infrastructure sous-jacente. OpenShift Container Platform aide à développer, déployer et gérer les applications basées sur des conteneurs. Il offre une plateforme en libre-service pour créer, modifier et déployer des applications à la demande, ce qui accélère le développement et la commercialisation des cycles de vie. OpenShift Container Platform est dotée d'une architecture basée sur des microservices de petites unités découplées. Elle s'exécute sur un cluster Kubernetes, et les données relatives aux objets stockés dans

ETCD, un magasin de clés à valeur ajoutée en cluster fiable.

L'image suivante présente la plateforme de conteneurs Red Hat OpenShift.



Infrastructure Kubernetes

Dans OpenShift Container Platform, Kubernetes gère les applications conteneurisées sur un ensemble d'hôtes d'exécution CRI-O, et fournit des mécanismes pour le déploiement, la maintenance et l'évolutivité des applications. Les packages de service CRI-O, instancient et exécutent des applications conteneurisées.

Un cluster Kubernetes comprend un ou plusieurs maîtres et un ensemble de nœuds workers. Cette solution intègre les fonctionnalités de haute disponibilité (HA) au niveau du matériel et de la pile logicielle. Un cluster Kubernetes est conçu pour s'exécuter en mode HA avec trois nœuds maîtres et au moins deux nœuds workers afin de vous aider à assurer que le cluster ne présente aucun point de défaillance unique.

Système d'exploitation Red Hat Core

OpenShift Container Platform exploite Red Hat Enterprise Linux CoreOS (RHCOS), un système d'exploitation orienté conteneurs qui combine les meilleures fonctionnalités des systèmes d'exploitation hôtes atomiques CoreOS et Red Hat. RHCOS est spécialement conçu pour exécuter des applications conteneurisées à partir d'OpenShift Container Platform et fonctionne avec de nouveaux outils pour permettre une installation rapide, une gestion basée sur l'opérateur et des mises à niveau simplifiées.

RHCOS inclut les fonctions suivantes :

- Ignition, qu'OpenShift Container Platform utilise comme première configuration de système de démarrage pour l'initialisation et la configuration des machines.
- CRI-O, implémentation d'un exécution de conteneurs natif Kubernetes qui s'intègre étroitement au système d'exploitation pour offrir une expérience Kubernetes efficace et optimisée. CRI-O permet de faire fonctionner, d'arrêter et de redémarrer les conteneurs. Elle remplace entièrement le moteur de conteneurs Docker, qui a été utilisé dans OpenShift Container Platform 3.

- Kubelet, l'agent de nœud principal pour Kubernetes, est responsable du lancement et de la surveillance des conteneurs.

VMware vSphere 7.0

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière holistique de vastes ensembles d'infrastructures (ressources notamment les processeurs, le stockage et le réseau), sous la forme d'un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation traditionnels qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un data Center dans son ensemble pour créer une seule puissance avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application, selon les besoins.

Pour plus d'informations, voir "VMware vSphere".

VMware vSphere vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Révisions matérielles et logicielles

Cette solution peut être étendue à tout environnement FlexPod qui exécute des versions logicielles, micrologicielles et matérielles prises en charge, telles que définies dans le "Matrice d'interopérabilité NetApp" et "Liste de compatibilité matérielle Cisco UCS." Le cluster OpenShift est installé sur FlexPod sans système d'exploitation, ainsi que sur VMware vSphere.

Une seule instance d'Astra Control Center est nécessaire pour gérer plusieurs clusters OpenShift (k8), tandis que Trident CSI est installé sur chaque cluster OpenShift. Astra Control Center peut être installé sur l'un de ces clusters OpenShift. Dans cette solution, Astra Control Center est installé sur le cluster OpenShift bare-Metal.

Le tableau suivant répertorie les révisions matérielles et logicielles FlexPod pour OpenShift.

Composant	Solution NetApp	Version
Calcul	Cisco UCS Fabric Interconnect 6454	4.1(3c)
	Serveurs Cisco UCS B200 M5	4.1(3c)
Le réseau	Cisco Nexus 9336C-FX2 NX-OS	9.3(8)
Stockage	NetApp AFF A700	9.11.1
	NetApp Astra Control Center	22.04.0
	Plug-in NetApp Astra Trident CSI	22.04.0
	NetApp Active IQ Unified Manager	9.11
Logiciel	Pilote Ethernet nenic VMware ESXi	1.0.35.0
	VSphere ESXi	7.0(U2)

Composant	Solution NetApp	Version
	Appliance VMware vCenter	7.0 U2b
	Appliance virtuelle Cisco InterSight Assist	1.0.9-342
	Plateforme de conteneurs OpenShift	4.9
	Nœud principal OpenShift Container Platform	RHCOS 4.9
	Nœud de travail OpenShift Container Platform	RHCOS 4.9

Le tableau suivant répertorie les versions logicielles d'OpenShift sur AWS.

Composant	Solution NetApp	Version
Calcul	Type d'instance maître : m5.XLarge	s/o
	Type d'instance de travailleur : m5.large	s/o
Le réseau	Passerelle de transit du cloud privé virtuel	s/o
Stockage	NetApp Cloud Volumes ONTAP	9.11.1
	Plug-in NetApp Astra Trident CSI	22.04.0
Logiciel	Plateforme de conteneurs OpenShift	4.9
	Nœud principal OpenShift Container Platform	RHCOS 4.9
	Nœud de travail OpenShift Container Platform	RHCOS 4.9

"Suivant : installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation."

Installation et configuration

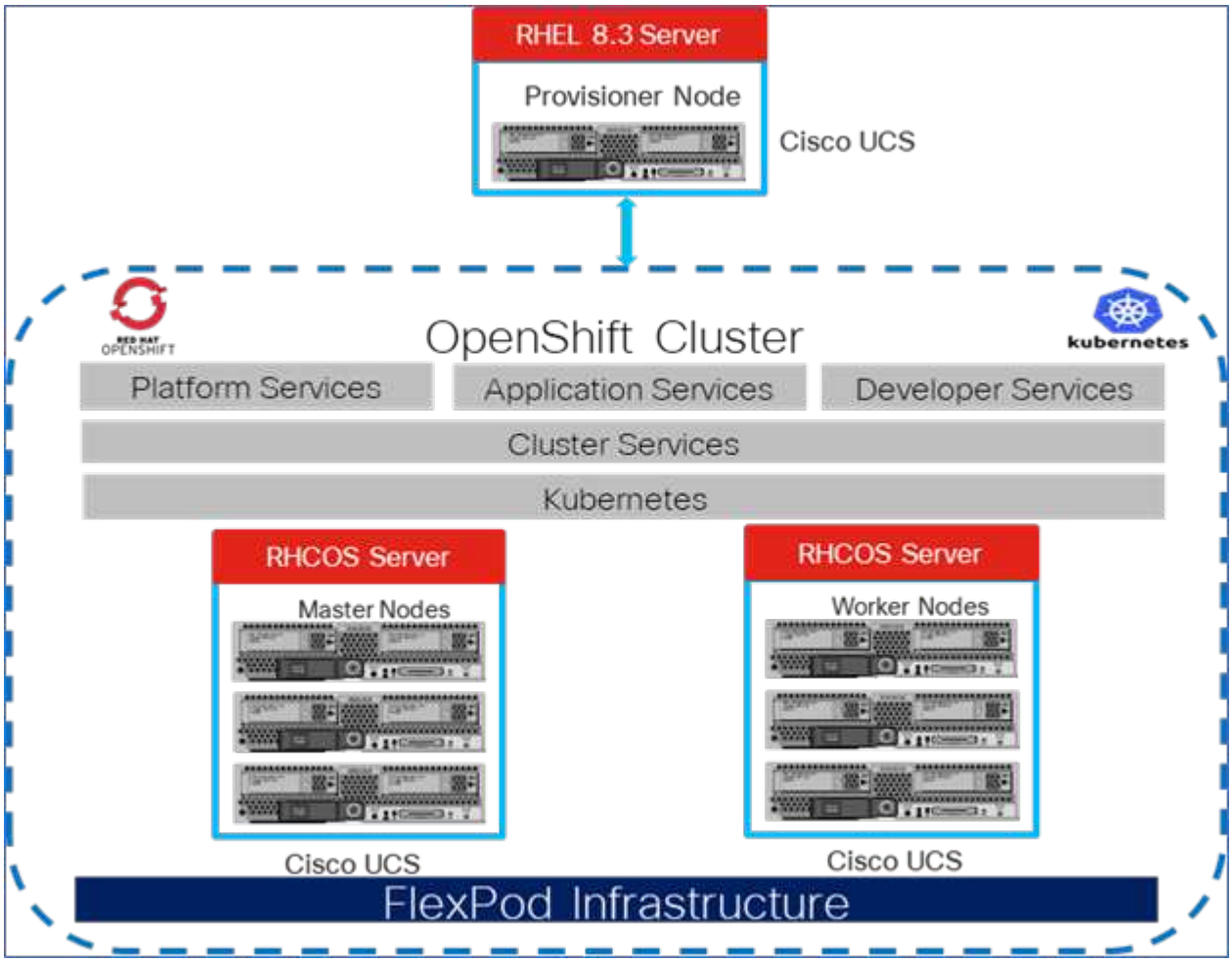
Installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation

"Précédent : composants de la solution."

Pour comprendre la conception sans système d'exploitation FlexPod pour OpenShift Container Platform 4, les détails du déploiement et l'installation et la configuration de NetApp Astra Trident, consultez "Guide de déploiement et de conception validée par Cisco pour FlexPod avec OpenShift Cisco (CVD)". Ce CVD couvre le déploiement d'FlexPod et de OpenShift Container Platform avec Ansible. Le CVD fournit également des informations détaillées sur la préparation des nœuds de travail, de l'installation d'Astra Trident, du système de stockage back-end et des configurations de classes de stockage, qui sont les quelques prérequis au déploiement et à la configuration d'Astra

Control Center.

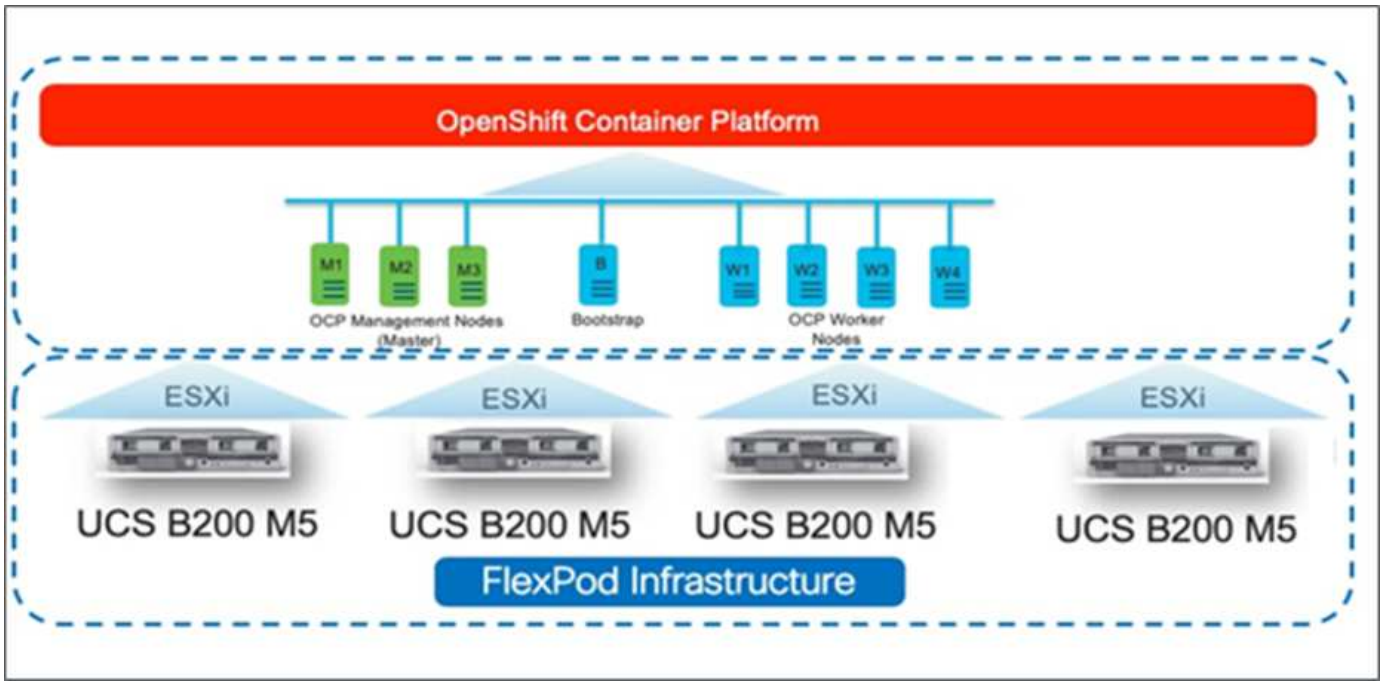
La figure suivante illustre la plateforme de conteneurs OpenShift 4 sans système d'exploitation sur FlexPod.



FlexPod pour OpenShift Container Platform 4 sur installation VMware

Pour en savoir plus sur le déploiement de Red Hat OpenShift Container Platform 4 sur un système FlexPod exécutant VMware vSphere, consultez la page "FlexPod Datacenter pour OpenShift Container Platform 4".

La figure suivante illustre FlexPod pour OpenShift Container Platform 4 sur vSphere.



"Suivant : Red Hat OpenShift sur AWS."

Red Hat OpenShift sur AWS

"Précédent : installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation."

Un cluster OpenShift Container Platform 4 autogéré est déployé sur AWS en tant que site de reprise après incident. Les nœuds maîtres et workers s'étendent sur trois zones de disponibilité pour une haute disponibilité.

Instances (6) Info

Search

ocp | Clear filters

Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift est déployé en tant que A. "cluster privé" Dans un VPC existant sur AWS. Un cluster OpenShift Container Platform privé n'expose pas les terminaux externes. Il est accessible uniquement à partir d'un réseau interne et n'est pas visible sur Internet. NetApp Cloud Volumes ONTAP est déployé à un seul nœud à l'aide de NetApp Cloud Manager qui fournit un système back-end de stockage à Astra Trident.

Pour plus d'informations sur l'installation d'OpenShift sur AWS, consultez "Documentation OpenShift".

"Suivant : NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Précédent : Red Hat OpenShift sur AWS."

L'instance NetApp Cloud Volumes ONTAP est déployée sur AWS et sert de stockage back-end à Astra Trident. Avant d'ajouter un environnement de travail Cloud Volumes ONTAP, un connecteur doit être déployé. Cloud Manager vous invite à créer votre premier environnement de travail Cloud Volumes ONTAP sans connecteur. Pour déployer un connecteur dans AWS, voir "Créer un connecteur".

Pour déployer Cloud Volumes ONTAP sur AWS, consultez la section "Démarrage rapide pour AWS".

Une fois Cloud Volumes ONTAP déployé, vous pouvez installer Astra Trident et configurer le système de stockage back-end et la classe Snapshot sur le cluster OpenShift Container Platform.

"Suivant : installation d'Astra Control Center sur OpenShift Container Platform."

Installation d'Astra Control Center sur OpenShift Container Platform

"Précédent : NetApp Cloud Volumes ONTAP."

Vous pouvez installer Astra Control Center sur un cluster OpenShift qui s'exécute sur FlexPod ou sur AWS avec un système de stockage back-end Cloud Volumes ONTAP. Dans cette solution, Astra Control Center est déployé sur le cluster OpenShift bare-Metal.

Le centre de contrôle Astra peut être installé selon la procédure standard décrite "ici" Ou depuis Red Hat OpenShift OperatorHub. L'opérateur de contrôle Astra est un opérateur certifié Red Hat. Dans cette solution, Astra Control Center est installé à l'aide de Red Hat OperatorHub.

De l'environnement

- Astra Control Center prend en charge plusieurs distributions Kubernetes. Pour Red Hat OpenShift, les

versions prises en charge incluent Red Hat OpenShift Container Platform 4.8 ou 4.9.

- Astra Control Center requiert les ressources suivantes en plus des exigences de l'environnement et de l'utilisateur final en matière de ressources applicatives :

Composants	Conditions requises
Capacité du système back-end	Au moins 500 Go disponibles
Nœuds worker	Au moins 3 nœuds workers et doté de 4 cœurs de processeurs et de 12 Go de RAM chacun
Adresse de nom de domaine complet (FQDN)	Une adresse FQDN pour Astra Control Center
Astra Trident	Astra Trident 21.04 ou plus récent installé et configuré
Contrôleur d'entrée ou équilibreur de charge	Configurez le contrôleur d'entrée pour exposer Astra Control Center avec un URL ou un équilibreur de charge afin de fournir une adresse IP qui sera définie pour le FQDN

- Vous devez disposer d'un registre d'images privées existant dans lequel vous pouvez pousser les images de création d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous téléchargez les images.

Certaines images sont extraites lors de l'exécution de certains flux de travail et des conteneurs sont créés et détruits si nécessaire.

- Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. Le centre de contrôle Astra prend en charge les pilotes ONTAP suivants fournis par Astra Trident :
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-économie

Nous supposons qu'Astra Trident est installé et configuré avec un système back-end ONTAP, et qu'une classe de stockage par défaut est également définie.

- En ce qui concerne le clonage d'applications dans les environnements OpenShift, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Pour modifier la export policy ONTAP pour permettre ces opérations, lancer les commandes suivantes :

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

Pour ajouter un deuxième environnement opérationnel OpenShift comme ressource de calcul gérée, assurez-vous que la fonctionnalité de snapshot de volume Astra Trident est activée. Pour activer et tester des copies Snapshot de volume avec Astra Trident, consultez le responsable "Instructions d'Astra Trident".

- A "Classe VolumeSnapClass" Doit être configuré sur tous les clusters Kubernetes à partir de l'emplacement de gestion des applications. Ceci peut également inclure le cluster K8s sur lequel Astra Control Center est installé. Astra Control Center peut gérer les applications du cluster K8s sur lequel il est exécuté.

De gestion des applications

- **Licence.** pour gérer des applications à l'aide d'Astra Control Center, vous avez besoin d'une licence Astra Control Center.
- **Espaces de noms.** Un espace de noms est la plus grande entité qui peut être gérée en tant qu'application par Astra Control Center. Vous pouvez choisir de filtrer les composants en fonction des étiquettes d'application et des étiquettes personnalisées dans un espace de noms existant et de gérer un sous-ensemble de ressources en tant qu'application.
- **StorageClass.** si vous installez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage explicitement définie vers un cluster ne présentant pas la même classe de stockage échoue.
- **Ressources Kubernetes.** les applications qui utilisent des ressources Kubernetes non capturées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control peut capturer les ressources Kubernetes suivantes :

Ressources Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	Ressource CustomResource	Cronjob
Ensemble de démonstrations	HorizontalPodAutoscaler	Entrée
Déploiement.Config	MutatingWebhook	Demande de volume persistant
Pod	PodPetitionBudget	PodTemplate
Stratégie réseau	Et de réplication	Rôle
RoleBinding	Itinéraire	Secret
ValidétingWebhook		

Installez Astra Control Center à l'aide d'OpenShift OperatorHub

La procédure suivante permet d'installer Astra Control Center à l'aide de Red Hat OperatorHub. Dans cette solution, Astra Control Center est installé sur un cluster OpenShift bare-Metal exécuté sur FlexPod.

1. Téléchargez le pack Astra Control Center (`astra-control-center-[version].tar.gz`) du "Site de support NetApp".
2. Téléchargez le fichier .zip pour les certificats et clés Astra Control Center à partir du "Site de support NetApp".
3. Vérifiez la signature du lot.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraire les images Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Passez au répertoire Astra.

```
cd astra-control-center-[version]
```

6. Ajoutez les images à votre registre local.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Utilisez le script approprié pour charger les images, les marquer et les pousser dans votre registre local.

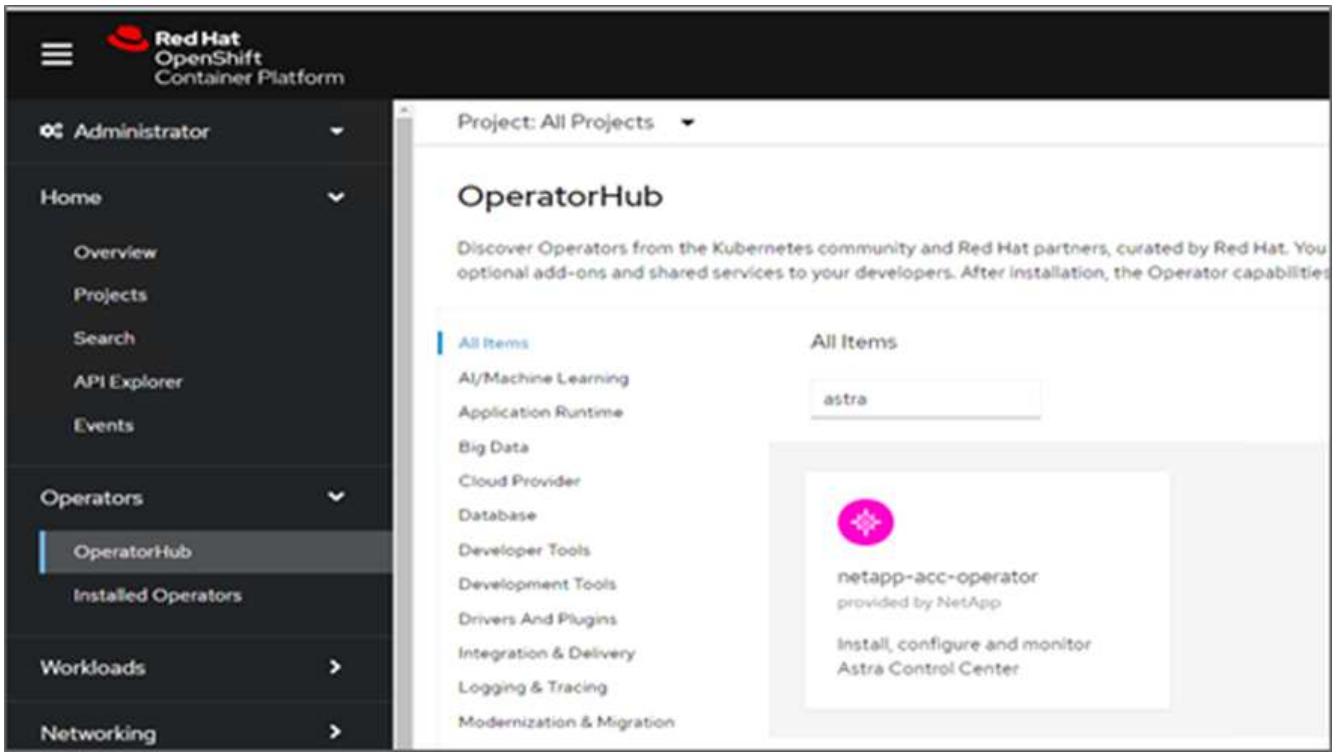
   Pour Docker :

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Pour Podman :

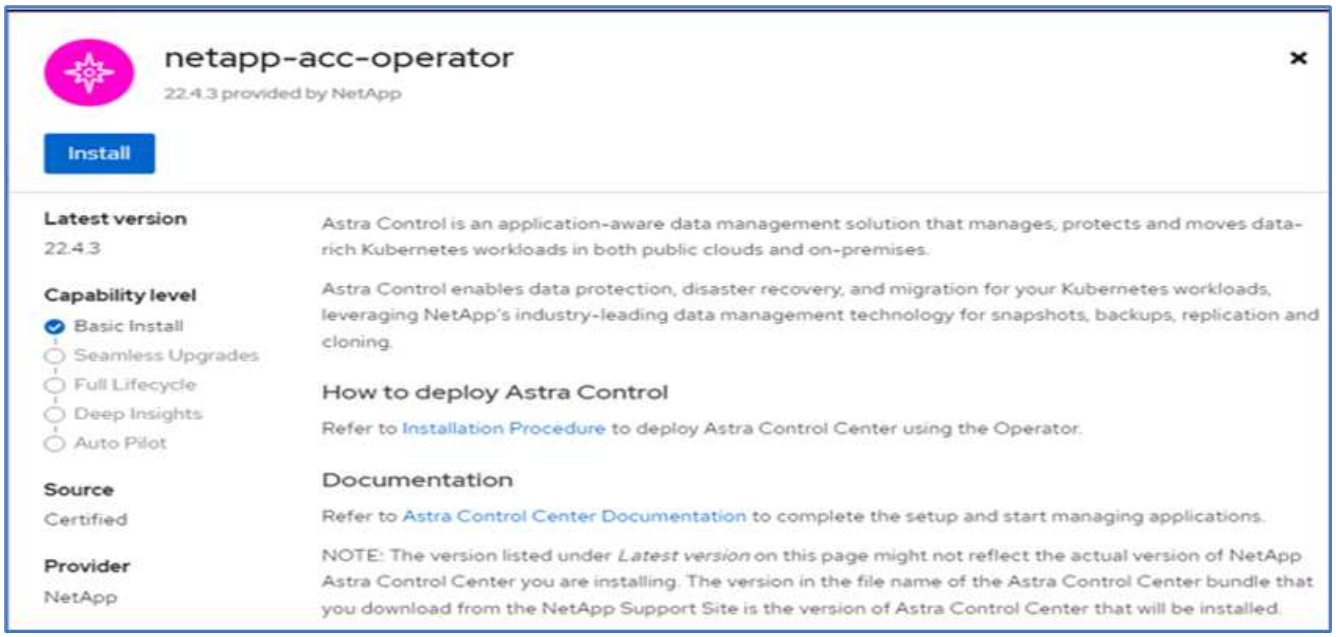
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Connectez-vous à la console web du cluster OpenShift sans système d'exploitation. Dans le menu latéral, sélectionnez opérateurs > OperatorHub. Entrez `astra` pour afficher la liste `netapp-acc-operator`.

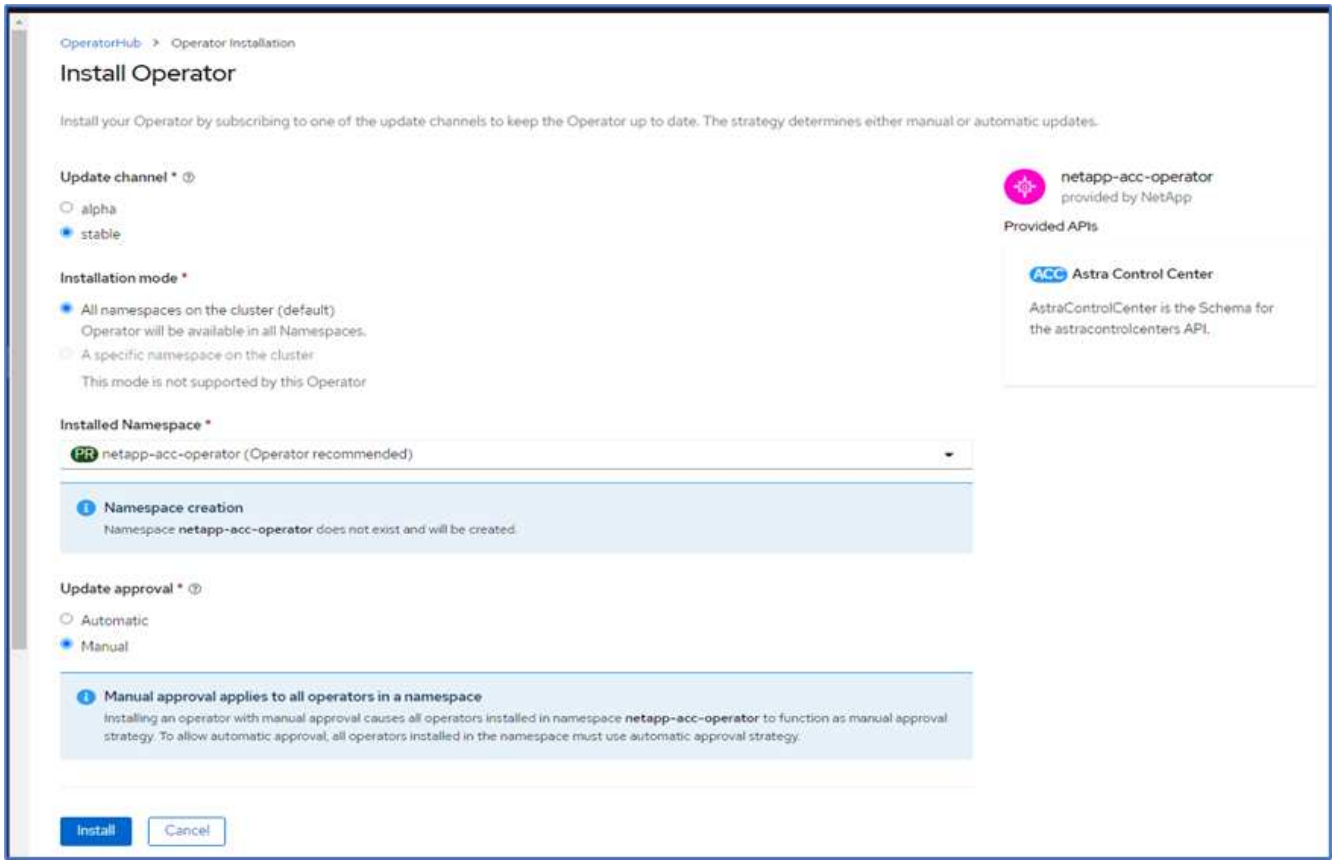


`netapp-acc-operator` Est un opérateur Red Hat OpenShift certifié. Il est répertorié dans le catalogue OperatorHub.

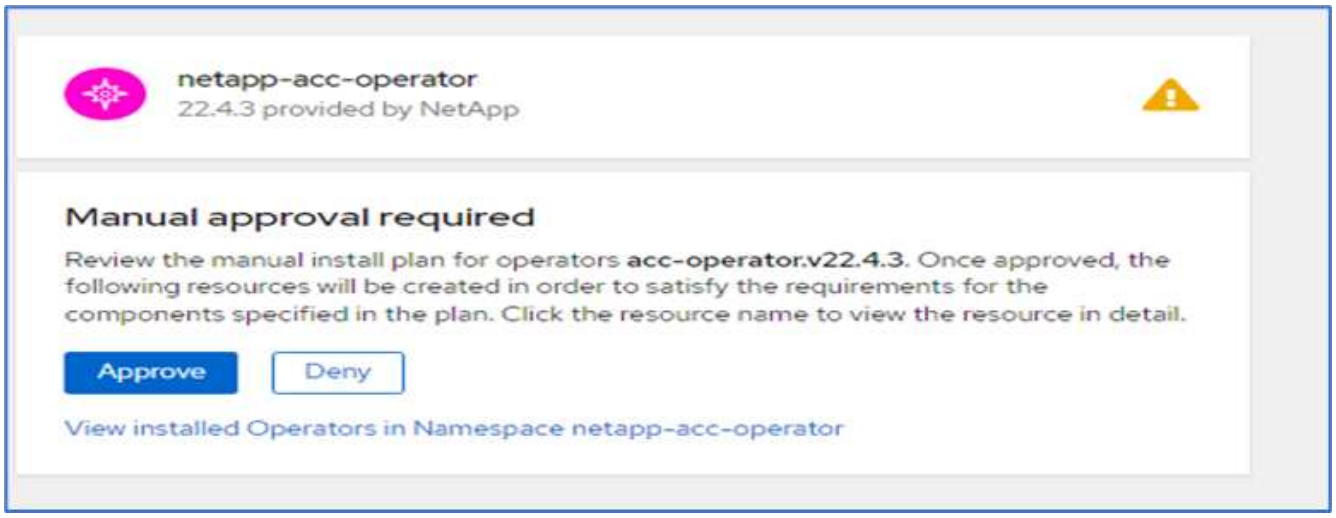
9. Sélectionnez `netapp-acc-operator` Cliquez ensuite sur installation.



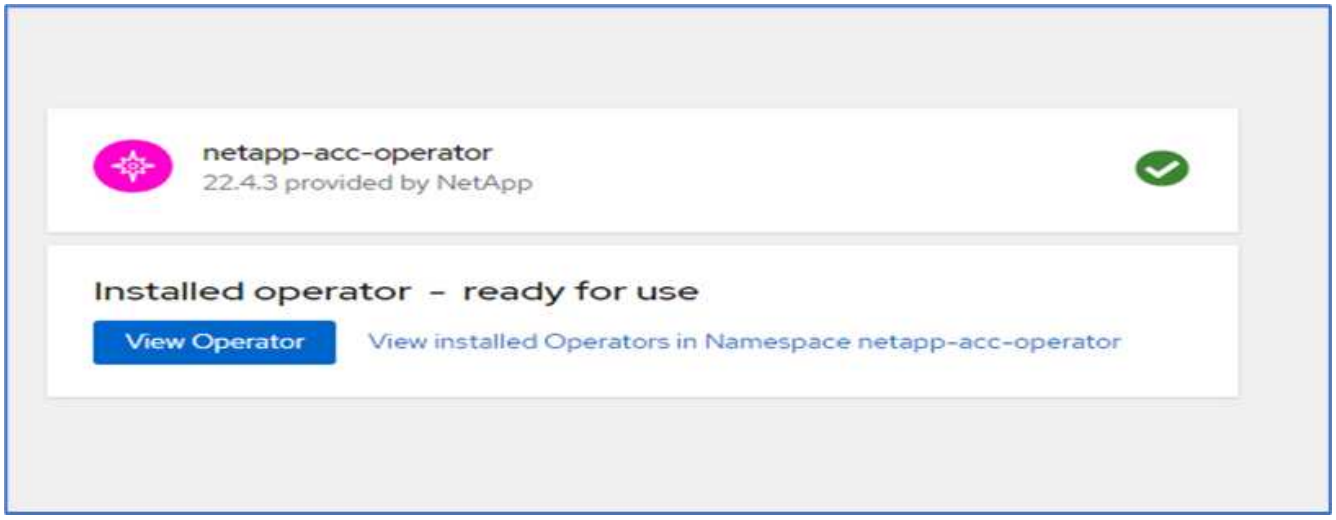
10. Sélectionnez les options appropriées et cliquez sur installer.



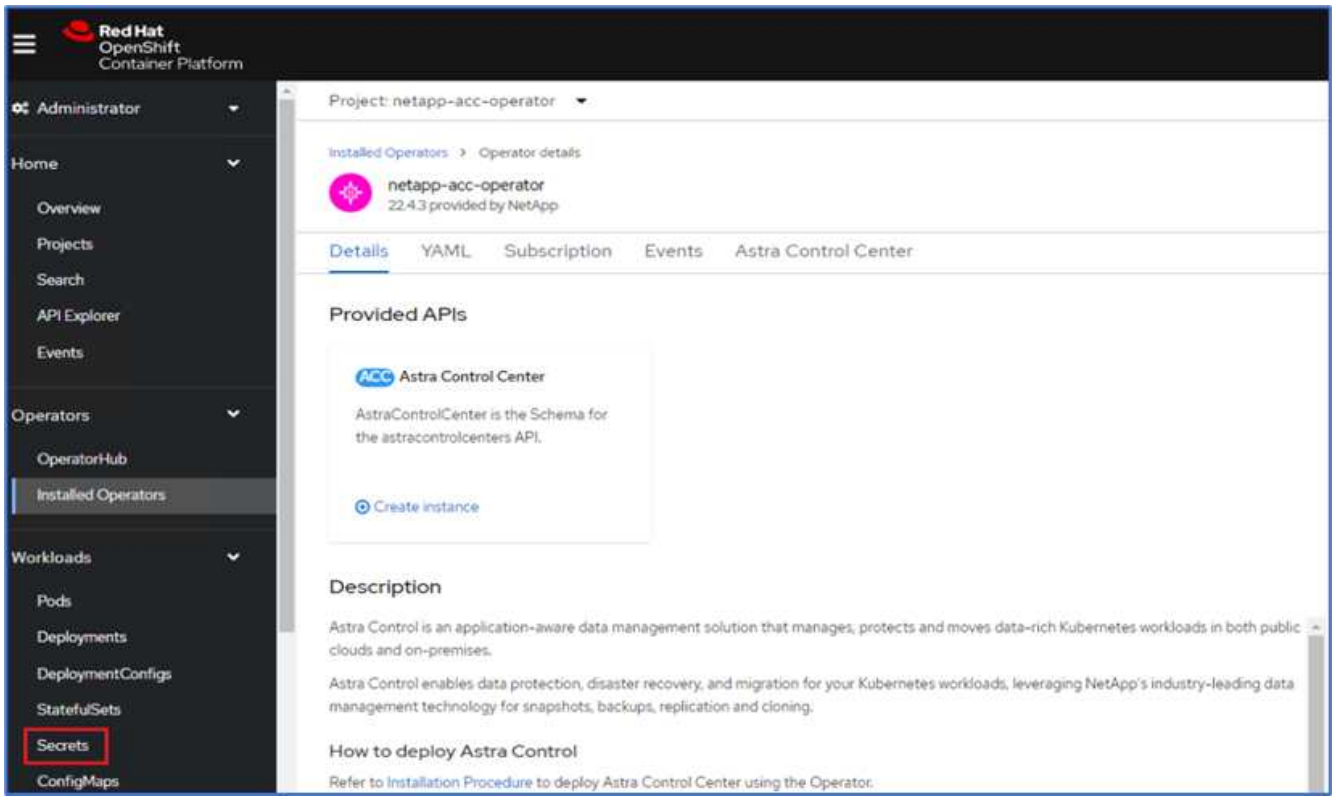
11. Approuver l'installation et attendre que l'opérateur soit installé.



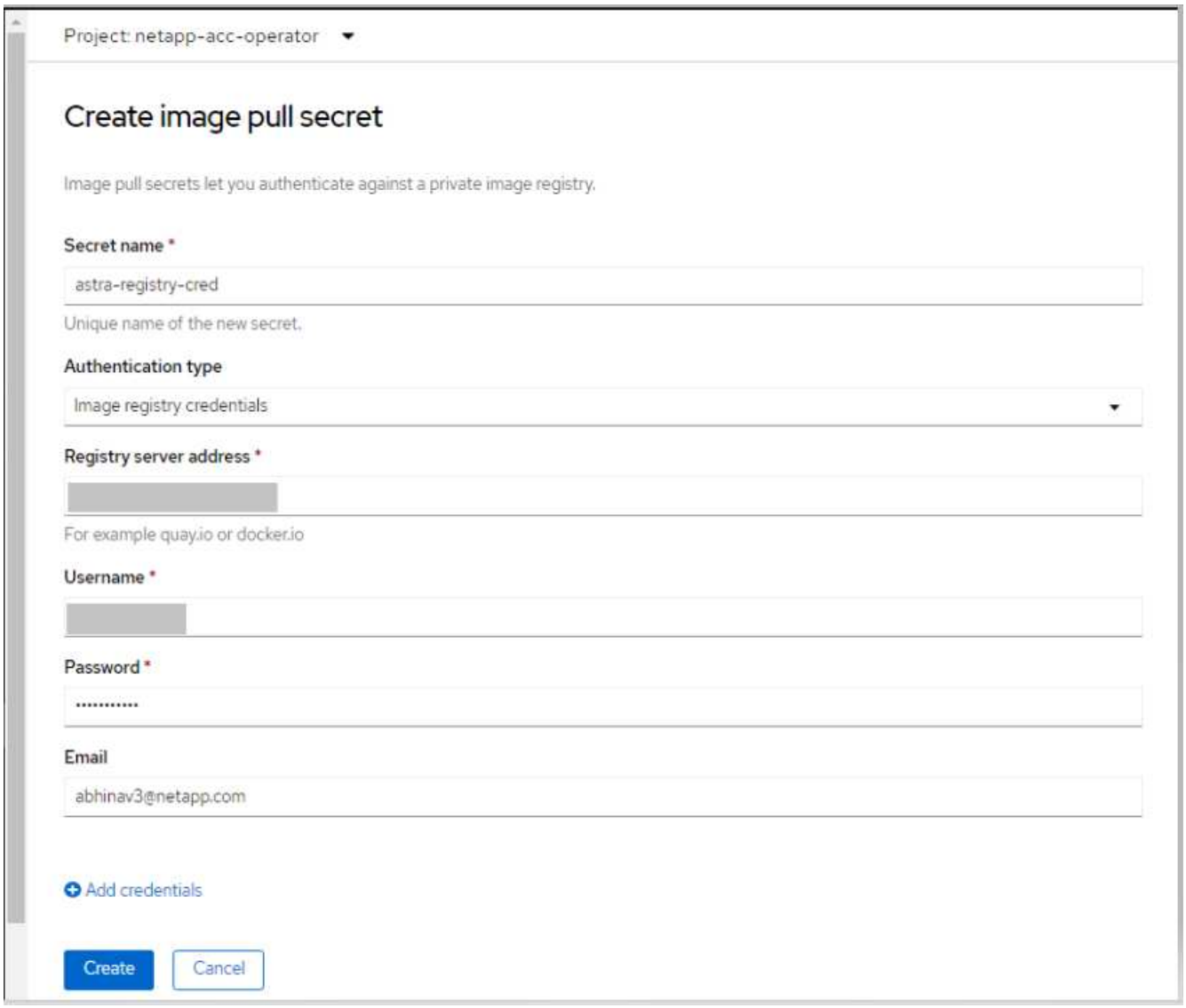
12. À ce stade, l'opérateur est installé avec succès et prêt à l'emploi. Cliquez sur Afficher l'opérateur pour démarrer l'installation du centre de contrôle Astra.



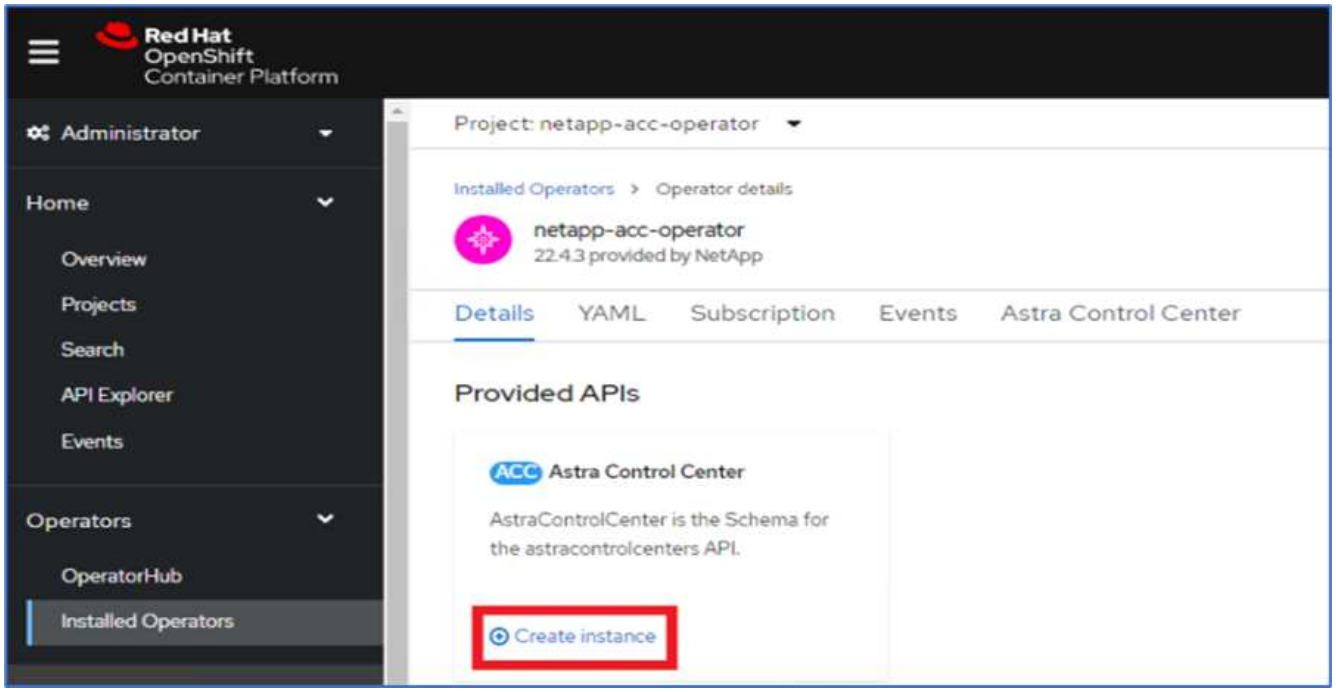
13. Avant d'installer Astra Control Center, créez le secret pour télécharger des images Astra à partir du registre Docker que vous avez poussé plus tôt.



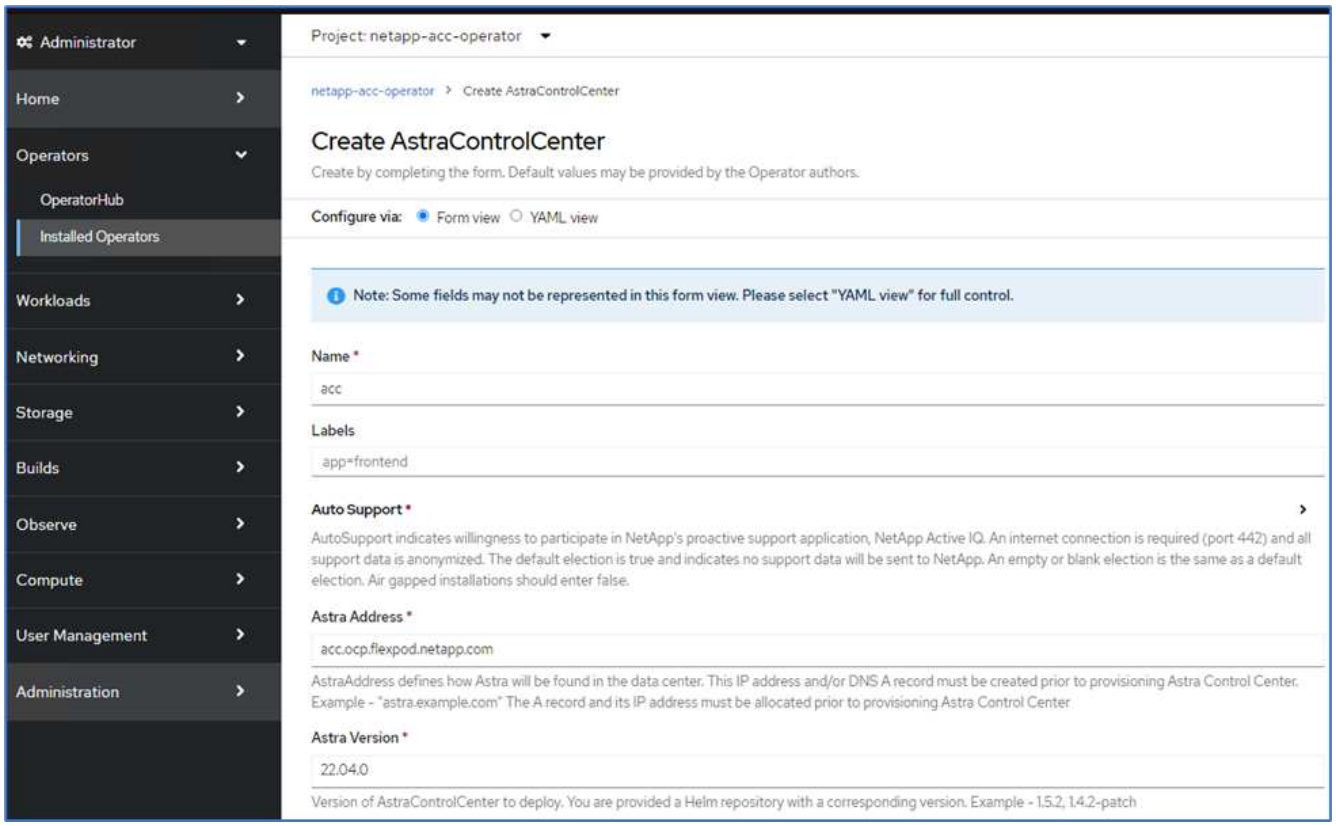
14. Pour extraire les images du centre de contrôle Astra de votre repo privé Docker, créez un secret dans le `netapp-acc-operator` espace de noms. Ce nom secret est fourni dans le manifeste YAML du Centre de contrôle Astra dans une étape ultérieure.



15. Dans le menu latéral, sélectionnez opérateurs > opérateurs installés et cliquez sur Créer une instance dans la section API fournie.



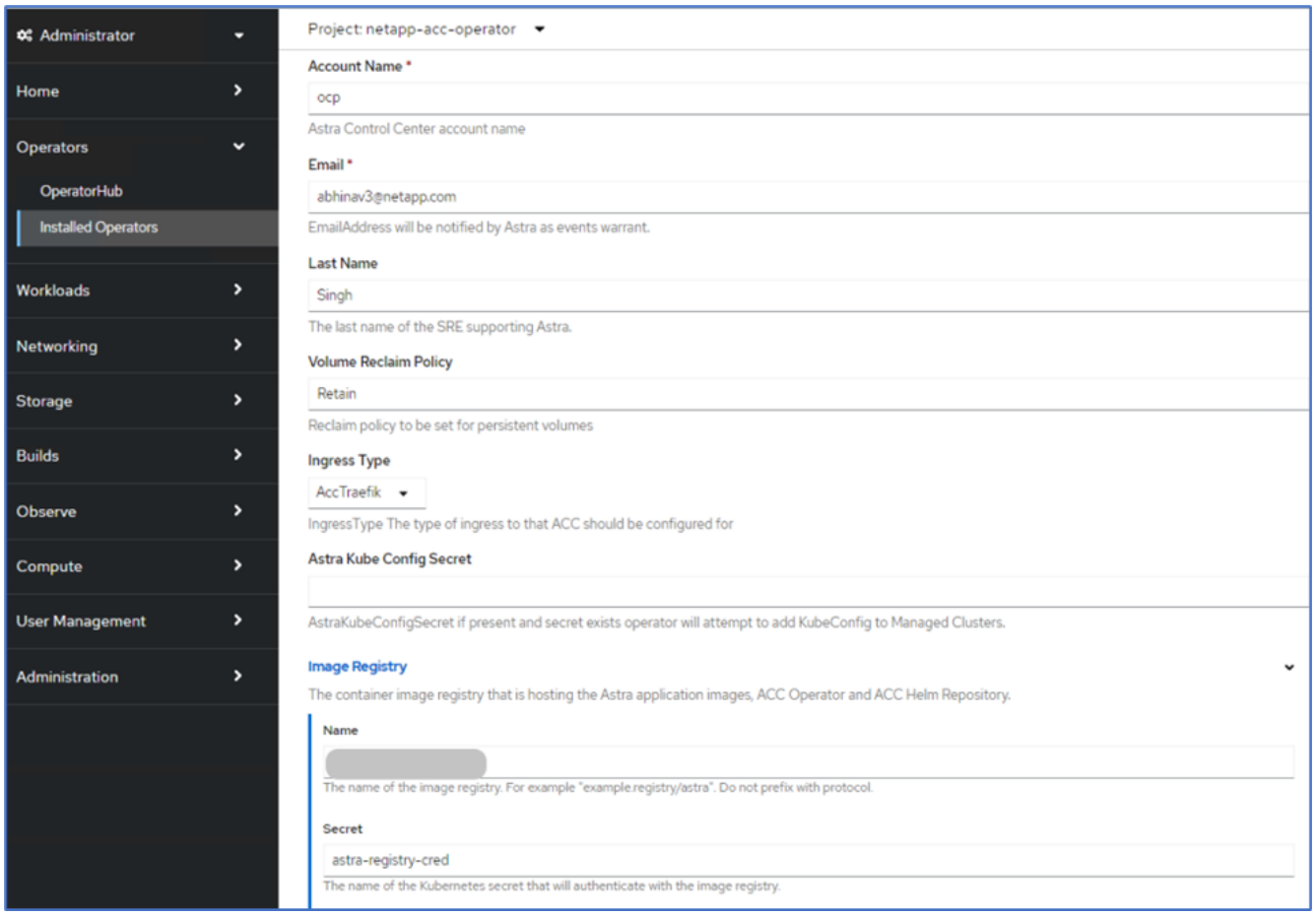
16. Remplissez le formulaire Create AstrakControlCenter. Indiquez le nom, l'adresse Astra et la version Astra.



Sous adresse Astra, indiquez l'adresse FQDN pour Astra Control Center. Cette adresse permet d'accéder à la console Web Astra Control Center. Le FQDN doit également se résoudre à un réseau IP accessible et doit être configuré dans le DNS.

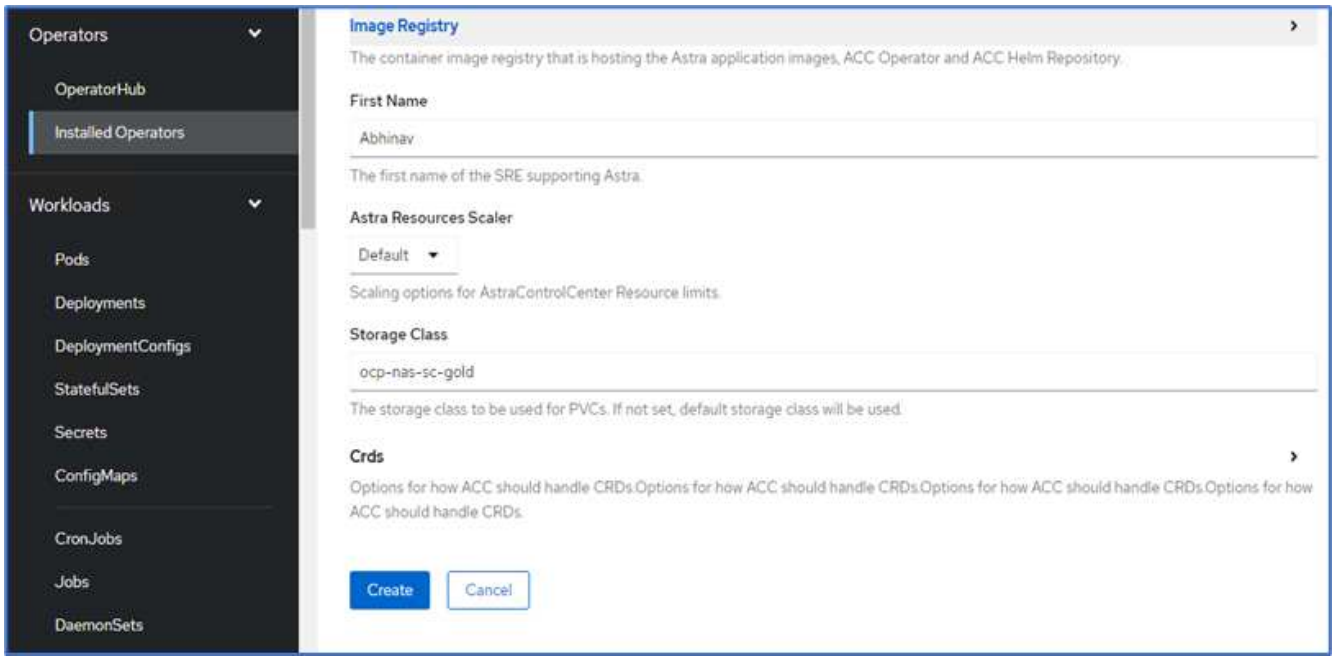
17. Entrez un nom de compte, une adresse e-mail, un nom d'administrateur et conservez la stratégie de récupération du volume par défaut. Si vous utilisez un équilibreur de charge, définissez le Type d'entrée

sur `AccTraefik`. Sinon, sélectionnez générique pour `Ingress.Controller`. Sous Registre d'images, entrez le chemin et le secret du registre d'images du conteneur.

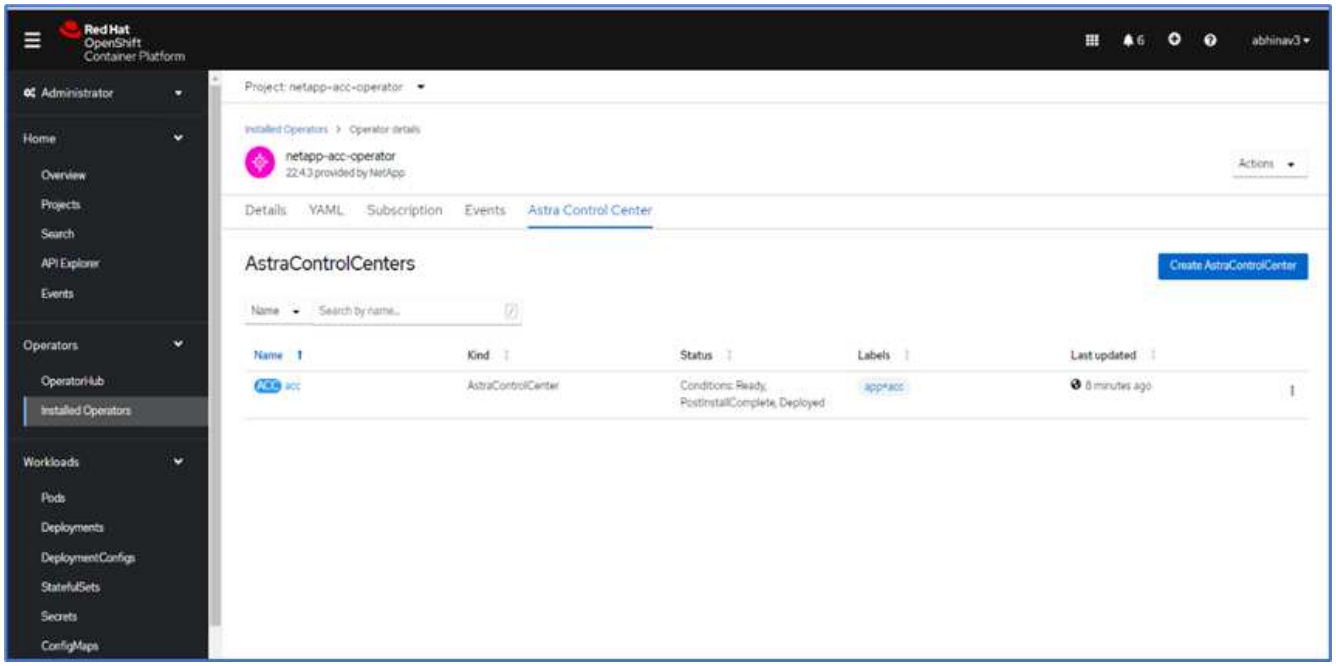


Dans cette solution, l'équilibreur de charge Metallb est utilisé. Par conséquent, le type d'entrée est AccTraefik. Cela expose la passerelle Ttrafik Astra Control Center en tant que service Kubernetes de type LoadBalancer.

18. Entrez le prénom de l'administrateur, configurez la mise à l'échelle des ressources et fournissez la classe de stockage. Cliquez sur Créer .



L'état de l'instance Astra Control Center doit passer de déploiement à prêt.



19. Vérifiez que tous les composants du système ont été correctement installés et que tous les modules fonctionnent.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

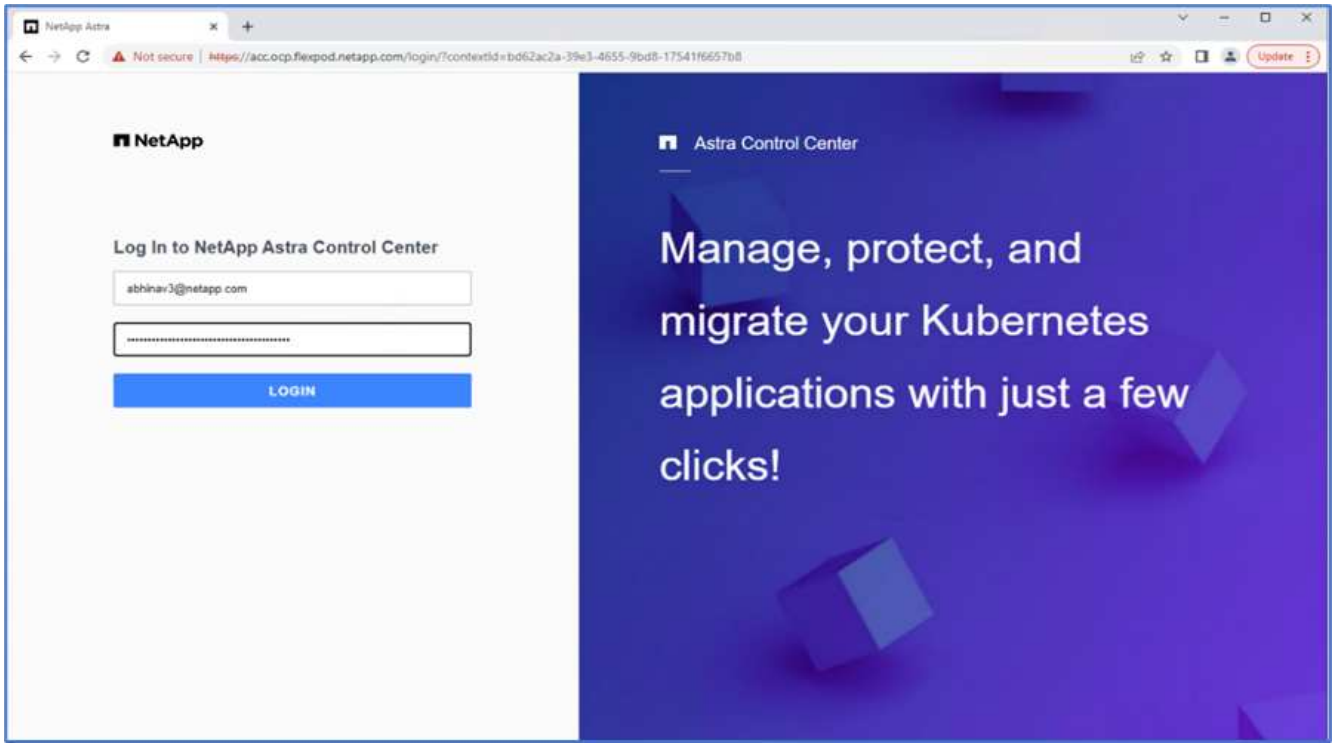
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

Chaque pod doit avoir l'état en cours d'exécution. Le déploiement des modules du système peut prendre plusieurs minutes.

20. Lorsque tous les pods s'exécutent, exécutez la commande suivante pour récupérer le mot de passe à une seule fois. Dans la version YAML de la sortie, vérifiez le `status.deploymentState` pour la valeur déployée, puis copiez le `status.uuid` valeur. Le mot de passe est `ACC-` Suivi de la valeur UUID. (ACC-[UUID]).

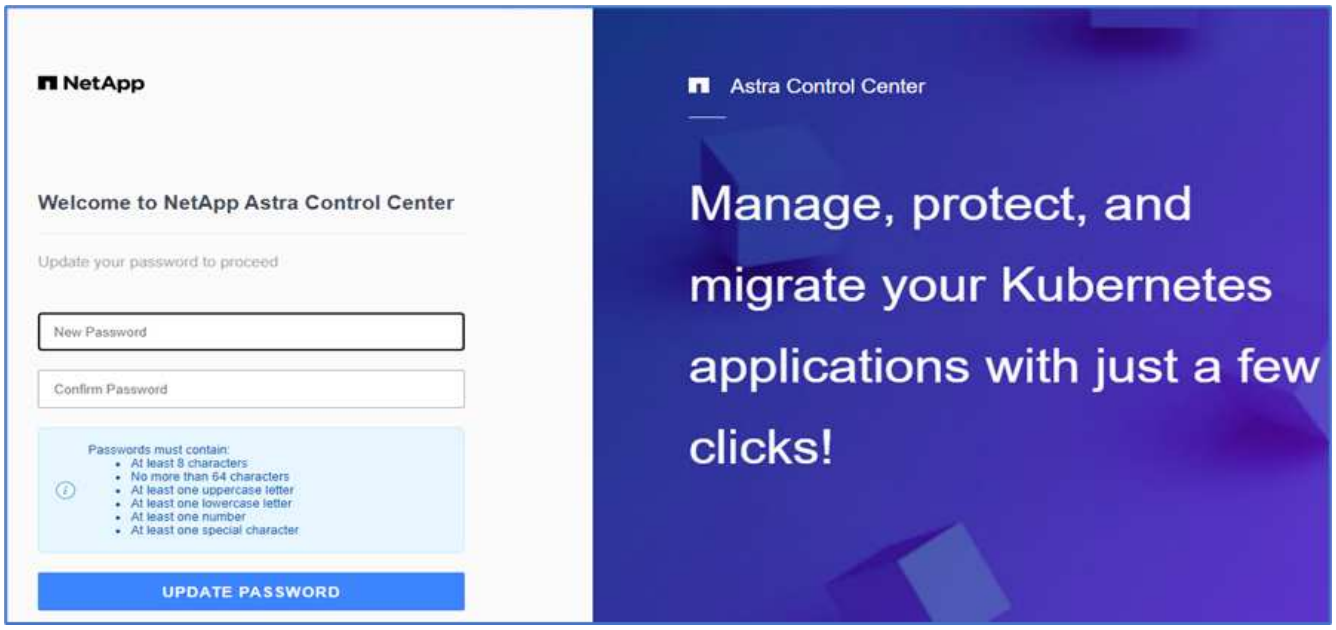
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. Dans un navigateur, accédez à l'URL en utilisant le FQDN que vous avez fourni.
22. Connectez-vous à l'aide du nom d'utilisateur par défaut, à savoir l'adresse électronique fournie lors de l'installation et le mot de passe à usage unique ACC-[UUID].



Si vous saisissez trois fois un mot de passe incorrect, le compte administrateur est verrouillé pendant 15 minutes.

23. Modifiez le mot de passe et continuez.

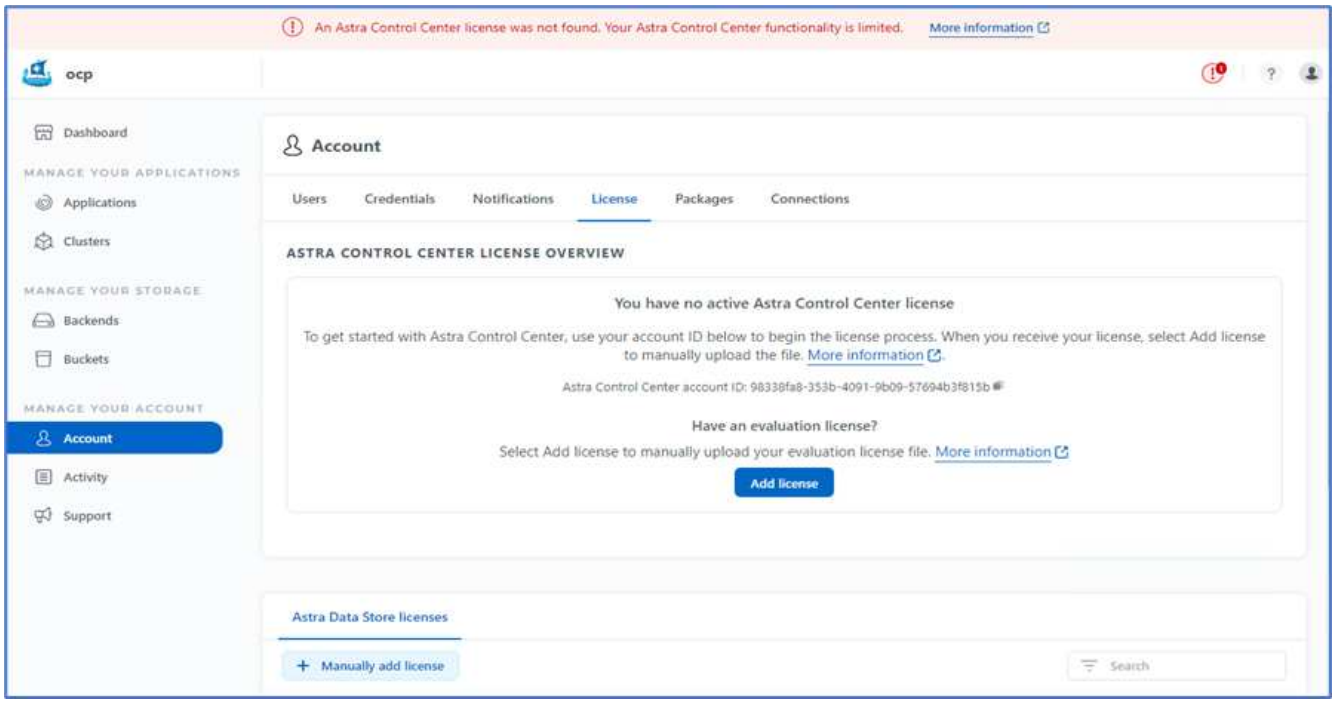


Pour en savoir plus sur l'installation du centre de contrôle Astra, consultez le "Présentation de l'installation du centre de contrôle Astra" page.

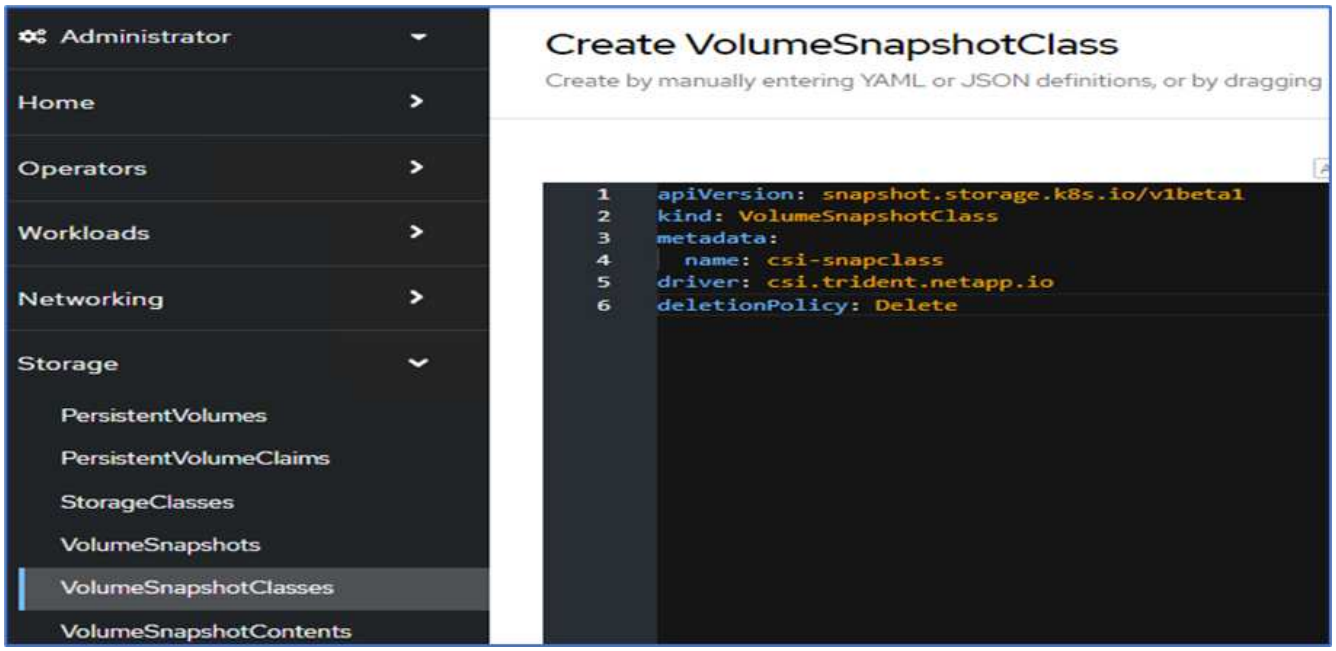
Configurer le centre de contrôle Astra

Une fois Astra Control Center installé, connectez-vous à l'interface utilisateur, téléchargez la licence, ajoutez des clusters, gérez le stockage et ajoutez des compartiments.

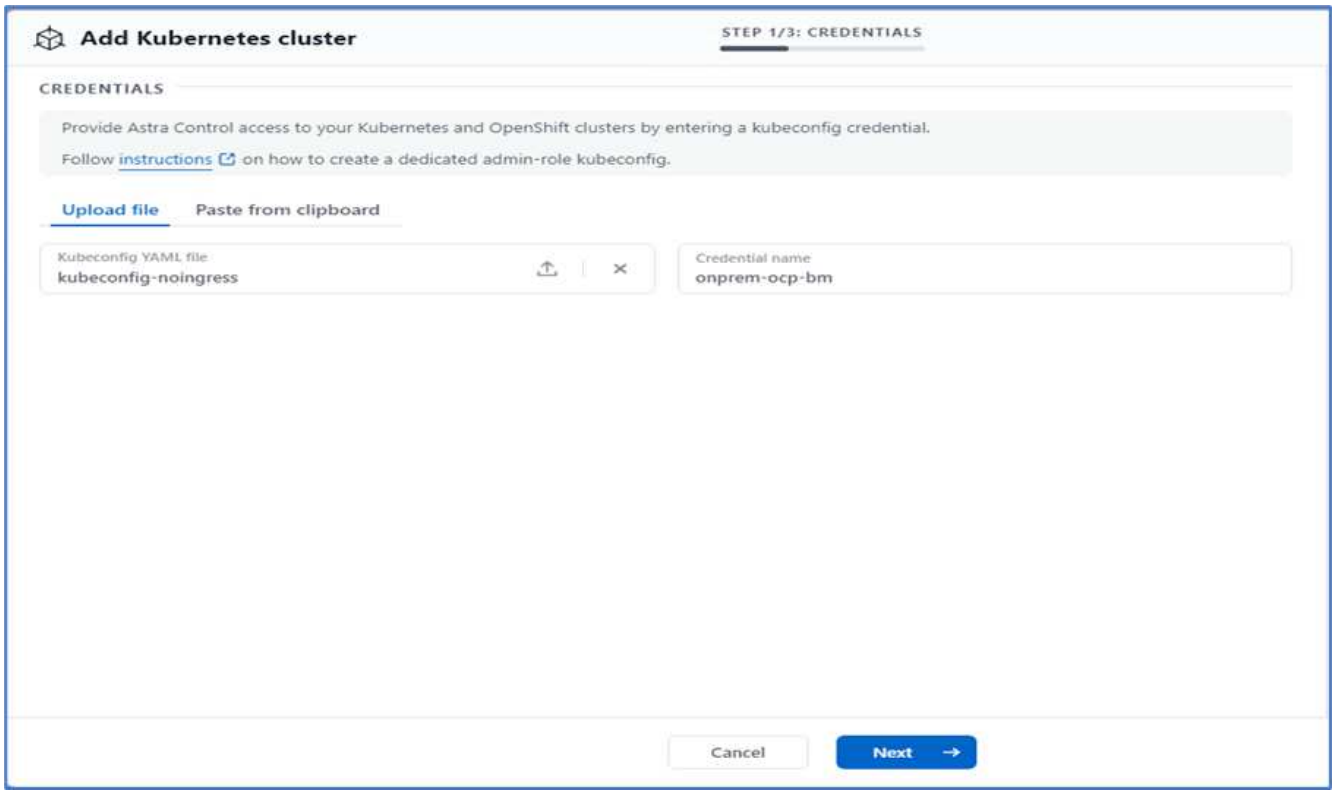
1. Sur la page d'accueil sous compte, accédez à l'onglet Licence et sélectionnez Ajouter une licence pour télécharger la licence Astra.



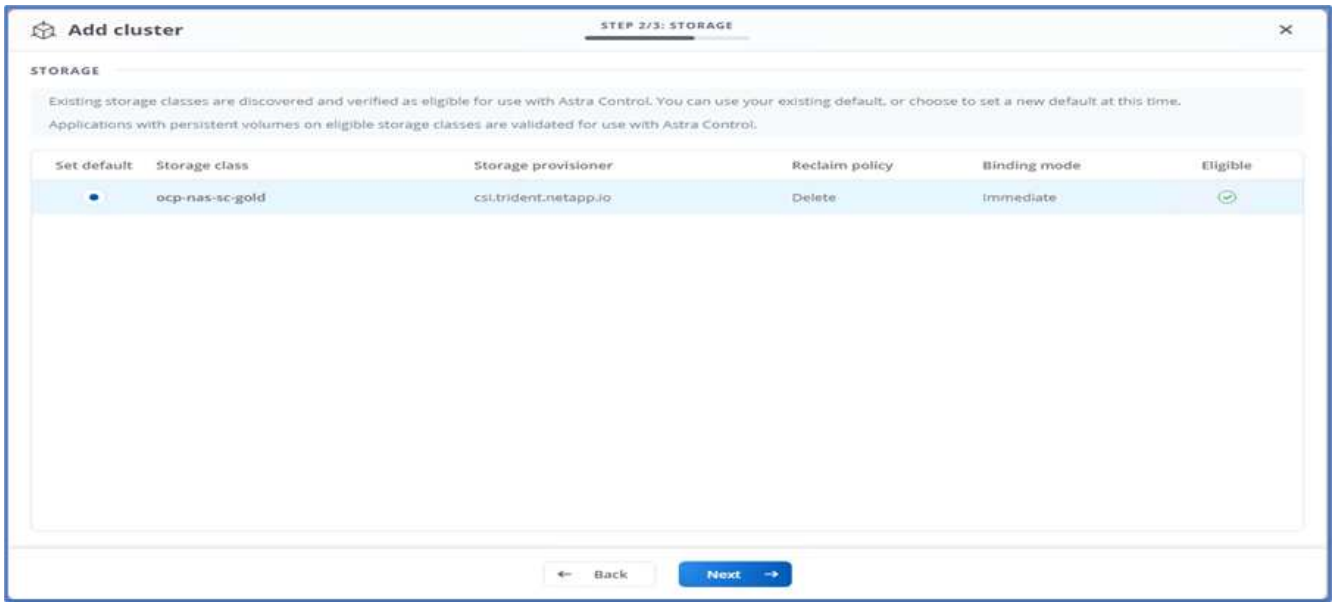
2. Avant d'ajouter le cluster OpenShift, créez une classe de snapshot de volume Astra Trident à partir de la console web OpenShift. La classe de snapshot de volume est configurée avec le `csi.trident.netapp.io` conducteur.



3. Pour ajouter le cluster Kubernetes, accédez à clusters sur la page d'accueil et cliquez sur Ajouter un cluster Kubernetes. Téléchargez ensuite le `kubeconfig` fichier du cluster et indiquez un nom d'identifiant. Cliquez sur Suivant.



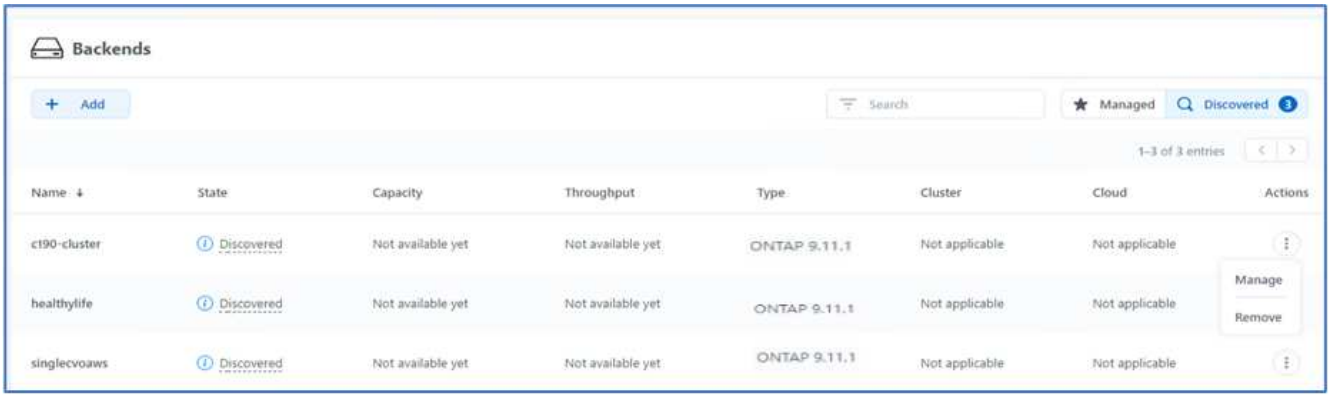
4. Les classes de stockage existantes sont automatiquement découvertes. Sélectionnez la classe de stockage par défaut, cliquez sur Suivant, puis sur Ajouter un cluster.



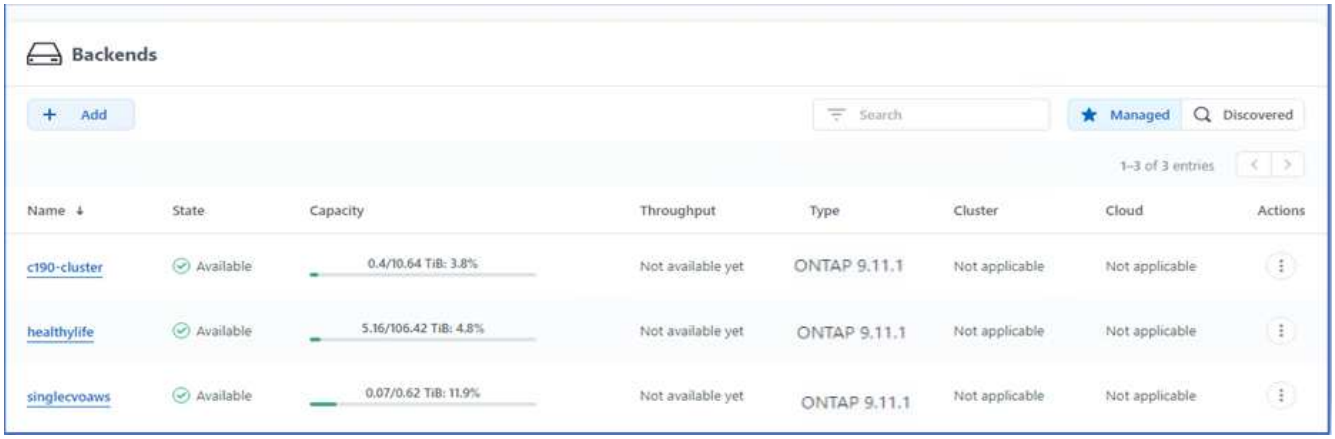
5. Le cluster est ajouté en quelques minutes. Pour ajouter d'autres clusters OpenShift Container Platform, répétez les étapes 1 à 4.

> Pour ajouter un environnement opérationnel OpenShift supplémentaire en tant que ressource de calcul gérée, assurez-vous qu'Astra Trident "Objets VolumeSnapshotClass" sont définis.

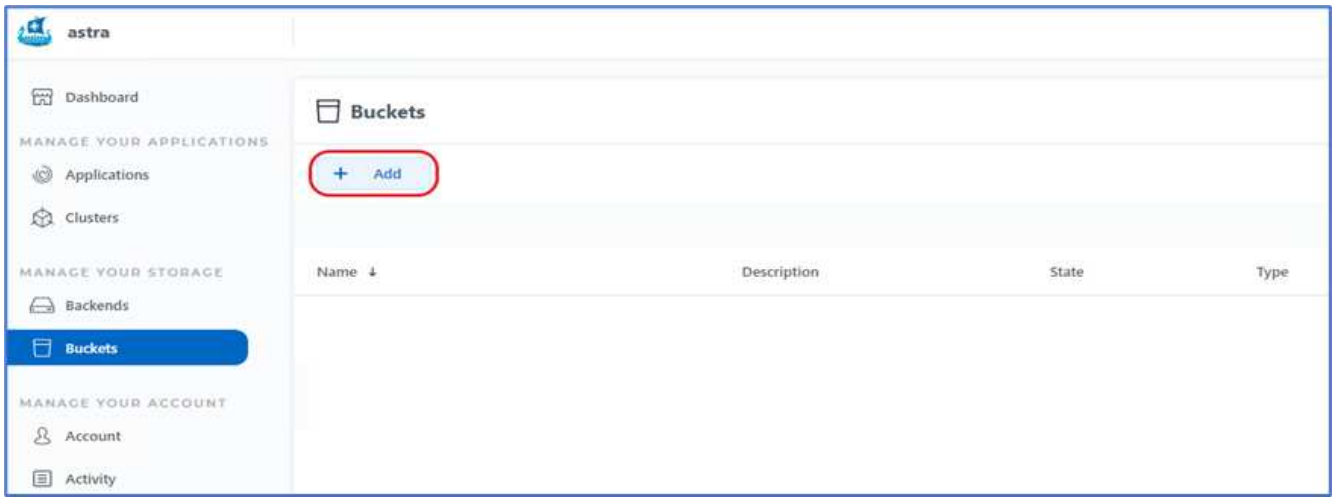
6. Pour gérer le stockage, accédez à Backends, cliquez sur les trois points sous actions par rapport au back-end que vous souhaitez gérer. Cliquez sur gérer.



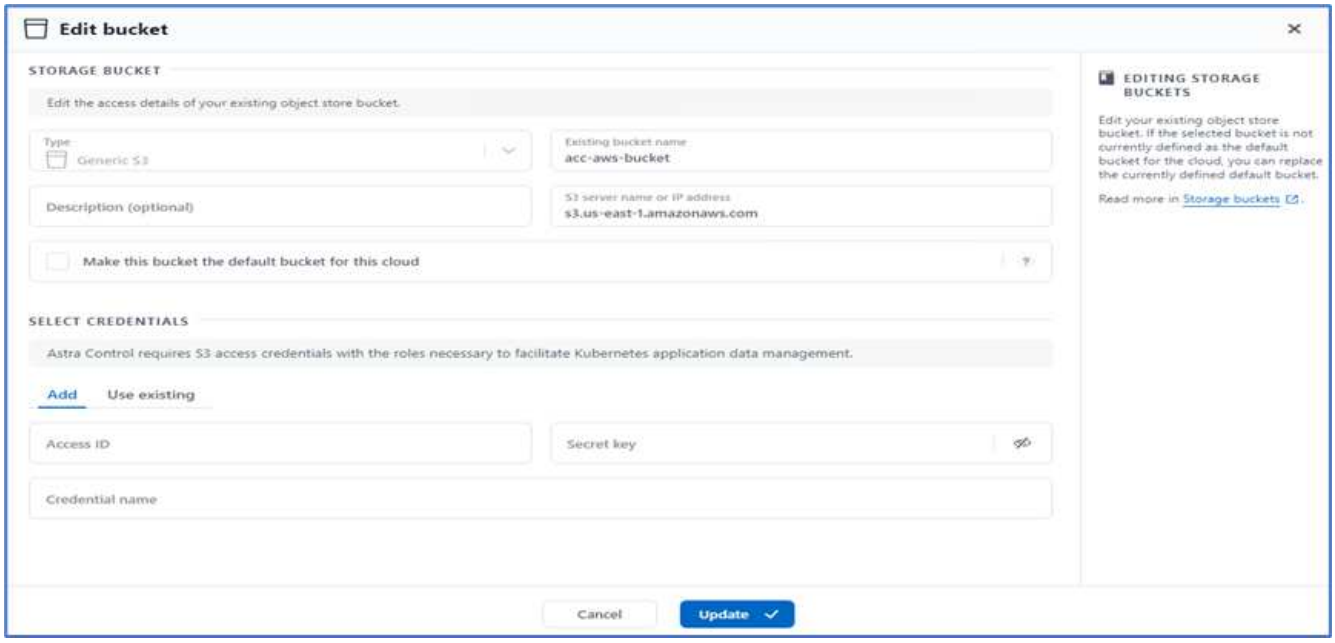
7. Indiquez les identifiants ONTAP et cliquez sur Next (Suivant). Vérifiez les informations et cliquez sur géré. Le système back-end doit être semblable à l'exemple suivant.



8. Pour ajouter un godet à la commande Astra, sélectionnez godets et cliquez sur Ajouter.

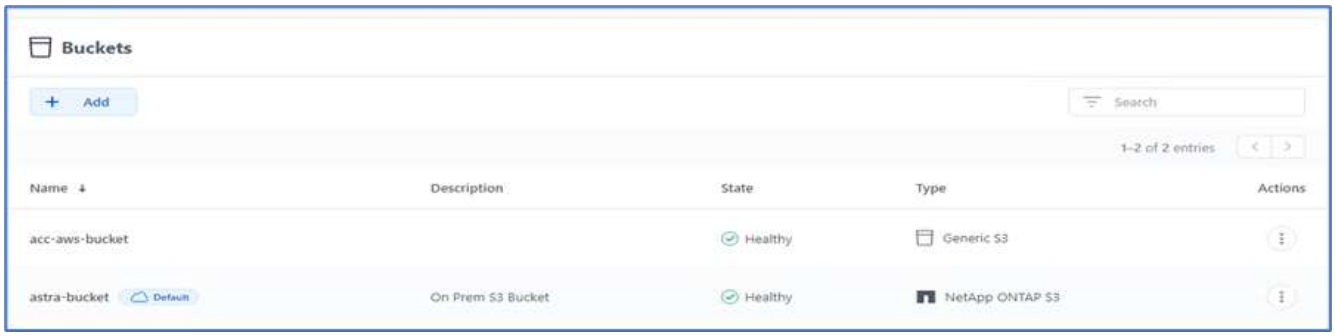


9. Sélectionnez le type de compartiment et indiquez le nom du compartiment, le nom du serveur S3 ou l'adresse IP et les identifiants S3. Cliquez sur mettre à jour.



Dans cette solution, des compartiments AWS S3 et ONTAP S3 sont tous deux utilisés. Vous pouvez également utiliser StorageGRID.

L'état du godet doit être sain.



Dans le cadre de l'enregistrement de clusters Kubernetes avec Astra Control Center pour la gestion des données intégrant la cohérence applicative, Astra Control crée automatiquement des liaisons de rôles et un espace de noms de contrôle NetApp qui contrôle la collecte de metrics et de journaux à partir des pods d'applications et des nœuds workers. Définir l'une des classes de stockage ONTAP par défaut prises en charge.

Après vous "Ajoutez un cluster à la gestion Astra Control", Vous pouvez installer des applications sur le cluster (en dehors d'Astra Control), puis aller à la page applications d'Astra Control pour gérer les applications et leurs ressources. Pour en savoir plus sur la gestion des applications avec Astra, consultez le "Besoins en termes de gestion des applications".

"Ensuite : présentation de la validation de la solution."

Validation des solutions

Présentation

"Précédent : installation d'Astra Control Center sur OpenShift Container Platform."

Dans cette section, nous revisiterons la solution en incluant quelques cas d'utilisation :

- Restauration d'une application avec état d'une sauvegarde à distance vers un autre cluster OpenShift exécuté dans le cloud.
- Restauration d'une application avec état dans le même espace de noms du cluster OpenShift
- Mobilité des applications par clonage d'un système FlexPod (OpenShift Container Platform bare Metal) vers un autre système FlexPod (OpenShift Container Platform sur VMware).

En particulier, seules quelques utilisations ont été validées dans cette solution. Cette validation ne correspond en aucune façon à l'ensemble des fonctionnalités d'Astra Control Center.

"Ensuite : restauration des applications avec sauvegardes distantes."

Restauration d'applications avec sauvegardes distantes

"Précédent : présentation de la validation de la solution."

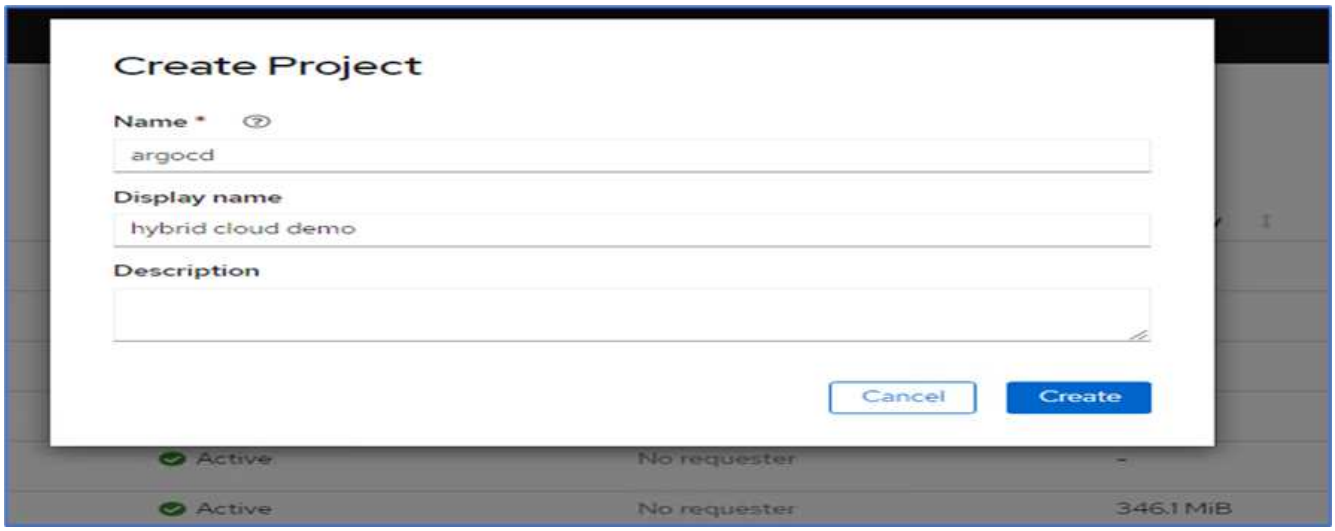
Avec Astra, vous pouvez effectuer une sauvegarde complète et cohérente avec les

applications qui permet de restaurer les données de votre application vers un autre cluster Kubernetes qui s'exécute dans un data Center sur site ou dans un cloud public.

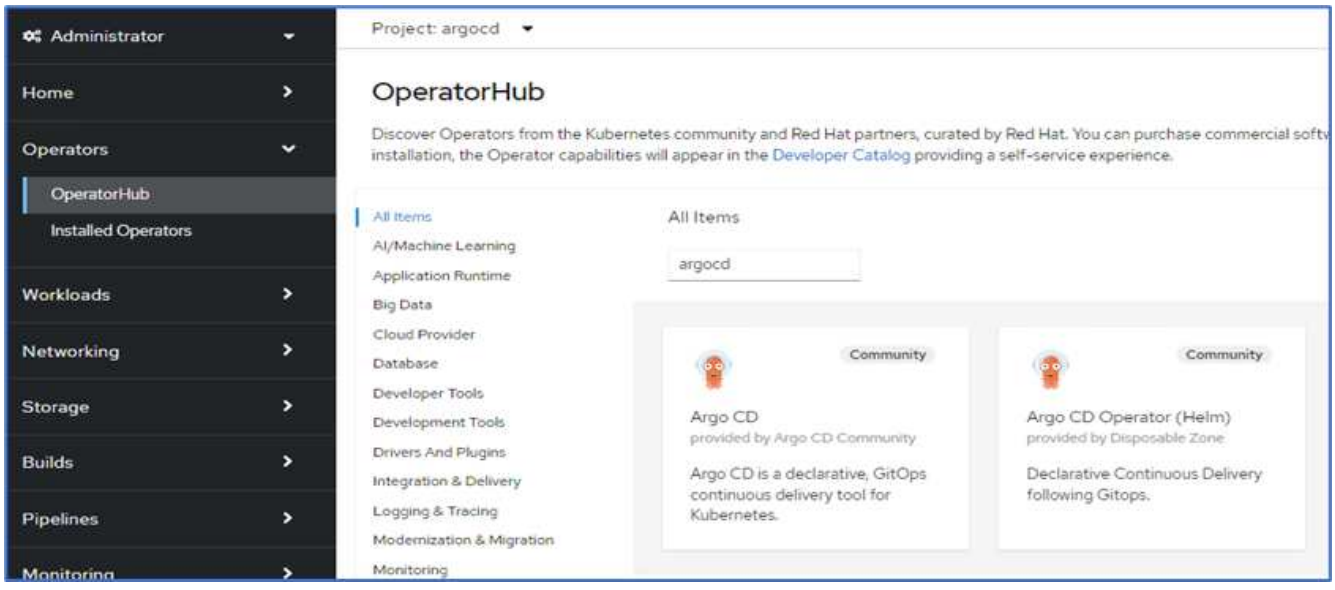
Pour valider la restauration d'application, simulez une défaillance sur site d'une application exécutée sur le système FlexPod et restaurez l'application sur un cluster K8s dans le cloud à l'aide d'une sauvegarde à distance.

L'exemple d'application est une application de liste de prix qui utilise MySQL pour la base de données. Pour automatiser le déploiement, nous avons utilisé le "CD Argo" outil. Argo CD est un outil de livraison continue déclaratif, GitOps.

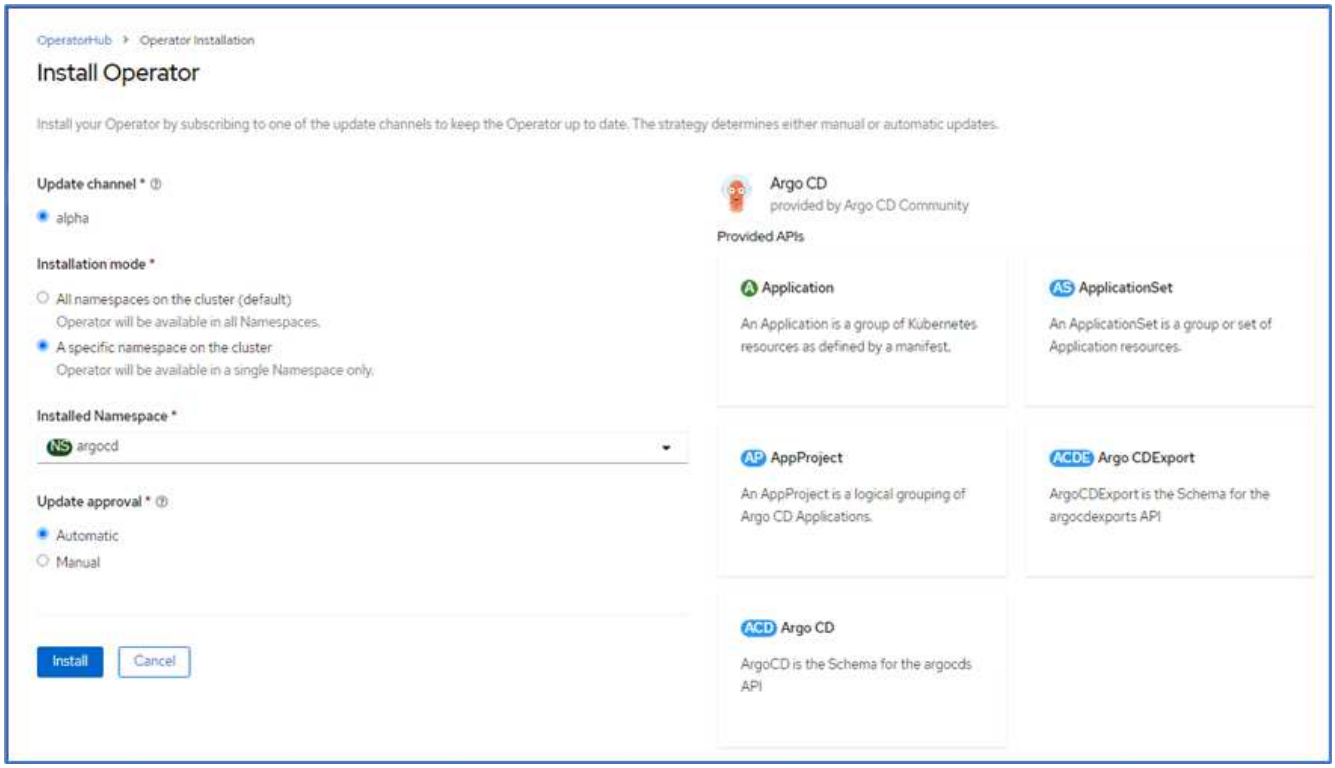
1. Connectez-vous au cluster OpenShift sur site et créez un nouveau projet sous son nom `argocd`.



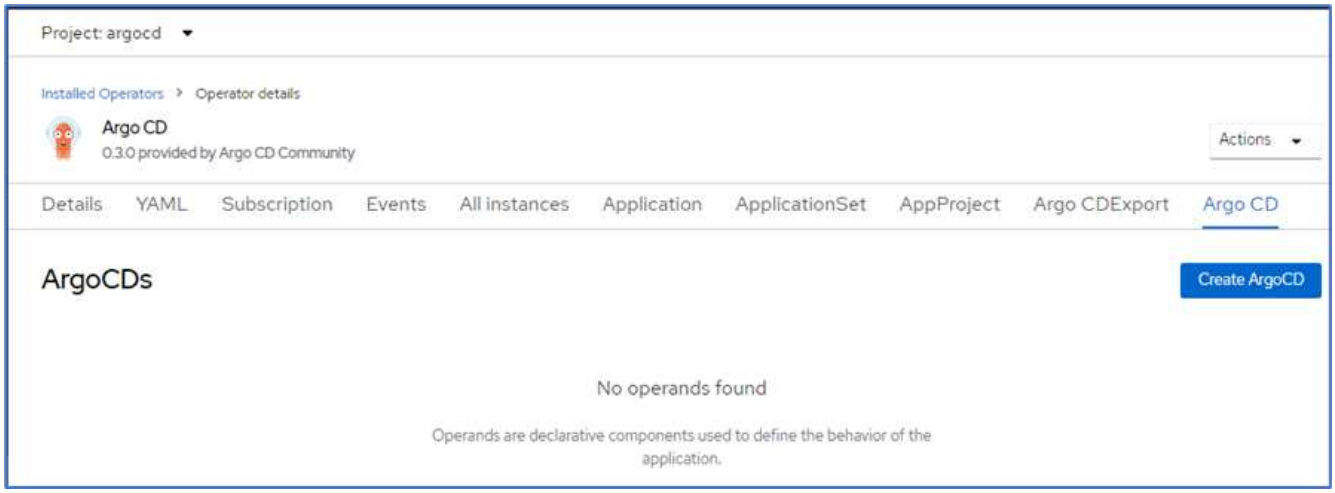
2. Dans OperatorHub, recherchez `argocd` Et sélectionnez opérateur du CD Argo.



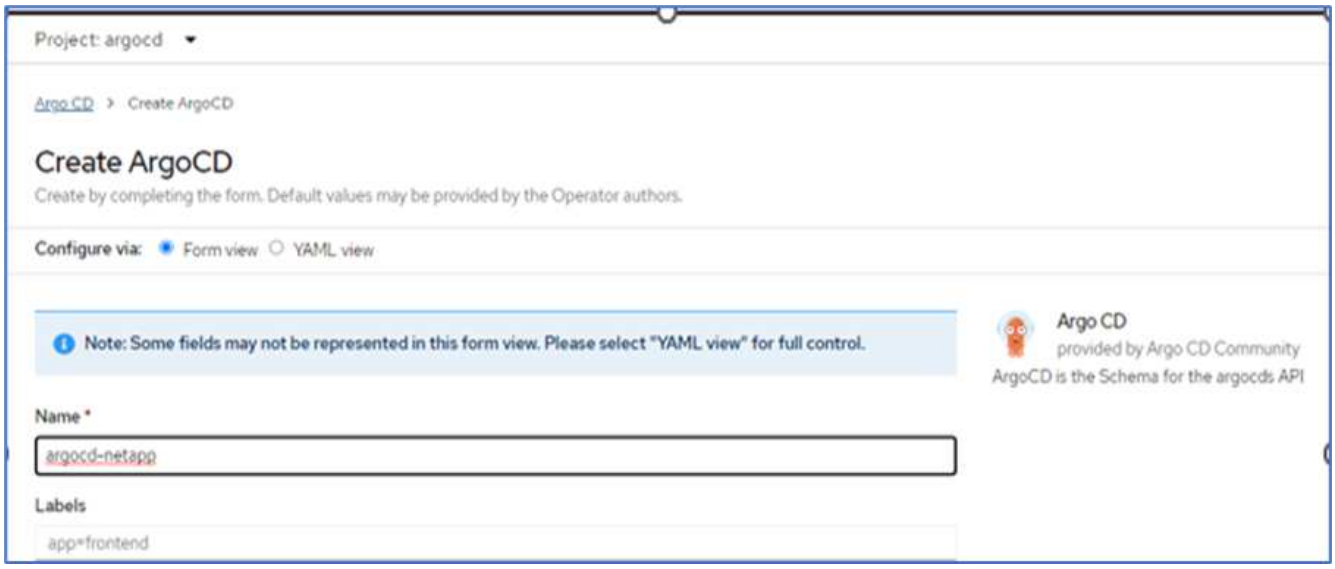
3. Installer l'opérateur dans le `argocd` espace de noms.



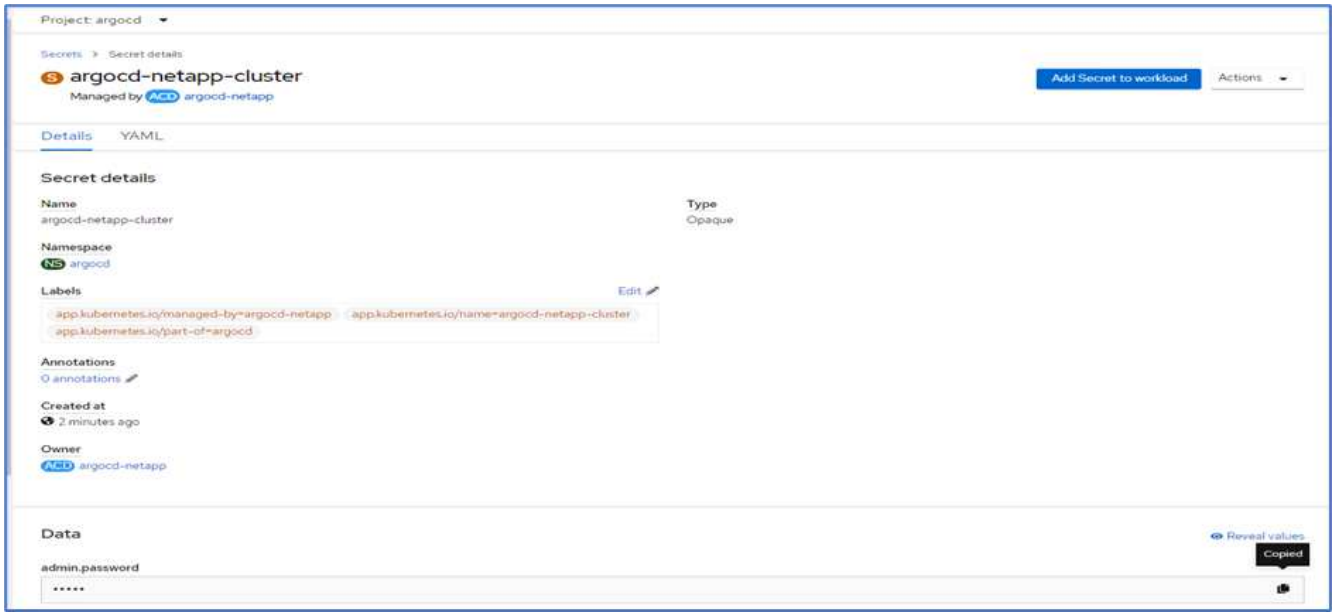
4. Accédez à l'opérateur et cliquez sur Créer un ArgoCD.



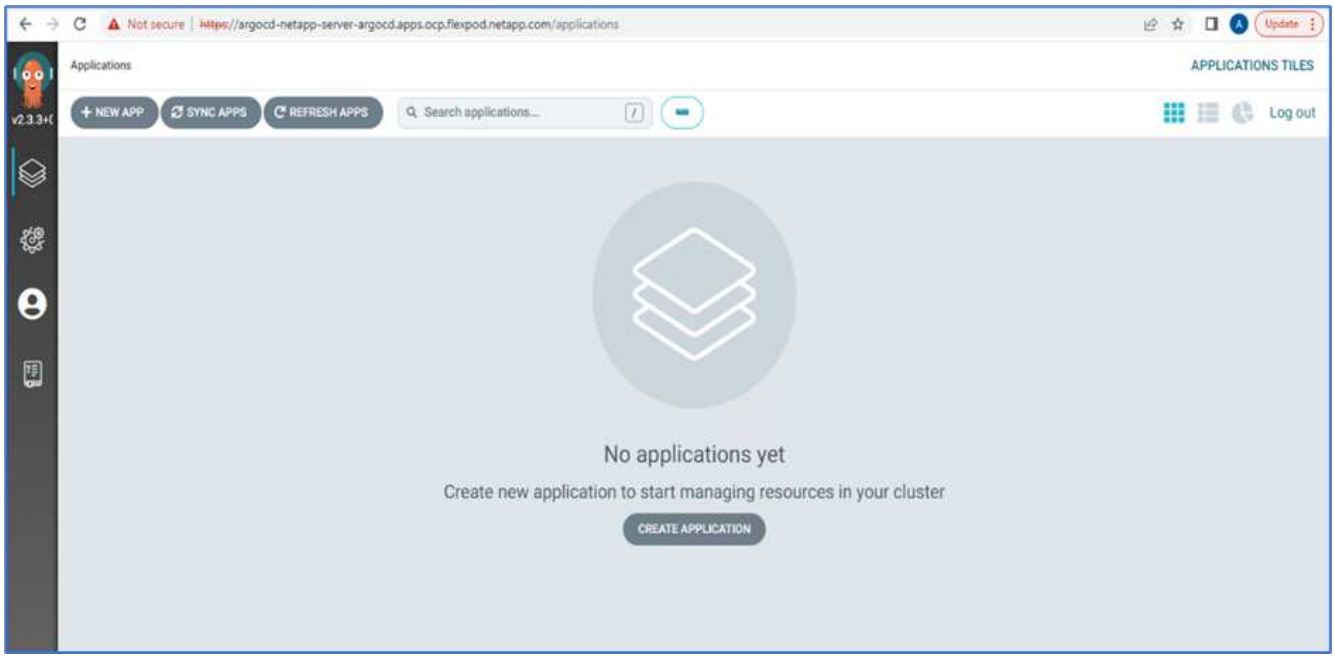
5. Pour déployer l'instance de CD Argo dans le `argocd` Donnez un nom au projet, puis cliquez sur Créer.



6. Pour vous connecter au CD Argo, l'utilisateur par défaut est admin et le mot de passe se trouve dans un fichier secret portant le nom `argocd-netapp-cluster`.



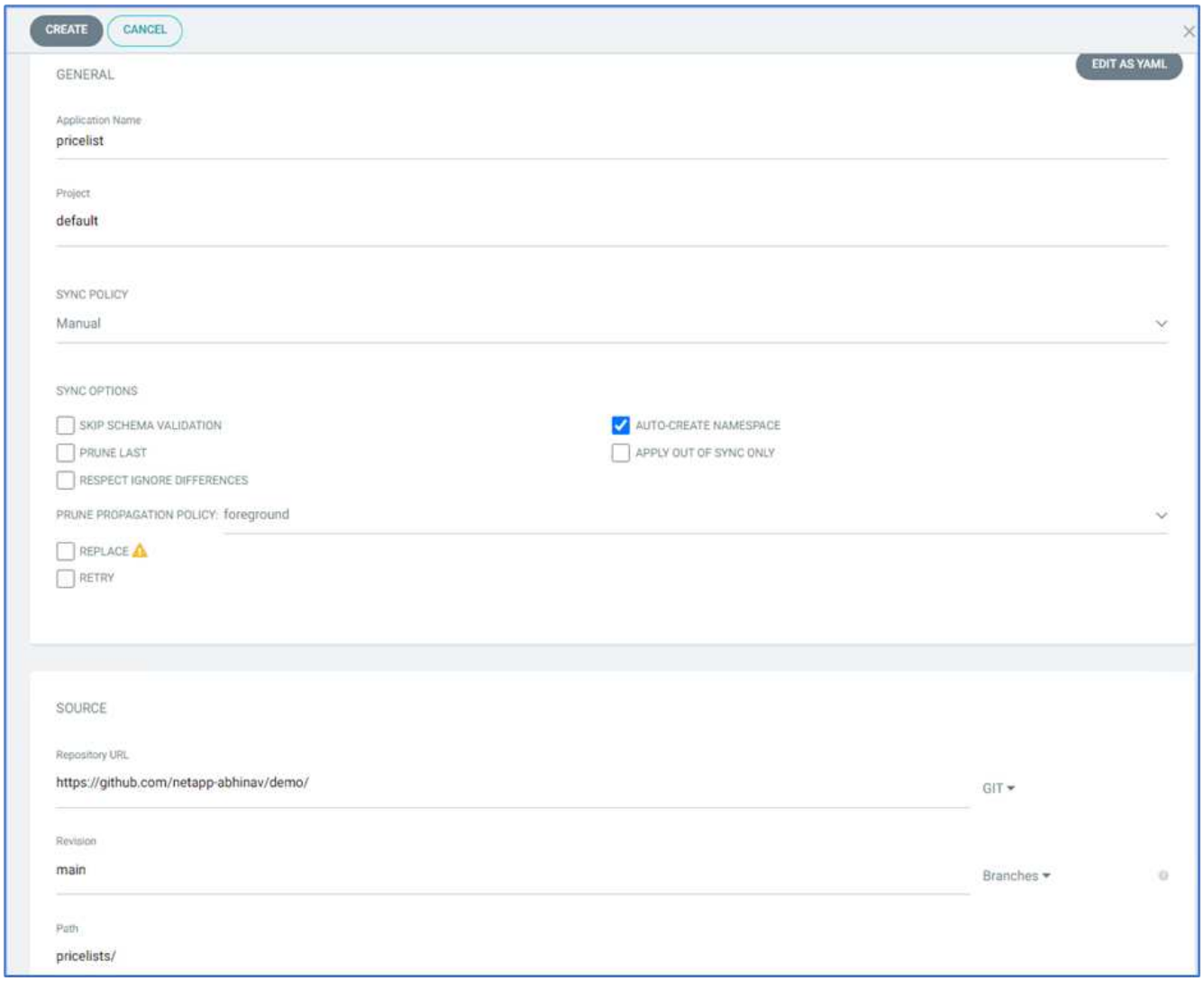
7. Dans le menu latéral, sélectionnez routes > emplacement et cliquez sur l'URL de l' `argocd` itinéraires. Entrez le nom d'utilisateur et le mot de passe.



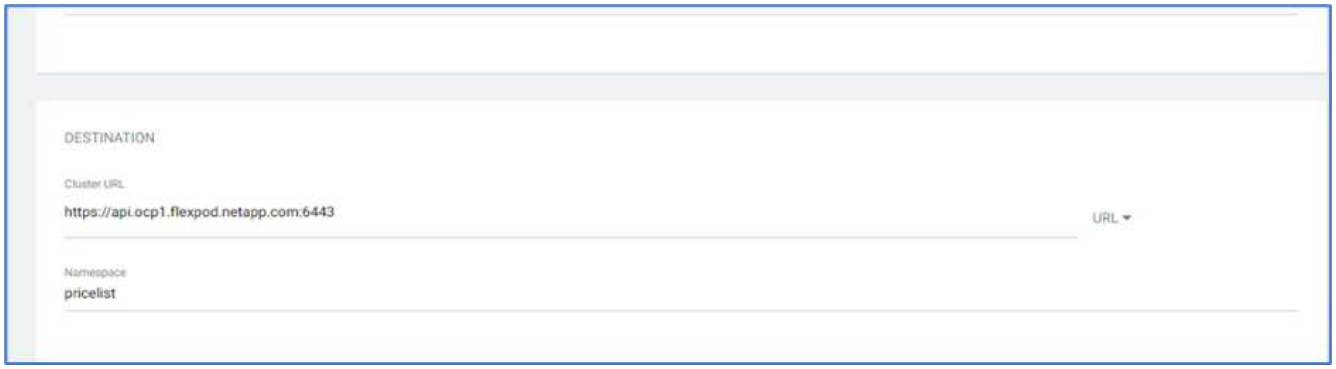
8. Ajoutez le cluster OpenShift sur site au CD Argo via l'interface de ligne de commande.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

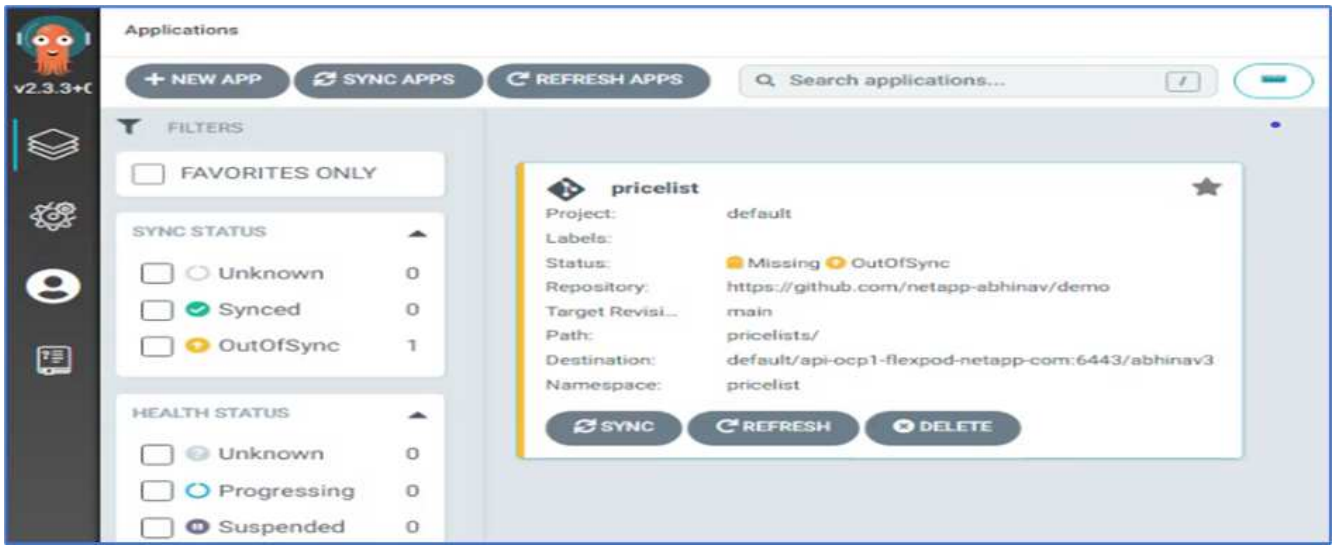
9. Dans l’interface utilisateur ArgoCD, cliquez sur NOUVELLE APPLICATION et entrez les détails du nom de l’application et du référentiel de code.



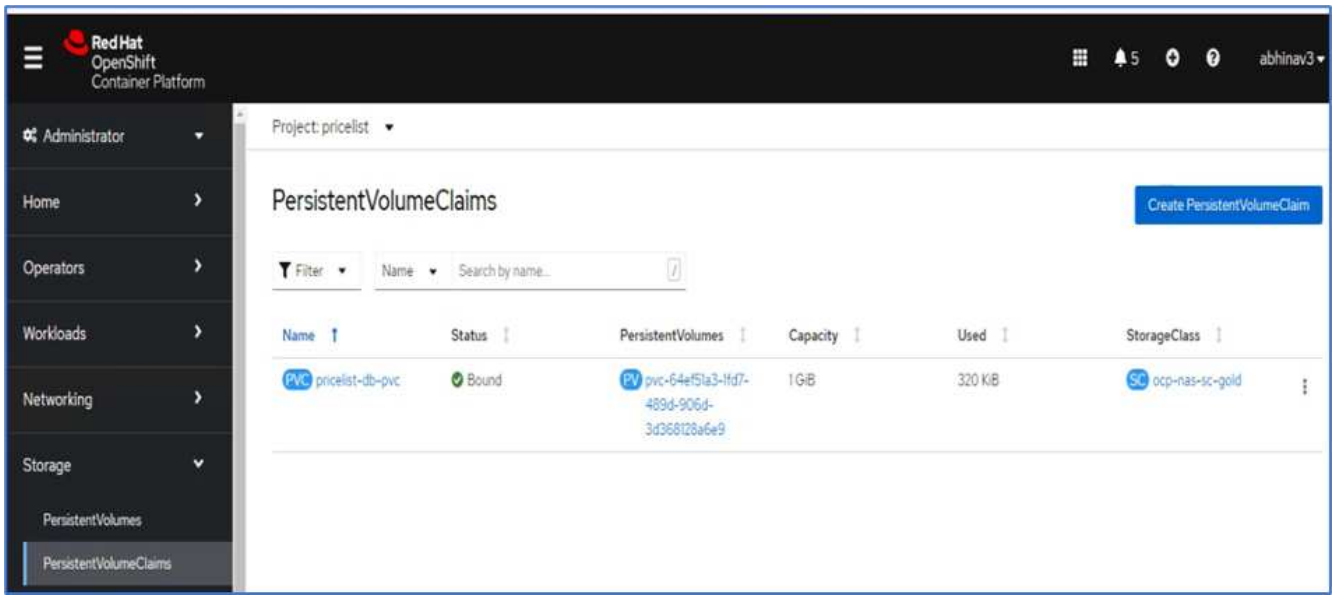
10. Entrez le cluster OpenShift où l'application sera déployée avec le namespace.



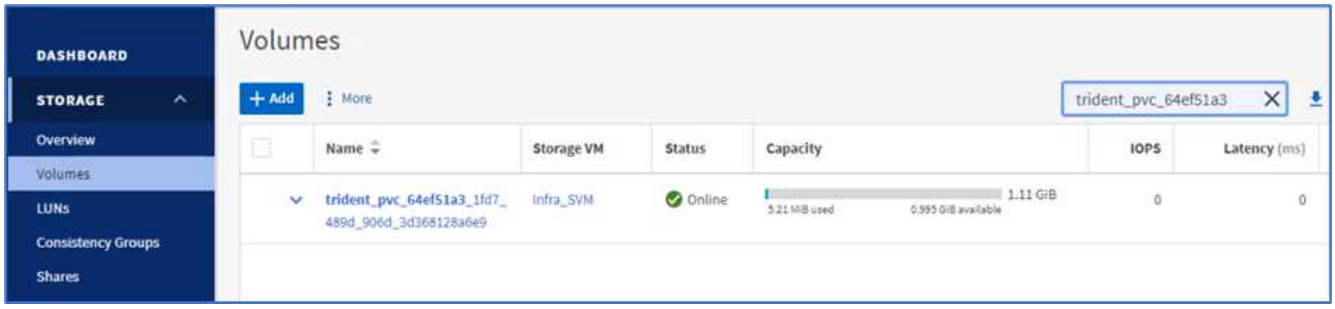
11. Pour déployer l'application sur le cluster OpenShift sur site, cliquez sur SYNC.



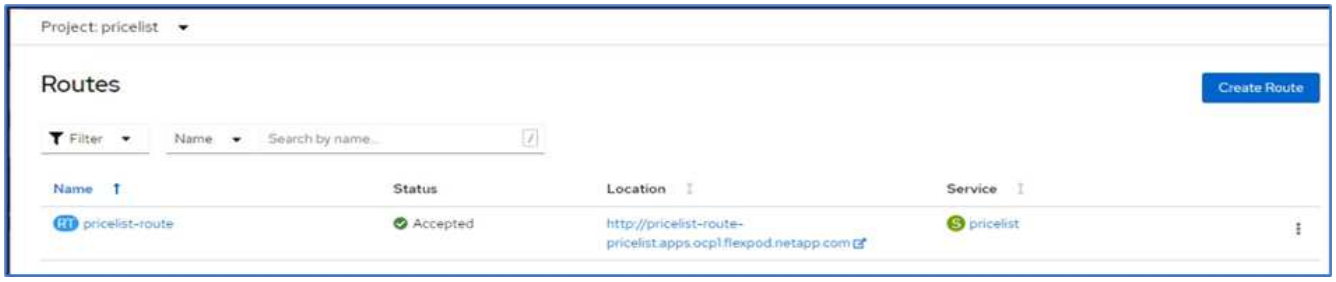
12. Dans la console OpenShift Container Platform, accédez à la liste des tarifs du projet et, sous Storage, vérifiez le nom et la taille de la demande de volume persistant.



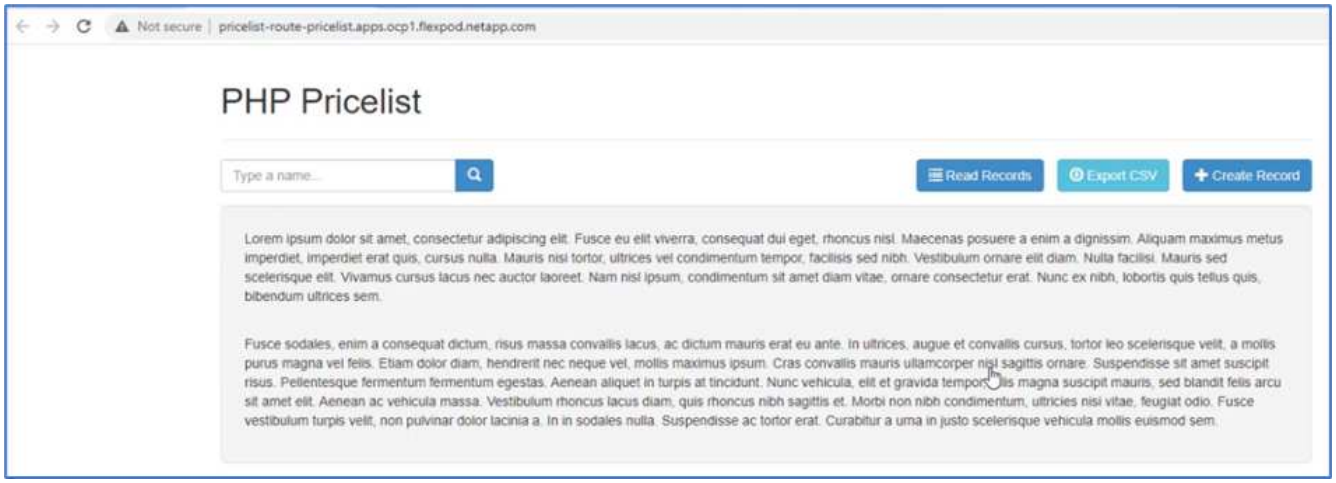
13. Connectez-vous à System Manager et vérifiez le volume persistant.



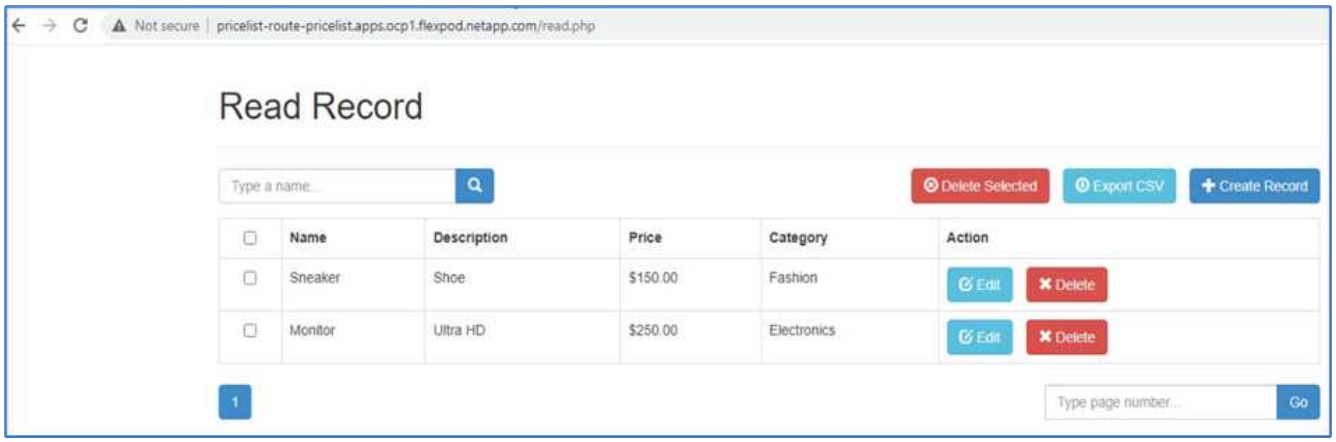
14. Une fois les pods en cours d'exécution, sélectionnez réseau > routes dans le menu latéral, puis cliquez sur l'URL sous emplacement.



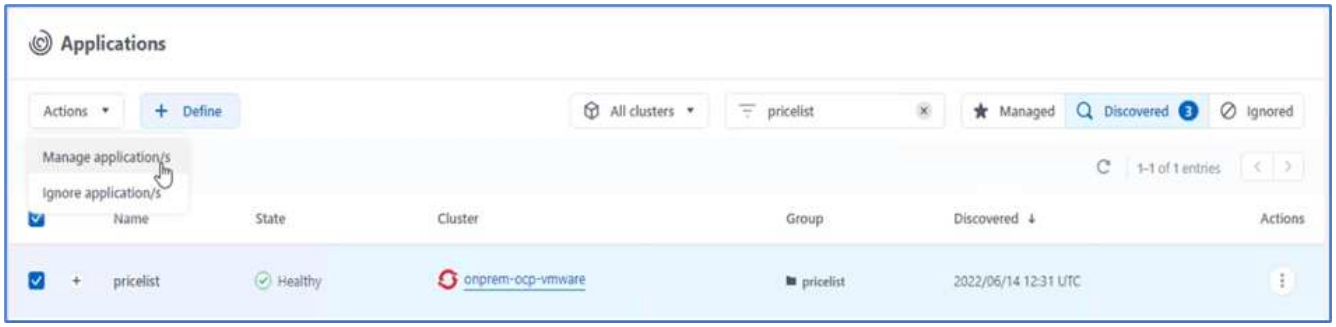
15. La page d'accueil de l'application Tarifs s'affiche.



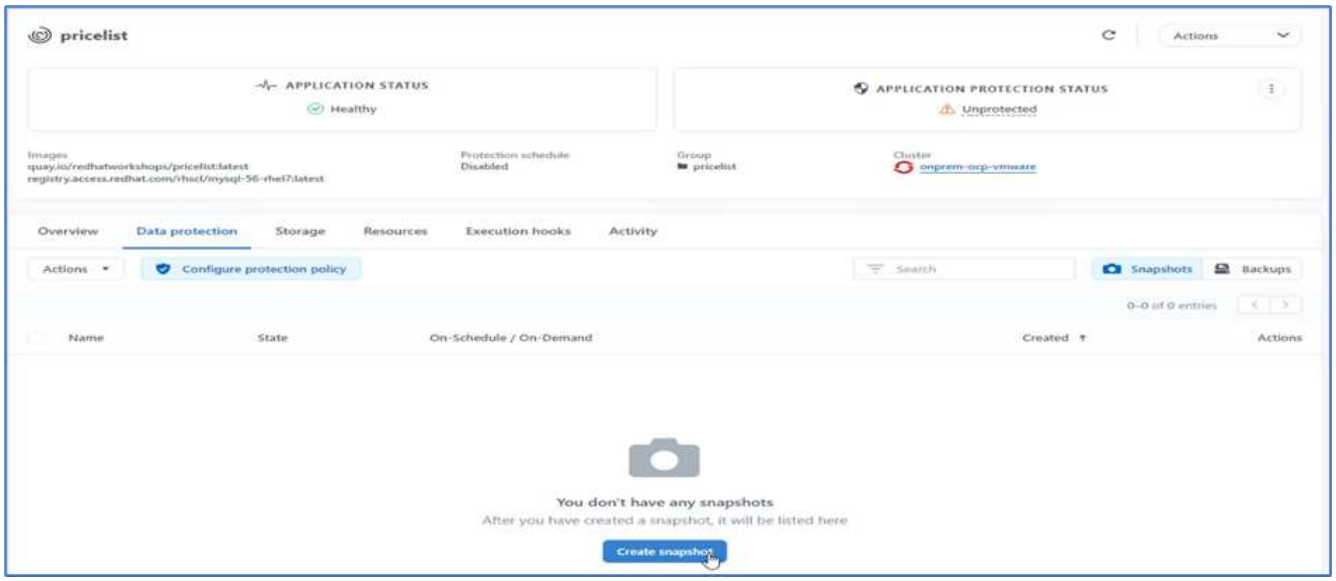
16. Créez quelques enregistrements sur la page Web.



17. L'application est découverte dans Astra Control Center. Pour gérer l'application, accédez à applications > découverte, sélectionnez l'application Barème des prix, puis cliquez sur gérer les applications sous actions.

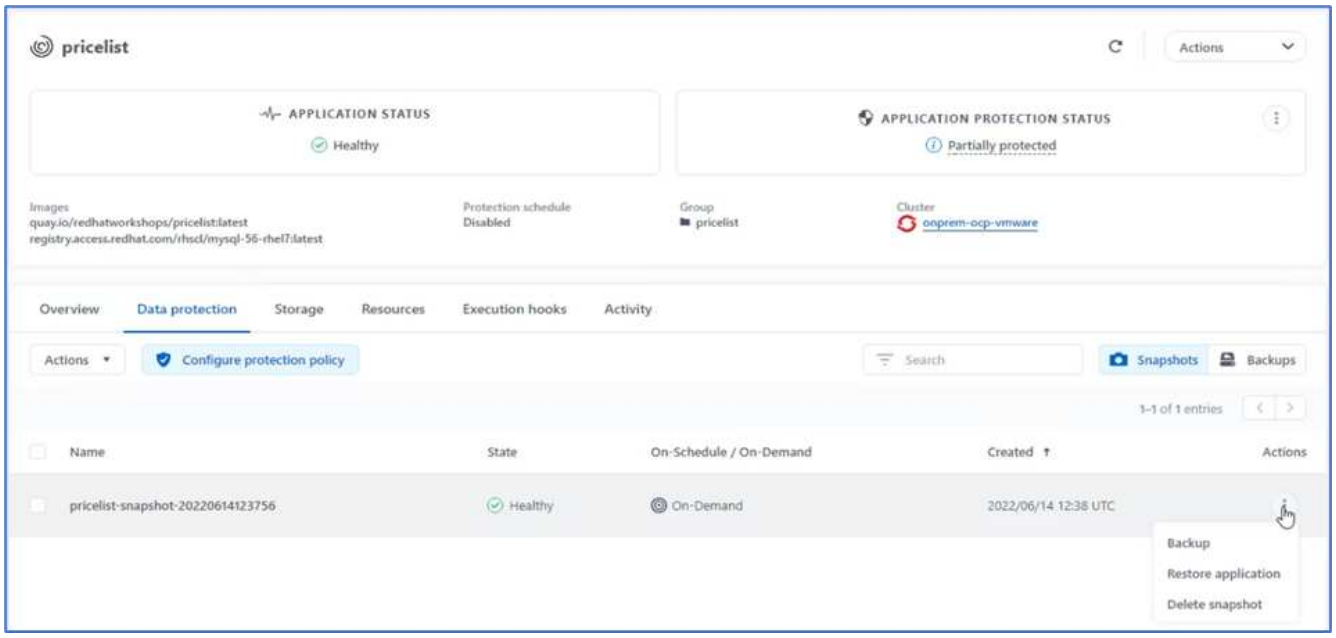


18. Cliquez sur l'application Barème des prix et sélectionnez protection des données. À ce stade, il ne doit y avoir aucun Snapshot ni aucune sauvegarde. Cliquez sur Créer un snapshot pour créer un snapshot à la demande.

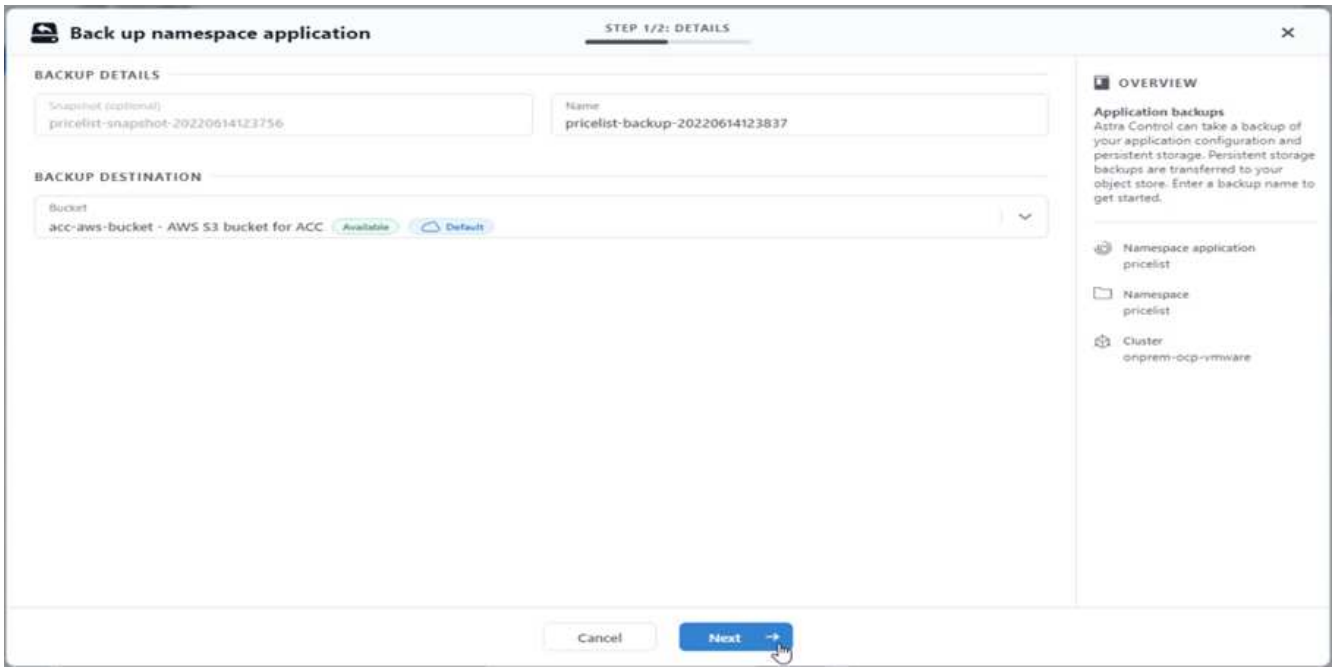


Le NetApp Astra Control Center prend en charge à la demande et les sauvegardes Snapshot et planifiées.

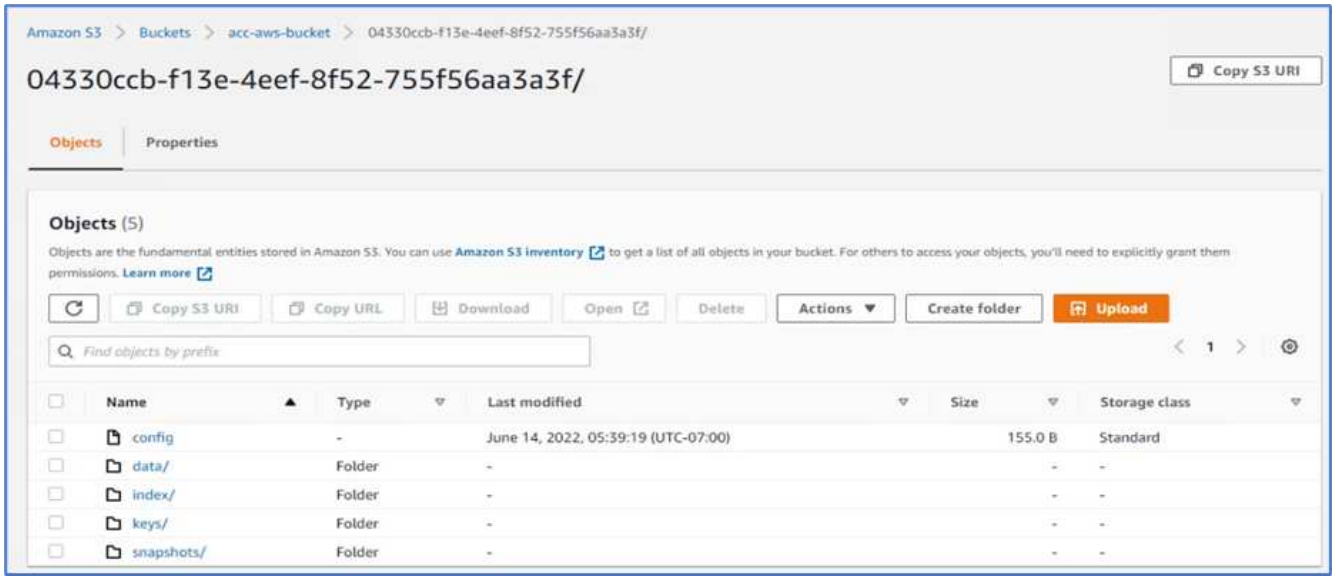
19. Une fois le snapshot créé et l'état fonctionnel, créez une sauvegarde à distance à l'aide de ce snapshot. Cette sauvegarde est stockée dans le compartiment S3.



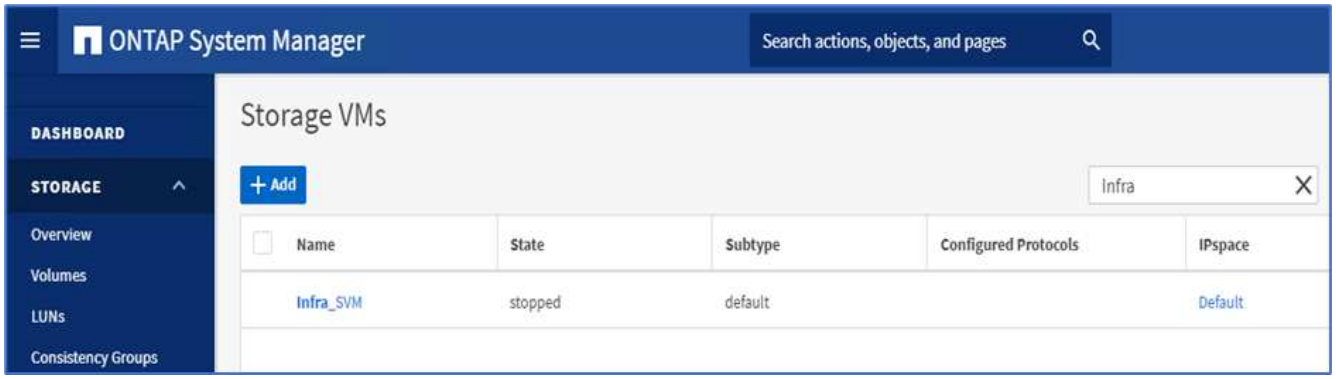
20. Sélectionnez le compartiment AWS S3 et lancez l'opération de sauvegarde.



21. L'opération de sauvegarde doit créer un dossier contenant plusieurs objets dans le compartiment AWS S3.



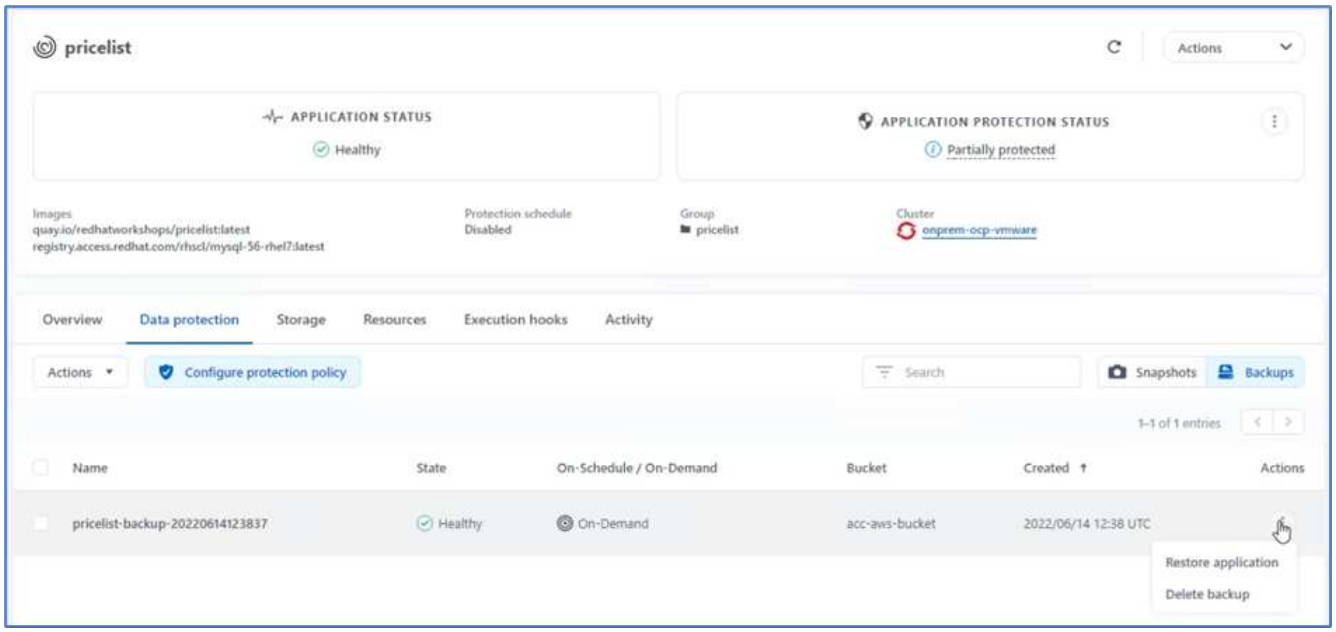
22. Une fois la sauvegarde à distance terminée, simulez un incident sur site en arrêtant la machine virtuelle de stockage (SVM) qui héberge le volume de support du volume persistant.



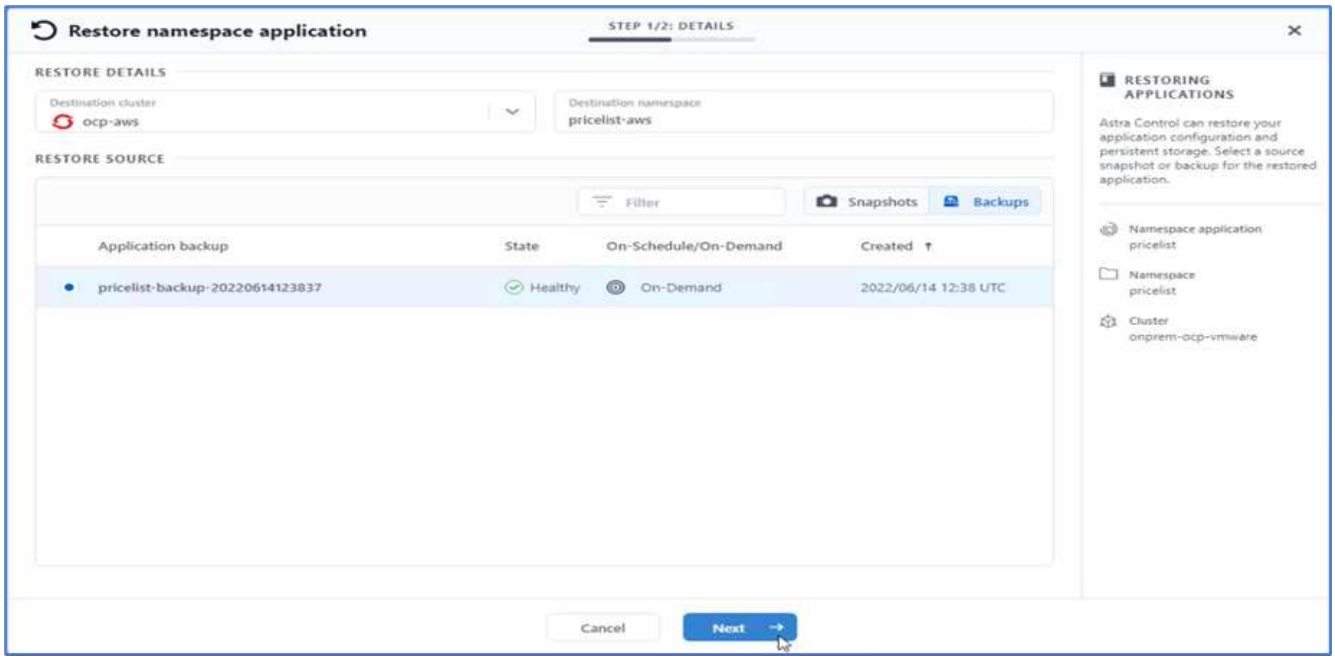
23. Actualisez la page Web pour confirmer l'interruption. La page Web n'est pas disponible.

Comme on pouvait s'y attendre, le site Web est en panne. Restaurez rapidement l'application à partir de la sauvegarde à distance en utilisant Astra vers le cluster OpenShift exécuté dans AWS.

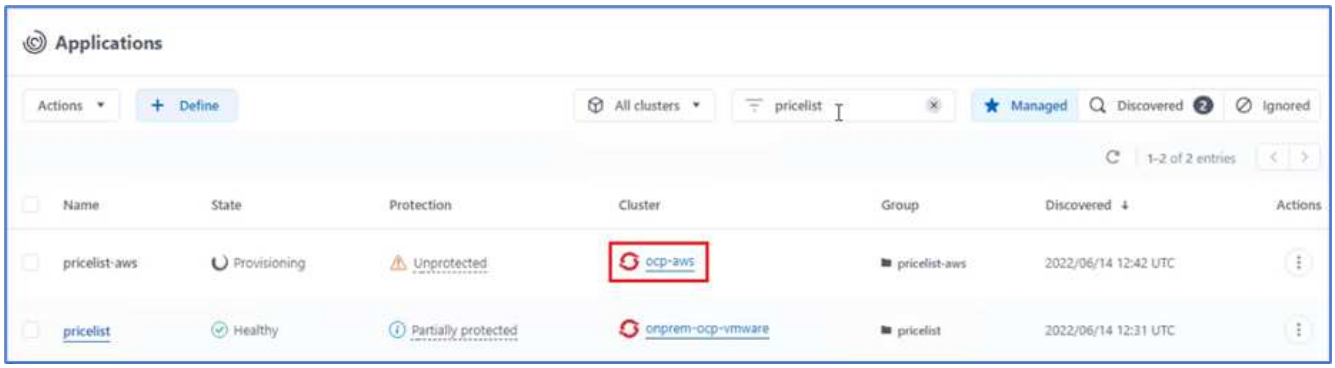
24. Dans Astra Control Center, cliquez sur l'application Pricelist et sélectionnez protection des données > sauvegardes. Sélectionnez la sauvegarde, puis cliquez sur Restaurer l'application sous action.



25. Sélectionnez `ocp-aws` comme cluster de destination et donner un nom au namespace. Cliquez sur sauvegarde à la demande, puis sur Suivant, puis sur Restaurer.

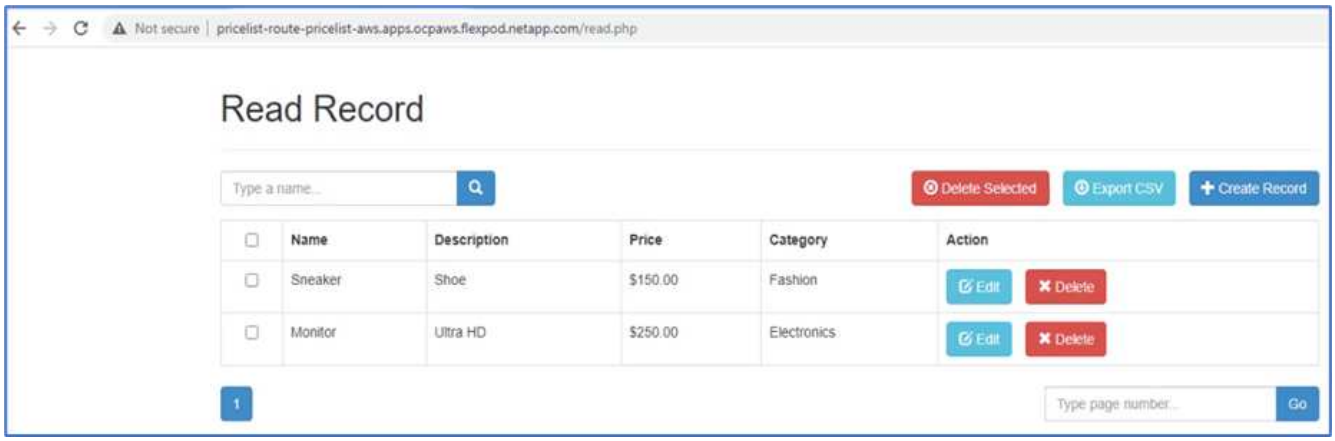


26. Une nouvelle application portant le nom `pricelist-app` Est mise à la disposition du cluster OpenShift exécuté dans AWS.



27. Vérifiez la même chose dans la console web OpenShift.

28. Après toutes les gousses sous le `pricelist-aws` Le projet est en cours d'exécution, accédez aux itinéraires et cliquez sur l'URL pour lancer la page Web.



Ce processus valide la restauration de l'application prichère et le maintien de l'intégrité des données sur le cluster OpenShift fonctionnant de façon transparente sur AWS avec l'aide d'Astra Control Center.

Protection des données avec les copies Snapshot et mobilité des applications pour DevTest

Ce cas d'utilisation se compose de deux parties, comme décrit dans les sections suivantes.

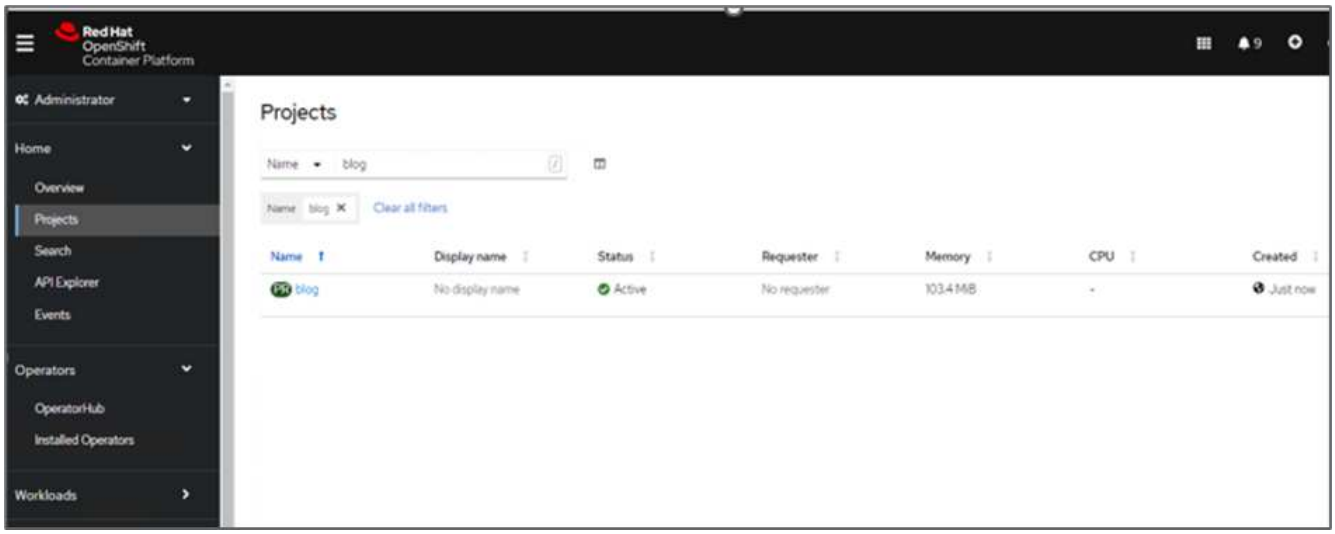
Partie 1

Avec Astra Control Center, vous pouvez créer des snapshots respectueux des applications pour une protection locale des données. Si vous supprimez ou corrompre accidentellement vos données, vous pouvez restaurer vos applications et les données associées à un état correct connu à l'aide d'un instantané précédemment enregistré.

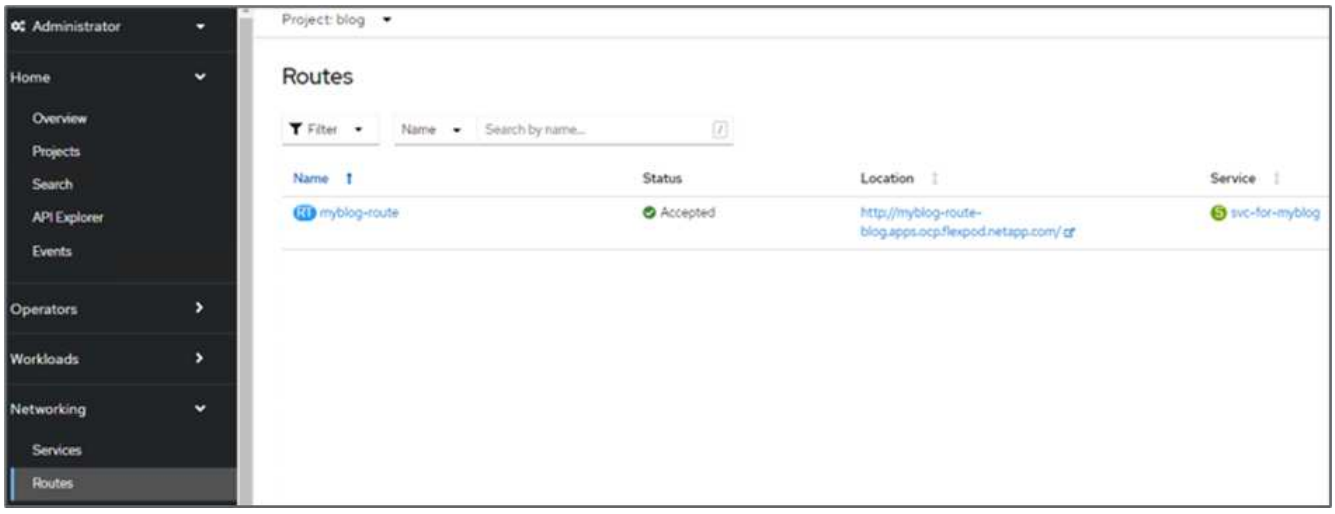
Dans ce scénario, une équipe de développement et de test (DevTest) déploie un exemple d'application avec état (site de blog) qui est une application de blog Ghost, ajoute du contenu et met à niveau l'application vers la dernière version disponible. L'application Ghost utilise SQLite pour la base de données. Avant de mettre à niveau l'application, un snapshot (à la demande) est utilisé avec Astra Control Center pour la protection des données. Les étapes détaillées sont les suivantes :

1. Déployez l'application exemple de blogging et synchronisez-la à partir d'ArgoCD.

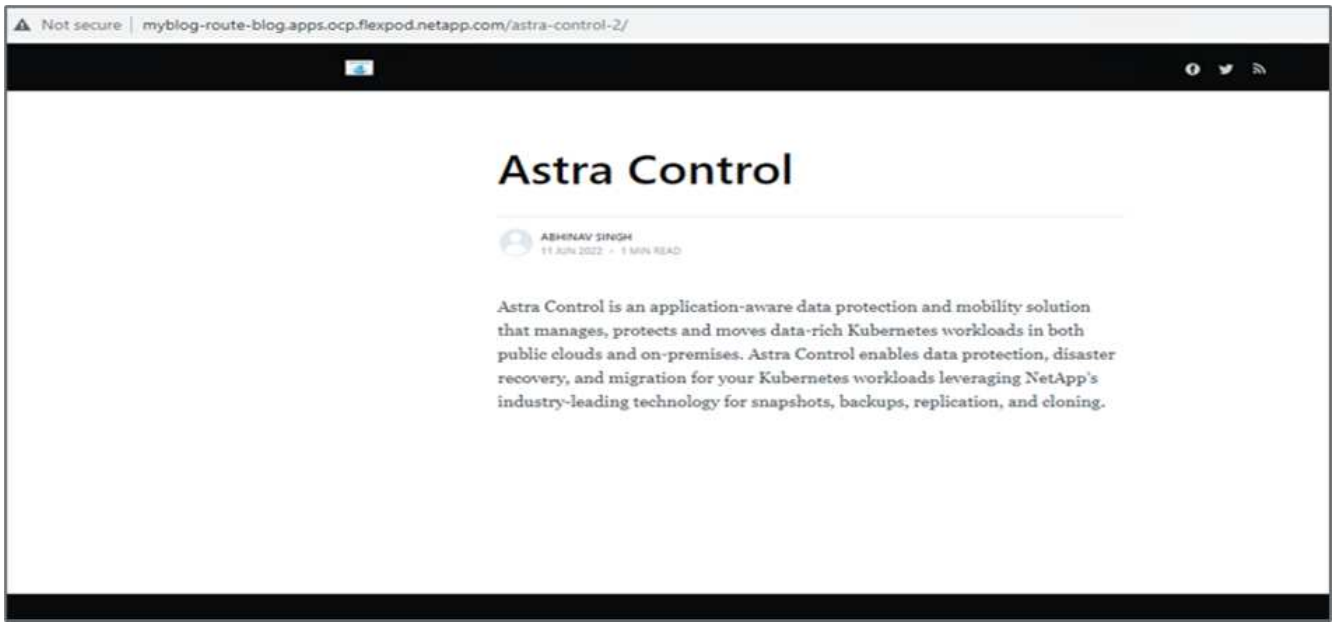
2. Connectez-vous au premier cluster OpenShift, accédez à Project et entrez Blog dans la barre de recherche.



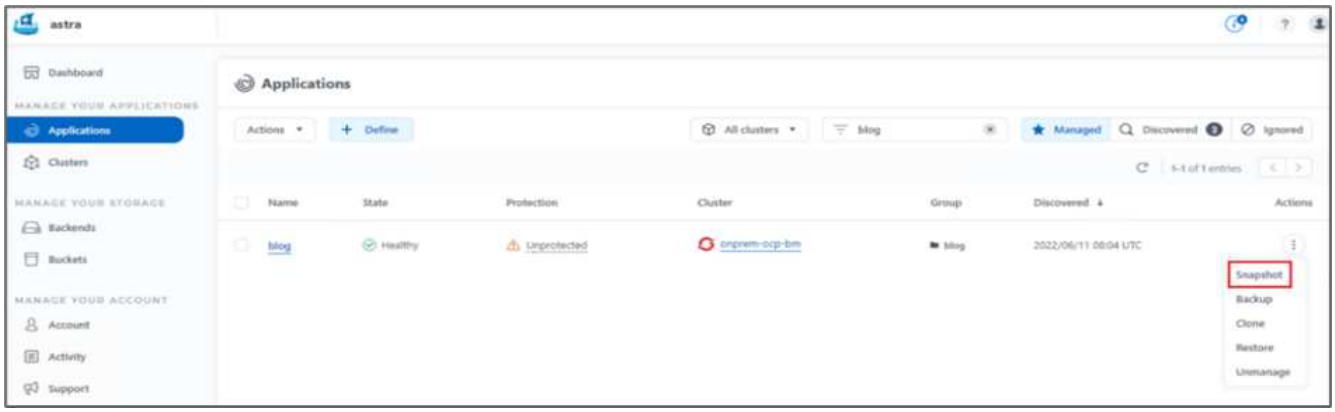
3. Dans le menu latéral, sélectionnez réseau > routes et cliquez sur l'URL.



4. La page d'accueil du blog s'affiche. Ajoutez du contenu au site du blog et publiez-le.



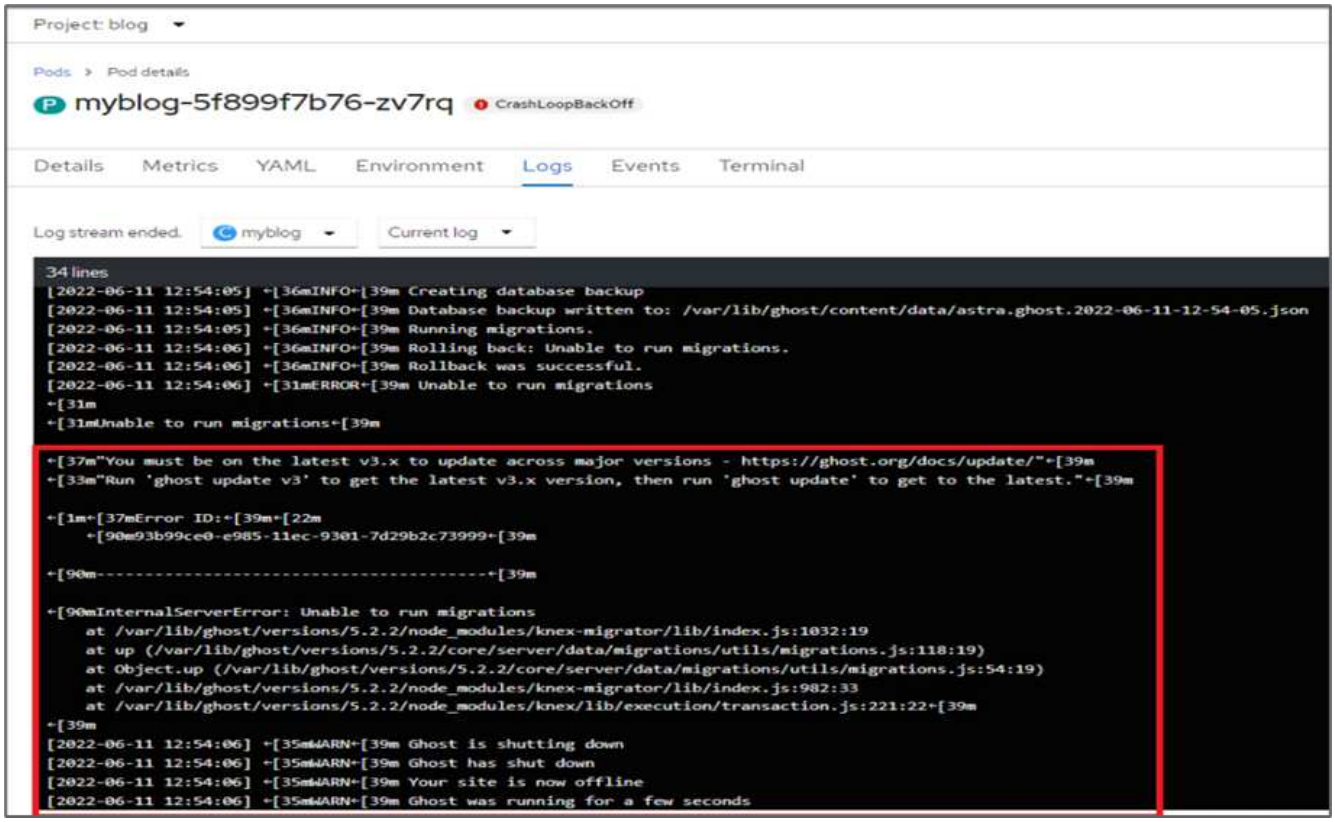
5. Rendez-vous à Astra Control Center. Commencez par gérer l'application à partir de l'onglet découverte, puis effectuez une copie Snapshot.



Vous pouvez également protéger vos applications en créant des snapshots, des sauvegardes ou les deux à un calendrier défini. Pour plus d'informations, voir "Protéger les applications avec les snapshots et les sauvegardes".

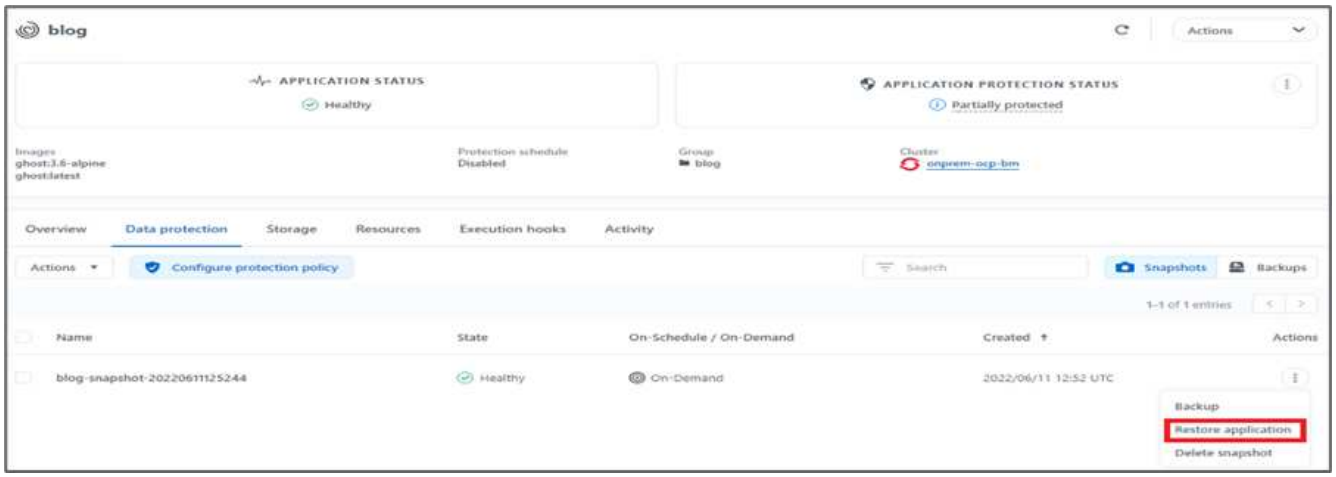
6. Une fois le snapshot à la demande créé, mettez l'application à niveau vers la dernière version. La version actuelle de l'image est `ghost: 3.6-alpine` et la version cible est `ghost:latest`. Pour mettre à niveau l'application, apportez directement des modifications au référentiel Git et synchronisez-les sur le CD Argo.

7. Vous pouvez voir que la mise à niveau directe vers la dernière version n'est pas prise en charge car le site du blog est en panne et l'application entière est corrompue.

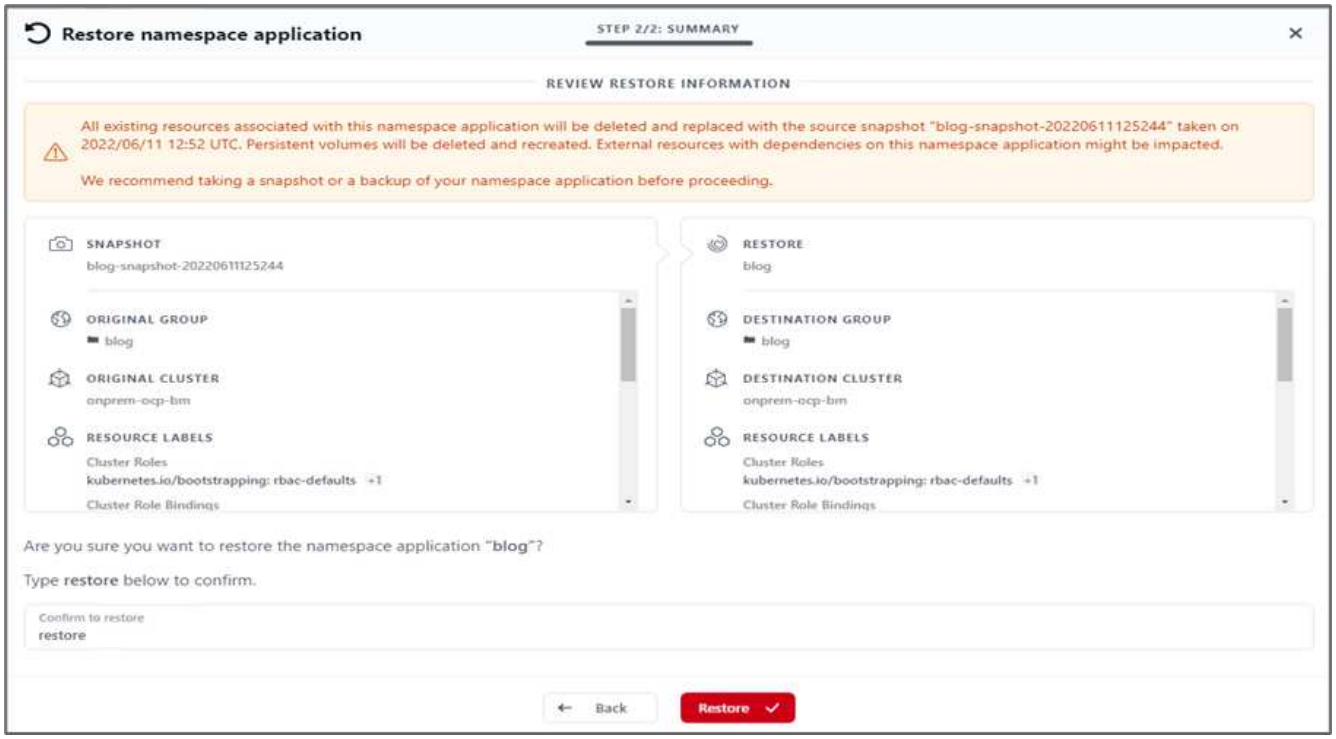


8. Pour confirmer l’indisponibilité du site du blog, actualisez l’URL.

9. Restaurez l’application à partir du snapshot.



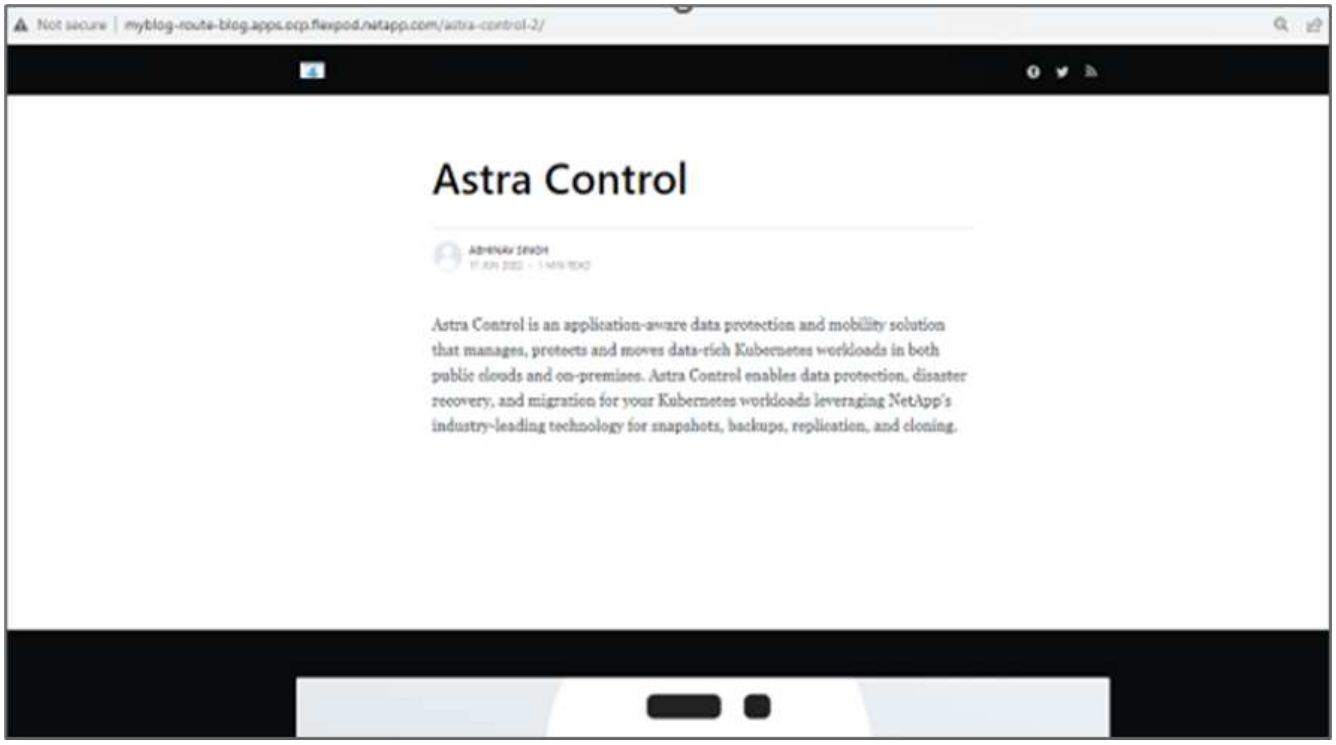
10. L'application est restaurée sur le même cluster OpenShift.



11. Le processus de restauration des applications démarre immédiatement.

12. En quelques minutes, l'application est restaurée à partir du snapshot disponible.

13. Pour voir si la page Web est disponible, actualisez l'URL.

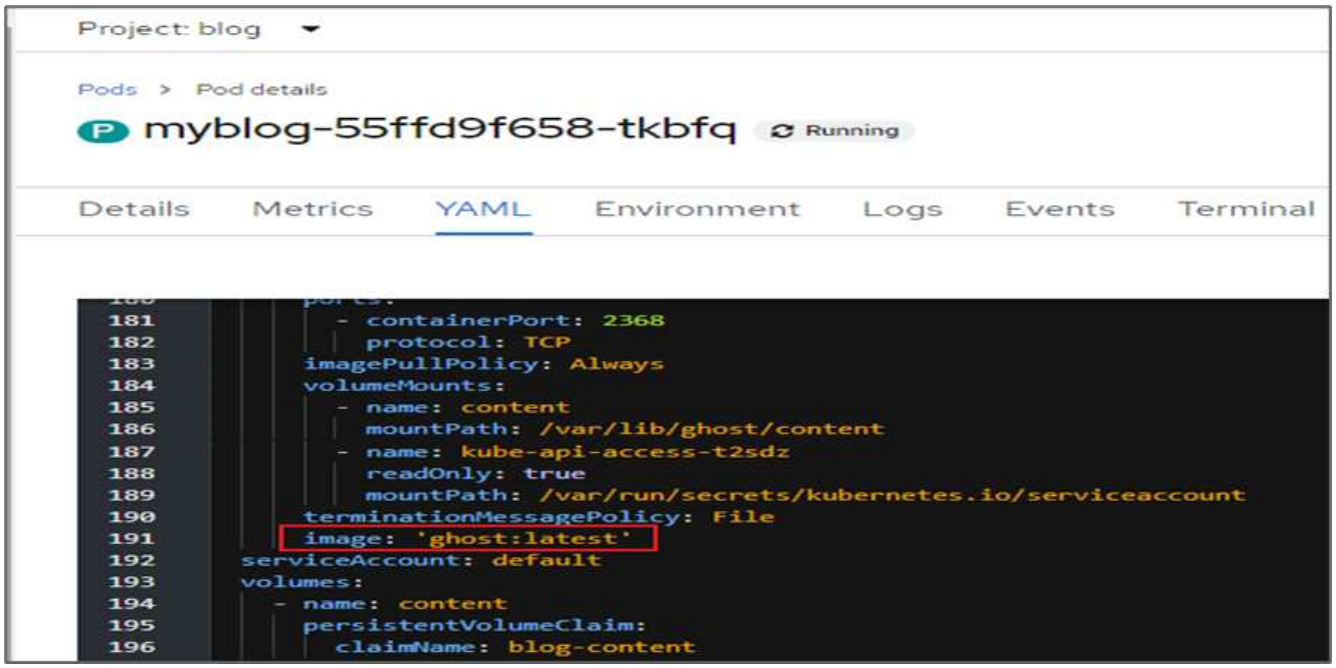


Avec l'aide d'Astra Control Center, une équipe DevTest peut réussir la récupération d'une application de blog et de ses données associées à l'aide de la capture d'écran.

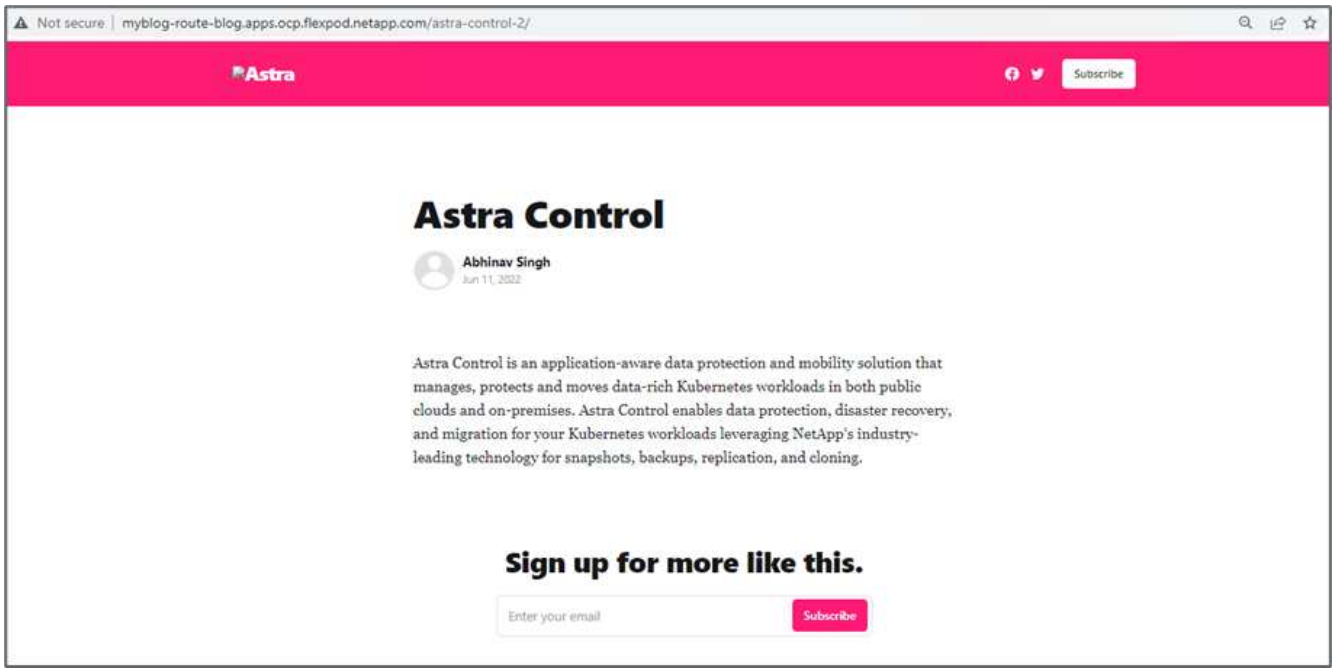
Partie 2

Avec Astra Control Center, vous pouvez déplacer l'ensemble d'une application avec ses données d'un cluster Kubernetes vers un autre, quel que soit l'emplacement des clusters (sur site ou dans le cloud).

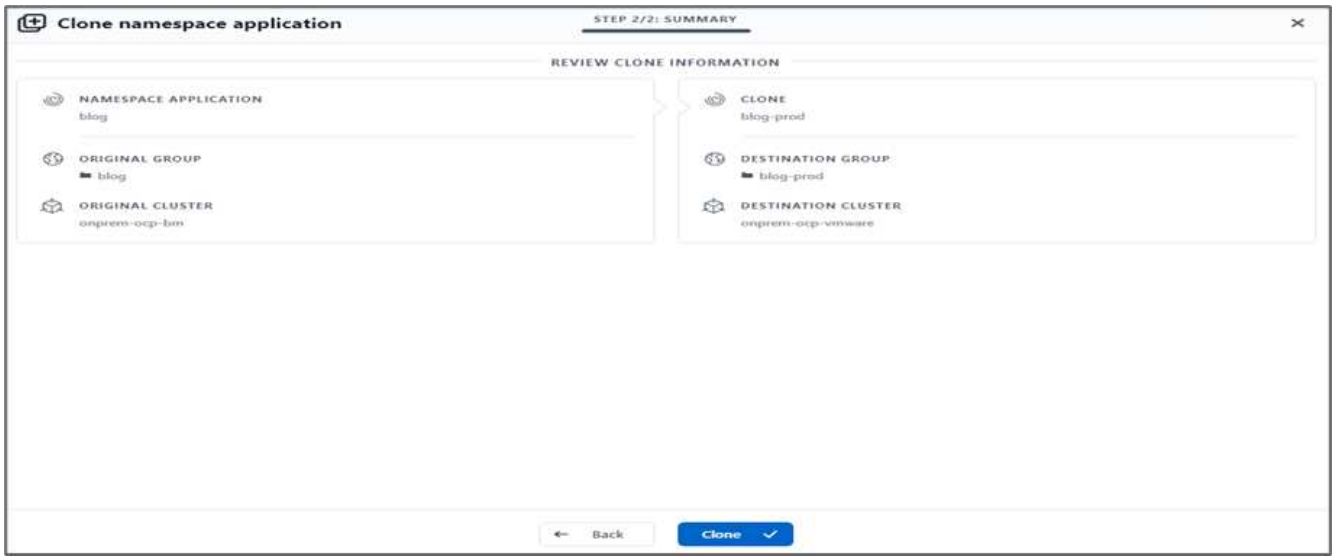
1. L'équipe DevTest met initialement à niveau l'application vers la version prise en charge (`ghost-4.6-alpine`) avant la mise à niveau vers la version finale (`ghost-latest`) pour la préparer à la production. Ils publient ensuite une mise à niveau de l'application clonée vers le cluster OpenShift de production s'exécutant sur un autre système FlexPod.
2. À ce stade, l'application est mise à niveau vers la dernière version et prête à être clonée sur le cluster de production.



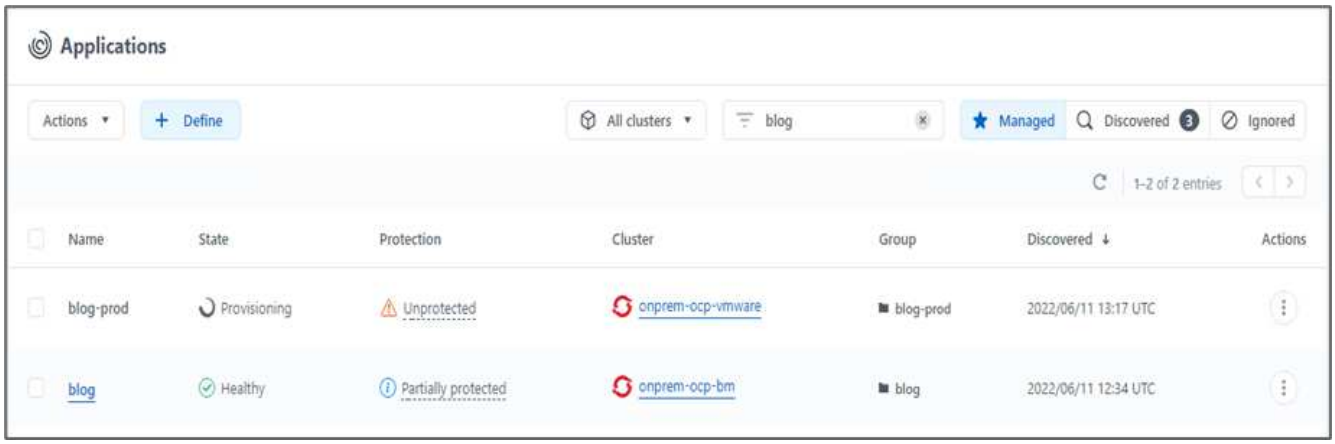
3. Pour vérifier le nouveau thème, actualisez le site du blog.



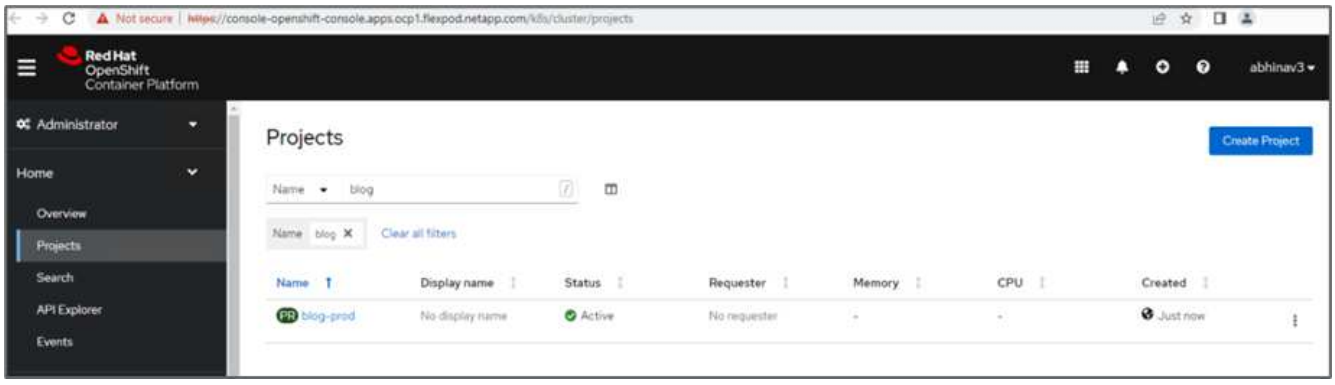
4. À partir d'Astra Control Center, clonez l'application vers l'autre cluster OpenShift de production qui s'exécute sur VMware vSphere.



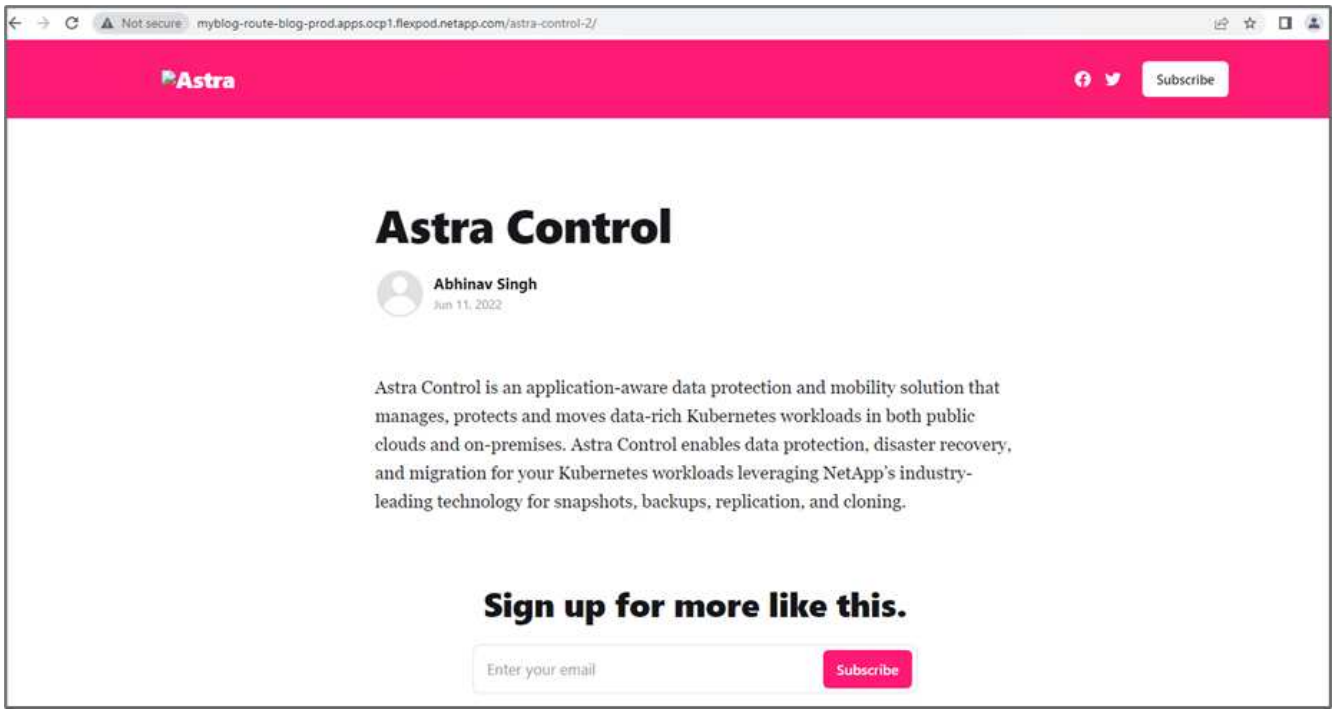
Un nouveau clone d'application est désormais provisionné dans le cluster OpenShift de production.



5. Connectez-vous au cluster OpenShift de production et recherchez le blog du projet.



6. Dans le menu latéral, sélectionnez réseau > itinéraires et cliquez sur l'URL sous emplacement. La même page d'accueil avec le contenu s'affiche.



La validation de la solution Astra Control Center est maintenant terminée. Vous pouvez désormais cloner une application et ses données d'un cluster Kubernetes à un autre, quel que soit l'emplacement du cluster Kubernetes.

"Suivant: Conclusion."

Conclusion

"Précédente : restauration d'applications avec sauvegardes distantes."

Avec cette solution, nous avons mis en œuvre un plan de protection pour les applications conteneurisées qui sont exécutées sur FlexPod et AWS à l'aide du portefeuille NetApp Astra. NetApp Astra Control Center et Astra Trident, ainsi que Cloud Volumes ONTAP, Red Hat OpenShift et l'infrastructure FlexPod, ont constitué les principaux composants de cette solution.

Nous avons démontré la protection des applications en capturant des snapshots et en exécutant des sauvegardes complètes afin de restaurer les applications sur différents clusters K8s exécutés sur les environnements cloud et sur site.

Nous avons également démontré le clonage des applications sur les clusters K8s, afin de permettre aux clients de migrer leurs applications vers les clusters K8s de leur choix.

FlexPod a constamment évolué pour permettre à ses clients de moderniser leurs applications et leurs processus de fourniture d'informations. Avec cette solution, les clients de FlexPod peuvent créer en toute confiance leur plan de reprise après incident BCDR pour leurs applications cloud natives, en utilisant le cloud public comme emplacement dans le cadre d'un plan de reprise après incident transitoire ou à temps complet, tout en conservant le coût de la solution le plus bas.

Astra Control vous permet de déplacer une application avec ses données d'un cluster Kubernetes vers un autre, quel que soit l'emplacement des clusters. Elle accélère également le déploiement, les opérations et la protection de vos applications cloud.

Dépannage

Pour obtenir des conseils de dépannage, reportez-vous à la section "documentation en ligne".

Où trouver des informations complémentaires

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

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Déploiement de FlexPod avec Infrastructure as code pour VMware avec Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Déploiement de FlexPod avec Infrastructure as code pour Red Hat OpenShift bare Metal avec Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Fiche technique Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentation NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Matrice d'interopérabilité NetApp

  "http://support.netapp.com/matrix/"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Juillet 2022	Lancement de l'ACC 22.04.0.

NetApp Cloud Insights pour FlexPod

Tr-4868 : NetApp Cloud Insights pour FlexPod

Alan Cowles, NetApp

En partenariat avec : 

Dans ce rapport technique, la solution détaillée est la configuration du service NetApp Cloud Insights pour surveiller le système de stockage NetApp AFF A800 exécutant NetApp ONTAP, qui est déployé dans le cadre d'une solution FlexPod Datacenter.

En valeur pour le client

La description détaillée de cette solution apporte une valeur ajoutée aux clients qui souhaitent bénéficier d'une solution de surveillance complète pour leurs environnements de cloud hybride, dans lesquels ONTAP est déployé comme système de stockage principal. Cela inclut les environnements FlexPod qui utilisent les systèmes de stockage NetApp AFF et FAS.

Cas d'utilisation

Cette solution s'applique aux cas d'utilisation suivants :

- Organisations qui souhaitent surveiller différentes ressources et l'utilisation de leur système de stockage ONTAP déployé dans le cadre d'une solution FlexPod.
- Les entreprises qui souhaitent résoudre les problèmes et réduire le temps de résolution des incidents survenant dans la solution FlexPod avec leurs systèmes AFF ou FAS.
- Les entreprises intéressées par des projections d'optimisation des coûts, notamment des tableaux de bord personnalisés qui fournissent des informations détaillées sur la perte de ressources et permettent de réaliser des économies dans leur environnement FlexPod, y compris ONTAP.

Public visé

La solution cible plusieurs groupes d'utilisateurs :

- Cadres informatiques et ceux chargés de l'optimisation des coûts et de la continuité de l'activité.
- Architectes de solutions intéressés par la conception et la gestion de data centers ou de clouds hybrides.
- Ingénieurs du support technique chargés du dépannage et de la résolution d'incident.

Vous pouvez configurer Cloud Insights pour fournir plusieurs types de données utiles que vous pouvez utiliser pour vous aider dans la planification, la résolution de problèmes, la maintenance et la continuité de l'activité. En surveillant la solution de data Center de FlexPod avec Cloud Insights et présentant les données agrégées sous forme de tableaux de bord personnalisés facilement digestibles ; non seulement il est possible de prévoir quand les ressources d'un déploiement doivent évoluer pour répondre à leurs besoins, mais également d'identifier des applications ou des volumes de stockage spécifiques qui causent des problèmes au sein du système. Cela permet de s'assurer que l'infrastructure surveillée est prévisible et fonctionne selon les attentes, ce qui permet à une organisation de respecter les SLA définis et de faire évoluer l'infrastructure en fonction des besoins, éliminant ainsi le gaspillage et les coûts supplémentaires.

Architecture

Dans cette section, nous analysons l'architecture d'une infrastructure convergée FlexPod Datacenter, dont un système NetApp AFF A800 surveillé par Cloud Insights.

Technologie de la solution

La solution de data Center FlexPod comprend les composants minimum suivants afin de fournir un environnement d'infrastructure convergée haute disponibilité, facilement évolutif, validé et pris en charge.

- Deux nœuds de stockage NetApp ONTAP (une paire haute disponibilité)
- Deux commutateurs réseau pour data Center Cisco Nexus
- Deux commutateurs de structure Cisco MDS (en option pour les déploiements FC)
- Deux interconnexions de fabric Cisco UCS
- Un châssis lame Cisco UCS avec deux serveurs lames Cisco UCS B-Series

Ou

- Deux serveurs Cisco UCS C-Series montés en rack

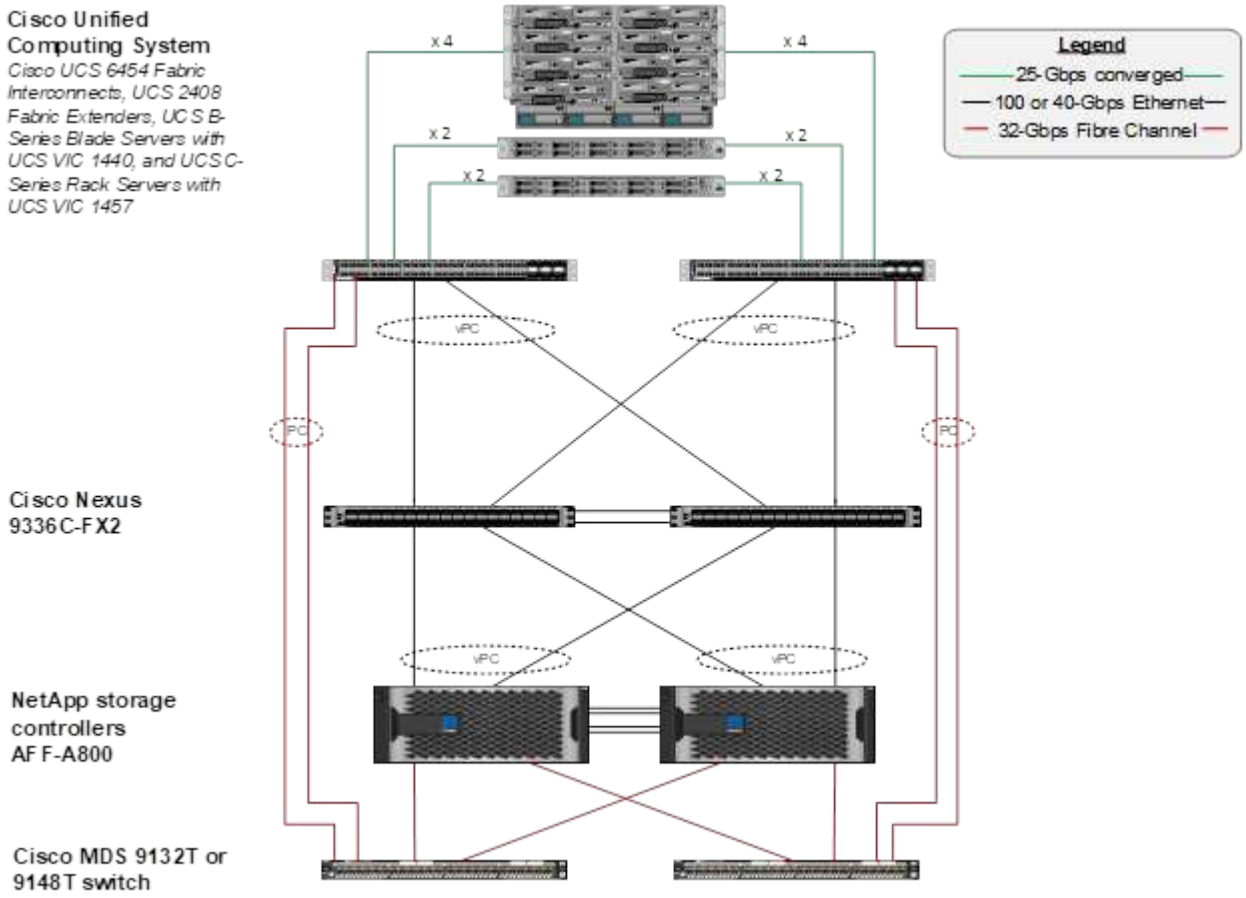
Pour que Cloud Insights puisse collecter des données, une entreprise doit déployer une unité d'acquisition en tant que machine virtuelle ou physique dans son environnement FlexPod Datacenter ou sur un emplacement où elle peut contacter les composants à partir desquels elle collecte les données. Vous pouvez installer le logiciel acquisition Unit sur un système exécutant plusieurs systèmes d'exploitation Windows ou Linux pris en charge. Le tableau suivant répertorie les composants de la solution pour ce logiciel.

Système d'exploitation	Version
Microsoft Windows	10
Serveur Microsoft Windows	2012, 2012 R2, 2016, 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6

Système d'exploitation	Version
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

Diagramme architectural

La figure suivante illustre l'architecture de la solution.



Configuration matérielle requise

Le tableau suivant répertorie les composants matériels requis pour implémenter la solution. Ils peuvent varier selon la mise en œuvre de la solution et les besoins du client.

Sous-jacent	Quantité
Cisco Nexus 9336C-FX2	2
Fabric Interconnect Cisco UCS 6454	2
Châssis lame Cisco UCS 5108	1
Cisco UCS 2408 Fabric Extender	2
Lames Cisco UCS B200 M5	2

Sous-jacent	Quantité
NetApp AFF A800	2

Configuration logicielle requise

Le tableau suivant répertorie les composants logiciels requis pour implémenter la solution. Ils peuvent varier selon la mise en œuvre de la solution et les besoins du client.

Logiciel	Version
Firmware Cisco Nexus	9.3(5)
Version de Cisco UCS	4.1(2a)
Version de NetApp ONTAP	9.7
Version de NetApp Cloud Insights	Septembre 2020, Basic
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3

Détails du cas d'utilisation

Cette solution s'applique aux cas d'utilisation suivants :

- L'analyse de l'environnement avec des données fournies au conseiller digital NetApp Active IQ pour évaluer les risques liés aux systèmes de stockage et formuler des recommandations sur l'optimisation du stockage.
- Résolution des problèmes dans le système de stockage ONTAP déployé dans une solution de data Center FlexPod en examinant les statistiques système en temps réel.
- Création de tableaux de bord personnalisés afin de surveiller facilement les points d'intérêt spécifiques pour les systèmes de stockage ONTAP déployés dans une infrastructure convergée FlexPod Datacenter.

Considérations relatives à la conception

La solution FlexPod Datacenter est une infrastructure convergée conçue par Cisco et NetApp offrant un environnement de data Center dynamique, extrêmement disponible et évolutif pour l'exécution des charges de travail d'entreprise. Les ressources de calcul et de réseau de la solution sont fournies par les produits Cisco UCS et Nexus, et les ressources de stockage sont fournies par le système de stockage ONTAP. La conception de la solution est régulièrement optimisée lorsque des modèles matériels ou logiciels et micrologiciels mis à jour sont disponibles. Ces détails, ainsi que les meilleures pratiques de conception et de déploiement de solutions, sont publiés régulièrement dans des documents CVD (Cisco Validated Design) ou NVA (NetApp Verified Architecture).

Le dernier document CVD détaillant la conception de la solution FlexPod Datacenter est disponible "ici".

Déployez Cloud Insights pour FlexPod

Pour déployer la solution, vous devez effectuer les tâches suivantes :

1. Abonnez-vous au service Cloud Insights
2. Créez une machine virtuelle VMware (VM) à configurer comme unité d'acquisition
3. Installez l'hôte Red Hat Enterprise Linux (RHEL)
4. Créez une instance d'unité d'acquisition dans le portail Cloud Insights et installez le logiciel
5. Ajoutez le système de stockage surveillé du data Center FlexPod à Cloud Insights.

Abonnez-vous au service NetApp Cloud Insights

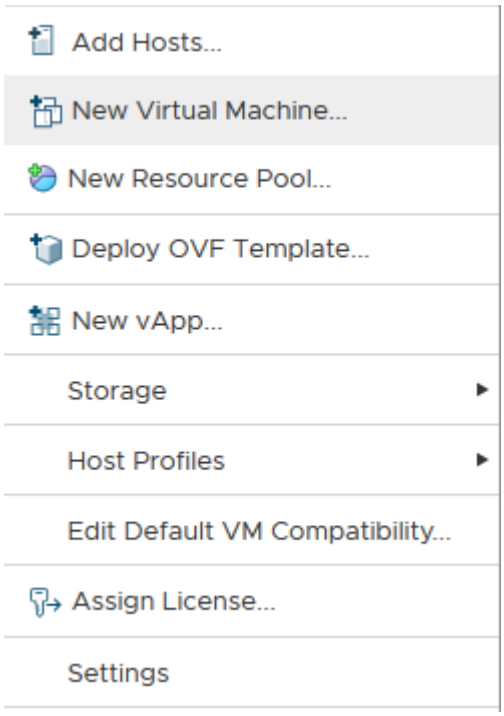
Pour vous inscrire au service NetApp Cloud Insights, procédez comme suit :

1. Accédez à "https://cloud.netapp.com/cloud-insights"
2. Cliquez sur le bouton au centre de l'écran pour lancer l'essai gratuit de 14 jours ou sur le lien en haut à droite pour vous inscrire ou vous connecter à un compte NetApp Cloud Central.

Créez une machine virtuelle VMware à configurer en tant qu'unité d'acquisition

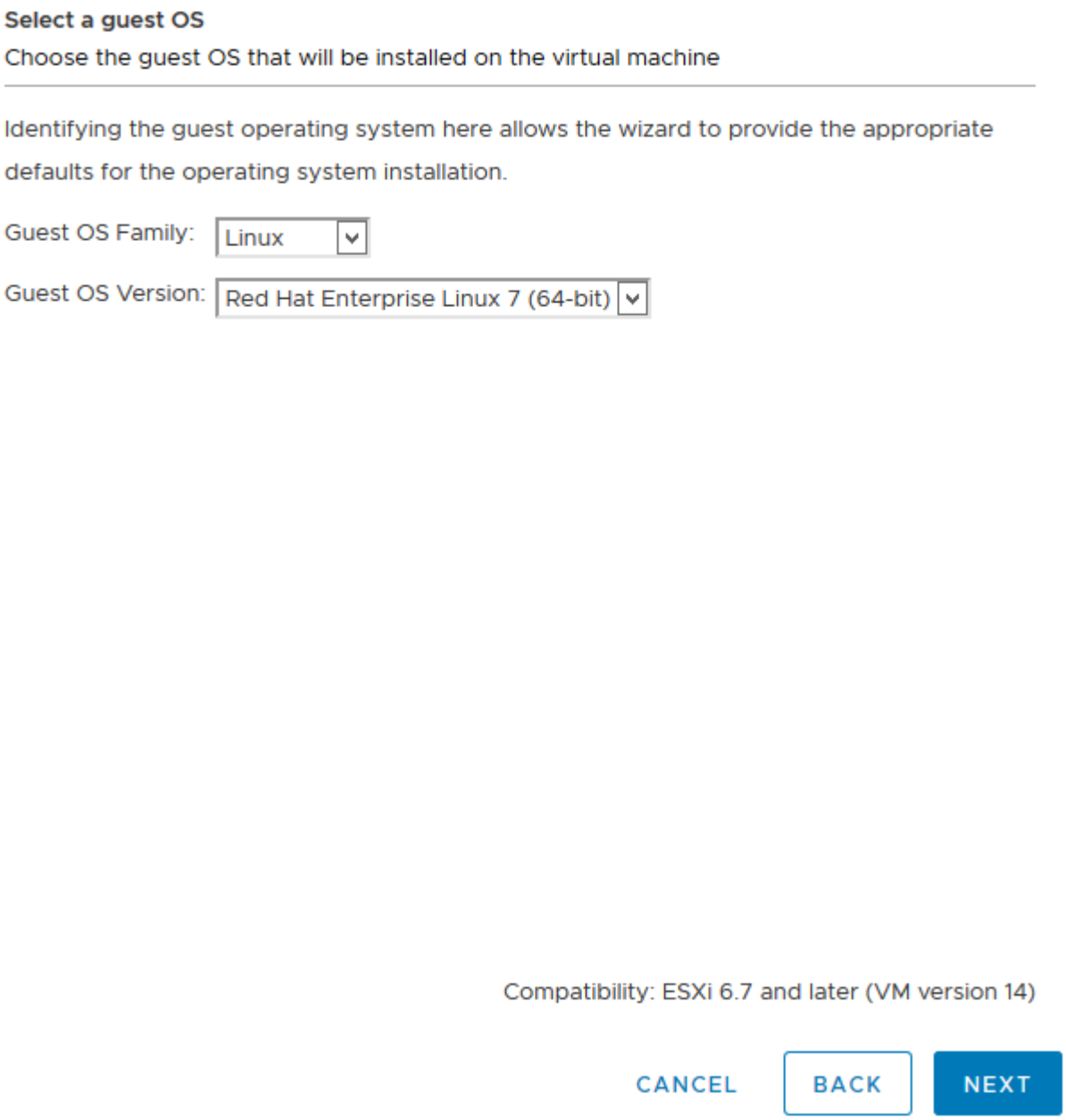
Pour créer un VM VMware à configurer comme unité d'acquisition, procédez comme suit :

1. Lancez un navigateur Web, connectez-vous à VMware vSphere et sélectionnez le cluster que vous souhaitez héberger.
2. Cliquez avec le bouton droit de la souris sur ce cluster et sélectionnez Créer Une machine virtuelle dans le menu.



3. Dans l'assistant New Virtual machine (Nouvelle machine virtuelle), cliquez sur Next (Suivant).
4. Indiquez le nom de la machine virtuelle, puis sélectionnez le data Center auquel vous souhaitez l'installer, puis cliquez sur Next (Suivant).
5. Sur la page suivante, sélectionnez le cluster, les nœuds ou le groupe de ressources auquel vous souhaitez installer la machine virtuelle, puis cliquez sur Suivant.

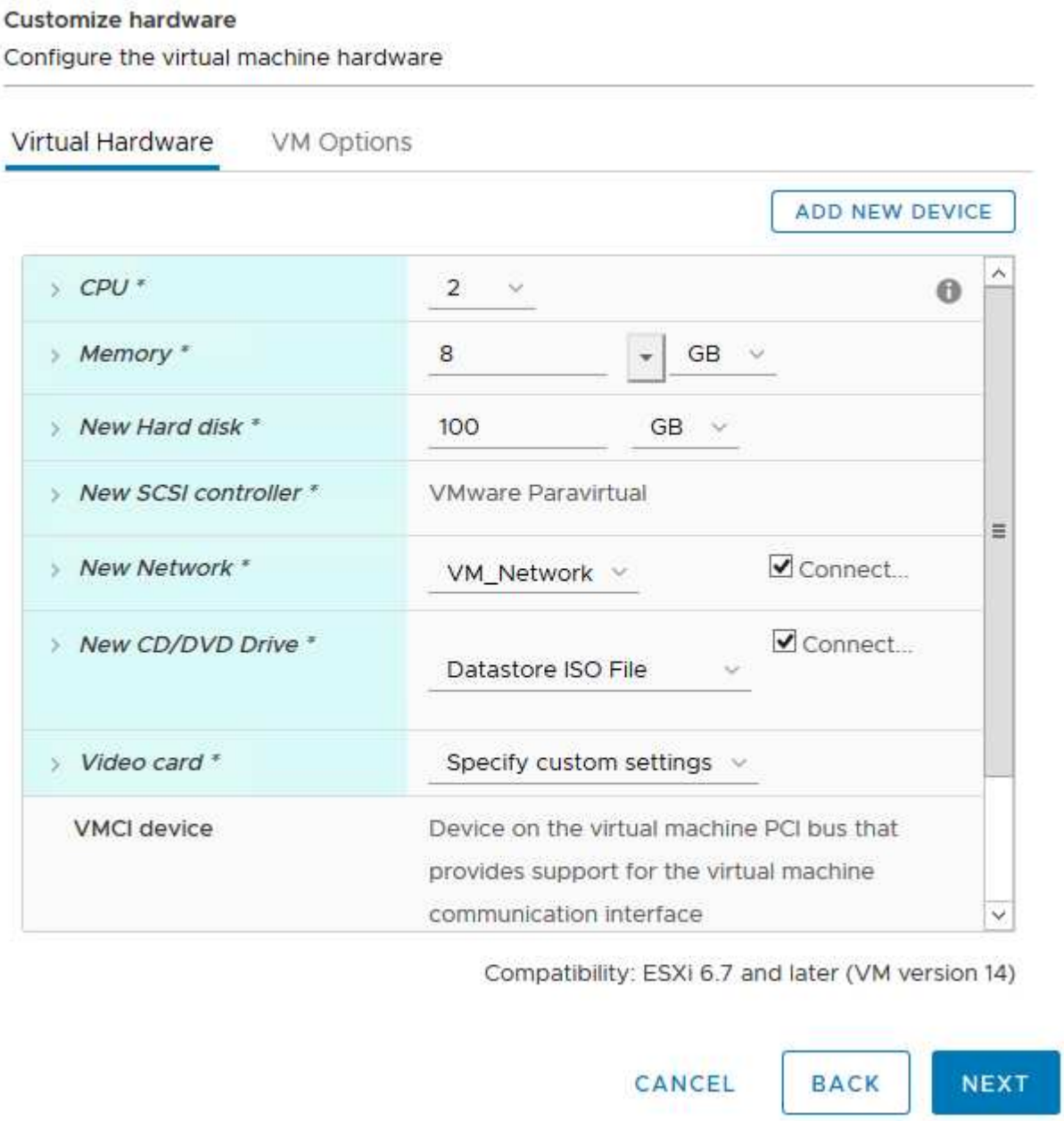
6. Sélectionnez le datastore partagé qui héberge vos machines virtuelles et cliquez sur Next (Suivant).
7. Vérifiez que le mode de compatibilité de la machine virtuelle est défini sur `ESXi 6.7 or later` Et cliquez sur Suivant.
8. Sélectionnez Guest OS Family Linux, Guest OS version : Red Hat Enterprise Linux 7 (64 bits).



9. La page suivante permet la personnalisation des ressources matérielles sur la machine virtuelle. L'unité d'acquisition Cloud Insights nécessite les ressources suivantes. Une fois les ressources sélectionnées, cliquez sur Suivant :
   a. Deux processeurs
   b. 8 Go de RAM
   c. 100 Go d'espace disque
   d. Réseau pouvant accéder aux ressources dans le centre de données FlexPod et le serveur Cloud

Insights via une connexion SSL sur le port 443.

e. Image ISO de la distribution Linux choisie (Red Hat Enterprise Linux) à partir de laquelle démarrer.

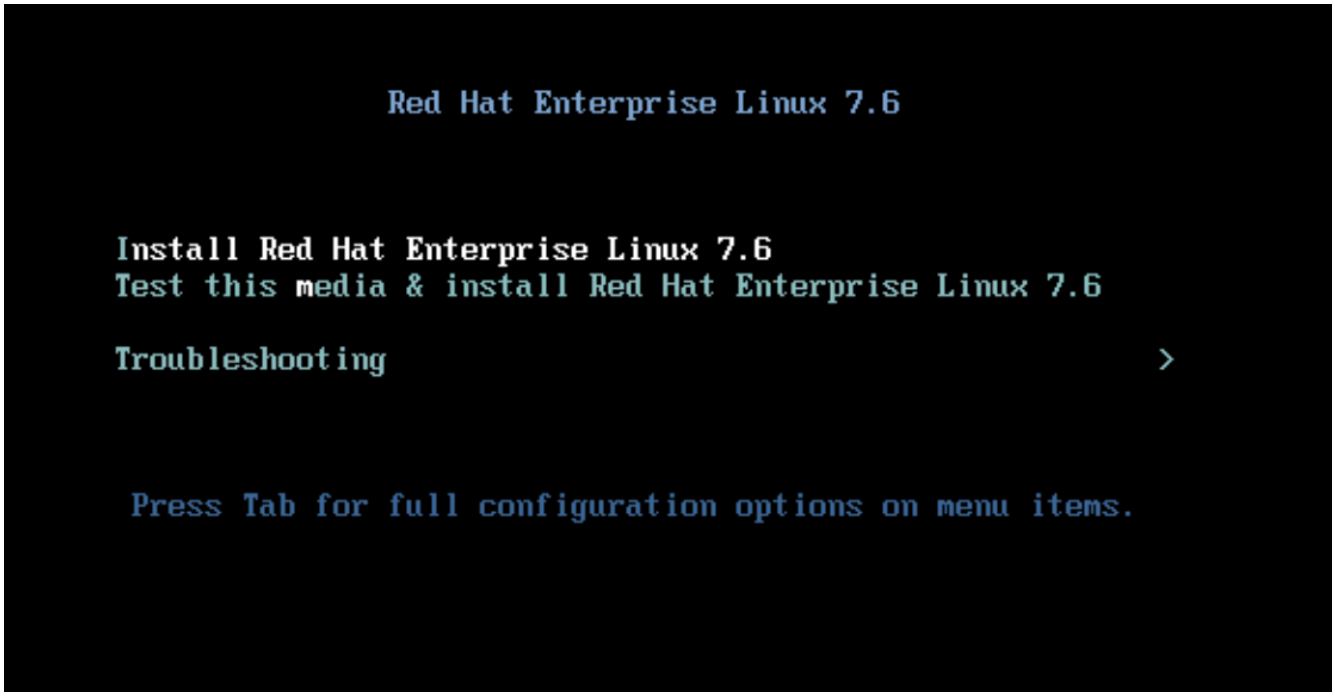


10. Pour créer la machine virtuelle, sur la page Ready to Complete (prêt à terminer), vérifiez les paramètres et cliquez sur Finish (Terminer).

Installez Red Hat Enterprise Linux

Pour installer Red Hat Enterprise Linux, procédez comme suit :

1. Mettez la machine virtuelle sous tension, cliquez sur la fenêtre pour lancer la console virtuelle, puis sélectionnez l'option d'installation de Red Hat Enterprise Linux 7.6.



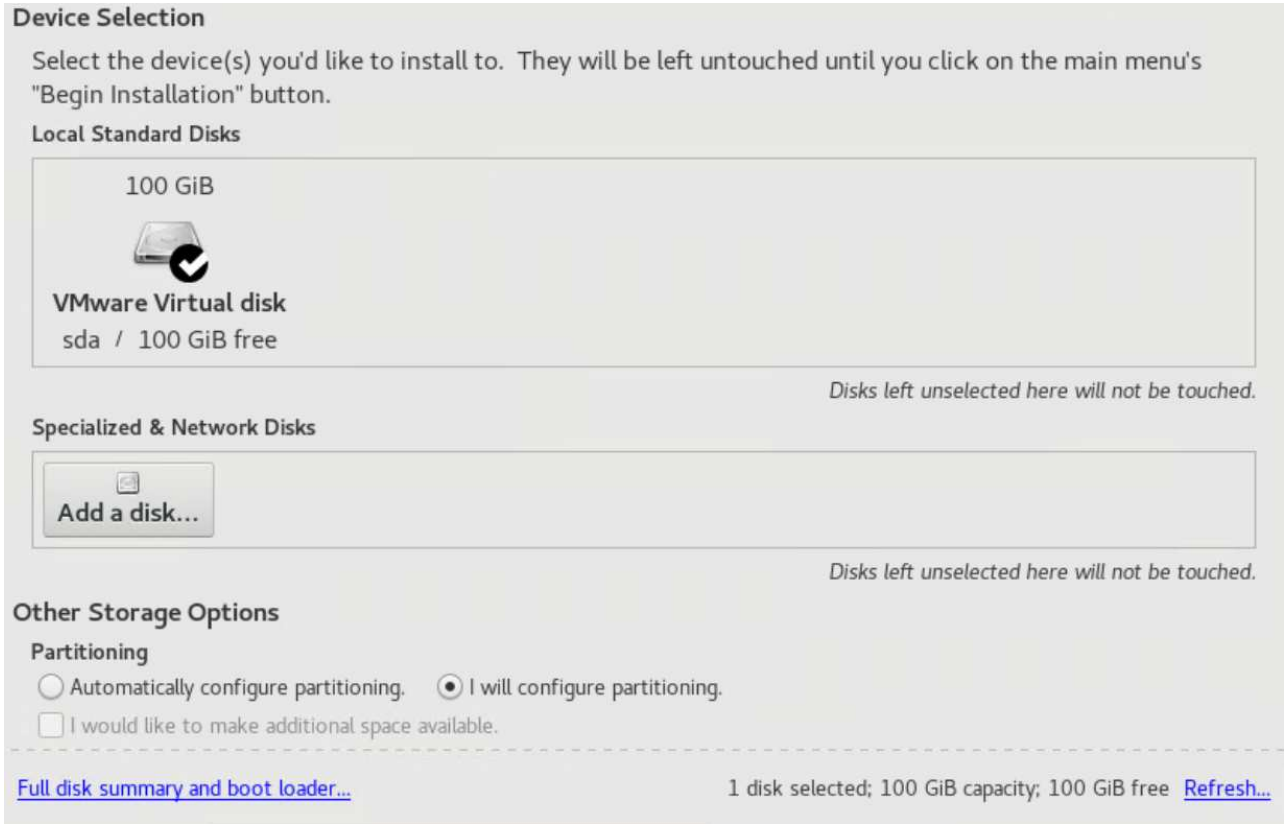
2. Sélectionnez la langue de votre choix et cliquez sur Continuer.

   La page suivante est le résumé de l'installation. Les paramètres par défaut doivent être acceptables pour la plupart de ces options.

3. Vous devez personnaliser l'organisation du stockage en effectuant les options suivantes :

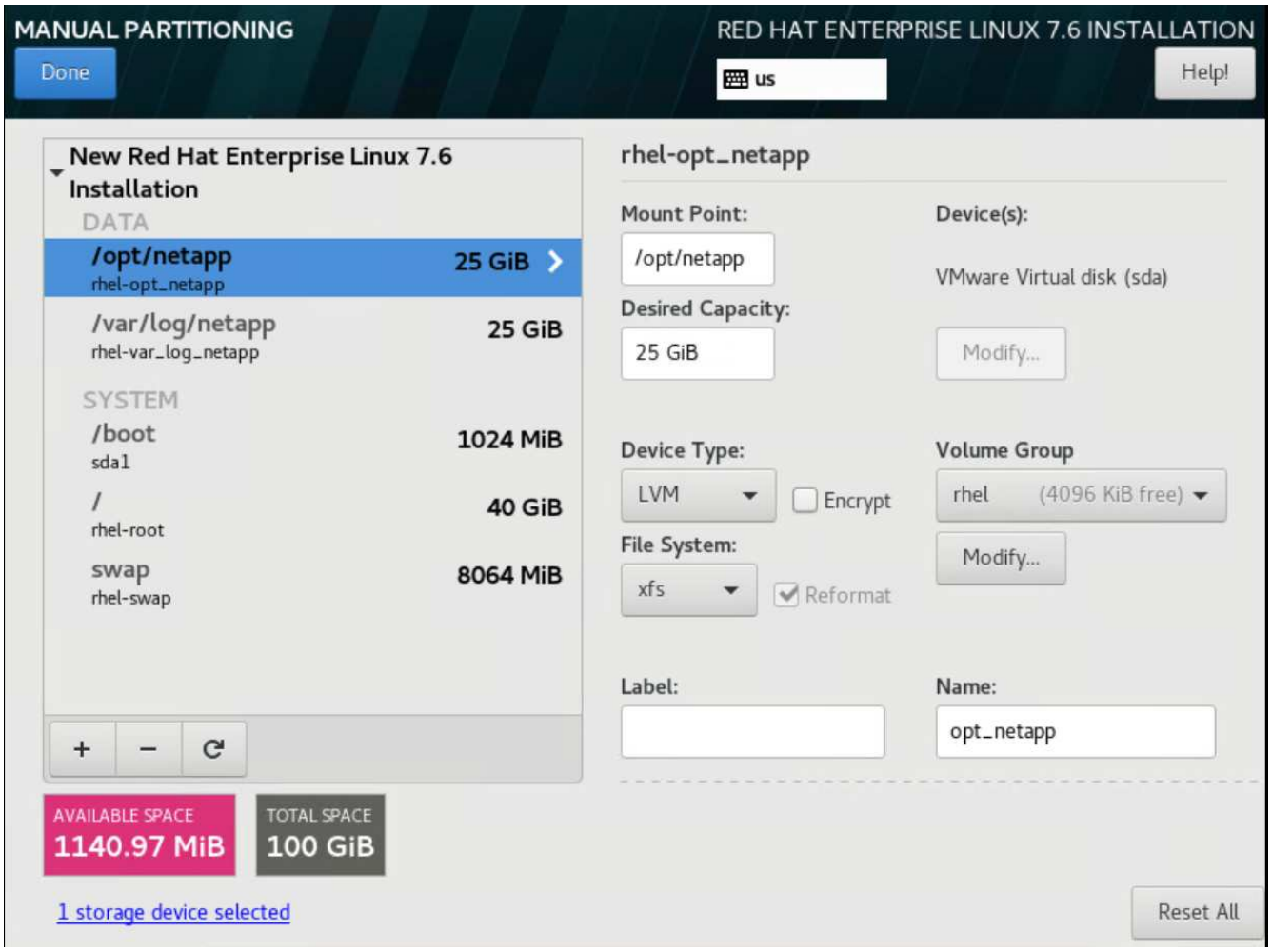
   a. Pour personnaliser le partitionnement du serveur, cliquez sur destination de l'installation.

   b. Vérifier que le disque virtuel VMware de 100 Gio est sélectionné avec une coche noire et sélectionner le bouton radio I will configure Partitioning.



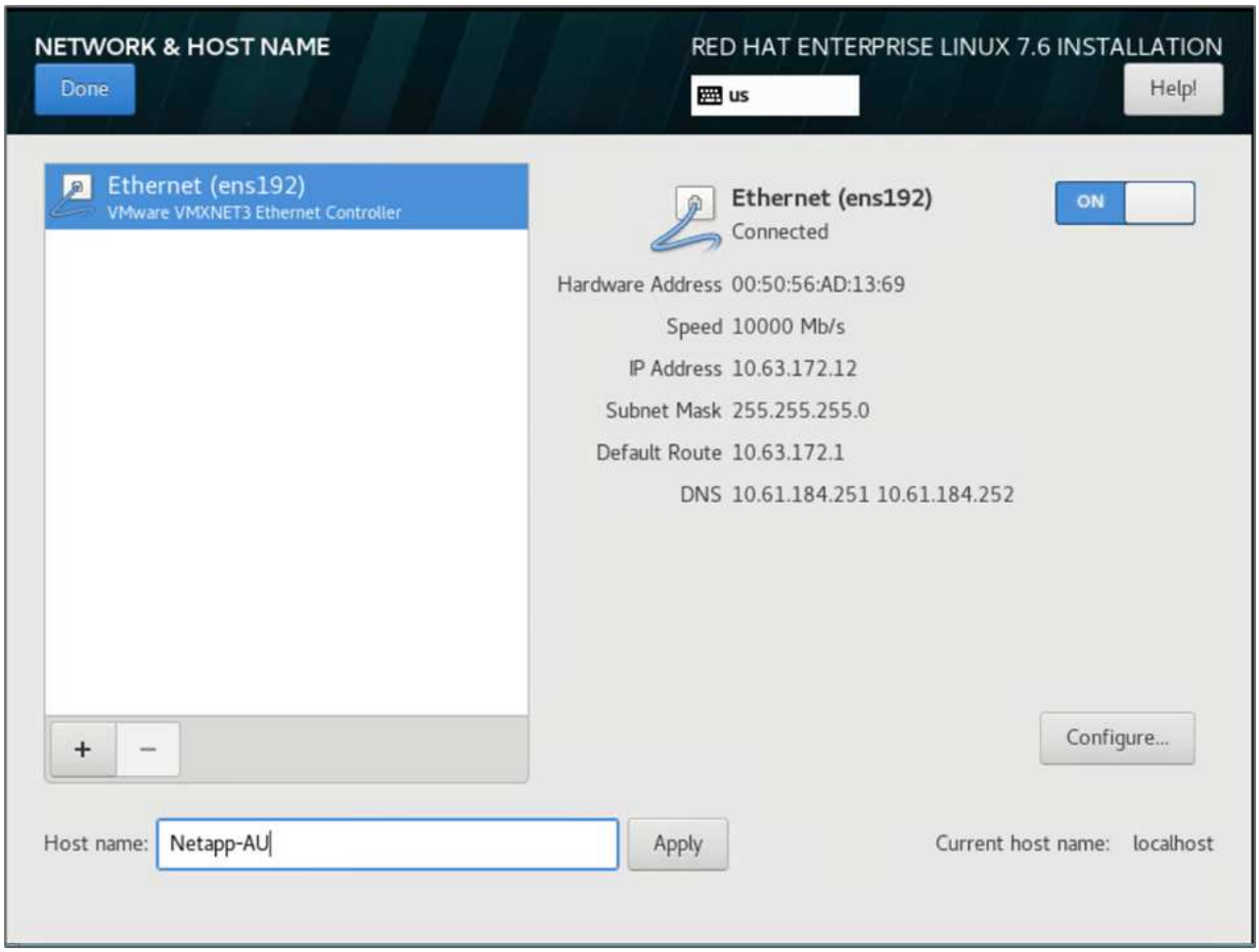
c. Cliquez sur terminé.

   Un nouveau menu s'affiche pour vous permettre de personnaliser la table de partition. Dédier 25 Go à chaque `/opt/netapp` et `/var/log/netapp`. Vous pouvez allouer automatiquement le reste du stockage au système.



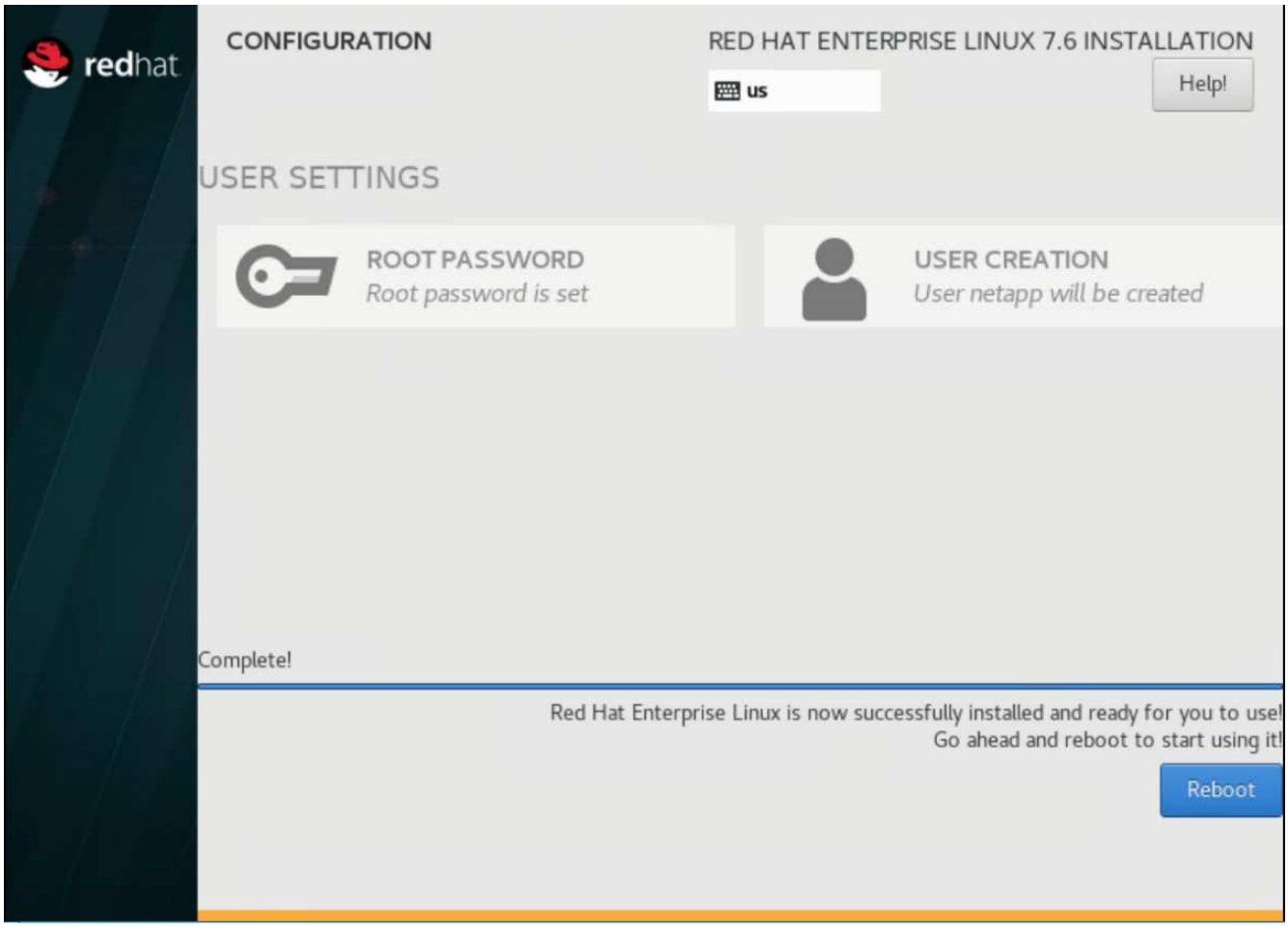
a. Pour revenir au résumé de l'installation, cliquez sur terminé.

4. Cliquez sur Nom du réseau et de l'hôte.
   a. Entrez un nom d'hôte pour le serveur.
   b. Activez la carte réseau en cliquant sur le curseur. Si le protocole DHCP (Dynamic Host Configuration Protocol) est configuré sur votre réseau, vous recevrez une adresse IP. Si ce n'est pas le cas, cliquez sur configurer et attribuez une adresse manuellement.



c. . Cliquez sur terminé pour revenir au résumé de l'installation.

5. Sur la page Récapitulatif d'installation, cliquez sur commencer l'installation.
6. Sur la page progression de l'installation, vous pouvez définir le mot de passe racine ou créer un compte utilisateur local. Une fois l'installation terminée, cliquez sur redémarrer pour redémarrer le serveur.



7. Une fois le système redémarré, connectez-vous à votre serveur et enregistrez-le à l'aide de Red Hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

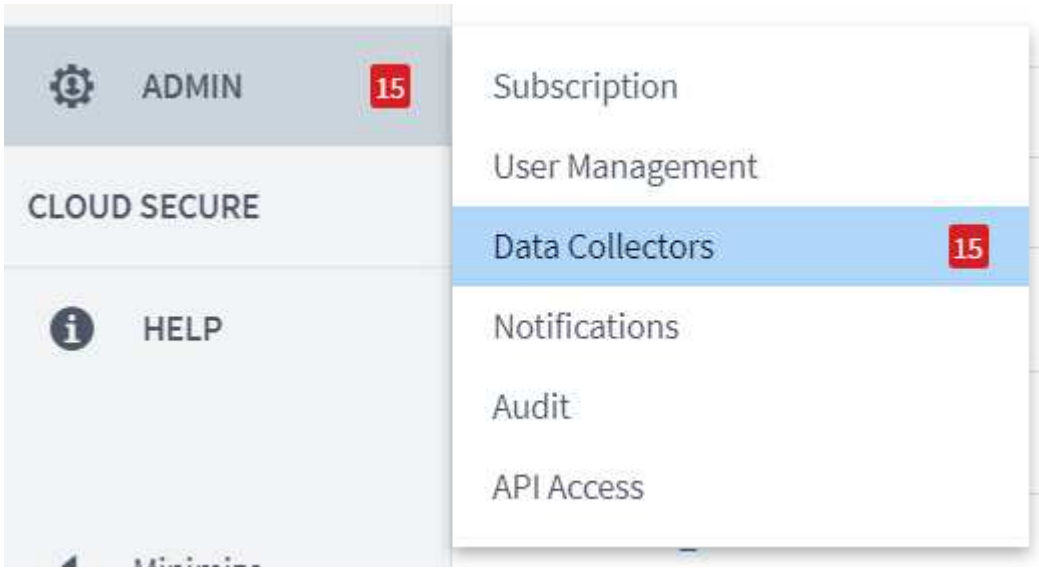
8. Joignez un abonnement disponible à Red Hat Enterprise Linux.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Créez une instance d'unité d'acquisition dans le portail Cloud Insights et installez le logiciel

Pour créer une instance d'unité d'acquisition sur le portail Cloud Insights et installer le logiciel, procédez comme suit :

1. Sur la page d'accueil de Cloud Insights, passez le curseur de la souris sur l'entrée Admin du menu principal vers la gauche et sélectionnez Data Collectors dans le menu.

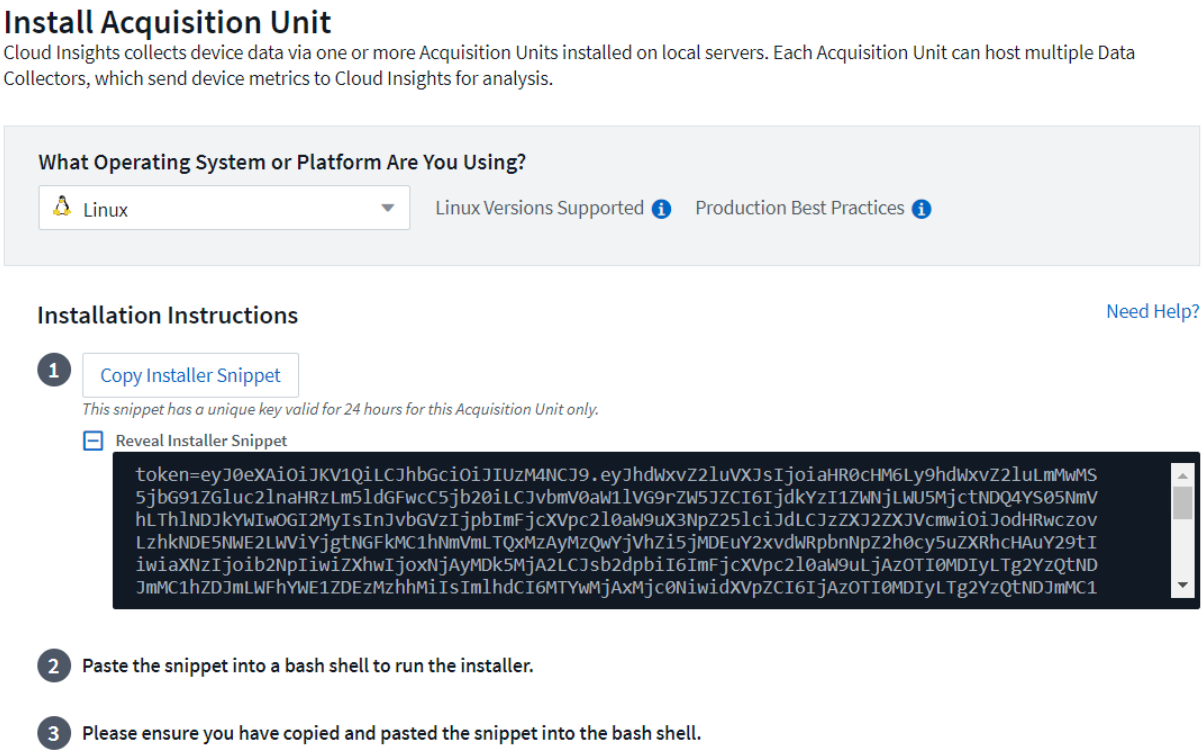


2. En haut au centre de la page collecteurs de données, cliquez sur le lien unités d'acquisition.

3. Pour créer une nouvelle unité d'acquisition, cliquez sur le bouton à droite.

4. Sélectionnez le système d'exploitation que vous souhaitez utiliser pour héberger votre unité d'acquisition et suivez les étapes pour copier le script d'installation à partir de la page Web.

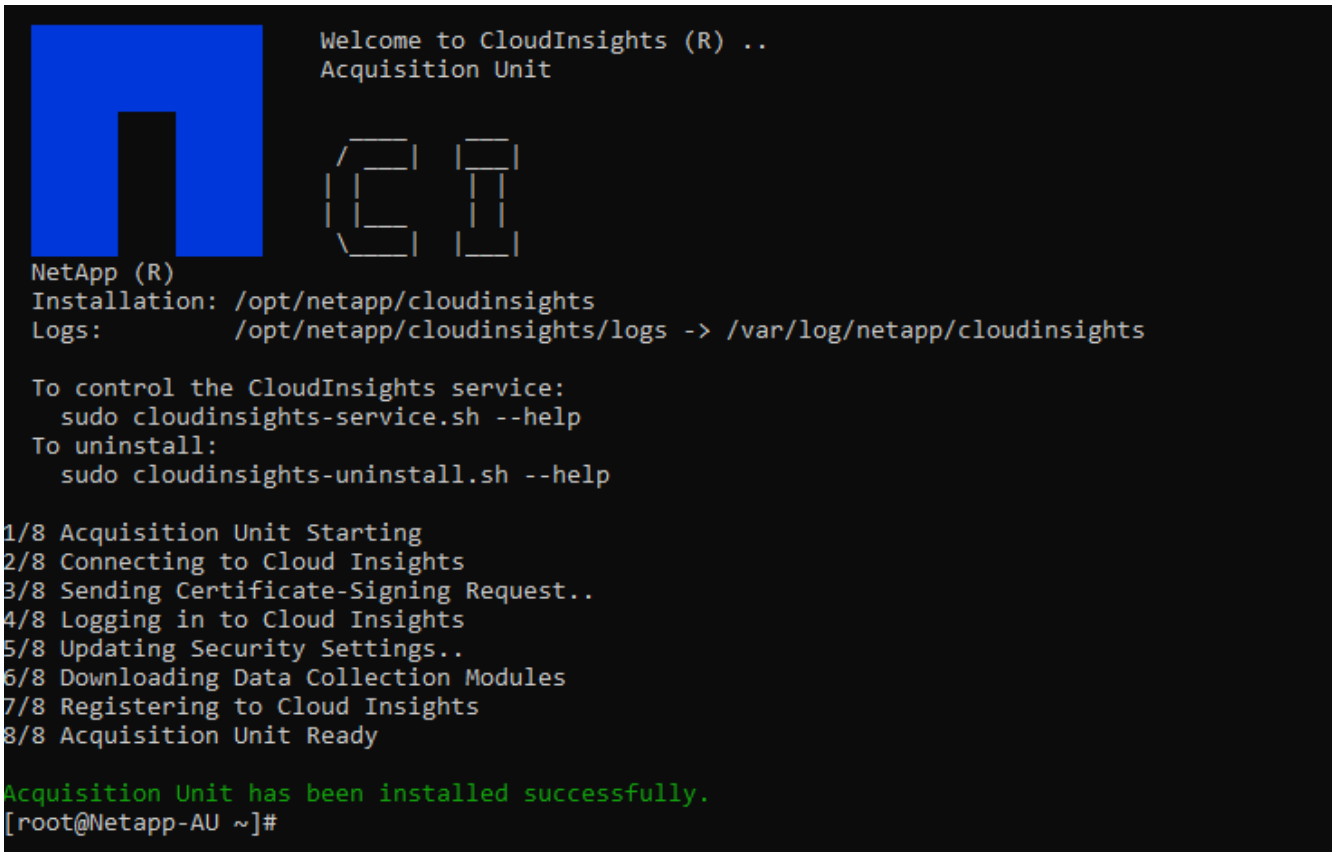
   Dans cet exemple, il s'agit d'un serveur Linux, qui fournit un fragment et un jeton à coller dans la CLI de notre hôte. La page Web attend que l'unité d'acquisition se connecte.



5. Collez le fragment dans la CLI de la machine Red Hat Enterprise Linux qui a été provisionnée, puis cliquez sur entrée.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

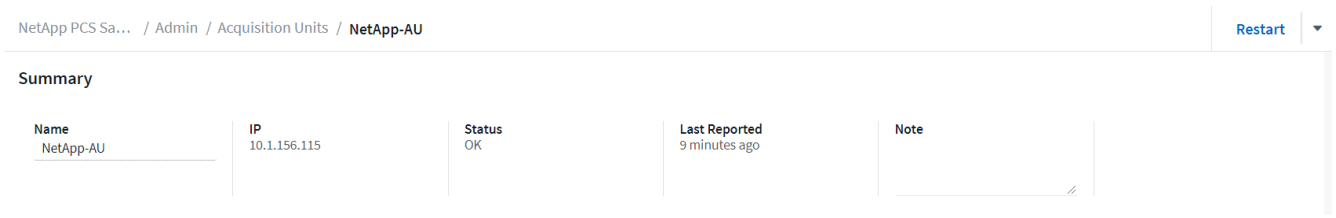
Le programme d'installation télécharge un package compressé et commence l'installation. Une fois l'installation terminée, vous recevez un message indiquant que l'unité d'acquisition a été enregistrée auprès de NetApp Cloud Insights.



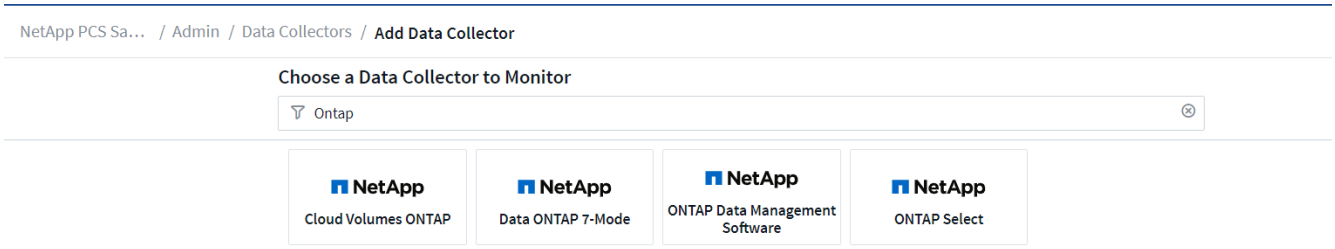
Ajoutez le système de stockage surveillé du data Center FlexPod à Cloud Insights

Pour ajouter le système de stockage ONTAP à partir d'un déploiement FlexPod, procédez comme suit :

1. Revenez à la page unités d'acquisition sur le portail Cloud Insights et recherchez l'unité nouvellement enregistrée. Pour afficher un résumé de l'unité, cliquez sur l'unité.

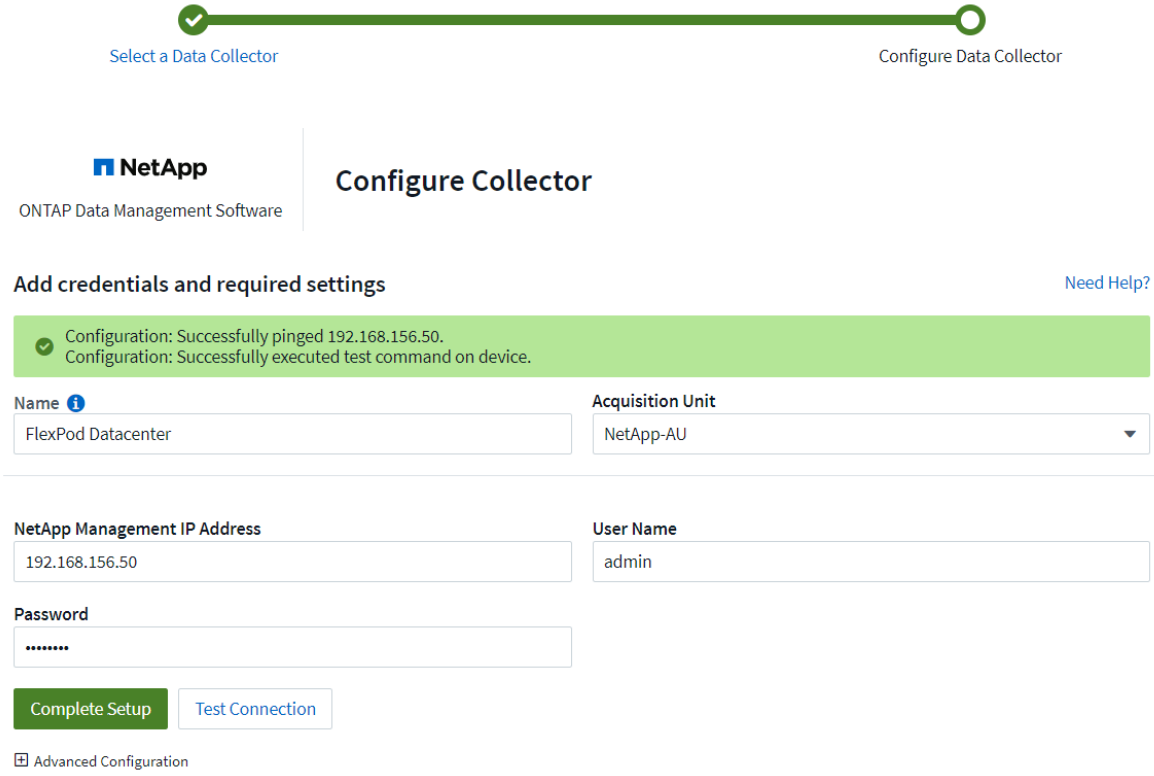


2. Pour démarrer un assistant pour ajouter le système de stockage, sur la page Résumé, cliquez sur le bouton de création d'un collecteur de données. La première page affiche tous les systèmes à partir desquels les données peuvent être collectées. Utilisez la barre de recherche pour rechercher ONTAP.



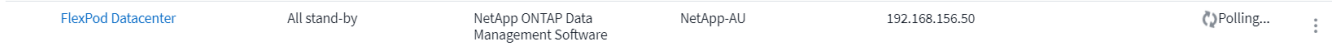
3. Sélectionnez logiciel de gestion des données ONTAP.

   Une page s'affiche pour vous permettre de nommer votre déploiement et de sélectionner l'unité d'acquisition que vous souhaitez utiliser. Vous pouvez fournir les informations d'identification et les informations de connectivité du système ONTAP et tester la connexion pour confirmer.



4. Cliquez sur Terminer la configuration.

   Le portail revient sur la page Data Collectors et le collecteur de données commence son premier sondage pour collecter les données du système de stockage ONTAP dans le FlexPod Datacenter.



Cas d'utilisation

Grâce à l'installation et à la configuration de Cloud Insights, nous FlexPod examinons

certaines des tâches que vous pouvez effectuer sur le tableau de bord afin d'évaluer et de contrôler votre environnement. Dans cette section, nous nous concentrons sur cinq cas d'utilisation principaux de Cloud Insights :

- Intégration avec Active IQ
- Exploration des tableaux de bord en temps réel
- Création de tableaux de bord personnalisés
- Dépannage avancé
- Optimisation du stockage

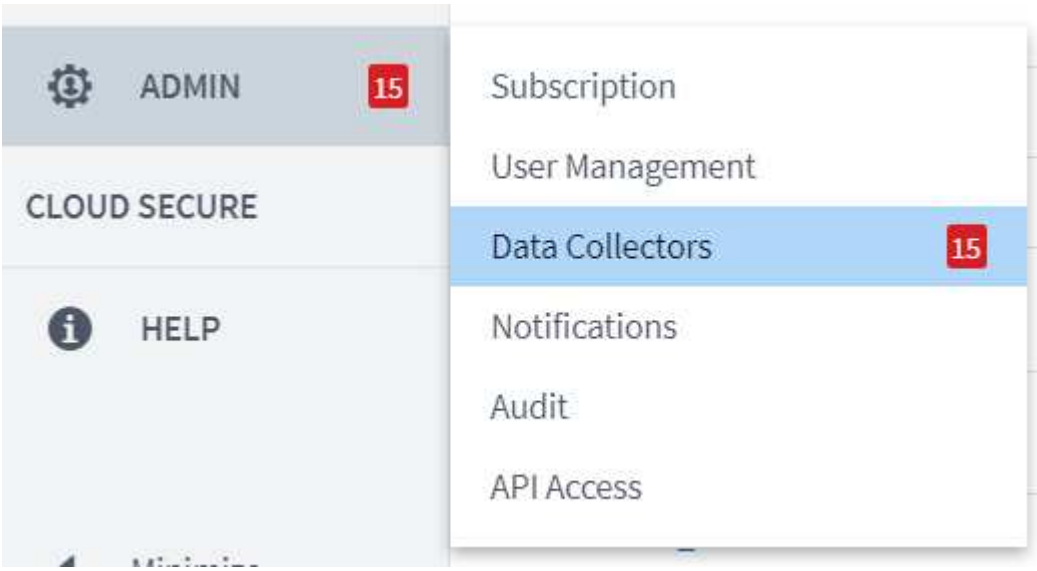
Intégration avec Active IQ

Cloud Insights est totalement intégré à la plateforme de surveillance du stockage Active IQ. Un système ONTAP, déployé dans le cadre d'une solution de data Center FlexPod, est automatiquement configuré pour renvoyer les informations à NetApp via la fonction AutoSupport, qui est intégrée à chaque système. Ces rapports sont générés de manière programmée ou dynamique lorsqu'une panne est détectée dans le système. Les données communiquées via AutoSupport sont agrégées et affichées dans des tableaux de bord facilement accessibles sous le menu Active IQ de Cloud Insights.

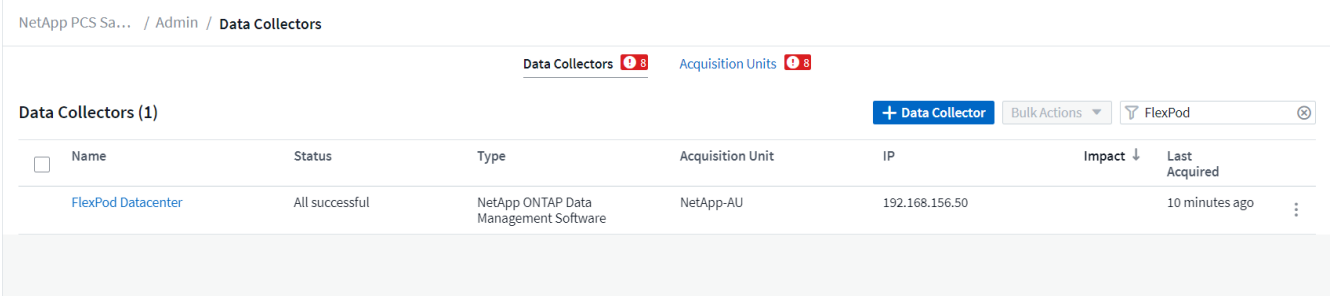
Accédez aux informations Active IQ via le tableau de bord Cloud Insights

Pour accéder aux informations de Active IQ via le tableau de bord Cloud Insights, effectuez les opérations suivantes :

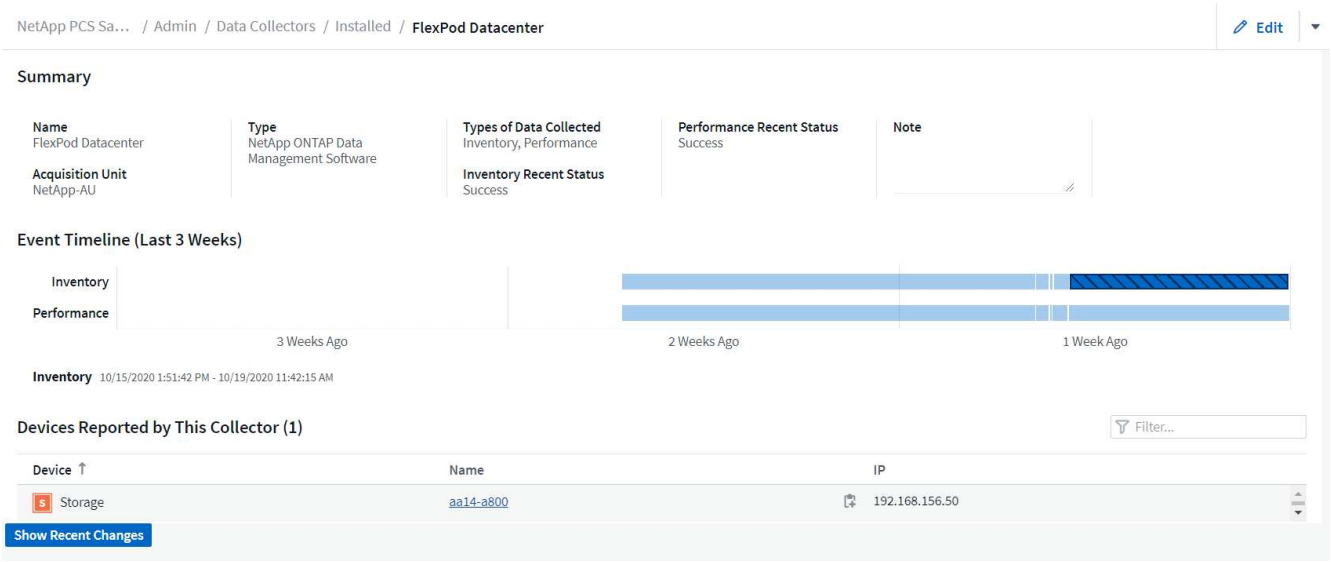
1. Cliquez sur l'option Data Collector dans le menu Admin à gauche.



2. Filtre pour le Data Collector spécifique à votre environnement. Dans cet exemple, nous filtrons par le terme FlexPod.

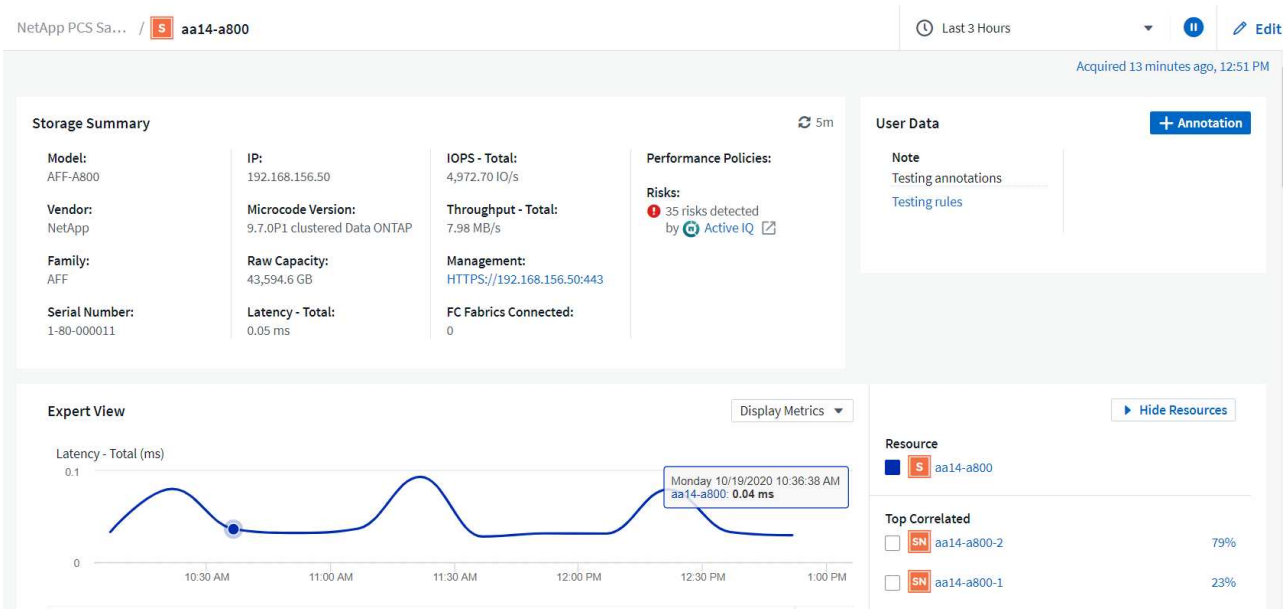


3. Cliquez sur le Data Collector pour obtenir un résumé de l'environnement et des périphériques surveillés par ce collecteur.

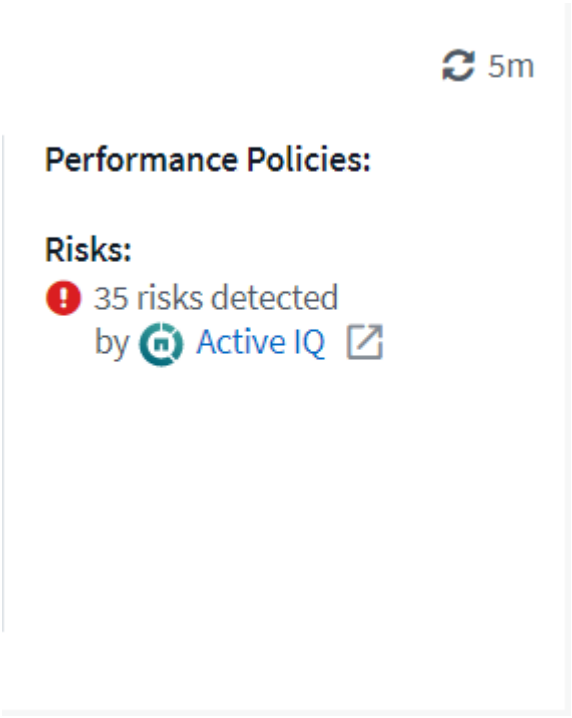


Sous la liste des périphériques en bas, cliquez sur le nom du système de stockage ONTAP surveillé. Un tableau de bord des informations collectées à propos du système s'affiche, avec les informations suivantes :

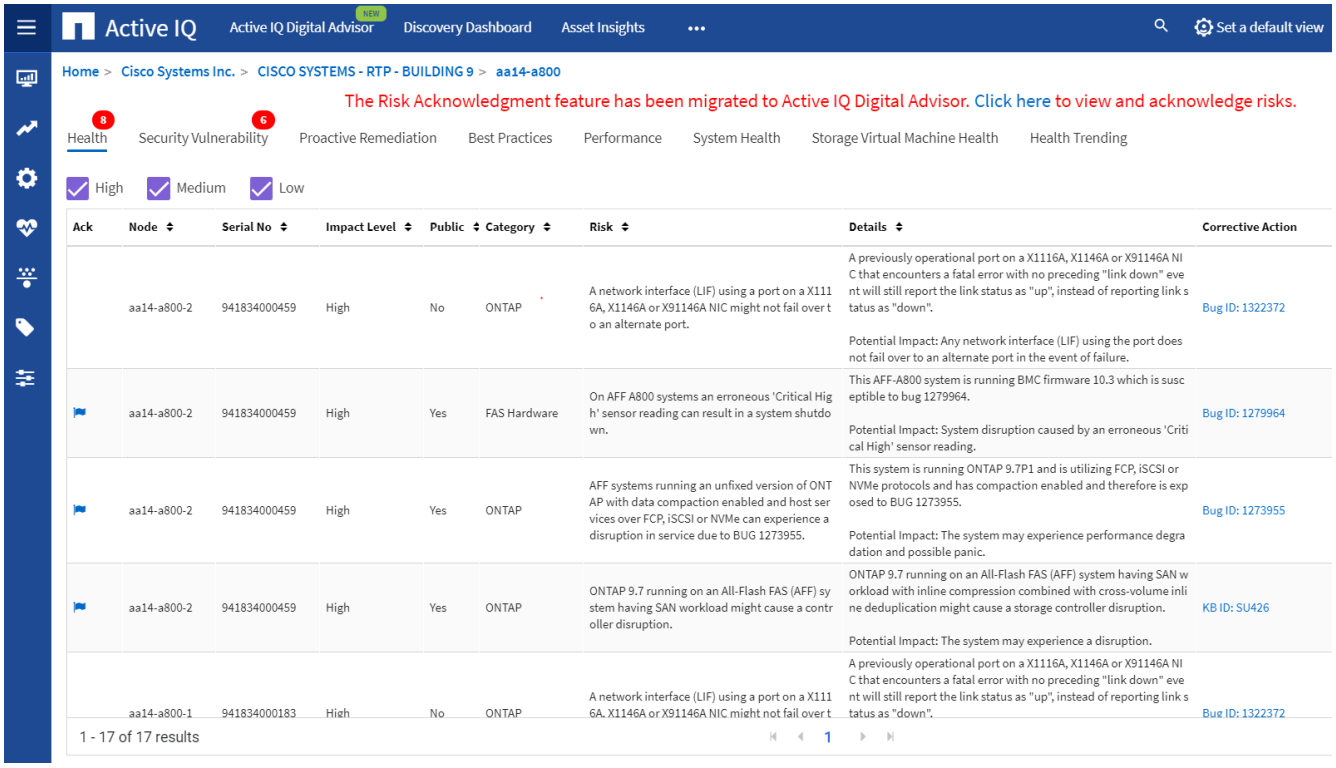
- Modèle
- Famille
- Version ONTAP
- Capacité brute
- IOPS moyennes
- Latence moyenne
- Débit moyen



De plus, sur cette page, sous la section politiques de performances, vous trouverez un lien vers NetApp Active IQ.



4. Pour ouvrir un nouvel onglet de navigateur et accéder à la page de réduction des risques, qui affiche les nœuds concernés et les risques critiques, et les actions à entreprendre pour corriger les problèmes identifiés, cliquez sur le lien Active IQ.

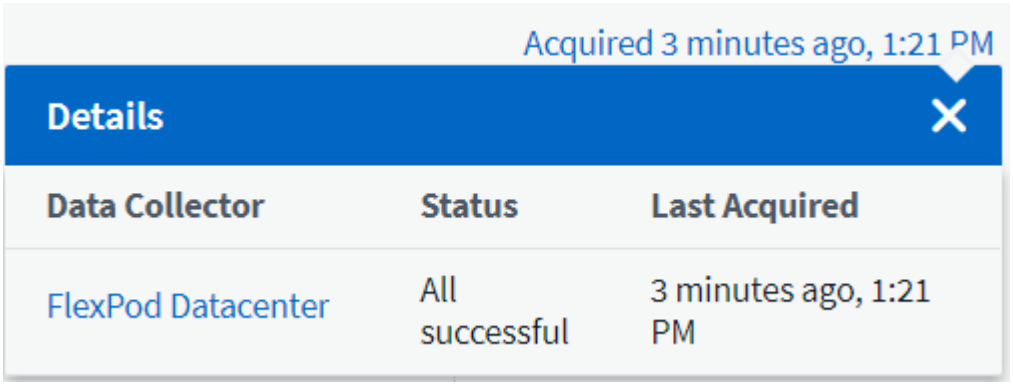


Explorez les tableaux de bord en temps réel

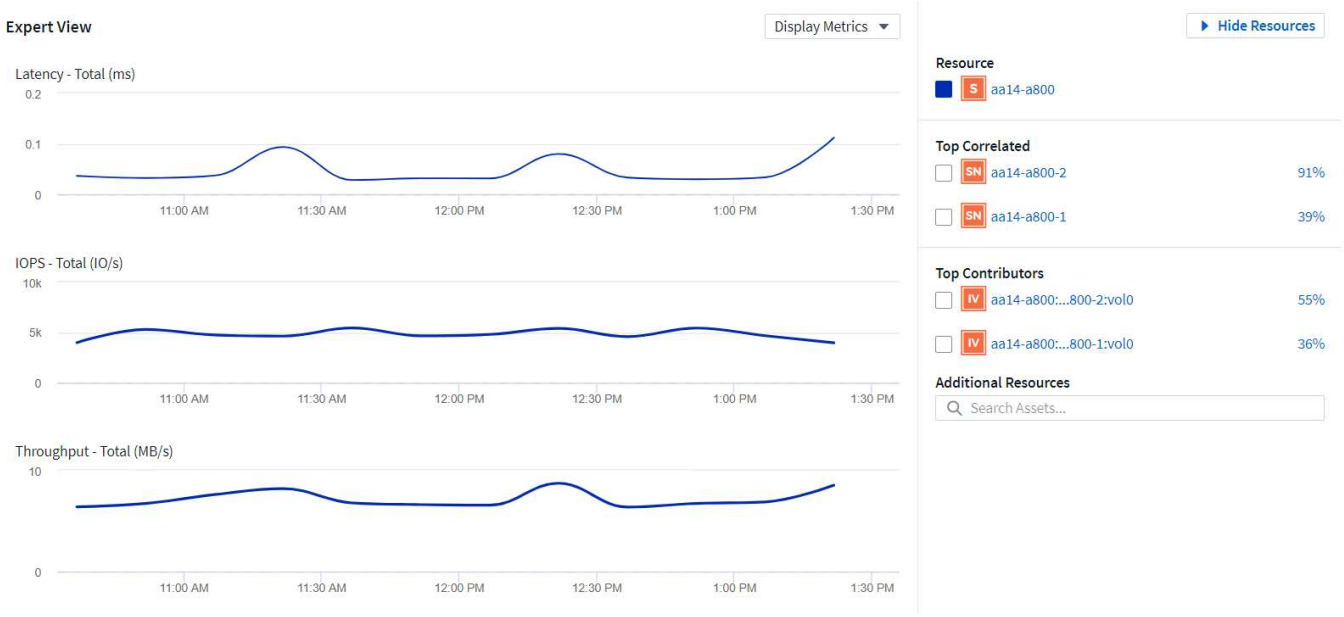
Cloud Insights peut afficher les tableaux de bord en temps réel des informations interrogées à partir du système de stockage ONTAP déployé dans une solution de data Center FlexPod. L'unité d'acquisition Cloud Insights collecte les données à intervalles réguliers et renseigne le tableau de bord du système de stockage par défaut avec les informations collectées.

Accédez aux graphiques en temps réel à partir du tableau de bord Cloud Insights

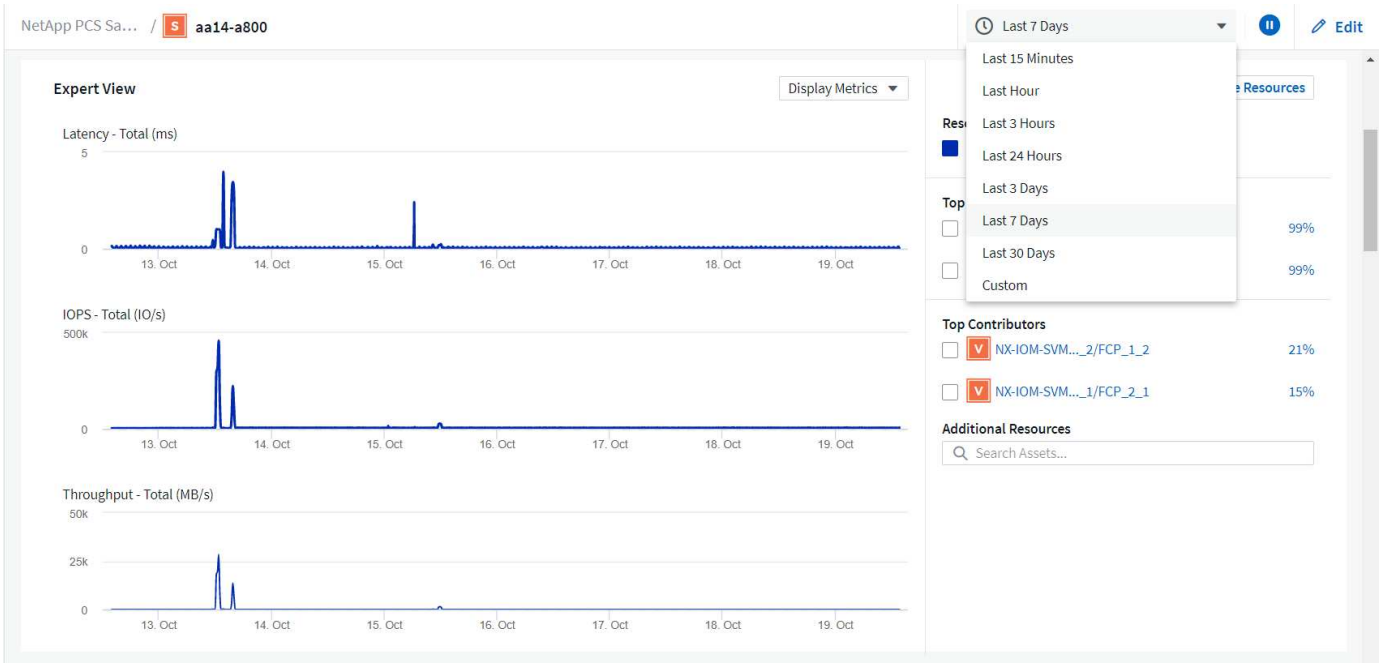
À partir du tableau de bord du système de stockage, vous pouvez voir la dernière mise à jour des informations par le Data Collector. La figure ci-dessous en est un exemple.



Par défaut, le tableau de bord du système de stockage affiche plusieurs graphiques interactifs qui présentent les metrics système de stockage interrogés ou à partir de chaque nœud, notamment la latence, les IOPS et le débit. La figure ci-dessous présente des exemples de ces graphiques par défaut.



Par défaut, les graphiques affichent des informations des trois dernières heures, mais vous pouvez les définir sur un certain nombre de valeurs différentes ou sur une valeur personnalisée dans la liste déroulante située en haut à droite du tableau de bord du système de stockage. Ceci est illustré dans la figure ci-dessous.



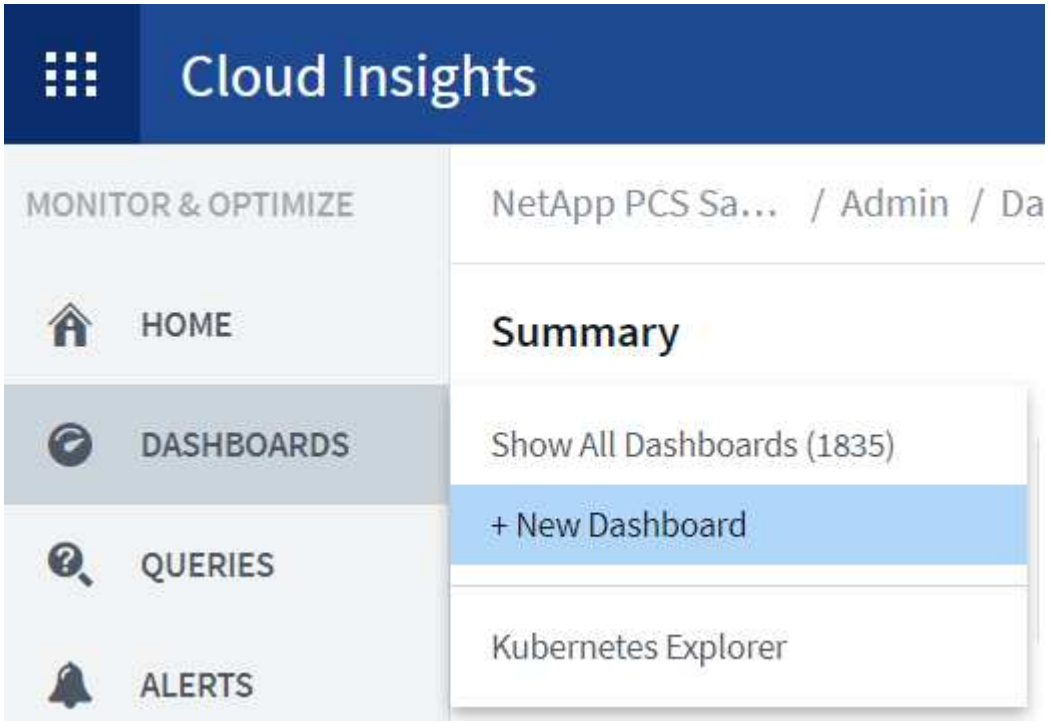
Création de tableaux de bord personnalisés

Outre l'utilisation des tableaux de bord par défaut qui affichent des informations à l'échelle du système, vous pouvez utiliser Cloud Insights pour créer des tableaux de bord entièrement personnalisés qui vous permettent de donner la priorité à l'utilisation des ressources pour des volumes de stockage spécifiques dans la solution FlexPod Datacenter, les applications déployées dans l'infrastructure convergée qui dépendent de ces volumes peuvent donc s'exécuter efficacement. Ainsi, vous pouvez améliorer la visualisation des applications spécifiques et des ressources utilisées dans l'environnement du centre de données.

Création d'un tableau de bord personnalisé pour évaluer les ressources de stockage

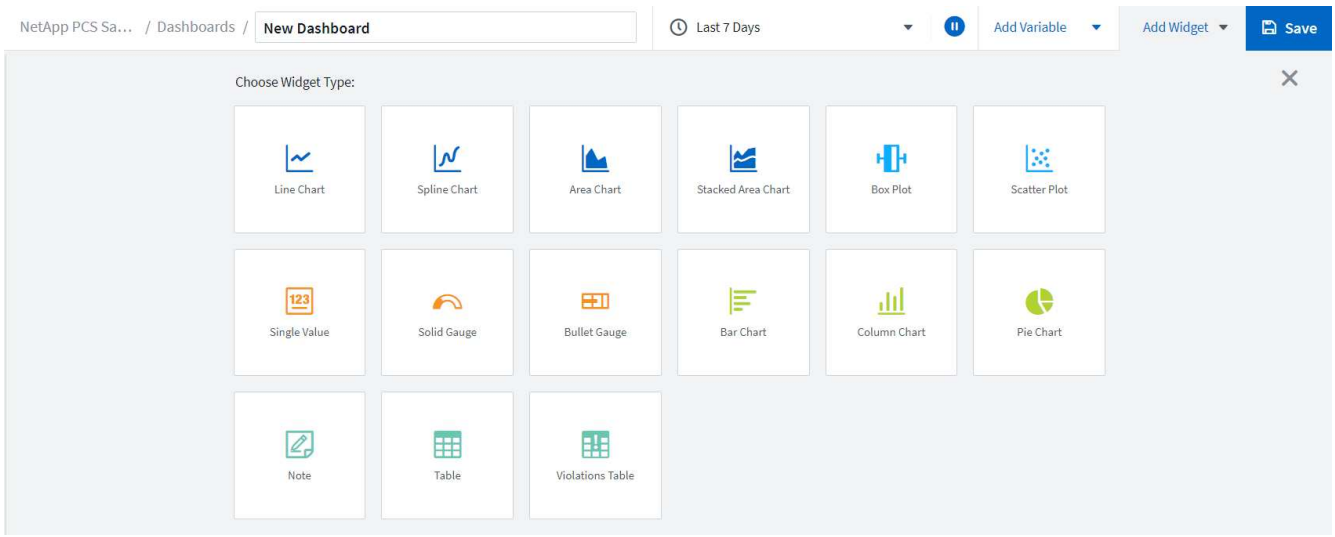
Pour créer un tableau de bord personnalisé afin d'évaluer les ressources de stockage, effectuez les opérations suivantes :

1. Pour créer un tableau de bord personnalisé, placez le pointeur de la souris sur tableaux de bord dans le menu principal de Cloud Insights, puis cliquez sur + Nouveau tableau de bord dans la liste déroulante.



   La fenêtre Nouveau tableau de bord s'ouvre.

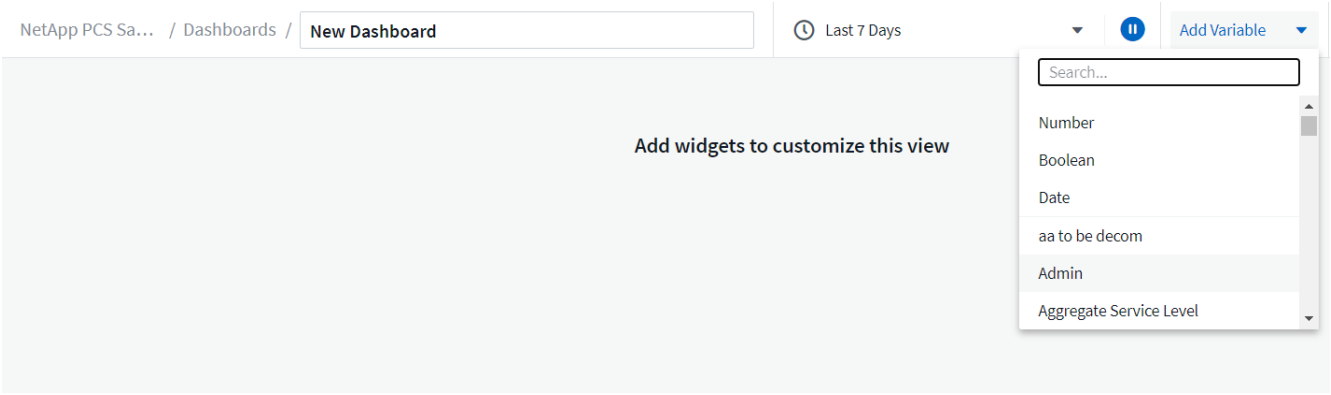
2. Nommez le tableau de bord et sélectionnez le type de widget utilisé pour afficher les données. Vous pouvez choisir parmi un certain nombre de types de graphique, même des notes ou des types de table pour présenter les données collectées.



3. Choisissez des variables personnalisées dans le menu Ajouter une variable.

   Cela permet de concentrer les données présentées pour afficher des facteurs plus spécifiques ou plus

spécialisés.



4. Pour créer un tableau de bord personnalisé, sélectionnez le type de widget que vous souhaitez utiliser, par exemple, un graphique à secteurs pour afficher l'utilisation du stockage par volume :

   a. Sélectionnez le widget Pie Chart dans la liste déroulante Ajouter un widget.

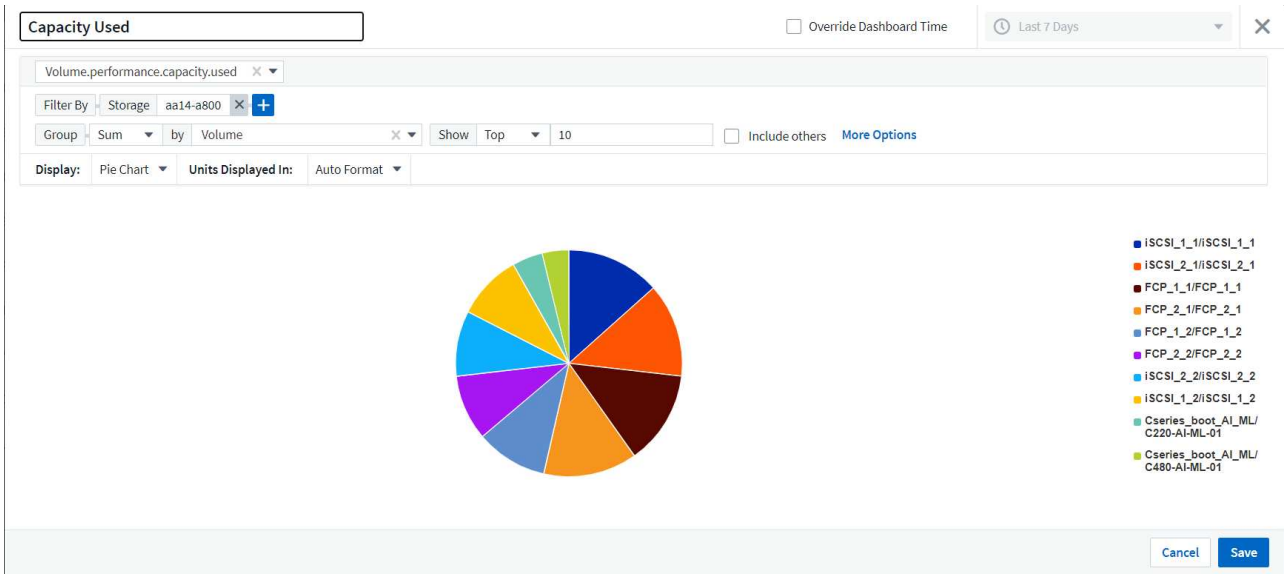
   b. Nommez le widget avec un identificateur descriptif, tel que `Capacity Used`.

   c. Sélectionnez l'objet à afficher. Par exemple, vous pouvez effectuer une recherche à l'aide de la touche terme volume et sélectionner `volume.performance.capacity.used`.

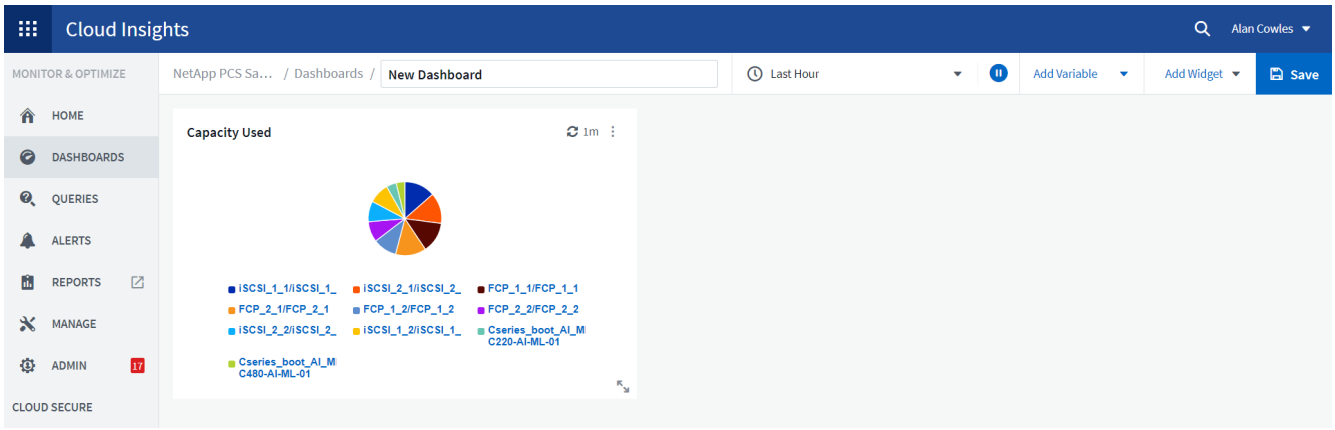
   d. Pour les filtrer par système de stockage, utilisez le filtre et tapez le nom du système de stockage de la solution FlexPod Datacenter.

   e. Personnalisez les informations à afficher. Par défaut, cette sélection affiche les volumes de données ONTAP et liste les 10 premiers.

   f. Pour enregistrer le tableau de bord personnalisé, cliquez sur Enregistrer.



   Après avoir enregistré le widget personnalisé, le navigateur retourne à la page Nouveau tableau de bord, où il affiche le widget nouvellement créé et permet de réaliser une action interactive, telle que la modification de la période d'interrogation des données.



Dépannage avancé

Cloud Insights permet d'appliquer des méthodes avancées de dépannage à n'importe quel environnement de stockage d'une infrastructure convergée FlexPod Datacenter. À l'aide des composants de chacune des fonctionnalités mentionnées ci-dessus : intégration d'Active IQ, tableaux de bord par défaut avec statistiques en temps réel et tableaux de bord personnalisés, les problèmes susceptibles d'apparaître sont détectés rapidement et résolus. Grâce à la liste des risques dans Active IQ, un client peut trouver des erreurs de configuration signalées qui pourraient entraîner un problème ou la détection de bogues qui ont été signalés et corrigés des versions de code, ce qui peut les résoudre. Les tableaux de bord en temps réel sur la page d'accueil de Cloud Insights permettent d'identifier des modèles de performances système qui pourraient être un indicateur précoce d'un problème en hausse et aider à le résoudre rapidement. Enfin, la possibilité de créer des tableaux de bord personnalisés permet aux clients de se concentrer sur les ressources les plus importantes de leur infrastructure et de les surveiller directement pour assurer la continuité de leurs objectifs.

Optimisation du stockage

Outre la résolution de problèmes, Cloud Insights peut utiliser les données collectées pour optimiser le système de stockage ONTAP déployé dans une solution d'infrastructure convergée FlexPod Datacenter. Si un volume présente une latence élevée, peut-être parce que plusieurs ordinateurs virtuels exigeant des performances élevées partagent le même datastore, ces informations sont affichées dans le tableau de bord de Cloud Insights. Avec ces informations, l'administrateur de stockage peut choisir de migrer un ou plusieurs VM vers d'autres volumes, de migrer des volumes de stockage entre les niveaux d'agrégats ou entre les nœuds du système de stockage ONTAP, pour obtenir un environnement optimisé pour les performances. Les informations fournies par l'intégration de Active IQ à Cloud Insights permettent de mettre en évidence les problèmes de configuration qui entraînent des performances supérieures aux prévisions et de proposer les actions correctives recommandées qui, si elles sont mises en œuvre, peuvent résoudre les problèmes et garantir un système de stockage parfaitement réglé.

Vidéos et démonstrations

Vous pouvez voir une démonstration vidéo de l'utilisation de NetApp Cloud Insights pour évaluer les ressources d'un environnement sur site "ici".

Vous pouvez voir une démonstration vidéo de l'utilisation de NetApp Cloud Insights pour surveiller l'infrastructure et définir des seuils d'alerte pour l'infrastructure "ici".

Vous pouvez voir une démonstration vidéo de l'utilisation de NetApp Cloud Insights pour évaluer les applications individuelles dans l'environnement "ici".

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce document, consultez les sites web suivants :

- Documentation des produits Cisco

  "https://www.cisco.com/c/en/us/support/index.html"

- Data Center FlexPod

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- Documentation produit NetApp

  "https://docs.netapp.com"

FlexPod avec FabricPool : Tiering des données inactives vers Amazon AWS S3

Tr-4801 : FlexPod avec FabricPool - Tiering des données inactives vers Amazon AWS S3

Scott Kovacs, NetApp

Les prix du stockage Flash continuent de baisser, ce qui est désormais disponible pour les charges de travail et les applications qui n'étaient pas considérées comme des candidats auparavant pour le stockage Flash. Toutefois, l'utilisation la plus efficace de l'investissement de stockage est encore cruciale pour les responsables INFORMATIQUES. Le service IT reste contraintes de fournir des services plus performants avec peu ou pas d'augmentation budgétaire. En réponse à ces besoins, NetApp FabricPool vous permet d'exploiter les économies du cloud en transférant les données peu utilisées hors de votre stockage Flash sur site, cher, vers un Tier de stockage plus économique dans le cloud public. Le transfert des données peu utilisées vers le cloud libère un espace de stockage Flash précieux sur les systèmes AFF ou FAS, ce qui permet d'obtenir davantage de capacité pour les workloads stratégiques vers le Tier Flash haute performance.

Dans ce rapport technique, nous passons en revue la fonctionnalité de Tiering des données FabricPool de NetApp ONTAP dans le cadre d'une architecture d'infrastructure convergée FlexPod de NetApp et Cisco. Vous devez maîtriser l'architecture d'infrastructure convergée FlexPod Datacenter et le logiciel de stockage ONTAP pour exploiter pleinement les concepts abordés dans ce rapport technique. Connaissant bien FlexPod et ONTAP, nous présentons le FabricPool, son fonctionnement et la façon dont il peut être utilisé pour une utilisation plus efficace du stockage Flash sur site. Une grande partie du contenu de ce rapport est abordée de manière plus détaillée dans le "Tr-4598 meilleures pratiques de FabricPool" Et documentation des produits ONTAP. Le contenu a été condensé pour une infrastructure FlexPod et ne couvre pas tous les cas d'utilisation

de FabricPool. Toutes les fonctionnalités et concepts abordés sont disponibles dans ONTAP 9.6.

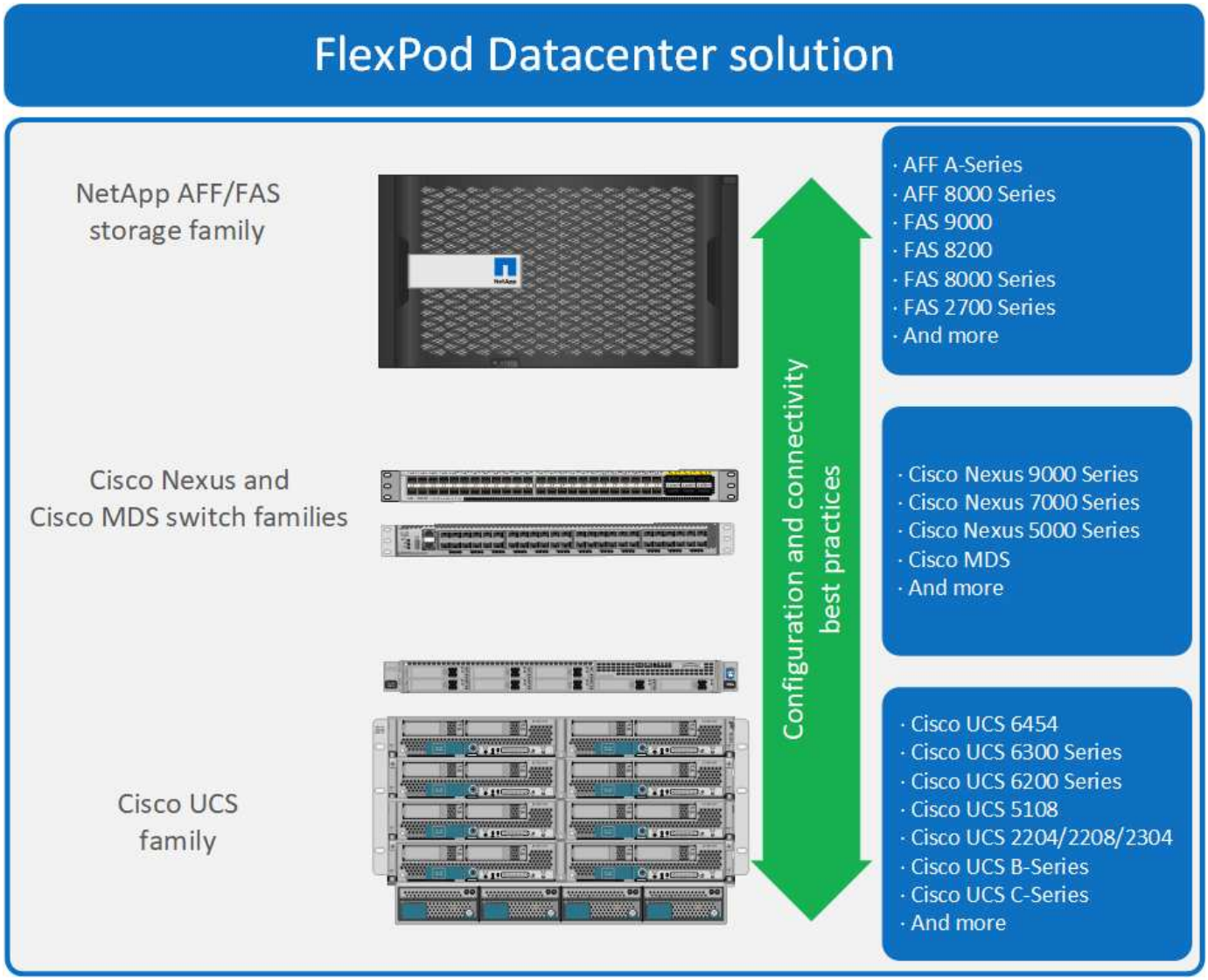
Pour plus d'informations sur FlexPod, consultez le "Tr-4036 spécifications techniques du data Center FlexPod".

Présentation et architecture de FlexPod

Présentation de FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp AFF, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS, Cisco Unified Computing System (Cisco UCS) et le logiciel VMware vSphere dans une seule offre. La conception est suffisamment flexible pour que les réseaux, l'informatique et le stockage s'adaptent à un seul rack de data Center ou puissent être déployés selon la conception du data Center du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

L'un des avantages de l'architecture FlexPod est la possibilité de personnaliser l'environnement en fonction des exigences du client. Une unité FlexPod peut facilement évoluer en fonction des besoins et de la demande. Une unité peut évoluer verticalement (ajout de ressources à une unité FlexPod) et horizontalement (ajout d'unités FlexPod). L'architecture de référence FlexPod met en avant la résilience, les avantages financiers et la facilité de déploiement d'une solution de stockage Fibre Channel et IP. Un système de stockage capable de prendre en charge plusieurs protocoles sur une interface unique offre aux clients le choix et protège leur investissement, car il s'agit d'une architecture à une seule étape. La figure suivante montre de nombreux composants matériels de FlexPod.

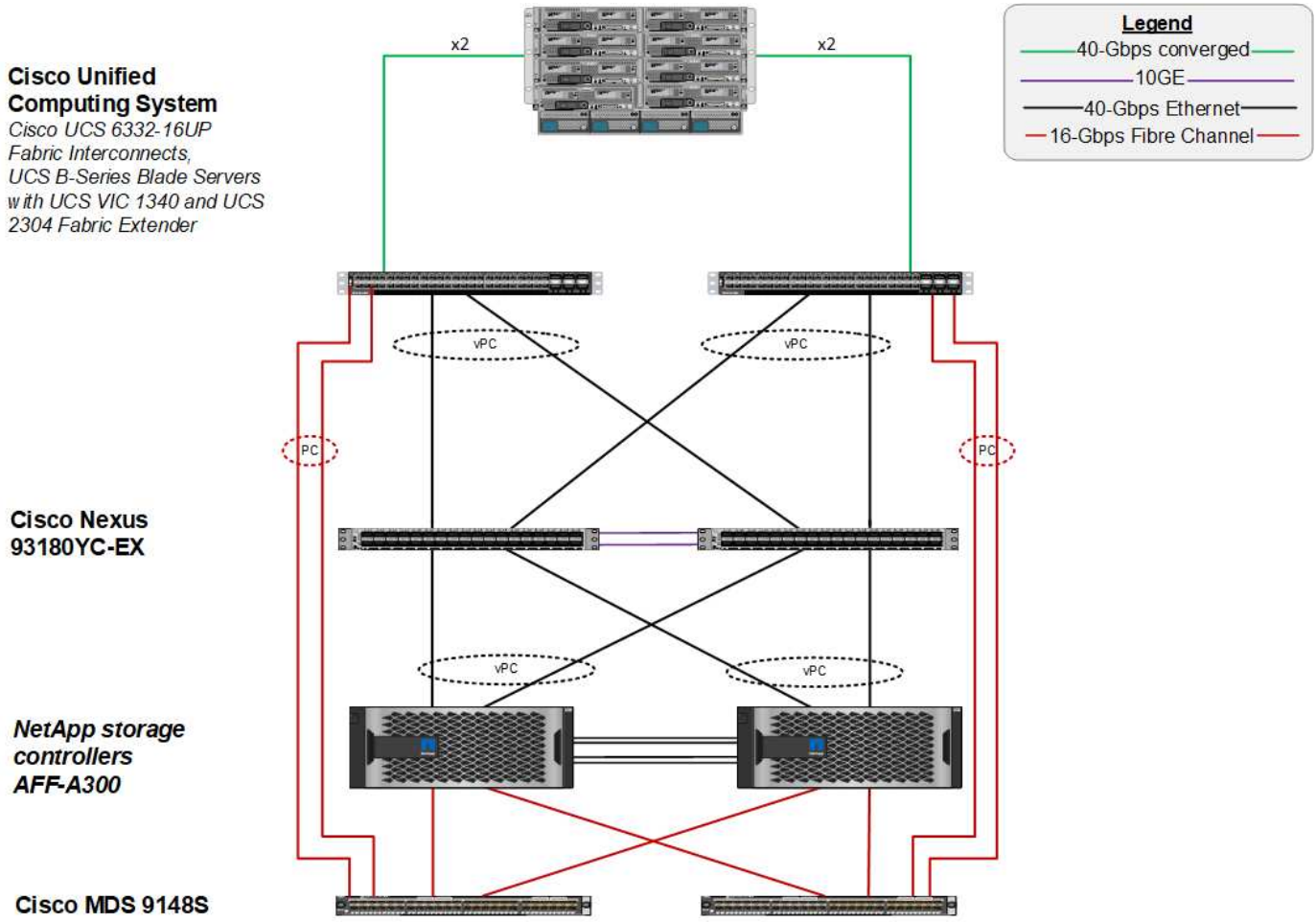


Architecture FlexPod

La figure suivante montre les composants d'une solution VMware vSphere et FlexPod, ainsi que les connexions réseau nécessaires aux interconnexions de fabric Cisco UCS 6454. Cette conception comprend les composants suivants :

- Des connexions Ethernet 40 Gb canalisées entre le châssis lame Cisco UCS 5108 et les interconnexions de fabric Cisco UCS
- Connexions Ethernet de 40 Go entre l'interconnexion de fabric Cisco UCS et le commutateur Cisco Nexus 9000
- Connexions Ethernet de 40 Go entre Cisco Nesxus 9000 et la baie de stockage NetApp AFF A300

Ces options d'infrastructure sont étendues avec l'introduction de commutateurs Cisco MDS entre le Fabric Interconnect Cisco UCS et le système NetApp AFF A300. Cette configuration fournit des hôtes FC démarrés avec un accès FC 16 Gb au niveau des blocs au stockage partagé. L'architecture de référence renforce la stratégie à un seul réseau. En effet, lors de l'ajout de stockage à l'architecture, aucune désactivation n'est requise entre les hôtes et le Fabric Interconnect Cisco UCS.



FabricPool

Présentation de FabricPool

FabricPool est une solution de stockage hybride dans ONTAP qui utilise un agrégat 100 % Flash (SSD) comme Tier de performance et un magasin d'objets dans un service de cloud public en tant que Tier cloud. Cette configuration permet le déplacement des données basé sur des règles, en fonction de l'accès fréquent ou non aux données. FabricPool est pris en charge dans ONTAP pour les agrégats AFF et 100 % SSD sur les plateformes FAS. Le traitement des données est effectué au niveau des blocs, dans la mesure où les blocs de données sont fréquemment utilisés dans le Tier de performance 100 % Flash et où les blocs fortement sollicités sont balisés comme inactives.

FabricPool permet de réduire les coûts de stockage sans nuire aux performances, à l'efficacité, à la sécurité ou à la protection. FabricPool est transparent pour les applications d'entreprise et capitalise sur l'efficacité du cloud en réduisant le TCO du stockage sans devoir repenser l'architecture de l'infrastructure applicative.

FlexPod bénéficie des fonctionnalités de hiérarchisation du stockage de FabricPool pour une utilisation plus efficace du stockage Flash ONTAP. Les machines virtuelles inactives, les modèles de machine virtuelle peu utilisés et les sauvegardes des machines virtuelles depuis NetApp SnapCenter pour vSphere peuvent consommer un espace précieux dans le volume du datastore. Le déplacement des données inactives vers le Tier cloud libère de l'espace et des ressources pour les applications stratégiques haute performance hébergées sur l'infrastructure FlexPod.

Les protocoles Fibre Channel et iSCSI prennent généralement plus de temps avant que le délai d'attente ne soit dépassé (60 à 120 secondes), mais ils ne tentatives pas d'établir de connexion de la même manière que les protocoles NAS. Si un protocole SAN est à court de temps, l'application doit être redémarrée. Même une courte interruption peut avoir des conséquences désastreuses pour les applications de production grâce aux protocoles SAN, car il n'existe pas de moyen de garantir la connectivité aux clouds publics. Pour éviter ce problème, NetApp recommande d'utiliser des clouds privés pour le Tiering des données accessibles par les protocoles SAN.

Dans ONTAP 9.6, FabricPool s'intègre avec tous les principaux fournisseurs de cloud public : Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage et Microsoft Azure Blob Storage. Ce rapport est axé sur le stockage Amazon AWS S3 en tant que Tier objet cloud de votre choix.

L'agrégat composite

Une instance FabricPool est créée en associant un agrégat Flash ONTAP à un magasin d'objets cloud, par exemple un compartiment AWS S3, afin de créer un agrégat composite. Lorsque les volumes sont créés dans l'agrégat composite, ils peuvent bénéficier des fonctionnalités de Tiering de FabricPool. Lorsque les données sont écrites sur le volume, ONTAP attribue une température à chacun des blocs de données. Lors de la première écriture du bloc, une température de stockage est affectée. Lorsque le temps passe, si les données ne sont pas utilisées, elles sont soumises à un processus de refroidissement jusqu'à ce qu'elles soient finalement attribuées à l'état froid. Ces blocs de données peu utilisés sont ensuite hiérarchisés à partir de l'agrégat SSD de performance et vers le magasin d'objets cloud.

Période entre le moment où un bloc est désigné comme étant froid et le moment où il est transféré vers le stockage objet cloud par la règle de Tiering des volumes dans ONTAP. Une granularité supérieure est obtenue en modifiant les paramètres de ONTAP qui contrôlent le nombre de jours nécessaires à la mise à froid d'un bloc. Ils peuvent également être utilisés pour le Tiering des données : snapshots de volume traditionnels, sauvegardes de machine virtuelle SnapCenter pour vSphere et autres sauvegardes NetApp Snapshot, blocs peu utilisés dans un datastore vSphere, modèles de machine virtuelle et données de machine virtuelle rarement utilisées.

Reporting des données inactives

Le reporting pour les données inactives est disponible dans ONTAP pour vous aider à évaluer la quantité de données inactives pouvant être hiérarchisées à partir d'un agrégat. L'IDR est activé par défaut dans ONTAP 9.6 et utilise une stratégie de refroidissement de 31 jours par défaut pour déterminer quelles données du volume sont inactives.

La quantité de données inactives dans le Tier dépend des règles de Tiering définies sur le volume. Cette quantité peut être différente de la quantité de données inactives détectée par l'IDR au moyen de la période de refroidissement par défaut de 31 jours.

La création d'objets et le déplacement des données

FabricPool fonctionne au niveau bloc NetApp WAFL, les blocs de refroidissement, les concaténer en objets de stockage et les migrer vers un Tier cloud. Chaque objet FabricPool est de 4 Mo et comprend 1,024 blocs de 4 Ko. La taille d'objet est fixée à 4 Mo en fonction des recommandations de performances des principaux fournisseurs cloud, et ne peut pas être modifiée. Si les blocs inactifs sont lus et mis à chaud, seuls les blocs requis de l'objet 4 Mo sont récupérés et transférés vers le Tier de performance Ni l'objet dans son intégralité, ni le fichier ne sont migrés à nouveau. Seuls les blocs nécessaires sont migrés.

Si ONTAP détecte une opportunité pour les lectures séquentielles, il demande des blocs à partir du Tier cloud avant leur lecture pour améliorer les performances.

Par défaut, les données ne sont déplacées vers le Tier cloud que lorsque l'agrégat de performances est supérieur à 50 % utilisé. Ce seuil peut être défini sur un pourcentage inférieur pour permettre le transfert d'une quantité réduite de stockage des données dans le Tier Flash de performance vers le cloud. Cette possibilité peut être utile si la stratégie de Tiering consiste à transférer les données inactives uniquement lorsque l'agrégat approche de la capacité.

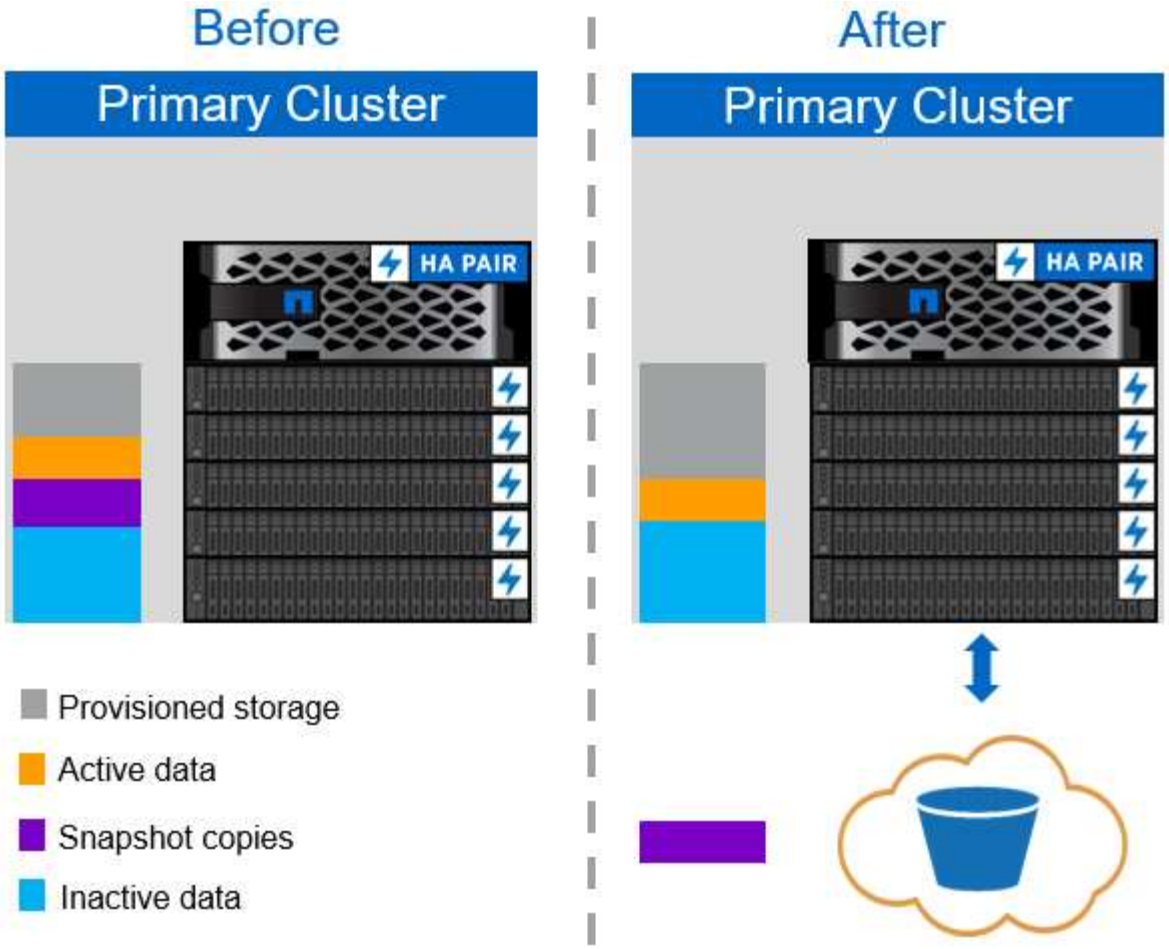
Si l'utilisation du Tier de performance dépasse les 70 % de capacité, les données inactives sont lues directement depuis le Tier cloud sans être écrites à nouveau sur le Tier de performance. En empêchant la rétro-écriture des données inactives sur les agrégats largement utilisés, FabricPool préserve l'agrégat pour les données actives.

Récupération de l'espace de Tier de performance

Comme mentionné précédemment, l'utilisation principale de FabricPool est de faciliter l'utilisation la plus efficace du stockage Flash sur site haute performance. Les données inactives sous forme de snapshots de volume et de sauvegardes de machines virtuelles au sein de l'infrastructure virtuelle FlexPod peuvent occuper une quantité significative de stockage Flash coûteux. Pour libérer les fonctionnalités de stockage au niveau de la performance, deux règles de Tiering sont disponibles : Snapshot uniquement ou Auto.

Règle de Tiering uniquement Snapshot

La règle de Tiering uniquement Snapshot, illustrée dans la figure suivante, déplace les données Snapshot des volumes inactives et les sauvegardes SnapCenter pour vSphere des machines virtuelles qui occupent de l'espace, mais qui ne partagent pas les blocs avec le système de fichiers actif dans un magasin d'objets cloud. La règle de Tiering uniquement pour Snapshot déplace les blocs de données inactives vers le Tier cloud. Pour restaurer les données, les blocs à froid dans le cloud sont fortement sollicités et sont déplacés vers le Tier de performance Flash sur site.

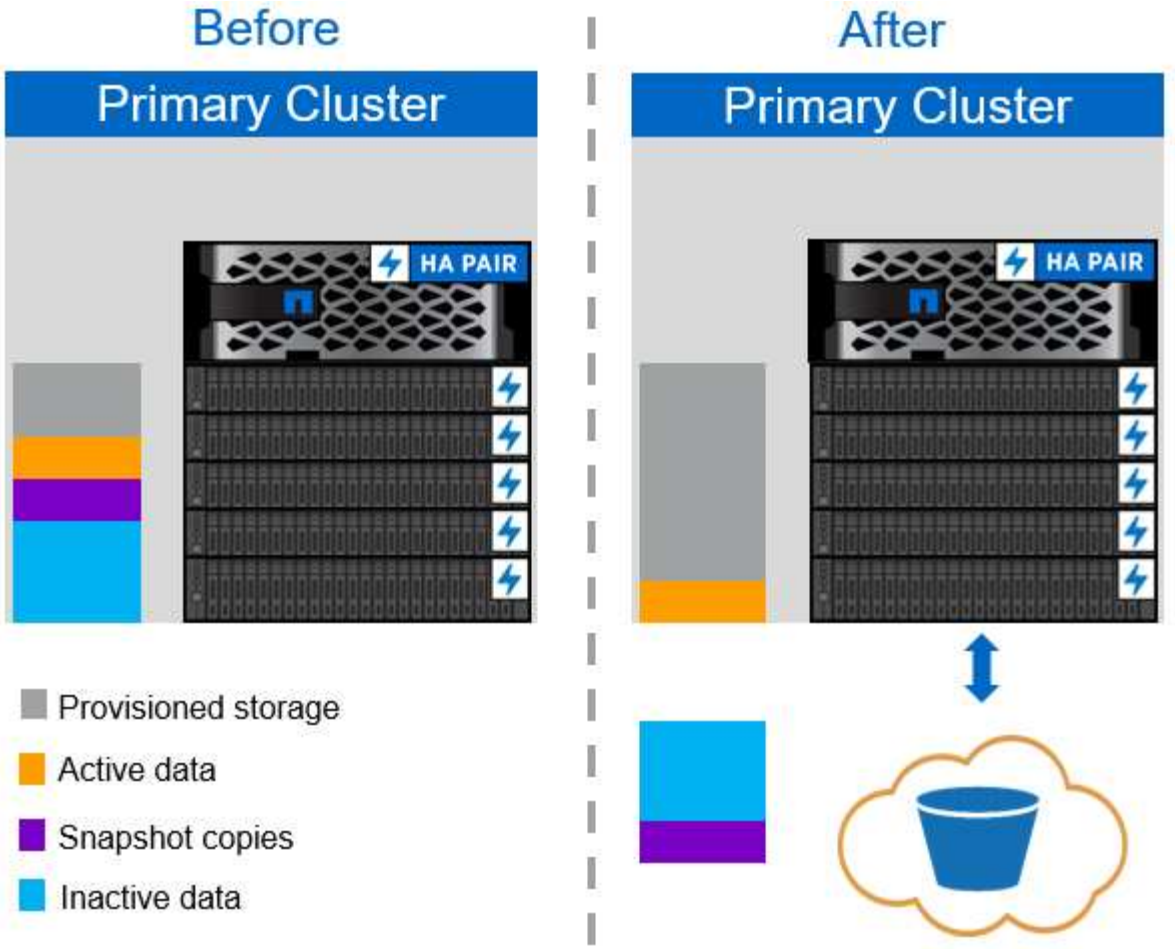


Règle de hiérarchisation automatique

La règle de hiérarchisation automatique du stockage FabricPool, illustrée dans la figure suivante, déplace non seulement les blocs de données des snapshots inactifs vers le cloud, mais déplace également les blocs de données inactives du système de fichiers actif. Cela peut inclure les modèles de VM et toutes les données de VM inutilisées dans le volume du datastore. Les blocs froids déplacés sont contrôlés par le `tiering-minimum-cooling-days` réglage du volume. Si les blocs inactifs du Tier cloud sont lus de manière aléatoire par une application, les blocs fortement sollicités sont alors retransférés vers le Tier de performance. Toutefois, si les blocs inactifs sont lus par un processus séquentiel tel qu'un antivirus, les blocs restent inactifs et restent conservés dans le magasin d'objets cloud. Ils ne sont pas déplacés vers le Tier de performance.

Lors de l'utilisation de la règle de Tiering automatique, les blocs fréquemment utilisés sont retirés du Tier cloud au débit de la connectivité cloud. Cela peut affecter les performances des machines virtuelles si l'application est sensible à la latence, qui doit être prise en compte avant d'utiliser la règle de hiérarchisation automatique sur le datastore. NetApp recommande de placer les LIFs intercluster sur des ports présentant une vitesse de 10GbE pour des performances adéquates.

Le profileur de magasin d'objets doit être utilisé pour tester la latence et le débit vers le magasin d'objets avant de le rattacher à un agrégat FabricPool.



Toutes les règles de Tiering

À la différence des règles Auto et Snapshot uniquement, toutes les règles de Tiering déplacent immédiatement des volumes entiers de données vers le Tier cloud. Cette règle convient mieux aux volumes secondaires de protection des données ou d'archivage pour lesquels les données doivent être conservées à des fins historiques ou réglementaires, mais peu utilisées. La règle All n'est pas recommandée pour les volumes du datastore VMware car les données écrites sur le datastore sont immédiatement déplacées vers le niveau cloud. Les opérations de lecture suivantes sont effectuées depuis le cloud et peuvent éventuellement introduire des problèmes de performances pour les machines virtuelles et les applications qui résident dans le volume du datastore.

Sécurité

La sécurité est une préoccupation majeure pour le cloud et pour FabricPool. Toutes les fonctions de sécurité natives d'ONTAP sont prises en charge dans le Tier de performance, et le déplacement des données est sécurisé lors de leur transfert vers le Tier cloud. FabricPool utilise le "AES-256-GCM" algorithme de chiffrement sur le tier de performance et maintien de ce chiffrement de bout en bout dans le tier cloud. Les blocs de données qui sont déplacés vers le magasin d'objets cloud sont sécurisés par la sécurité de la couche de transport (TLS) v1.2 afin de préserver la confidentialité et l'intégrité des données entre les tiers de stockage.

La communication avec le magasin d'objets cloud sur une connexion non chiffrée est prise en charge, mais non recommandée par NetApp.

Chiffrement des données

Le cryptage des données est indispensable à la protection de la propriété intellectuelle, des informations commerciales et des informations personnellement identifiables des clients. FabricPool prend entièrement en charge NVE (NetApp Volume Encryption) et NetApp Storage Encryption (NSE) pour conserver les stratégies de protection des données existantes. Toutes les données chiffrées stockées sur le Tier de performance restent chiffrées lors de leur déplacement vers le Tier cloud. Les clés de chiffrement côté client sont la propriété de ONTAP, et les clés de chiffrement de magasin d'objets côté serveur sont la propriété de leur magasin d'objets cloud respectif. Les données qui ne sont pas chiffrées avec NVE sont chiffrées à l'aide de l'algorithme AES-256-GCM. Aucun autre chiffrement AES-256 n'est pris en charge.

L'utilisation de NSE ou NVE est facultative et n'est pas requise pour l'utilisation de FabricPool.

Conditions requises pour le FabricPool

FabricPool nécessite ONTAP 9.2 ou une version ultérieure et des agrégats SSD sur l'une des plateformes répertoriées dans cette section. D'autres exigences d'FabricPool dépendent du niveau de cloud associé. Si vous disposez de plateformes AFF d'entrée de gamme dont la capacité est fixe et relativement faible, comme le système NetApp AFF C190, FabricPool peut bénéficier d'une grande efficacité pour déplacer les données inactives vers le Tier cloud.

Plateformes

FabricPool est pris en charge sur les plateformes suivantes :

- NetApp AFF
  - A800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 ET AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 ET FAS8040
  - FAS2750, FAS2720
  - FAS2650 ET FAS2620

Seuls les agrégats SSD des plateformes FAS peuvent utiliser FabricPool.

- Tiers cloud
  - Alibaba Cloud Object Storage Service (Standard, Infrequent Access)
  - Amazon S3 (Standard, Standard-IA, une zone-IA, Tiering intelligent)

- Amazon commercial Cloud Services (C2S)
- Google Cloud Storage (multirégional, régional, Nearline, Coldline)
- Stockage objet cloud IBM (Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (chaud et froid)

LIF intercluster

Les paires haute disponibilité du cluster qui utilisent FabricPool nécessitent deux interfaces logiques intercluster pour communiquer avec le niveau du cloud. NetApp recommande de créer un LIF intercluster sur des paires haute disponibilité supplémentaires pour relier de manière transparente des niveaux cloud aux agrégats sur ces nœuds.

Le LIF utilisé par ONTAP pour se connecter avec le magasin d'objets AWS S3 doit se trouver sur un port 10 Gbit/s.

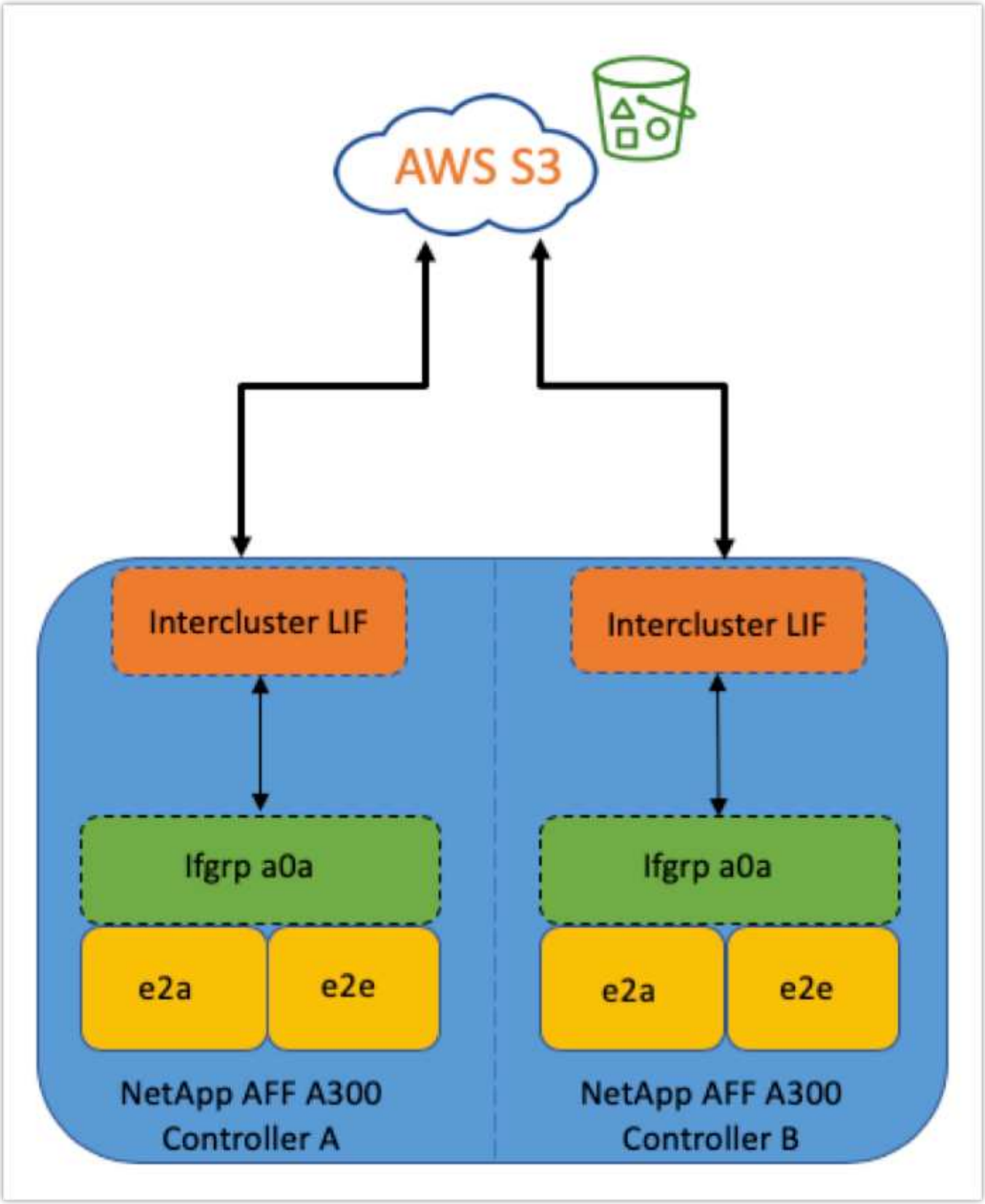
Si plusieurs LIF Intercleuser sont utilisées sur un nœud avec un routage différent, NetApp recommande de les placer dans différents IPspaces. Lors de la configuration, FabricPool peut choisir parmi plusieurs IPspaces, mais il est impossible de sélectionner des LIF intercluster spécifiques au sein d'un IPspace.

La désactivation ou la suppression d'une LIF intercluster interrompt la communication au niveau du cloud.

Connectivité

La latence de lecture d'FabricPool dépend de la connectivité au niveau cloud. Les LIF intercluster utilisant des ports 10 Gbits/s, illustrées dans la figure suivante, offrent des performances adéquates. NetApp recommande de valider les latences et le débit d'un environnement réseau spécifique afin de déterminer son impact sur les performances d'FabricPool.

Lorsque vous utilisez FabricPool dans des environnements à faibles performances, les exigences minimales de performance des applications client doivent rester respectées et les objectifs de délai de restauration doivent être ajustés en conséquence.



Profileur de magasin d'objets

Le profileur de magasin d'objets, comme illustré ci-dessous, est disponible via l'interface de ligne de commandes de ONTAP. Il teste la latence et les performances de débit des magasins d'objets avant qu'ils ne soient connectés à un agrégat FabricPool.

Le Tier de cloud doit être ajouté à ONTAP avant de pouvoir être utilisé avec le profileur de magasin d'objets.

Démarrez le profileur de magasin d'objets à partir du mode privilèges avancés dans ONTAP à l'aide de la commande suivante :

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Pour afficher les résultats, lancer la commande suivante :

```
storage aggregate object-store profiler show
```

Les tiers cloud n'offrent pas des performances similaires à celles du Tier de performance (généralement Go par seconde). Même si les agrégats FabricPool peuvent facilement fournir des performances similaires aux disques SATA, ils tolèrent une latence pouvant atteindre 10 secondes et un faible débit pour les solutions de Tiering qui ne nécessitent pas de performances SATA.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                          min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817     69.55MB
GET     4KB        158636    0         27        1132      41       32.22MB
GET     8KB        0         0         0         0         0        0B
GET     32KB       0         0         0         0         0        0B
GET     256KB      0         0         0         0         0        0B
5 entries were displayed.
```

Volumes

Le provisionnement fin du stockage est une pratique standard pour l'administrateur d'infrastructures virtuelles FlexPod. NetApp Virtual Storage Console (VSC) provisionne des volumes de stockage pour les datastores VMware sans les garanties d'espace (provisionnement fin) et avec des paramètres d'efficacité du stockage optimisés conformément aux meilleures pratiques NetApp. Si VSC est utilisé pour créer des datastores VMware, aucune action supplémentaire n'est requise, car aucune garantie d'espace ne doit être attribuée au volume du datastore.

FabricPool ne peut pas associer un Tier cloud à un agrégat contenant des volumes grâce à une garantie d'espace autre que aucune (par exemple, Volume).

```
volume modify -space-guarantee none
```

Réglage du `space-guarantee none` paramètre fournit le provisionnement fin pour le volume. La quantité d'espace consommée par les volumes avec ce type de garantie augmente à mesure que des données sont ajoutées au lieu d'être déterminées par la taille du volume initial. Cette approche est essentielle pour FabricPool, car les volumes doivent prendre en charge les données de Tier cloud actives et renvoyé vers le Tier de performance.

Licences

Une licence basée sur la capacité est nécessaire pour connecter des fournisseurs de stockage objet tiers (tels qu'Amazon S3) à des tiers cloud pour les systèmes AFF et FAS Flash hybrides. FabricPool

Les licences FabricPool sont disponibles en mode perpétuel ou par période (1 an ou 3 ans).

Le Tiering dans le cloud s'arrête lorsque la quantité de données (capacité utilisée) stockée sur le Tier cloud atteint la capacité sous licence. Les données supplémentaires, y compris les copies SnapMirror vers les volumes utilisant la règle de hiérarchisation, ne peuvent pas être hiérarchisées tant que la capacité de licence n'est pas augmentée. Même si le Tiering s'arrête, les données restent accessibles à partir du Tier cloud. Les données inactives supplémentaires restent sur les disques SSD jusqu'à ce que la capacité sous licence augmente.

Une licence FabricPool gratuite de 10 To basée sur une durée de validité est incluse lors de l'achat d'un nouveau cluster ONTAP 9.5 ou version ultérieure, même si des coûts de support supplémentaires peuvent s'appliquer. Les licences FabricPool (y compris la capacité supplémentaire pour les licences existantes) peuvent être achetées par incréments de 1 To.

Une licence FabricPool ne peut être supprimée que d'un cluster ne contenant aucun agrégat FabricPool.

Les licences FabricPool portent sur l'ensemble du cluster. Vous devez avoir l'UUID disponible lors de l'achat d'une licence (`cluster identify show`). Pour plus d'informations sur la licence, reportez-vous au "Base de connaissances NetApp".

Configuration

Révisions logicielles

Le tableau suivant illustre les versions matérielles et logicielles validées.

Calque	Périphérique	Image	Commentaires
Stockage	NetApp AFF A300	ONTAP 9.6P2	
Calcul	Serveurs lames Cisco UCS B200 M5 avec Cisco UCS VIC 1340	Version 4.0(4b)	
Le réseau	Interconnexion de fabric Cisco Nexus 6332-16UP	Version 4.0(4b)	
	Commutateur Cisco Nexus 93180YC-EX en mode autonome NX-OS	Version 7.0(3)I7(6)	
Réseau de stockage	Cisco MDS 9148S	Version 8.3(2)	

Calque	Périphérique	Image	Commentaires
Hyperviseur		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		Serveur VMware vCenter	Version 6.7.0.30000 de vCenter Server 13639309
Ou du fournisseur cloud		Amazon AWS S3	Compartiment S3 standard avec options par défaut

Les critères de base pour FabricPool sont présentés dans le "Conditions requises pour le FabricPool". Une fois que toutes les conditions de base sont réunies, procédez comme suit pour configurer FabricPool :

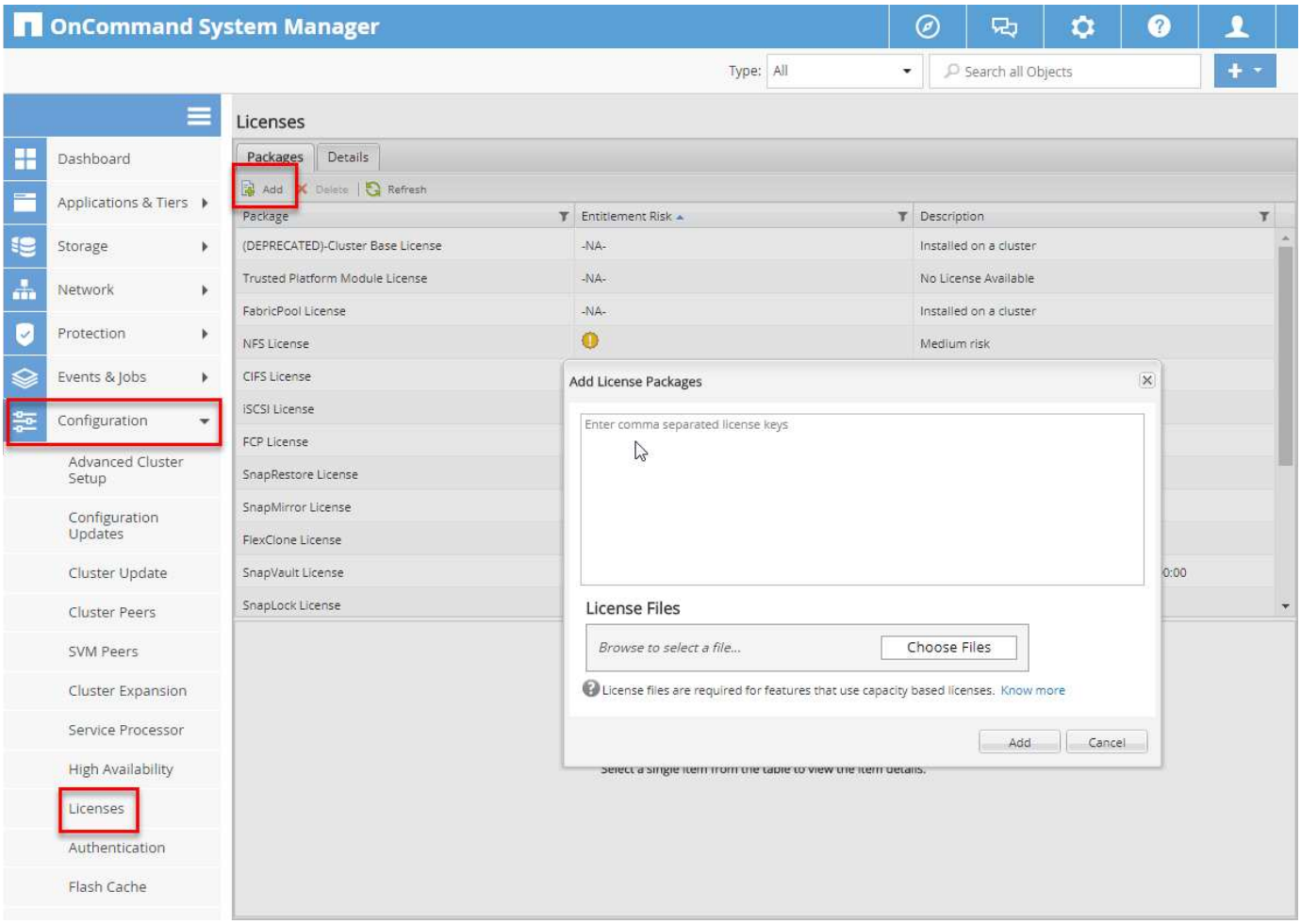
1. Installez une licence FabricPool.
2. Créez un compartiment de magasin d'objets AWS S3.
3. Ajoutez un Tier cloud à ONTAP.
4. Relier le Tier cloud à un agrégat.
5. Définissez la règle de Tiering du volume.

"Ensuite, installez la licence FabricPool."

Installez la licence FabricPool

Une fois que vous avez acquis un fichier de licence NetApp, vous pouvez l'installer avec OnCommand System Manager. Pour installer le fichier de licence, procédez comme suit :

1. Cliquez sur configurations.
2. Cliquez sur Cluster.
3. Cliquez sur licences.
4. Cliquez sur Ajouter.
5. Cliquez sur choisir les fichiers à parcourir et sélectionnez un fichier.
6. Cliquez sur Ajouter.



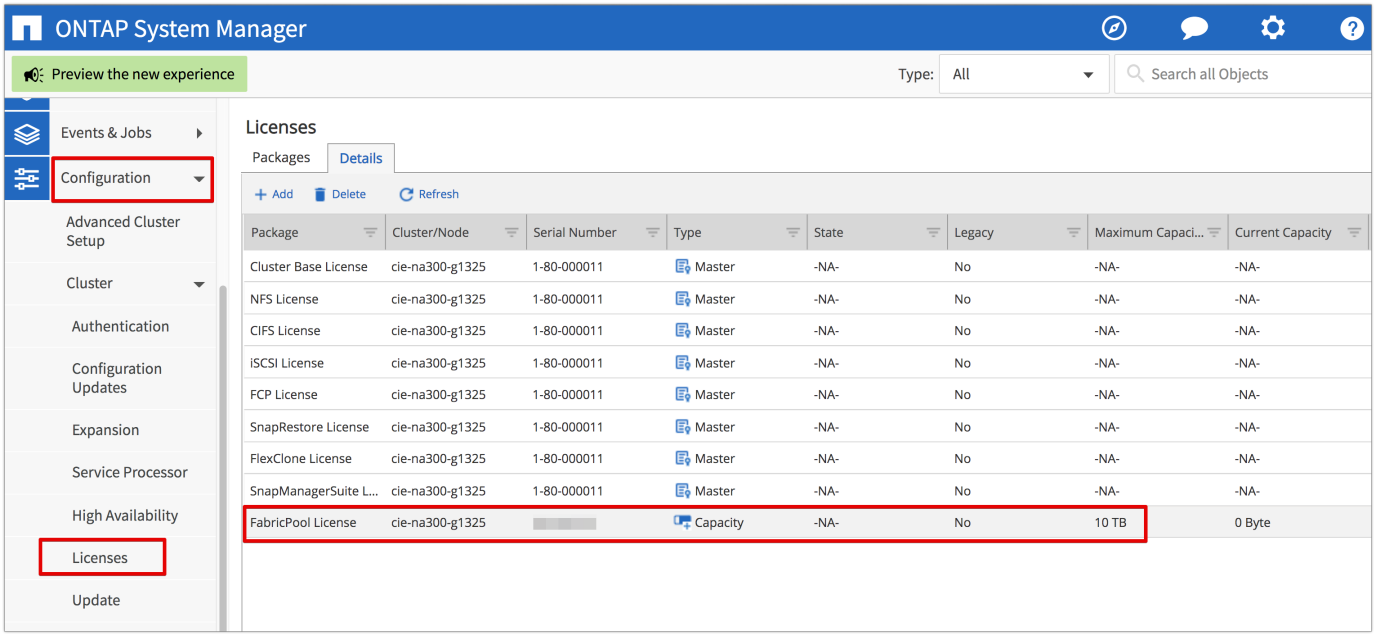
Capacité de la licence

Vous pouvez afficher la capacité de la licence à l'aide de l'interface de ligne de commandes ONTAP ou de OnCommand System Manager. Pour vérifier la capacité sous licence, exécutez la commande suivante dans l'interface de ligne de commandes de ONTAP :

```
system license show-status
```

Dans OnCommand System Manager, effectuez la procédure suivante :

1. Cliquez sur configurations.
2. Cliquez sur licences.
3. Cliquez sur l'onglet Détails.



La capacité maximale et la capacité actuelle sont indiquées sur la ligne de licence FabricPool.

"Ensuite, créez un compartiment AWS S3."

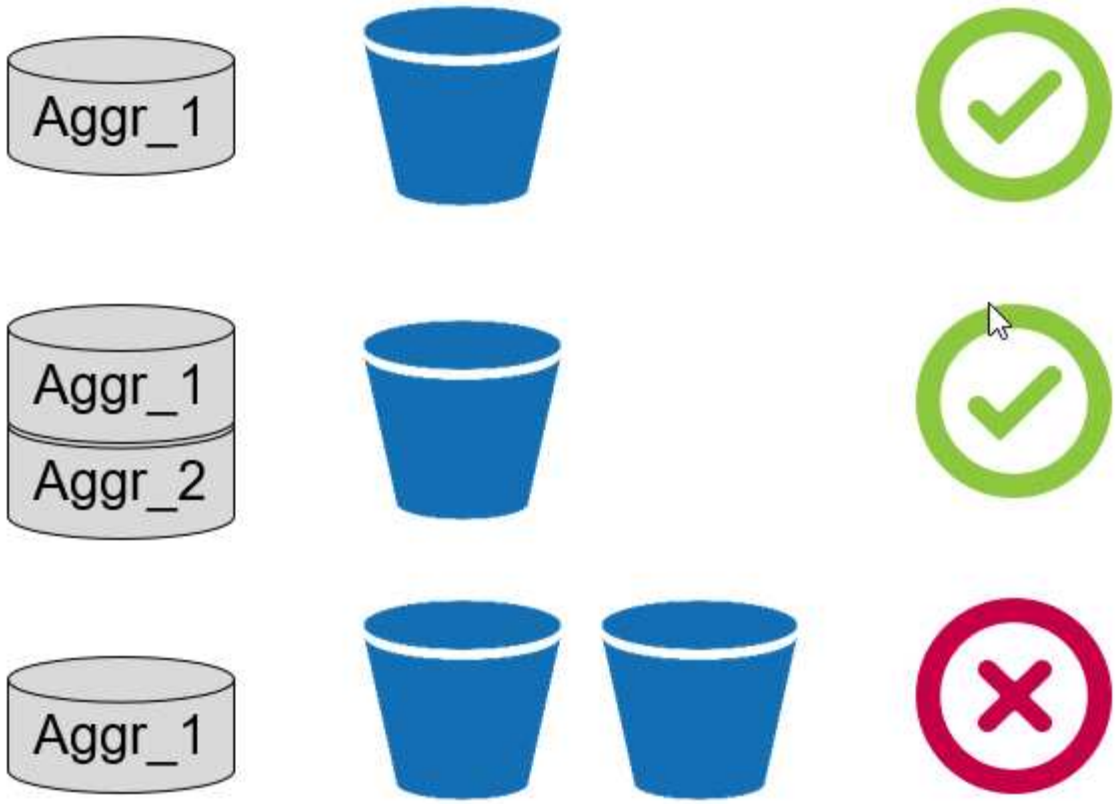
Création d'un compartiment AWS S3

Les compartiments sont des conteneurs de stockage objet qui hébergent les données. Vous devez fournir le nom et l'emplacement du compartiment dans lequel les données sont stockées avant de pouvoir être ajoutées à un agrégat en tant que Tier cloud.

Les compartiments ne peuvent pas être créés à l'aide de OnCommand System Manager, OnCommand Unified Manager ou ONTAP.

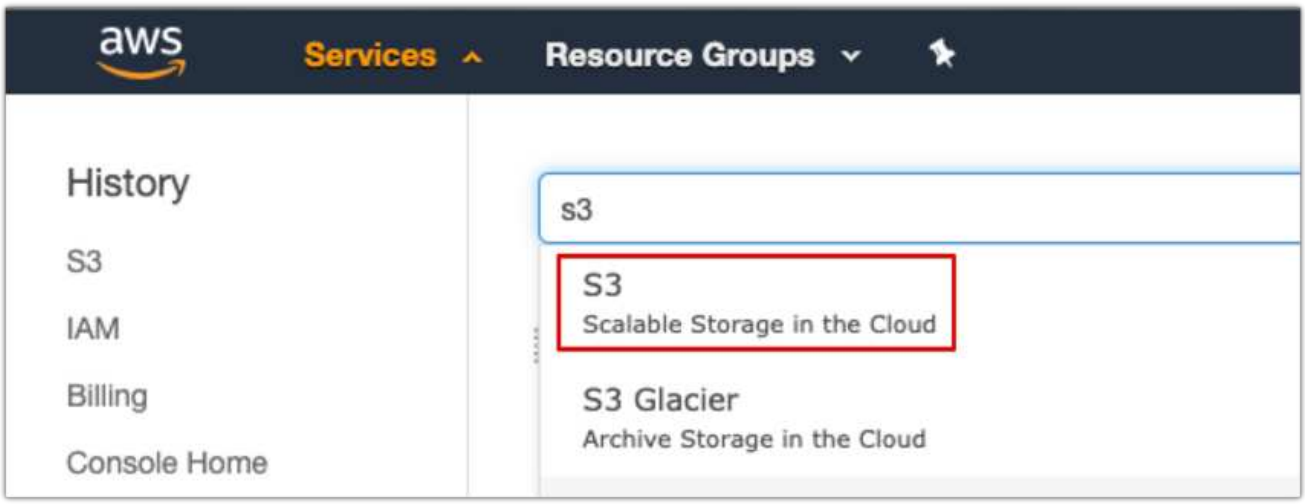
FabricPool prend en charge la connexion d'un compartiment par agrégat, comme illustré dans la figure suivante. Un seul compartiment peut être associé à un seul agrégat et un seul compartiment peut être relié à plusieurs agrégats. Toutefois, un seul agrégat ne peut pas être associé à plusieurs compartiments. Bien qu'un compartiment unique puisse être connecté à plusieurs agrégats du cluster, NetApp ne recommande pas de connecter un compartiment unique à des agrégats dans plusieurs clusters.

Lors de la planification d'une architecture de stockage, réfléchissez à l'impact possible de la relation entre compartiment et agrégat sur les performances. De nombreux fournisseurs de magasin d'objets définissent un nombre maximal d'IOPS pris en charge au niveau du compartiment ou du conteneur. Les environnements qui requièrent des performances maximales doivent utiliser plusieurs compartiments pour réduire l'éventualité où les limites des IOPS du stockage objet pouvaient affecter les performances de plusieurs agrégats FabricPool. Il est préférable de connecter un compartiment ou un conteneur unique à tous les agrégats FabricPool d'un cluster pour des environnements qui privilégient les performances de Tier cloud.

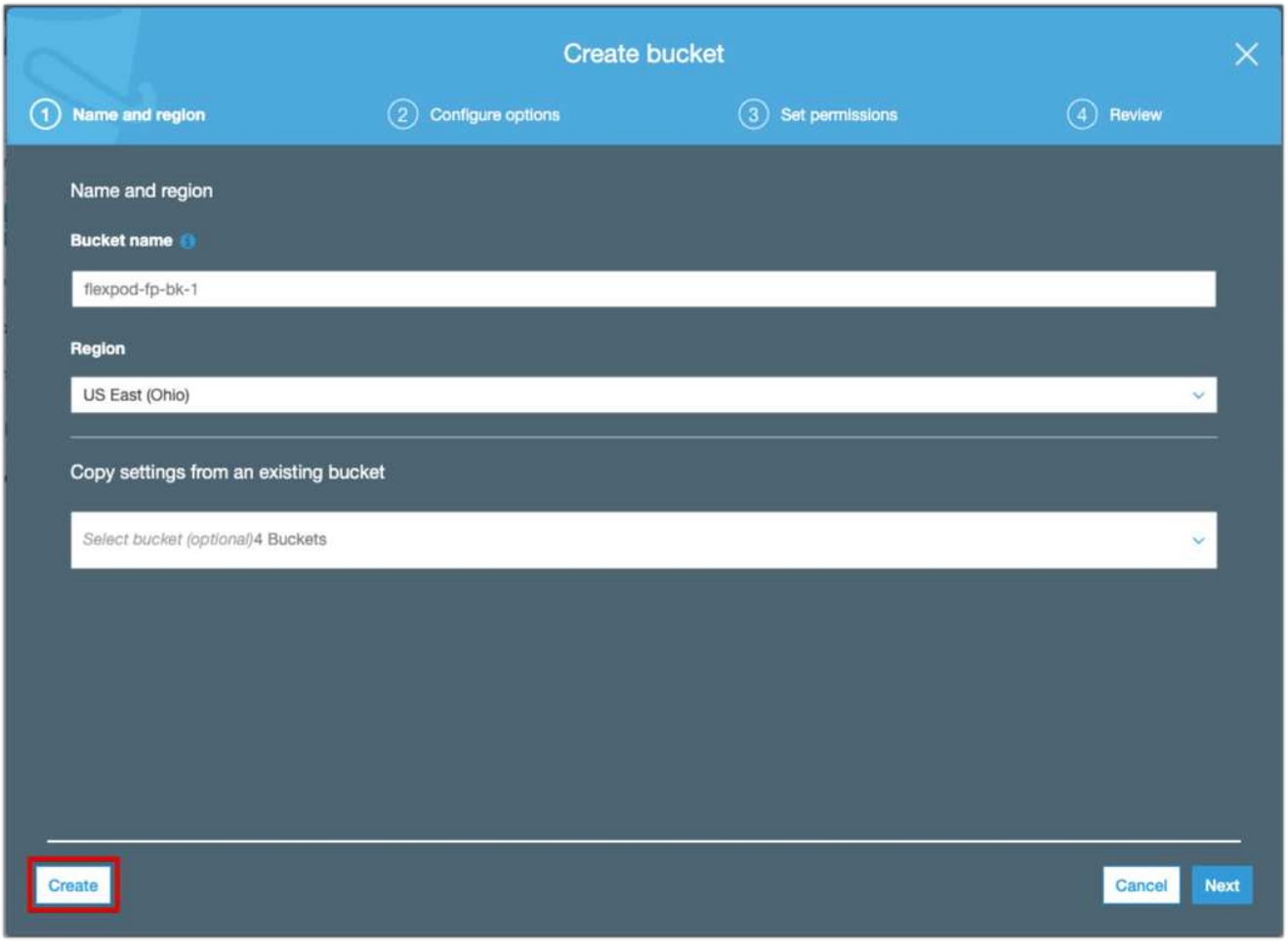


Créer un compartiment S3

1. Dans la console de gestion AWS depuis la page d'accueil, entrez S3 dans la barre de recherche.
2. Sélectionnez stockage évolutif S3 dans le cloud.



3. Sur la page d'accueil S3, sélectionnez Créer un compartiment.
4. Entrez un nom compatible DNS et choisissez la région pour créer le compartiment.



5. Cliquez sur Créer pour créer le compartiment de stockage d'objets.

"Ensuite, ajoutez un Tier cloud à ONTAP"

Ajoutez un Tier cloud à ONTAP

Avant de pouvoir joindre un magasin d'objets à un agrégat, il doit être ajouté à et identifié par ONTAP. Cette tâche peut être effectuée avec OnCommand System Manager ou l'interface de ligne de commandes de ONTAP.

FabricPool prend en charge Amazon S3, IBM Object Cloud Storage et les magasins d'objets Microsoft Azure Blob Storage en tant que tiers cloud.

Vous avez besoin des informations suivantes :

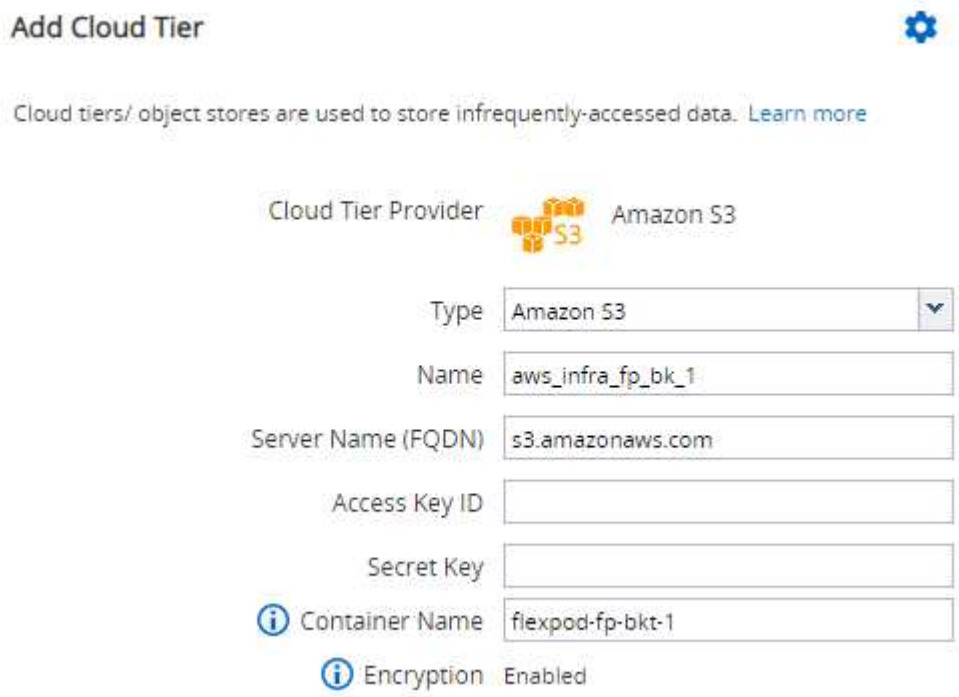
- Nom de serveur (FQDN) ; par exemple, `s3.amazonaws.com`
- ID de clé d'accès
- Clé secrète
- Nom du conteneur (nom de compartiment)

OnCommand System Manager

Pour ajouter un Tier cloud avec OnCommand System Manager, procédez comme suit :

1. Lancez OnCommand System Manager.
2. Cliquez sur stockage.
3. Cliquez sur Aggregates & disques.
4. Cliquez sur Cloud tiers.
5. Sélectionnez un fournisseur de magasin d'objets.
6. Renseignez les champs de texte requis pour le fournisseur de magasin d'objets.

   Dans le champ Nom du conteneur, entrez le nom de compartiment ou du conteneur du magasin d'objets.
7. Cliquez sur Save and Attach Aggregates.



INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour ajouter un Tier cloud à l'aide de l'interface de ligne de commandes ONTAP, entrez les commandes suivantes :

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Ensuite, associez un Tier cloud à un agrégat ONTAP."

Association d'un Tier cloud à un agrégat ONTAP

Lorsqu'un magasin d'objets est ajouté à et identifié par ONTAP, il doit être associé à un agrégat pour créer une FabricPool. Pour ce faire, utilisez OnCommand System Manager ou l'interface de ligne de commandes de ONTAP.

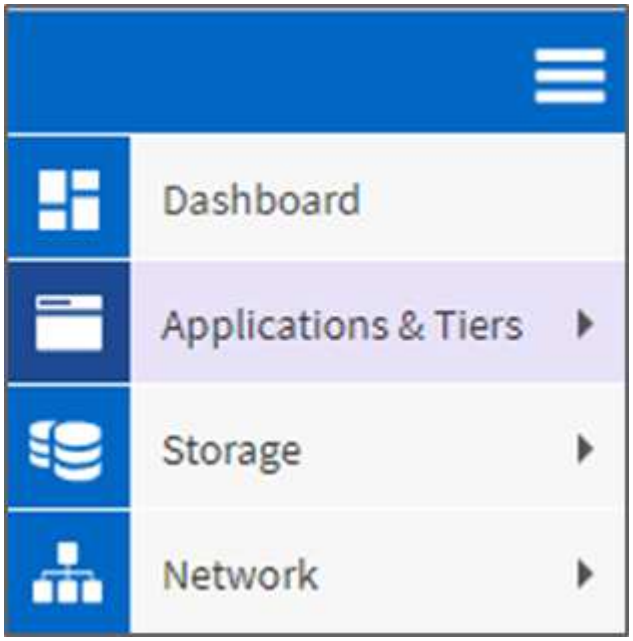
Plusieurs types de magasin d'objets peuvent être connectés à un cluster, mais un seul type de magasin d'objets peut être associé à chaque agrégat. Par exemple, un agrégat peut utiliser Google Cloud et un autre agrégat peut utiliser Amazon S3, mais un autre ne peut pas être associé aux deux.

L'association d'un Tier cloud à un agrégat est une opération permanente. Un niveau de cloud ne peut pas être dérattaché à un agrégat auquel il est rattaché.

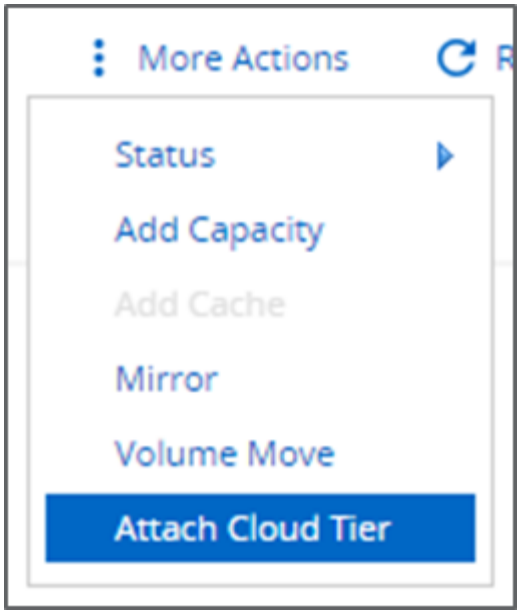
OnCommand System Manager

Pour rattacher un Tier cloud à un agrégat via OnCommand System Manager, effectuez les opérations suivantes :

1. Lancez OnCommand System Manager.
2. Cliquez sur applications et niveaux.



3. Cliquez sur niveaux de stockage.
4. Cliquer sur un agrégat.
5. Cliquez sur actions et sélectionnez attacher Cloud Tier.



6. Sélectionnez un Tier cloud.
7. Afficher et mettre à jour les règles de Tiering des volumes sur l'agrégat (facultatif). Par défaut, la règle de Tiering du volume est définie comme Snapshot uniquement.
8. Cliquez sur Enregistrer.

INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour attacher un Tier cloud à un agrégat via l'interface de ligne de commandes ONTAP, exécutez les commandes suivantes :

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Exemple :

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Ensuite : définissez la règle de Tiering du volume."

Définition de la règle de Tiering des volumes

Par défaut, les volumes utilisent la règle de Tiering aucun volume. Une fois la création de volume effectuée, la règle de Tiering des volumes peut être modifiée à l'aide de OnCommand System Manager ou de l'interface de ligne de commande de ONTAP.

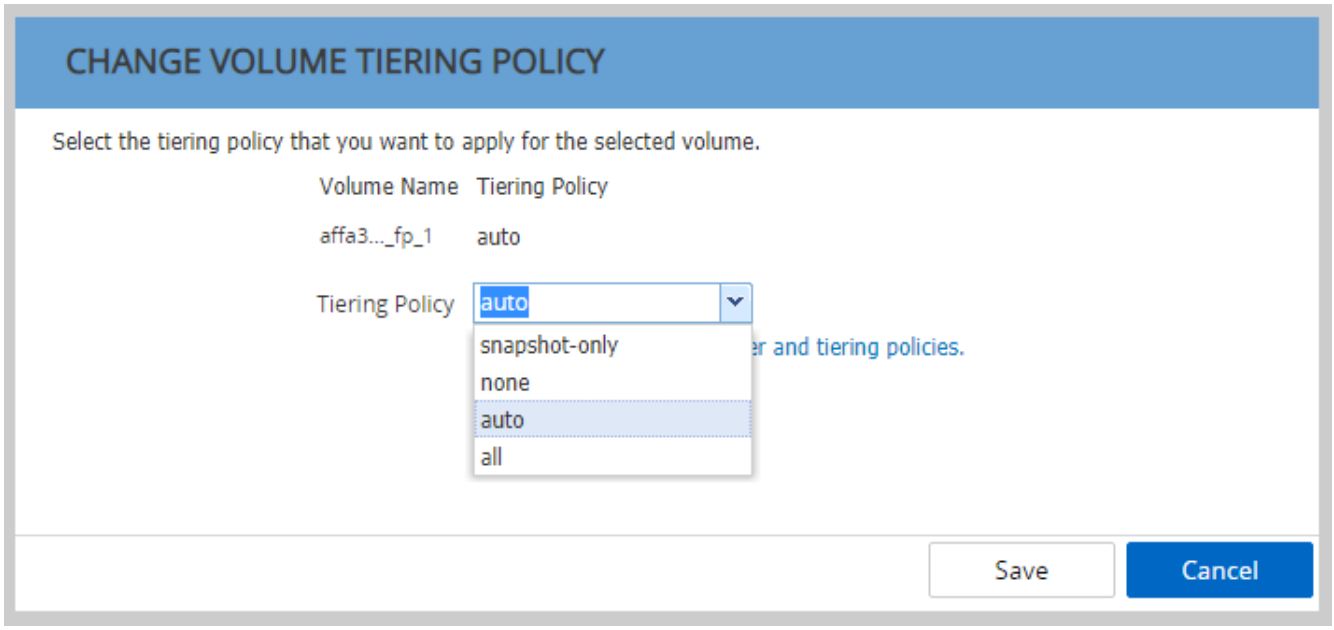
Lorsqu'il est utilisé avec FlexPod, FabricPool propose trois règles de Tiering des volumes : automatique, Snapshot uniquement et aucune.

- **Auto**
  - Tous les blocs inactifs du volume sont déplacés vers le cloud. Si l'agrégat est utilisé à plus de 50 %, il faut environ 31 jours pour que les blocs inactifs soient à froid. La période de refroidissement automatique est réglable entre 2 jours et 63 jours en utilisant le `tiering-minimum-cooling-days` réglage.
  - Lorsque les blocs inactifs d'un volume dont la règle de Tiering est définie sur Auto sont lus de manière aléatoire, ils sont écrits et mis à chaud sur le Tier de performance.
  - Lorsque les blocs inactifs dans un volume dont la règle de Tiering est définie sur Auto sont lus de manière séquentielle, ils restent inactifs et restent sur le Tier cloud. Ils ne sont pas écrits sur le Tier de performance.
- **Instantané uniquement**
  - Les blocs de snapshots inactifs dans le volume qui ne sont pas partagés avec le système de fichiers actif sont déplacés vers le Tier cloud. Si l'agrégat est utilisé à plus de 50 %, il faut environ 2 jours pour que les blocs de snapshot inactifs soient inactifs. La période de refroidissement uniquement à snapshot est réglable de 2 à 63 jours en utilisant le `tiering-minimum-cooling-days` réglage.
  - Lorsque les blocs inactifs dans un volume dont la règle de Tiering est définie sur Snapshot uniquement sont lus, ils sont écrits et mis à chaud sur le Tier de performance.
- **Aucun (par défaut)**
  - Les volumes définis sur aucune n'utilisent la règle de Tiering ne transfèrent pas les données inactives vers le Tier cloud.
  - La définition de la règle de Tiering sur aucun empêche la hiérarchisation.
  - Les données de volume précédemment transférées vers le Tier cloud restent dans le Tier cloud jusqu'à ce qu'elles soient fortement sollicitées et sont automatiquement retransférées vers le Tier de performance.

OnCommand System Manager

Pour modifier la règle de hiérarchisation d'un volume à l'aide de OnCommand System Manager, procédez comme suit :

1. Lancez OnCommand System Manager.
2. Sélectionnez un volume.
3. Cliquez sur autres actions et sélectionnez Modifier la règle de hiérarchisation.
4. Sélectionnez la règle de Tiering à appliquer au volume.
5. Cliquez sur Enregistrer.



INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour modifier la règle de hiérarchisation d'un volume à l'aide de l'interface de ligne de commandes ONTAP, exécutez la commande suivante :

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Ensuite, définissez le Tiering des volumes sur les jours de refroidissement minimum."

Définissez le Tiering des volumes sur les jours de refroidissement minimum

Le `tiering-minimum-cooling-days` Le paramètre détermine le nombre de jours devant être écoulés avant que les données inactives d'un volume à l'aide des règles Auto ou Snapshot uniquement sont considérées comme inactives et éligibles pour le Tiering.

Auto

La valeur par défaut `tiering-minimum-cooling-days` La définition de la règle de hiérarchisation automatique est définie sur 31 jours.

Étant donné que les lectures maintiennent une température élevée des blocs, l'augmentation de cette valeur peut réduire la quantité de données éligibles à un Tier et augmenter la quantité de données conservées sur le Tier de performances.

Si vous souhaitez réduire cette valeur par défaut de 31 jours, notez que les données ne doivent plus être actives avant d'être marquées comme étant inactives. Par exemple, si une charge de travail sur plusieurs jours doit effectuer un nombre important d'écritures au jour 7, celle du volume `tiering-minimum-cooling-days` le réglage ne doit pas être inférieur à 8 jours.

Le stockage objet n'est pas transactionnel de base comme le stockage de fichiers ou de blocs. Les modifications apportées aux fichiers stockés sous forme d'objets dans des volumes dont les jours de refroidissement sont trop serrés peuvent entraîner la création de nouveaux objets, la fragmentation des objets existants et l'ajout d'inefficacités du stockage.

Snapshot uniquement

La valeur par défaut `tiering-minimum-cooling-days` La définition de la règle de Tiering uniquement Snapshot est de 2 jours. Un délai minimum de 2 jours permet des processus en arrière-plan pour un stockage optimal et empêche les processus quotidiens de protection des données d'avoir à lire les données depuis le Tier cloud.

INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour modifier un volume `tiering-minimum-cooling-days` Pour le paramètre via l'interface de ligne de commandes de ONTAP, exécutez la commande suivante :

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

Le niveau de privilège avancé est requis.

La modification de la règle de Tiering entre Auto et Snapshot uniquement (ou vice-versa) entraîne une réinitialisation de la période d'inactivité des blocs sur le Tier de performance. Par exemple, un volume utilisant la règle de Tiering automatique des volumes avec des données inactives pendant 20 jours dispose que l'inactivité des données de Tier de performance est réinitialisée à 0 jours si la règle de Tiering est définie sur Snapshot uniquement.

Performances

Dimensionnez le Tier de performance

Lorsque vous envisagez de dimensionner, gardez à l'esprit que le Tier de performance doit être capable des tâches suivantes :

- Prise en charge des données fortement sollicitées
- La prise en charge des données inactives jusqu'à l'analyse du Tiering déplace les données vers le Tier cloud
- Prendre en charge les données de Tier cloud actives et écrites à nouveau sur le Tier de performance
- Prise en charge des métadonnées WAFL associées au niveau de cloud associé

Pour la plupart des environnements, un rapport performances/capacité de 1 à 10 sur les agrégats FabricPool est extrêmement prudent, tout en permettant des économies de stockage importantes. Par exemple, si l'objectif est de transférer des 200 To vers le Tier cloud, l'agrégat de Tier de performance doit atteindre 20 To au minimum.

Les écritures depuis le Tier cloud vers le Tier de performance sont désactivées si la capacité du Tier de performance est supérieure à 70 %. Dans ce cas, les blocs sont lus directement depuis le Tier cloud.

Dimensionnez le Tier cloud

Lors de l'évaluation du dimensionnement, le magasin d'objets agissant comme Tier cloud doit être capable de réaliser les tâches suivantes :

- Prise en charge des lectures de données inactives existantes
- Prise en charge des écritures de nouvelles données inactives
- Prise en charge de la suppression et de la défragmentation des objets

Le coût de possession

Le "Calculateur économique FabricPool" Disponible auprès du cabinet d'analyse indépendant Evaluator Group, cabinet d'analyse IT indépendant, afin de réaliser des économies sur site et dans le cloud pour le stockage des données inactives. Ce calculateur fournit une interface simple qui détermine le coût de stockage des données peu utilisées sur un Tier de performance plutôt que de les transférer vers un Tier cloud pour le reste du cycle de vie des données. Sur la base d'un calcul effectué sur 5 ans, les quatre facteurs clés (la capacité source, la croissance des données, la capacité Snapshot et le pourcentage de données inactives) sont utilisés pour déterminer les coûts de stockage sur la période.

Conclusion

La transition vers le cloud varie d'une entreprise à l'autre, et même d'une unité commerciale à l'autre. Si certains choisissent une adoption rapide, d'autres sont plus conservatrices. FabricPool s'intègre à la stratégie cloud des entreprises, quelle que soit leur taille, et quelle que soit la vitesse d'adoption du cloud. Une démonstration encore plus poussée de l'efficacité et de l'évolutivité d'une infrastructure FlexPod.

Où trouver des informations complémentaires

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

- Meilleures pratiques pour FabricPool

  "www.netapp.com/us/media/tr-4598.pdf"

- Documentation produit NetApp

  "https://docs.netapp.com"

- Tr-4036 : spécifications techniques de data Center FlexPod

  "https://www.netapp.com/us/media/tr-4036.pdf"

FlexPod Datacenter avec IBM Cloud Private

Sreenivasa Edula, Cisco Thanachit Wichianchai, IBM Jacky Ben-Bassat, IBM Global Alliance, NetApp

IBM Cloud Private (ICP) est une plateforme sur site qui permet de développer et de gérer des applications conteneurisées pour les utilisations cloud natives et de modernisation des applications. Il s'agit d'un environnement intégré basé sur Kubernetes pour l'orchestration de conteneurs. Il comprend un référentiel d'images privées pour les conteneurs Docker, une console de gestion, un framework de surveillance, de nombreuses applications open source et conteneurisées IBM, et bien plus encore. L'association de cette plateforme et de FlexPod simplifie le déploiement et la gestion de votre infrastructure grâce à l'infrastructure convergée de Cisco et NetApp. Vous bénéficiez également d'une efficacité du stockage, d'une meilleure protection des données, d'une réduction des risques et de la flexibilité nécessaires pour faire évoluer cette pile d'infrastructure haute disponibilité afin de répondre aux nouveaux besoins de l'entreprise et à d'autres évolutions au fil du temps.

"FlexPod Datacenter avec IBM Cloud Private"

FlexPod Datacenter pour le cloud hybride avec Cisco CloudCenter et NetApp Private Storage : conception

Haseeb Niazi, Cisco David Arnette, NetApp

Les conceptions validées par Cisco (CVD) proposent des systèmes et des solutions conçus, testés et documentés pour faciliter et améliorer les déploiements client. Ces conceptions intègrent une large gamme de technologies et de produits dans une gamme de solutions qui ont été développées pour répondre aux besoins commerciaux des clients et pour les guider de la conception au déploiement.

"FlexPod Datacenter pour le cloud hybride avec Cisco CloudCenter et NetApp Private Storage : conception"

FlexPod Datacenter pour le multicloud avec Cisco CloudCenter et NetApp Data Fabric

Haseeb Niazi, Cisco David Arnette, NetApp

Ce document contient des instructions détaillées de configuration et d'implémentation pour la configuration de FlexPod Datacenter pour le cloud hybride. Les éléments de conception suivants distinguent cette version de FlexPod des modèles précédents :

- Intégration de Cisco CloudCenter avec FlexPod Datacenter avec l'ACI comme Cloud privé
- Intégration de Cisco CloudCenter avec les clouds publics Amazon Web Services (AWS) et Microsoft Azure Resource Manager (MS Azure RM)
- Assurer une connectivité sécurisée entre le data Center FlexPod et les clouds publics pour sécuriser le trafic entre les machines virtuelles

- Connectivité sécurisée entre le data Center FlexPod et NetApp Private Storage (NPS) pour le trafic de réplication des données
- Possibilité de déployer des instances applicatives dans des clouds publics ou privés et d'obtenir les données applicatives à jour disponibles pour ces instances via l'orchestration pilotée par Cisco CloudCenter
- Configuration, validation et mise en avant des aspects opérationnels d'un environnement de développement et de test dans ce nouveau mode de cloud hybride.

"FlexPod Datacenter pour le multicloud avec Cisco CloudCenter et NetApp Data Fabric"

Les bases de données d’entreprise

SAP

Introduction à SAP sur FlexPod

La plateforme FlexPod est une architecture de data Center préconçue et conforme aux bonnes pratiques. Elle repose sur la plateforme Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus et les contrôleurs de stockage NetApp.

FlexPod est une plateforme adaptée pour exécuter des applications SAP. Les solutions fournies ici vous permettent de déployer rapidement et de manière fiable SAP HANA avec un modèle d’intégration personnalisée des data centers. FlexPod offre non seulement une configuration de base, mais également la possibilité d’être dimensionnée et optimisée afin de répondre à de nombreuses exigences et cas d’utilisation.

Centre de données FlexPod pour la solution SAP utilisant Fibre Channel SAN avec Cisco UCS Manager 4.0 et NetApp ONTAP 9.7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente le centre de données FlexPod de Cisco et NetApp avec NetApp ONTAP 9.7 sur le système de stockage NetApp AFF A400 et le logiciel unifié Cisco UCS Manager version 4.1(1) avec processeurs évolutifs Xeon de deuxième génération pour SAP HANA en particulier.

Le data Center FlexPod avec NetApp ONTAP 9.7 et le logiciel unifié Cisco UCS 4.1(1) est une architecture de data Center prédéfinie et basée sur les meilleures pratiques. Elle repose sur le système Cisco Unified Computing System (Cisco UCS), la famille de commutateurs Cisco Nexus 9000, les commutateurs de structure multicouche MDS 9000, Et les baies de stockage NetApp AFF A-Series exécutant le système d’exploitation du stockage ONTAP 9.7.

"Centre de données FlexPod pour la solution SAP utilisant Fibre Channel SAN avec Cisco UCS Manager 4.0 et NetApp ONTAP 9.7"

SAP non-HANA avec SQL - Design

Le secteur INFORMATIQUE actuel connaît une transformation radicale des solutions de data Center. Ces dernières années, les solutions de data Center prévalidées et spécialisées ont suscité un intérêt considérable. L’introduction de technologies de virtualisation dans des domaines critiques a eu un impact majeur sur les principes de conception et l’architecture de ces solutions. Elle a permis à de nombreuses applications s’exécutant sur des systèmes bare-Metal de migrer vers de nouvelles solutions intégrées virtualisées. FlexPod est une solution de data Center prévalidée et spécialisée conçue pour répondre à l’évolution rapide des besoins des services IT. Cisco et NetApp se sont associés pour proposer FlexPod, qui utilise les meilleurs composants de calcul, de réseau et de stockage pour la base de nombreux workloads d’entreprise, notamment les bases de données, la planification des ressources d’entreprise (ERP), la gestion de la relation client (CRM) et les applications web.

La consolidation des applications IT, en particulier des bases de données, a suscité un intérêt considérable ces dernières années. Microsoft SQL Server est la plateforme de base de données la plus utilisée et la plus déployée au cours des dernières années. Les bases de données SQL Server sont souvent confrontées à la prolifération des bases de données, ce qui entraîne des défis INFORMATIQUES tels que des serveurs sous-utilisés, des licences incorrectes, des problèmes de sécurité, des problèmes de gestion et des coûts d'exploitation colossaux. Par conséquent, les bases de données SQL Server sont de bons candidats à la consolidation sur une plateforme plus robuste, plus flexible et plus résiliente. Ce document présente une architecture de référence FlexPod pour le déploiement et la consolidation des bases de données SQL Server.

"SAP non-HANA avec SQL - Design"

Centre de données FlexPod pour solution SAP avec Cisco UCS, fabric de troisième génération et NetApp AFF A-Series

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document décrit la méthodologie de déploiement de Cisco et NetApp FlexPod Datacenter pour SAP HANA basée sur la deuxième génération de processeurs Intel Xeon Scalable compatibles avec Cisco UCS Computing System (Cisco UCS).

Cisco UCS Manager (UCSM) 4.0(4) assure la prise en charge consolidée de tous les modèles Cisco UCS Fabric Interconnect (6200, 6300, 6324 et 6454), d'un module de la gamme 2200/2300, d'un serveur lame Cisco UCS B-Series et de serveurs rack Cisco UCS C-Series. Le data Center FlexPod, associé au logiciel unifié Cisco UCS version 4.0(4d) et à NetApp ONTAP 9.6, est une architecture de data Center prédéfinie et basée sur les meilleures pratiques. Elle repose sur Cisco UCS, la gamme de commutateurs Cisco Nexus 9000 et les baies de stockage NetApp AFF A-Series.

"Centre de données FlexPod pour solution SAP avec Cisco UCS, structure de troisième génération et NetApp AFF A-Series"

Centre de données FlexPod pour la solution SAP utilisant Fibre Channel SAN avec Cisco UCS Manager 4.0 et NetApp ONTAP 9.7 - Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Cisco et NetApp se sont associés pour proposer une gamme de solutions FlexPod compatibles avec des plateformes de data Center stratégiques. La solution FlexPod propose une architecture intégrée qui intègre les meilleures pratiques de conception en matière de calcul, de stockage et de réseau, réduisant ainsi les risques INFORMATIQUES en validant l'architecture intégrée pour assurer la compatibilité entre les différents composants. La solution répond également aux problématiques IT en fournissant des conseils de conception, des conseils de déploiement et un support documentés qui peuvent être utilisés à différentes étapes (planification, conception et implémentation) d'un déploiement.

"Centre de données FlexPod pour la solution SAP utilisant Fibre Channel SAN avec Cisco UCS Manager 4.0 et NetApp ONTAP 9.7 - Design"

Centre de données FlexPod pour la solution SAP avec Cisco ACI, Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente la solution FlexPod intégrée de l'ACI Cisco comme une approche validée pour le déploiement des environnements SAP HANA TDI (Tailored Data Center Integration). Cette conception validée fournit des instructions et un cadre pour l'implémentation de SAP HANA avec les bonnes pratiques de Cisco et NetApp.

L'architecture de solution recommandée repose sur Cisco Unified Computing System (Cisco UCS) à l'aide d'une version logicielle unifiée qui prend en charge les plateformes matérielles Cisco UCS incluant les composants suivants :

- Les serveurs lames Cisco UCS B-Series et les serveurs rack Cisco UCS C-Series peuvent être configurés avec l'option Intel Optane Data Center persistent Memory module (DCPMM)
- Cisco UCS 6400 Series Fabric Interconnect
- Commutateurs lame et spine Cisco Nexus série 9000
- Baies de stockage de la gamme 100 % Flash de NetApp

En outre, ce document fournit des validations pour Red Hat Enterprise Linux et SUSE Linux Enterprise Server pour SAP HANA.

"Centre de données FlexPod pour la solution SAP avec Cisco ACI, Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design"

Centre de données FlexPod pour SAP avec Cisco ACI, Cisco UCS Manager 4.0, et NetApp AFF A-Series - déploiement

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente les procédures d'architecture et de déploiement de l'option SAP HANA Tailored datacenter Integration sur une infrastructure FlexPod, qui se compose des éléments suivants :

- Cisco UCS Computing System (Cisco UCS) pris en charge par la deuxième génération de processeurs Intel Xeon Scalable.
- Commutation de produits qui utilisent l'ACI (application Centric Infrastructure) de Cisco.
- Baies AFF NetApp A-Series

L'objectif de ce document est de présenter les étapes de configuration détaillées du déploiement de SAP HANA

"Centre de données FlexPod pour SAP avec Cisco ACI, Cisco UCS Manager 4.0, et NetApp AFF A-Series - déploiement"

Centre de données FlexPod pour la solution SAP avec Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente la solution FlexPod de Cisco et NetApp, une approche validée pour le déploiement des environnements SAP HANA TDI (Tailored Data Center Integration). Cette conception validée fournit des instructions et un cadre pour l'implémentation de SAP HANA avec les bonnes pratiques de Cisco et NetApp.

L'infrastructure intégrée de pointe FlexPod prend en charge un large éventail de charges de travail et d'utilisations. Cette solution vous permet de déployer SAP HANA rapidement et de manière fiable avec un modèle de mode d'intégration de data Center sur mesure.

"Centre de données FlexPod pour la solution SAP avec Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design"

Solution FlexPod Datacenter pour SAP avec Cisco ACI sur serveurs Cisco UCS M5 avec SLES 12 SP3 et RHEL 7.4

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document décrit les procédures d'architecture et de déploiement de l'option SAP HANA Tailored datacenter Integration sur une infrastructure FlexPod composée de produits de calcul et de commutation Cisco qui utilisent Cisco application Centric Infrastructure (ACI), la solution logicielle SDN (Software-Defined Networking) leader du secteur, et de baies AFF NetApp A-Series. L'objectif de ce document est de présenter les principes de conception ainsi que les étapes de configuration détaillées pour le déploiement de SAP HANA.

"Solution FlexPod Datacenter pour SAP avec Cisco ACI sur serveurs Cisco UCS M5 avec SLES 12 SP3 et RHEL 7.4"

Centre de données FlexPod pour solution SAP avec stockage basé sur IP, NetApp AFF A-Series et Cisco UCS Manager 3.2

Shailendra Mruthunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

L'architecture de référence détaillée dans ce document met en avant la résilience, les avantages financiers et la facilité de déploiement d'une solution de stockage IP. Un système de stockage capable de prendre en charge plusieurs protocoles sur une interface unique permet au client de choisir et de protéger son investissement, car il s'agit d'une véritable architecture « wire-Once ». La solution est conçue pour héberger des workloads SAP HANA évolutifs.

"Centre de données FlexPod pour solution SAP avec stockage basé sur IP, NetApp AFF A-Series et Cisco UCS Manager 3.2"

Centre de données FlexPod pour la solution SAP utilisant Fibre Channel SAN avec Cisco UCS Manager 4.0 et NetApp ONTAP 9.7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente le centre de données FlexPod de Cisco et NetApp avec NetApp

ONTAP 9.7 sur le système de stockage NetApp AFF A400 et le logiciel unifié Cisco UCS Manager version 4.1(1) avec processeurs évolutifs Xeon de deuxième génération pour SAP HANA en particulier.

Le data Center FlexPod avec NetApp ONTAP 9.7 et le logiciel unifié Cisco UCS 4.1(1) est une architecture de data Center prédéfinie et basée sur les meilleures pratiques. Elle repose sur le système Cisco Unified Computing System (Cisco UCS), la famille de commutateurs Cisco Nexus 9000, les commutateurs de structure multicouche MDS 9000, Et les baies de stockage NetApp AFF A-Series exécutant le système d'exploitation du stockage ONTAP 9.7.

"Centre de données FlexPod pour la solution SAP utilisant Fibre Channel SAN avec Cisco UCS Manager 4.0 et NetApp ONTAP 9.7"

Déployez des serveurs d'applications SAP sur FlexPod avec SQL

FlexPod est une solution de data Center spécialisée et prévalidée conçue pour répondre à l'évolution rapide des besoins des services IT. Cisco et NetApp se sont associés pour proposer FlexPod, qui utilise les meilleurs composants de calcul, de réseau et de stockage pour la base de nombreux workloads d'entreprise, notamment les bases de données, la planification des ressources d'entreprise (ERP), la gestion de la relation client (CRM) et les applications web. La consolidation des applications IT, en particulier des bases de données, a suscité un intérêt considérable ces dernières années. Microsoft SQL Server est la plateforme de base de données la plus utilisée et la plus déployée au cours des dernières années. Les bases de données SQL Server sont souvent confrontées à la prolifération des bases de données, ce qui entraîne des défis INFORMATIQUES tels que des serveurs sous-utilisés, des licences incorrectes, des problèmes de sécurité, des problèmes de gestion et des coûts d'exploitation colossaux. Par conséquent, les bases de données SQL Server sont de bons candidats à la consolidation sur une plateforme plus robuste, plus flexible et plus résiliente. Ce document présente une architecture de référence FlexPod pour le déploiement et la consolidation des bases de données SQL Server.

"Déployez des serveurs d'applications SAP sur FlexPod avec SQL"

Centre de données FlexPod pour SAP avec Cisco ACI, Cisco UCS Manager 4.0 et NetApp AFF A-Series

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente les procédures d'architecture et de déploiement de l'option SAP HANA Tailored datacenter Integration sur une infrastructure FlexPod, qui se compose des éléments suivants :

- Cisco UCS Computing System (Cisco UCS) pris en charge par la deuxième génération de processeurs Intel Xeon Scalable.
- Commutation de produits qui utilisent l'ACI (application Centric Infrastructure) de Cisco.
- Baies AFF NetApp A-Series

"Centre de données FlexPod pour SAP avec Cisco ACI, Cisco UCS Manager 4.0 et NetApp AFF A-Series"

Centre de données FlexPod pour la solution SAP avec Cisco ACI, Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente la solution FlexPod intégrée de l'ACI Cisco comme une approche validée pour le déploiement des environnements SAP HANA TDI (Tailored Data Center Integration). Cette conception validée fournit des instructions et un cadre pour l'implémentation de SAP HANA avec les bonnes pratiques de Cisco et NetApp.

L'architecture de solution recommandée repose sur Cisco Unified Computing System (Cisco UCS) à l'aide d'une version logicielle unifiée qui prend en charge les plateformes matérielles Cisco UCS incluant les composants suivants :

- Les serveurs lames Cisco UCS B-Series et les serveurs rack Cisco UCS C-Series peuvent être configurés avec l'option DCPMM (Data Center persistent Memory module) d'Intel Optane
- Cisco UCS 6400 Series Fabric Interconnect
- Commutateurs lame et spine Cisco Nexus série 9000
- Baies de stockage de la gamme 100 % Flash de NetApp

En outre, ce document fournit des validations pour Red Hat Enterprise Linux et SUSE Linux Enterprise Server pour SAP HANA.

"Centre de données FlexPod pour la solution SAP avec Cisco ACI, Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design"

Centre de données FlexPod pour la solution SAP avec Cisco UCS, une structure de troisième génération et NetApp AFF A-Series

Shailendra Mruthunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

Ce document décrit la méthodologie de déploiement de Cisco et NetApp FlexPod Datacenter pour SAP HANA basée sur le système Cisco UCS Computing System (Cisco UCS) pris en charge par les processeurs évolutifs Intel Xeon de deuxième génération.

Cisco UCS Manager (UCSM) 4.0(4) assure la prise en charge consolidée de tous les modèles Cisco UCS Fabric Interconnect (6200, 6300, 6324 et 6454), d'un module de la gamme 2200/2300, d'un serveur lame Cisco UCS B-Series et de serveurs rack Cisco UCS C-Series. FlexPod Datacenter avec les logiciels unifiés Cisco UCS version 4.0(4d) et NetApp ONTAP 9.6 est une architecture de data Center prédéfinie et basée sur les meilleures pratiques. Elle repose sur Cisco UCS, la gamme de commutateurs Cisco Nexus 9000 et les baies de stockage NetApp AFF A-Series.

"Centre de données FlexPod pour la solution SAP avec Cisco UCS, une structure de troisième génération et NetApp AFF A-Series"

Centre de données FlexPod pour la solution SAP avec Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Ce document présente la solution FlexPod de Cisco et NetApp, une approche validée pour le déploiement des environnements SAP HANA TDI (Tailored Data Center Integration). Cette conception validée fournit des instructions et un cadre pour l'implémentation de SAP HANA avec les bonnes pratiques de Cisco et NetApp.

L'infrastructure intégrée de pointe FlexPod prend en charge un large éventail de charges de travail et d'utilisations. Cette solution vous permet de déployer SAP HANA rapidement et de manière fiable avec un modèle de mode d'intégration de data Center sur mesure.

L'architecture de solution recommandée repose sur Cisco Unified Computing System (Cisco UCS) à l'aide d'une version logicielle unifiée qui prend en charge les plateformes matérielles Cisco UCS incluant les composants suivants :

- Les serveurs lames Cisco UCS B-Series et les serveurs rack Cisco UCS C-Series peuvent être configurés avec l'option du module de mémoire persistante Intel Optane Data Center (DCPMM)
- Cisco UCS 6300 Series Fabric Interconnect
- Commutateurs Cisco Nexus série 9000
- Baies de stockage de la gamme 100 % Flash de NetApp

En outre, ce document fournit des validations pour Red Hat Enterprise Linux et SUSE Linux Enterprise Server pour SAP HANA.

"Centre de données FlexPod pour la solution SAP avec Cisco UCS Manager 4.0 et NetApp AFF A-Series - Design"

Oracle

FlexPod Datacenter avec bases de données Oracle 19c RAC sur Cisco UCS et NetApp AFF avec NVMe over Fibre Channel

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Les conceptions validées par Cisco (CVD) se composent de systèmes et de solutions conçus, testés et documentés pour faciliter et améliorer les déploiements client. Ce document CVD décrit la solution FlexPod de Cisco et NetApp, une approche validée pour le déploiement d'un environnement de base de données RAC Oracle haute disponibilité. Cisco et NetApp ont validé l'architecture de référence avec diverses charges de travail de base de données, telles qu'OLTP (traitement transactionnel en ligne) et entrepôt de données dans le laboratoire Cisco UCS Datacenter. Ce document présente la configuration matérielle et logicielle des composants concernés et les résultats de divers tests. Par ailleurs, ce document offre une structure pour l'implémentation des bases de données Oracle RAC sur NVMe/FC à l'aide de Cisco UCS et de NetApp Storage System.

"FlexPod Datacenter avec bases de données Oracle 19c RAC sur Cisco UCS et NetApp AFF avec NVMe over Fibre Channel"

FlexPod Datacenter avec bases de données Oracle RAC sur Cisco UCS et NetApp AFF A-Series

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Les conceptions validées Cisco comprennent des systèmes et des solutions conçus, testés et documentés pour faciliter et améliorer les déploiements client. Ces conceptions intègrent une large gamme de technologies et de produits dans une gamme de solutions qui ont été développées pour répondre aux besoins commerciaux des clients. Cisco et NetApp se sont associés pour proposer FlexPod, qui sert de base à une grande variété de workloads, et permet des designs architecturaux efficaces basés sur les exigences des clients. Une solution FlexPod est une approche validée pour le déploiement des technologies Cisco et NetApp en tant qu'infrastructure cloud partagée.

Le data Center FlexPod associé au système AFF 100 % Flash de NetApp est une plateforme d'infrastructure convergée qui combine les meilleures technologies de Cisco et NetApp dans une puissante plateforme convergée pour les applications d'entreprise. Cisco et NetApp travaillent en étroite collaboration avec Oracle pour prendre en charge les bases de données transactionnelles et sensibles au temps de réponse les plus exigeantes dont les entreprises modernes ont besoin.

Cette conception validée par Cisco (CVD) décrit l'architecture de data Center FlexPod de référence qui utilise Cisco UCS et le stockage AFF 100 % Flash NetApp pour déployer un environnement de base de données RAC Oracle haute disponibilité. Ce document présente la configuration matérielle et logicielle des composants concernés et les résultats de divers tests. Ce document propose également des conseils sur l'implémentation et les bonnes pratiques à l'aide des serveurs de calcul Cisco UCS, des commutateurs d'interconnexion de fabric Cisco, des commutateurs Cisco MDS, des commutateurs Cisco Nexus, du stockage AFF NetApp et de la base de données Oracle RAC.

"FlexPod Datacenter avec bases de données Oracle RAC sur Cisco UCS et NetApp AFF A-Series"

FlexPod Datacenter avec Oracle RAC sur Oracle Linux

Tushar Patel, Cisco Niranjan Mohapatra, Cisco John Elliott, NetApp

Cisco Unified Computing System (Cisco UCS) est une plateforme de data Center de nouvelle génération qui réunit le calcul, le réseau, l'accès au stockage et la virtualisation au sein d'un système cohésif unique. Cisco UCS est la plateforme idéale pour gérer l'architecture des charges de travail stratégiques des bases de données. L'association de la plateforme Cisco UCS, du stockage NetApp et de l'architecture Oracle Real application Cluster (RAC) peut accélérer la transformation DE votre INFRASTRUCTURE INFORMATIQUE en accélérant les déploiements, en offrant une plus grande flexibilité de choix, une plus grande efficacité et des risques réduits. Ce CVD met en avant une architecture de référence FlexPod flexible, mutualisée, haute performance et résiliente incluant une base de données RAC Oracle 12c.

Développée par NetApp et Cisco, la plateforme FlexPod constitue une solution d'infrastructure intégrée flexible qui offre des technologies prévalidées de stockage, de réseau et de serveur. Son objectif est d'améliorer la réactivité DE L'IT face aux exigences du business tout en réduisant le coût total de l'informatique. Disponibilité maximale, risque minimal. Les composants FlexPod sont intégrés et standardisés afin d'assurer des déploiements rapides, reproductibles et cohérents. Vous pouvez ainsi prévoir avec précision l'alimentation

requise, l'espace au sol, la capacité exploitable, les performances et le coût de chaque déploiement FlexPod.

FlexPod s'appuie sur la toute dernière technologie et simplifie efficacement les workloads du data Center qui redéfinissent la façon dont ILS apportent de la valeur :

- Les baies hybrides NetApp FAS avec Flash Pool permettent de déployer la proportion précise de mémoire Flash sur des supports rotatifs pour votre application ou votre environnement spécifique.
- Tirez parti d'une plateforme prévalidée pour limiter les interruptions de l'activité, améliorer l'agilité DE VOTRE INFRASTRUCTURE IT et réduire le délai de déploiement à quelques semaines, contre plusieurs mois auparavant.
- Réduire le temps d'administration et le coût total de possession de 50 %.
- Répondre aux exigences de performances matérielles en constante augmentation des charges de travail du data Center, voire les dépasser

"FlexPod Datacenter avec Oracle RAC sur Oracle Linux"

FlexPod Datacenter avec bases de données Oracle RAC sur Cisco UCS et NetApp AFF A-Series

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Le data Center FlexPod associé au système AFF 100 % Flash de NetApp est une plateforme d'infrastructure convergée qui combine les meilleures technologies de Cisco et NetApp dans une puissante plateforme convergée pour les applications d'entreprise. Cisco et NetApp travaillent en étroite collaboration avec Oracle pour prendre en charge les bases de données transactionnelles et sensibles au temps de réponse les plus exigeantes dont les entreprises modernes ont besoin.

Cette conception validée par Cisco (CVD) décrit l'architecture de data Center FlexPod de référence qui utilise Cisco UCS et le stockage AFF 100 % Flash NetApp pour déployer un environnement de base de données RAC Oracle haute disponibilité. Ce document présente la configuration matérielle et logicielle des composants concernés et les résultats de divers tests. Ce document propose également des conseils sur l'implémentation et les bonnes pratiques à l'aide des serveurs de calcul Cisco UCS, des commutateurs d'interconnexion de fabric Cisco, des commutateurs Cisco MDS, des commutateurs Cisco Nexus, du stockage AFF NetApp et de la base de données Oracle RAC.

"FlexPod Datacenter avec bases de données Oracle RAC sur Cisco UCS et NetApp AFF A-Series"

Microsoft SQL Server

FlexPod Datacenter pour Microsoft SQL Server 2019 et VMware vSphere 6.7

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Ce document décrit une architecture de référence FlexPod utilisant les produits matériels et logiciels les plus récents et fournit des recommandations de déploiement pour l'hébergement de bases de données Microsoft SQL Server 2019 dans des environnements virtualisés VMware ESXi. Cette solution utilise également Cisco Workload Optimization Manager (CWOM), qui fournit des recommandations automatisées pour une utilisation optimale et efficace des ressources à la fois pour les

charges de travail et l'infrastructure SQL.

La solution est basée sur Cisco Unified Computing System (Cisco UCS) et utilise la version logicielle unifiée 4.1.1c pour prendre en charge les plateformes matérielles Cisco UCS, notamment les serveurs lames Cisco UCS B-Series, les interconnexions de fabric Cisco UCS 6400, les commutateurs Cisco Nexus 9000 et les baies de stockage NetApp AFF.

"FlexPod Datacenter pour Microsoft SQL Server 2019 et VMware vSphere 6.7"

FlexPod Datacenter avec Microsoft SQL Server 2016 et VMware vSphere 6.5

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco David Arnette, NetApp

Ce document présente une architecture de référence FlexPod utilisant les derniers produits matériels et logiciels et fournit des recommandations de configuration pour le déploiement de bases de données Microsoft SQL Server dans un environnement virtualisé.

L'architecture de solution recommandée repose sur Cisco Unified Computing System (Cisco UCS) avec la version logicielle unifiée pour prendre en charge les plateformes matérielles Cisco UCS, notamment les serveurs lames Cisco UCS B-Series, Cisco UCS 6300 Fabric Interconnect, les commutateurs de la gamme Cisco Nexus 9000 et les baies de stockage 100 % Flash NetApp. En outre, cette solution inclut VMware vSphere 6.5 et vSphere 6.5. Elle offre un certain nombre de nouvelles fonctionnalités permettant d'optimiser l'utilisation du stockage et de faciliter le cloud privé.

"FlexPod Datacenter avec Microsoft SQL Server 2016 et VMware vSphere 6.5"

FlexPod Datacenter avec Microsoft SQL Server 2017 sur VM Linux s'exécutant sur VMware et Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Ce document présente une architecture de référence FlexPod utilisant les derniers produits matériels et logiciels et fournit des recommandations de déploiement pour l'hébergement de bases de données Microsoft SQL Server dans les environnements virtualisés VMware ESXi et Microsoft Windows Hyper-V avec prise en charge Linux par Microsoft pour le déploiement SQL Server.

L'architecture de solution recommandée est basée sur Cisco Unified Computing System (Cisco UCS) à l'aide de la version 4.0.1c du logiciel unifié pour prendre en charge les plateformes matérielles Cisco UCS, notamment les serveurs lames Cisco UCS B-Series, les interconnexions de fabric Cisco UCS 6300, les commutateurs Cisco Nexus 9000 et les baies de stockage NetApp AFF.

"FlexPod Datacenter avec Microsoft SQL Server 2017 sur VM Linux s'exécutant sur VMware et Hyper-V."

FlexPod Datacenter avec Microsoft SQL Server 2017 sur VM Linux s'exécutant sur VMware et Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Ce document présente une architecture de référence FlexPod utilisant les derniers

produits matériels et logiciels et fournit des recommandations de déploiement pour l'hébergement de bases de données Microsoft SQL Server dans les environnements virtualisés VMware ESXi et Microsoft Windows Hyper-V avec prise en charge Linux par Microsoft pour le déploiement SQL Server.

L'architecture de solution recommandée est basée sur Cisco Unified Computing System (Cisco UCS) et utilise la version 4.0.1c du logiciel unifié pour prendre en charge les plateformes matérielles Cisco UCS, notamment les serveurs lames Cisco UCS B-Series, les interconnexions de fabric Cisco UCS 6300, les commutateurs Cisco Nexus 9000 et les baies de stockage NetApp AFF.

"FlexPod Datacenter avec Microsoft SQL Server 2017 sur VM Linux s'exécutant sur VMware et Hyper-V."

Santé

FlexPod pour la génomique

Tr-4911 : génomique de l'FlexPod

JayaKishore Esanakula, NetApp

La génomique joue un rôle clé dans la recherche médicale et infirmière. Elle compte peu de domaines de médecine plus importants que la génomique au service de la santé et des sciences de la vie. La génomique, associée à l'imagerie médicale et à la pathologie digitale, nous permet de comprendre comment les gènes d'un patient peuvent être affectés par les protocoles de traitement. La réussite de la génomique dans le domaine de la santé dépend de plus en plus de l'interopérabilité des données à grande échelle. L'objectif final est de donner du sens aux énormes volumes de données génétiques et d'identifier des corrélations et variantes pertinentes sur le plan clinique qui améliorent le diagnostic et rendent la médecine de précision possible. La génomique nous aide à comprendre l'origine des épidémies, la façon dont les maladies évoluent et les traitements et stratégies susceptibles d'être efficaces. De toute évidence, la génomique offre de nombreux avantages qui couvrent la prévention, le diagnostic et le traitement. Les établissements de santé sont aux prises avec plusieurs défis, notamment :

- Amélioration de la qualité des soins
- Soins basés sur la valeur
- Explosion des données
- Médecine de précision
- Pandémies
- Wearables, télésurveillance et soins
- Cybersécurité

Les voies cliniques normalisées et les protocoles cliniques constituent l'une des composantes essentielles de la médecine moderne. L'interopérabilité entre les fournisseurs de soins, pas seulement pour les dossiers médicaux, mais aussi pour les données génomiques, est un des aspects clés de la standardisation. La question majeure est-ce que les établissements de santé vont abandonner la propriété des données génomiques au lieu de la propriété des patients pour leurs données génomiques personnelles et les dossiers médicaux connexes ?

L'interopérabilité des données des patients est essentielle pour permettre une médecine de précision, l'un des moteurs de la récente explosion des données. L'objectif de la médecine de précision est de rendre le maintien de la santé, la prévention des maladies, les diagnostics et les solutions de traitement plus efficaces et plus précis.

Le taux de croissance des données a été exponentiel. Début février 2021, les laboratoires américains ont séquencé environ 8,000 souches de COVID-19 par semaine. Le nombre de génomes séquencés était passé à 29,000 par semaine en avril 2021. Chaque génome humain complètement séquencé est d'environ 125 Go. Par conséquent, à un rythme de 29,000 génomes par semaine, le stockage total du génome au repos serait donc de plus de 180 pétaoctets par an. Divers pays ont consacré des ressources à l'épidémiologie génomique

afin d'améliorer la surveillance génomique et de se préparer à la prochaine vague de défis mondiaux en matière de santé.

La réduction du coût de la recherche génomique favorise les tests et la recherche génétiques à un rythme sans précédent. Les trois PS se situent à un point d'inflexion : la puissance informatique, la confidentialité des données et la personnalisation de la médecine. D'ici 2025, les chercheurs estiment que 100 millions à près de 2 milliards de génomes humains seront séquencés. Pour que la génomique soit efficace et une proposition précieuse, les capacités génomiques doivent faire partie intégrante des flux de travail des soins ; il doit être facile d'accéder et d'être exploitable lors de la visite d'un patient. Il est également important d'intégrer les données médicales électroniques des patients dans les données génomiques des patients. Avec l'arrivée de l'infrastructure convergée de pointe comme FlexPod, les entreprises peuvent intégrer leurs fonctionnalités génomiques dans les workflows quotidiens des médecins, des infirmiers et des responsables des cliniques. Pour obtenir les toutes dernières informations sur la plate-forme FlexPod, reportez-vous à ce document "Livre blanc FlexPod Datacenter avec Cisco UCS X-Series".

Pour un médecin, toute la valeur de la génomique inclut une médecine de précision et des plans de traitement personnalisés basés sur les données génomiques d'un patient. Par le passé, les médecins et les scientifiques des données n'ont jamais connu une telle synergie, et la génomique bénéficie des innovations technologiques récentes, ainsi que de partenariats réels entre les organismes de santé et les leaders technologiques du secteur.

Les centres médicaux universitaires et d'autres organismes de soins de santé et de sciences de la vie sont en bonne voie pour établir un centre d'excellence (COE) en science du génome. Selon M. Charlie Gersbach, Dr Greg Crawford, et le docteur Tim E Reddy de l'Université Duke : « nous savons que les gènes ne sont pas activés ou désactivés par un simple commutateur binaire, mais plutôt le résultat de multiples commutateurs de régulation génétique qui fonctionnent ensemble. Ils ont également déterminé que « aucune de ces parties du génome ne fonctionne isolément. Le génome est un web très complexe que l'évolution a tissé » ("réf").

NetApp et Cisco se sont acharné à mettre en œuvre des améliorations incrémentielles de la plateforme FlexPod depuis plus de 10 ans. Tous les commentaires des clients sont entendus, évalués et liés aux flux de valeur et aux fonctionnalités de FlexPod. C'est ce processus continu de retour d'informations, de collaboration, d'amélioration et de célébration qui fait de FlexPod une plateforme d'infrastructure convergée de confiance au monde entier. Elles ont été simplifiées et conçues dès le départ pour être la plateforme la plus fiable, robuste, polyvalente et agile des établissements de santé.

Portée

La plateforme d'infrastructure convergée FlexPod permet à un établissement de santé d'héberger un ou plusieurs workloads de génomique avec d'autres applications cliniques et non cliniques de santé. Dans ce rapport technique, nous fait appel à un outil génomique open source standard appelé GATK lors de la validation de la plateforme FlexPod. Toutefois, une discussion plus approfondie de la génomique ou de la GATK est en dehors de la portée de ce document.

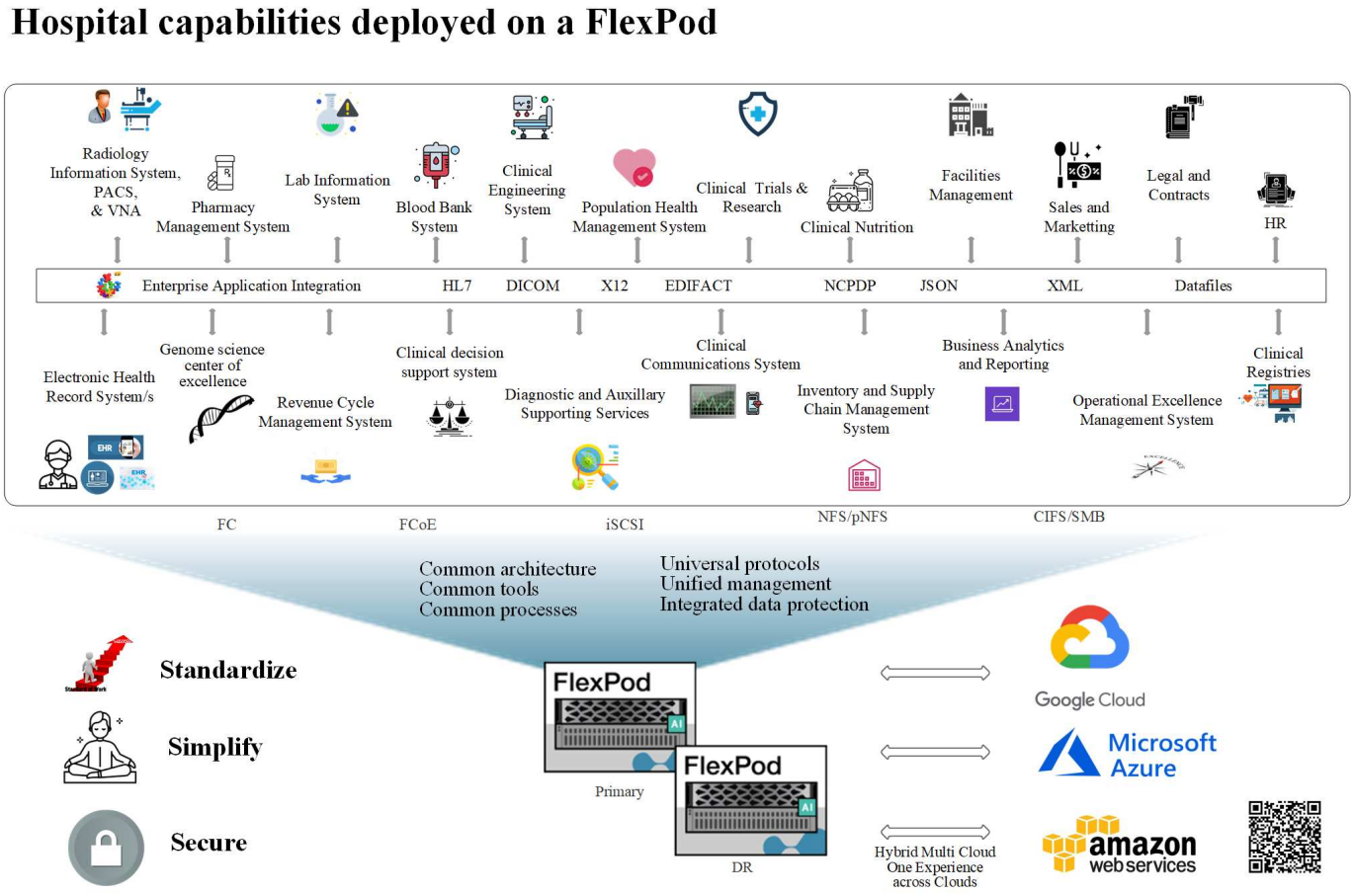
Public

Ce document est destiné aux leaders techniques du secteur de la santé, aux ingénieurs solutions partenaires Cisco et NetApp et aux équipes des services professionnels. NetApp suppose que le lecteur connaît bien les concepts de dimensionnement du stockage et du calcul, ainsi que la connaissance technique des menaces médicales, de la sécurité sanitaire, des systèmes IT de santé, de Cisco UCS et des systèmes de stockage NetApp.

Les capacités de l'hôpital sont déployées sur FlexPod

Un hôpital typique possède un ensemble diversifié de systèmes INFORMATIQUES. La majorité de ces systèmes sont achetés auprès d'un fournisseur, alors que très peu sont construits par le système hospitalier

en interne. C'est pourquoi le système hospitalier doit gérer un environnement d'infrastructure diversifié dans ses data centers. Lorsque les hôpitaux unifient leurs systèmes sur une plateforme d'infrastructure convergée telle que FlexPod, les entreprises peuvent standardiser les opérations de leur data Center. Avec FlexPod, les établissements de santé peuvent mettre en place des systèmes cliniques et non cliniques sur une même plateforme, unifiant ainsi les opérations du data Center.



"Ensuite, les avantages du déploiement de workloads génomiques avec FlexPod."

Avantages liés au déploiement de workloads génomiques avec FlexPod

"Précédent : introduction."

Dans cette section, vous trouverez un bref aperçu des avantages dont vous pouvez bénéficier pour exécuter un workload génomique sur une plateforme d'infrastructure convergée FlexPod. Décrire rapidement les capacités d'un hôpital. L'architecture métier suivante montre les capacités d'un hôpital déployées sur une plateforme d'infrastructure convergée FlexPod prête pour le cloud hybride.

- **Éviter les silos dans les soins de santé.** les silos dans les soins de santé sont une préoccupation très réelle. Elles sont souvent cloisonnées dans leur propre ensemble de matériel et de logiciels, et non pas selon leur choix, mais de façon organique par leur évolution. Par exemple, radiologie, cardiologie, EHR, génomique, les analyses, les cycles de revenus et les autres départements se terminent par leur jeu individuel de logiciels et de matériel dédiés. Les organismes de santé disposent d'un ensemble limité de professionnels IT pour gérer leurs ressources matérielles et logicielles. Le point d'inflexion s'est produit lorsque ce groupe de particuliers doit gérer un ensemble très diversifié de matériel et de logiciels. L'hétérogénéité est aggravée par un ensemble peu homogène de processus mis en place par les

fournisseurs dans l'organisation de soins de santé.

- **Démarrer petit et grandir.** le kit d'outils GATK est réglé pour l'exécution de la CPU, qui les meilleures suites plates-formes comme FlexPod. FlexPod offre une évolutivité indépendante du réseau, du calcul et du stockage. Commencez par une infrastructure de petite taille et faites-la évoluer à mesure que vos capacités en génomique et votre environnement se développent. Les organismes de santé n'ont pas à investir dans des plateformes spécialisées pour gérer des charges de travail génomiques. Les entreprises peuvent ainsi exploiter des plateformes polyvalentes telles qu'un système FlexPod pour exécuter des charges de travail génomiques et non génomiques sur une même plateforme. Par exemple, si le service de pédiatrie souhaite mettre en œuvre une fonctionnalité de génomique, le leadership INFORMATIQUE peut provisionner les ressources de calcul, de stockage et de réseau sur une instance FlexPod existante. À mesure que l'entité commerciale génomique se développe, le secteur de la santé peut faire évoluer sa plateforme FlexPod en fonction des besoins.
- **Panneau de contrôle unique et flexibilité inégalée.** Cisco Intersight simplifie considérablement les opérations INFORMATIQUES en rapprochant les applications de l'infrastructure, en fournissant la visibilité et la gestion des serveurs bare-Metal et des hyperviseurs aux applications sans serveur, réduisant ainsi les coûts et les risques. Cette plateforme SaaS unifiée s'intègre de façon native aux plateformes et outils tiers. Elle permet en outre de gérer l'ensemble des opérations de votre data Center sur site ou en tout lieu, à l'aide d'une application mobile.

  Les utilisateurs valorisent rapidement leur environnement en utilisant Intersight comme plateforme de gestion. En permettant l'automatisation de nombreuses tâches manuelles quotidiennes, InterSight élimine les erreurs et simplifie vos opérations quotidiennes. En outre, les capacités de support avancées offertes par Intersight permettent aux utilisateurs de garder une longueur d'avance et d'accélérer la résolution des problèmes. Combinées, les entreprises réduisent considérablement leur infrastructure applicative et consacrent plus de temps au développement de leur activité principale.

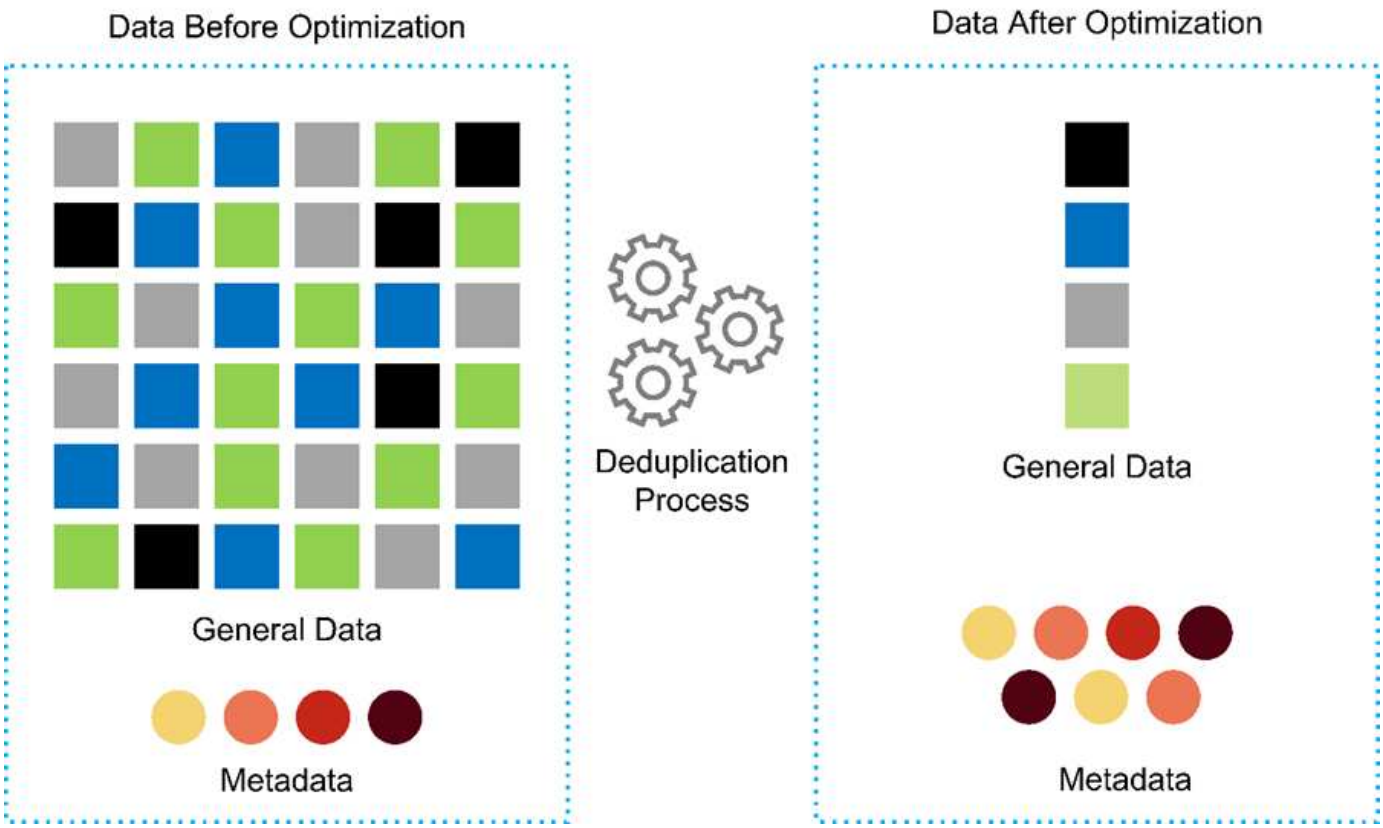
  En tirant parti de la gestion Intersight et de l'architecture facilement évolutive de FlexPod, les entreprises peuvent exécuter plusieurs charges de travail du génome sur une plateforme FlexPod unique, ce qui améliore le taux d'utilisation et réduit le coût total de possession (TCO). FlexPod offre des possibilités de dimensionnement flexibles, avec des choix parmi notre petite infrastructure FlexPod Express et une évolutivité vers de grandes implémentations FlexPod Datacenter. Grâce aux fonctionnalités de contrôle d'accès basées sur des rôles intégrées dans Cisco InterSight, les établissements de santé peuvent mettre en place des mécanismes de contrôle d'accès robustes, ce qui évite d'avoir recours à des piles d'infrastructure distinctes. Plusieurs entités commerciales peuvent exploiter la génomique comme une compétence clé dans le domaine de la santé.

  En définitive, FlexPod simplifie les opérations IT et réduit les coûts d'exploitation, et permet aux administrateurs D'infrastructure IT de se concentrer sur des tâches permettant aux médecins d'innover au lieu de rester relégués au second plan.

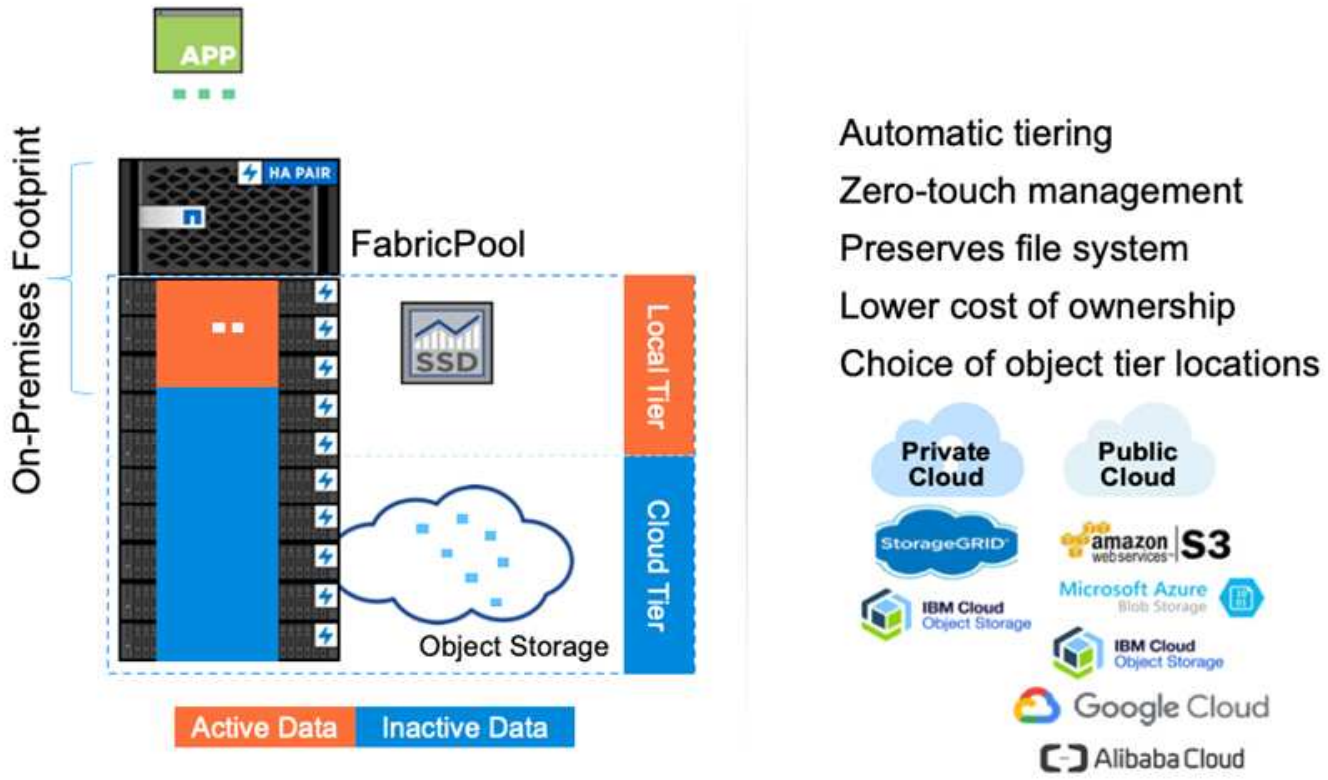
- **Conception validée et résultats garantis.** les guides de conception et de déploiement FlexPod sont validés de manière reproductible et couvrent les détails complets de la configuration et les meilleures pratiques du secteur nécessaires au déploiement en toute confiance d'un FlexPod. Les guides de conception validée par Cisco et NetApp, les guides de déploiement et les architectures aident votre département des soins de santé ou des sciences de la vie à éviter toute approximation lors de la mise en œuvre d'une plateforme validée et fiable dès le départ. Avec FlexPod, vous accélérez les délais de déploiement, tout en réduisant les coûts, la complexité et les risques. Les designs validés et les guides de déploiement de FlexPod établissent le FlexPod comme plateforme idéale pour de nombreuses charges de travail génomiques.
- **Innovation et agilité.** FlexPod est recommandé comme plate-forme idéale par les EHR comme Epic, Cerner, Meditech et les systèmes d'imagerie comme Agfa, GE, Philips. Pour plus d'informations sur "Le programme « Epic Honor roll »" Et l'architecture de la plateforme cible, consultez le site Web d'Epic userweb. Une bonne exécution de la génomique "FlexPod" permet aux établissements de santé de

poursuivre leur transition vers l'innovation avec agilité. Avec FlexPod, la mise en œuvre de changements organisationnels est naturelle. Lorsque les entreprises optent pour une plateforme FlexPod, les experts du secteur de la santé peuvent provisionner leur temps, leurs efforts et leurs ressources pour innover, et ainsi être aussi agiles que les besoins de l'écosystème.

- **Données libérées.** avec la plateforme d'infrastructure convergée FlexPod et un système de stockage NetApp ONTAP, les données génomiques peuvent être disponibles et accessibles à l'aide d'un large éventail de protocoles à grande échelle depuis une plateforme unique. FlexPod avec NetApp ONTAP propose une plateforme de cloud hybride simple, intuitive et puissante. Votre Data Fabric optimisé par NetApp ONTAP offre un maillage sur l'ensemble des sites, des emplacements physiques et des applications, Votre Data Fabric est conçue pour un monde centré sur la donnée. Les données étant créées et exploitées dans divers emplacements et, la plupart du temps, partagées avec d'autres sites, applications et infrastructures, C'est pourquoi il vous faut une méthode de gestion cohérente et intégrée. FlexPod permet à votre équipe IT de maîtriser et de simplifier une INFRASTRUCTURE IT toujours plus complexe.
- **Colocation sécurisée.** FlexPod utilise des modules cryptographiques conformes à la norme FIPS 140-2, ce qui permet aux entreprises de mettre en œuvre la sécurité comme élément fondamental, et non comme élément secondaire. FlexPod permet aux entreprises d'implémenter une colocation sécurisée à partir d'une plateforme d'infrastructure convergée unique, quelle que soit leur taille. FlexPod avec colocation sécurisée et qualité de service pour séparer les charges de travail et optimiser l'utilisation. Cela permet d'éviter que le capital soit dépendant de plateformes spécialisées sous-utilisées et que la gestion requiert une compétence spécialisée.
- **Efficacité du stockage.** la génomique exige que le stockage sous-jacent offre des fonctionnalités d'efficacité du stockage de pointe. Vous pouvez réduire les coûts du stockage grâce aux fonctionnalités d'efficacité du stockage NetApp, telles que la déduplication (à la volée et à la demande), la compression et la compaction des données ("réf"). La déduplication NetApp fournit une déduplication au niveau des blocs dans un volume FlexVol. Pour schématiser, la déduplication supprime les blocs dupliqués et ne stocke que les blocs uniques dans le volume FlexVol. La déduplication, qui fonctionne avec un niveau de granularité élevé, fonctionne sur le système de fichiers actif du volume FlexVol. La figure suivante présente le fonctionnement de la déduplication NetApp. La déduplication est transparente pour les applications. Par conséquent, elle peut être utilisée pour dédupliquer des données provenant de toute application qui utilise le système NetApp. Vous pouvez exécuter la déduplication volume comme processus à la volée ou en arrière-plan. Vous pouvez le configurer pour qu'il s'exécute automatiquement, de manière à être planifié ou manuellement via l'interface de ligne de commande, NetApp ONTAP System Manager ou NetApp Active IQ Unified Manager.



- **Activer l'interopérabilité génomique.** ONTAP FlexCache est une fonctionnalité de mise en cache à distance qui simplifie la distribution de fichiers, réduit la latence WAN et réduit les coûts de bande passante WAN ("réf"). L'une des principales activités durant l'identification et l'annotation des variantes génomiques est la collaboration entre les cliniciens. La technologie ONTAP FlexCache augmente le débit de données même lorsque les médecins travaillent en collaboration à différents endroits. Étant donné la taille type d'un fichier *.BAM (1 Go à des centaines de Go), il est essentiel que la plate-forme sous-jacente puisse mettre des fichiers à la disposition des cliniciens dans différents emplacements géographiques. Avec FlexPod et ONTAP FlexCache, les données et les applications génomiques sont réellement prêtes pour plusieurs sites afin que la collaboration entre les chercheurs du monde entier s'effectue de manière fluide, avec une faible latence et un débit élevé. Les organismes de santé qui exécutent des applications génomiques dans un environnement multisite peuvent évoluer horizontalement avec la Data Fabric pour équilibrer la gestion avec la vitesse et les coûts.
- **Utilisation intelligente de la plate-forme de stockage.** La gestion des données est simplifiée grâce à FlexPod avec le Tiering automatique ONTAP et la technologie NetApp FabricPool. FabricPool permet de réduire les coûts de stockage sans nuire aux performances, à l'efficacité, à la sécurité ou à la protection. FabricPool est transparent pour les applications d'entreprise et capitalise sur l'efficacité du cloud en réduisant le TCO du stockage sans devoir repenser l'architecture de l'infrastructure applicative. FlexPod bénéficie des fonctionnalités de hiérarchisation du stockage de FabricPool pour une utilisation plus efficace du stockage Flash ONTAP. Pour plus d'informations, voir "FlexPod avec FabricPool". Le diagramme suivant présente FabricPool et ses avantages.



- **Analyse et annotation des variantes plus rapides.** la plate-forme FlexPod est plus rapide à déployer et opérationnaliser. Avec la plateforme FlexPod, les médecins peuvent collaborer avec les médecins en rendant les données à grande échelle, avec une faible latence et un débit plus élevé. L'interopérabilité accrue favorise l'innovation. Les établissements de santé peuvent traiter leurs workloads génomiques et non génomiques, ce qui signifie qu'elles n'ont pas besoin de plateformes spécialisées pour commencer leur transition vers la génomique.

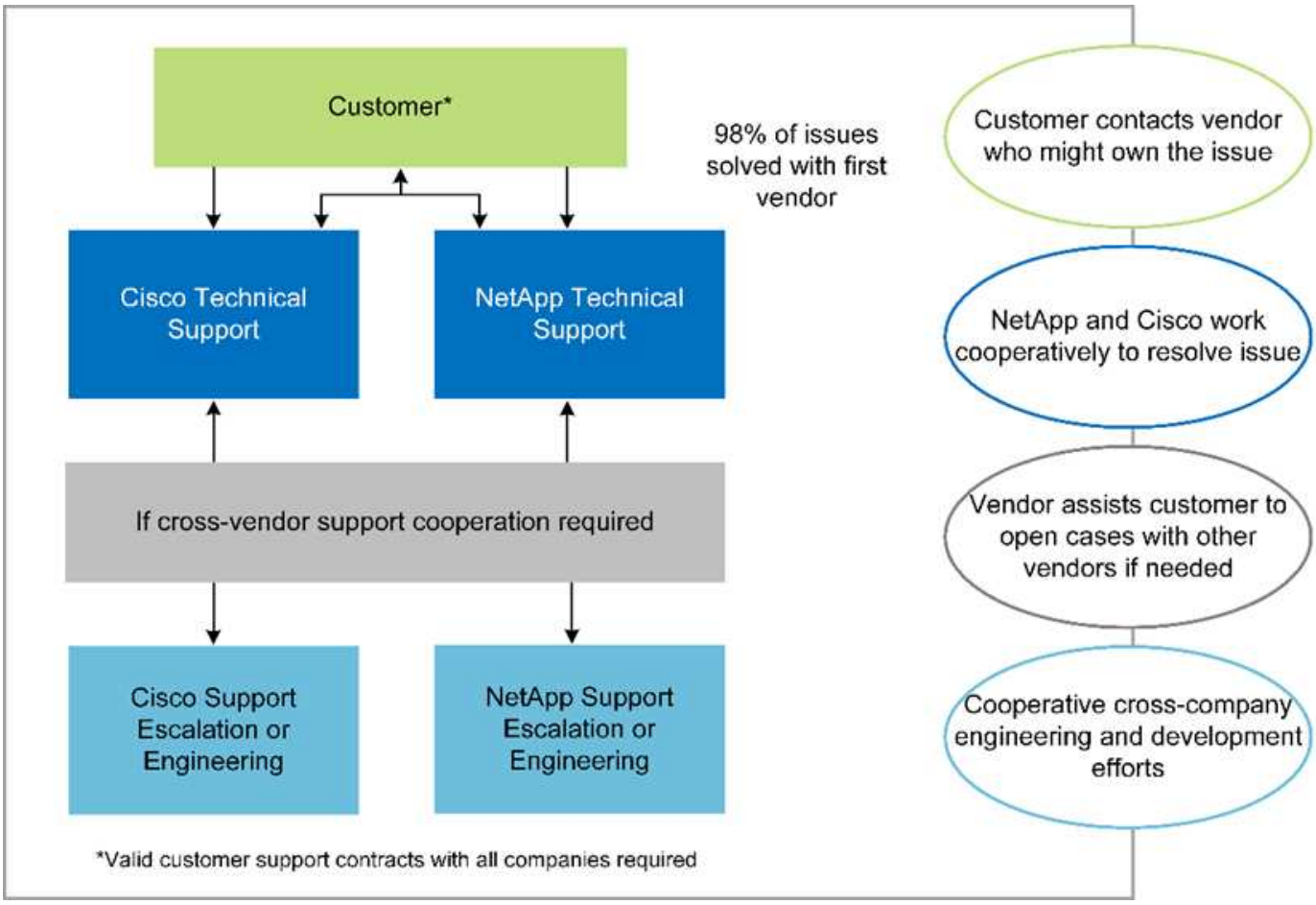
  FlexPod ONTAP ajoute régulièrement des fonctionnalités de pointe à la plateforme de stockage. FlexPod Datacenter constitue une base d'infrastructure partagée idéale pour déployer la technologie FC- NVMe afin d'autoriser l'accès au stockage haute performance aux applications en besoin. Au fur et à mesure que la connectivité FC- NVMe évolue, incluant la haute disponibilité, les chemins d'accès multiples et une prise en charge supplémentaire du système d'exploitation, FlexPod convient aussi bien à la plateforme de choix, offrant l'évolutivité et la fiabilité nécessaires pour prendre en charge ces fonctionnalités. Grâce à la technologie ONTAP dotée d'E/S plus rapides et à la technologie NVMe de bout en bout, les analyses génomiques sont plus rapides ("réf").

  Les données de génome brut séquencé génèrent des fichiers de grandes tailles et il est important que ces fichiers soient mis à la disposition des analyseurs variantes pour réduire le temps total nécessaire de la collecte des échantillons à l'annotation des variantes. NVMe (Nonvolatile Memory Express), utilisé comme protocole d'accès au stockage et de transport de données, offre un débit sans précédent et des délais de réponse très courts. FlexPod déploie le protocole NVMe en accédant au stockage Flash via le bus PCI express (PCIe). Grâce à l'implémentation de dizaines de milliers de files d'attente de commandes, il est possible d'augmenter la parallélisation et le débit. Un protocole unique, du stockage à la mémoire, permet un accès rapide aux données.

- * L'agilité pour la recherche clinique depuis le départ.* la capacité de stockage flexible et extensible et la performance permet aux organismes de recherche en santé d'optimiser l'environnement de façon élastique ou juste-à-temps (JIT). En découplant le stockage de l'infrastructure de calcul et de réseau, la plateforme FlexPod peut évoluer verticalement et horizontalement sans perturbation. Grâce à Cisco

Intersight, la plateforme FlexPod peut être gérée à l'aide de flux de travail automatisés intégrés et personnalisés. Les workflows Cisco Intersight permettent aux établissements de santé de réduire la durée de gestion du cycle de vie des applications. Lorsqu'un centre médical universitaire exige que les données des patients soient anonymisées et mises à disposition par son centre d'informatique pour la recherche et/ou d'un centre de qualité, le service IT peut exploiter les workflows Cisco Intersight FlexPod pour effectuer des sauvegardes de données sécurisées, cloner et restaurer les données en quelques secondes, et non plus en quelques heures. Avec NetApp Trident et Kubernetes, les départements IT peuvent provisionner de nouveaux data Scientists et rendre les données cliniques disponibles pour le développement des modèles en quelques minutes, parfois même en quelques secondes.

- **Protection des données du génome.** NetApp SnapLock offre un volume spécial dans lequel les fichiers peuvent être stockés et archivés à un état non effaçable et non réinscriptible. Les données de production de l'utilisateur résidant dans un volume FlexVol peuvent être mises en miroir ou archivées sur un volume SnapLock grâce à la technologie NetApp SnapMirror ou SnapVault. Les fichiers du volume SnapLock, le volume lui-même et son agrégat d'hébergement ne peuvent pas être supprimés avant la fin de la période de conservation. Grâce au logiciel ONTAP FPolicy, les organisations peuvent empêcher les attaques par ransomware en désautorisant les opérations sur des fichiers avec des extensions spécifiques. Un événement FPolicy peut être déclenché pour des opérations de fichiers spécifiques. L'événement est lié à une politique, qui appelle le moteur qu'il doit utiliser. Vous pouvez configurer une règle avec un ensemble d'extensions de fichiers qui pourraient éventuellement contenir un ransomware. Lorsqu'un fichier doté d'une extension non autorisée tente d'effectuer une opération non autorisée, FPolicy empêche cette opération ("réf").
- **Support coopératif FlexPod.** NetApp et Cisco ont mis en place le modèle de support coopératif FlexPod, un modèle de support solide, évolutif et flexible, afin de répondre aux exigences de support uniques de l'infrastructure convergée FlexPod. Ce modèle tire parti de l'expérience, des ressources et de l'expertise de NetApp et de Cisco pour simplifier l'identification et la résolution des problèmes de support FlexPod, et ce, quelle que soit l'origine du problème. La figure suivante présente le modèle de support coopératif FlexPod. Le client contacte le fournisseur responsable du problème et travaille en collaboration avec Cisco et NetApp pour le résoudre. Cisco et NetApp ont des équipes d'ingénierie et de développement interentreprises qui travaillent main dans la main pour résoudre les problèmes. Ce modèle de support réduit la perte d'informations pendant la traduction, favorise la confiance et réduit les temps d'arrêt.

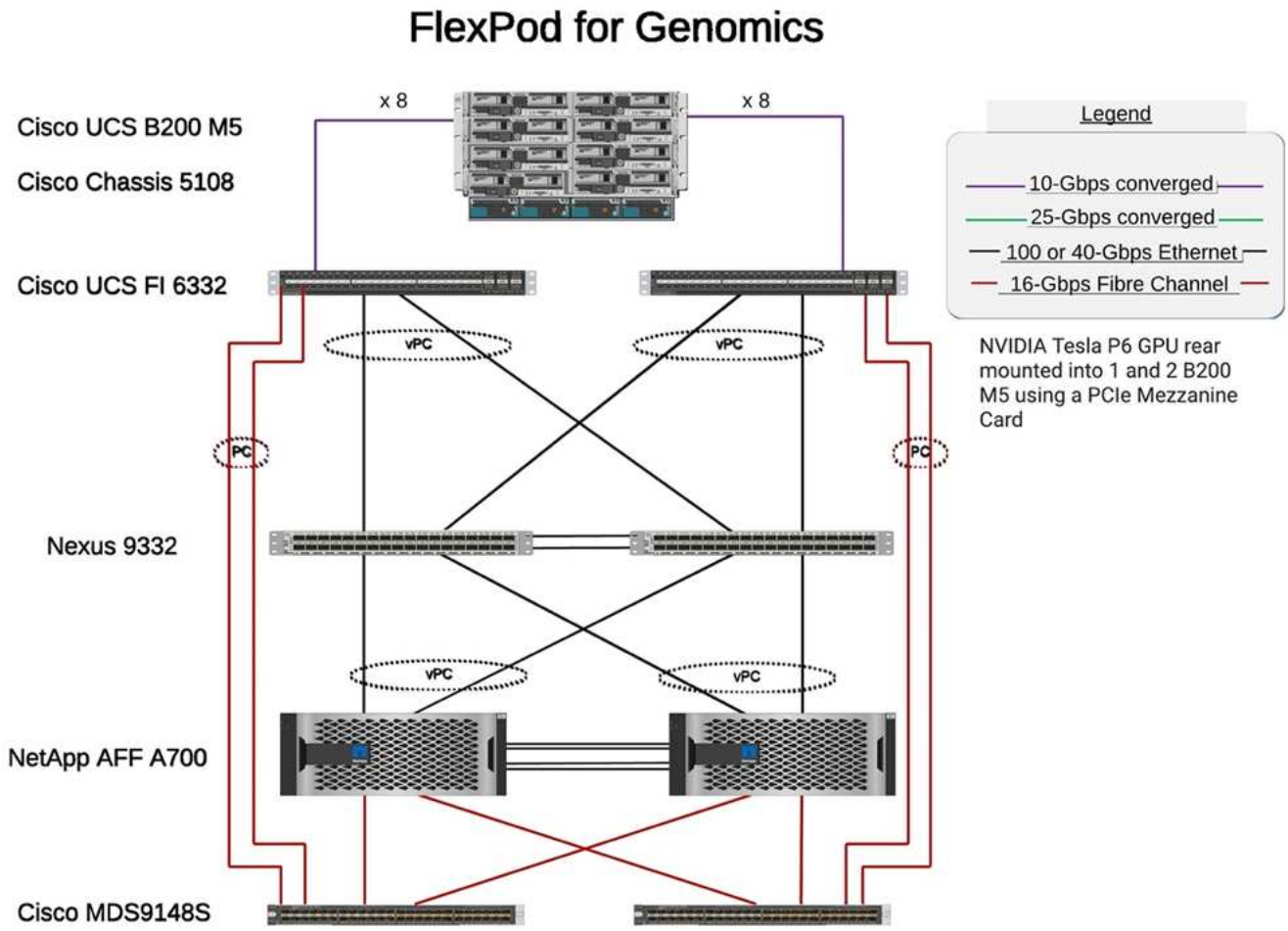


"Ensuite : composants matériels et logiciels de l’infrastructure de la solution."

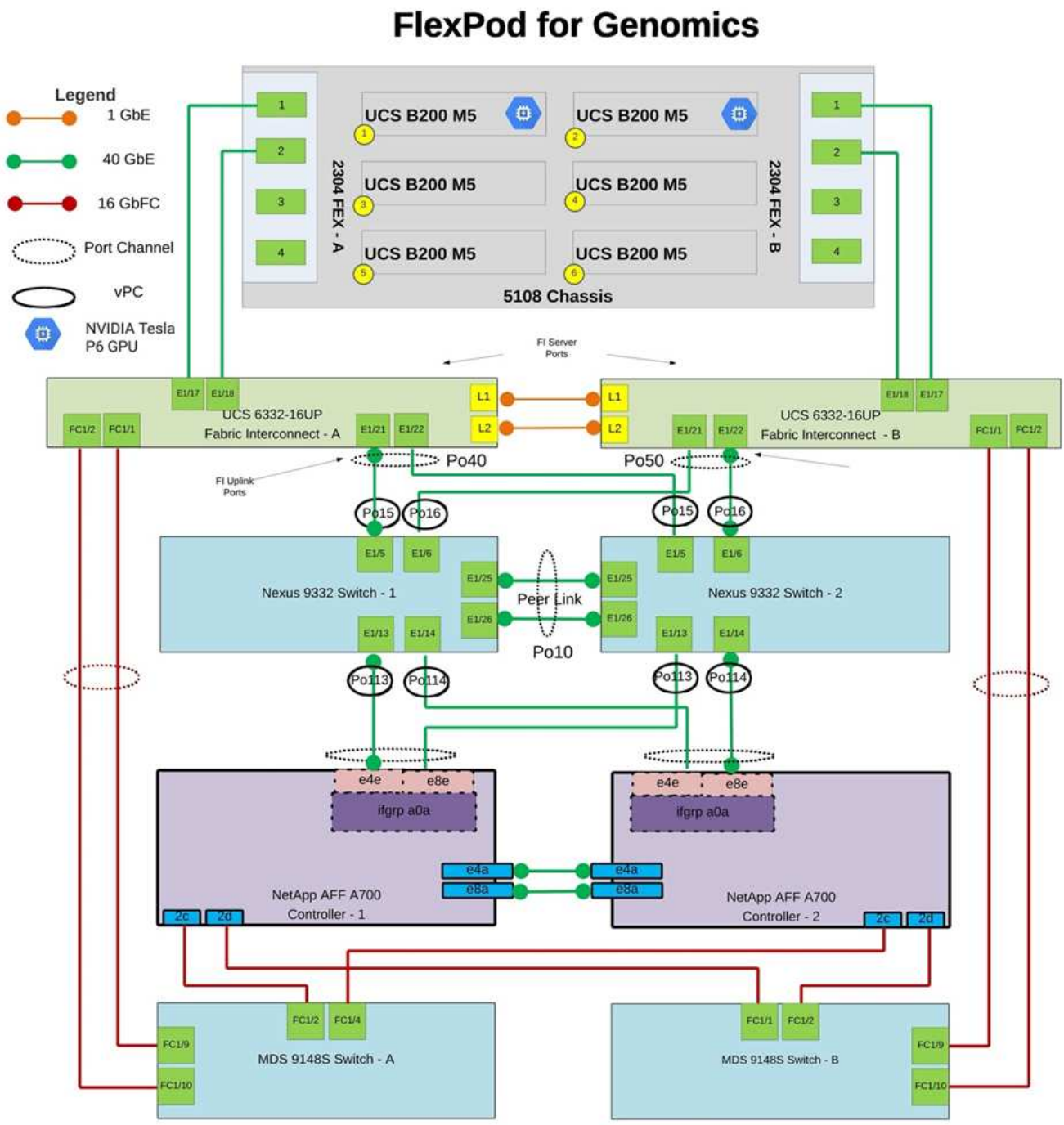
Composants matériels et logiciels de l’infrastructure de la solution

"Précédent : avantages liés au déploiement des workloads génomiques avec FlexPod."

La figure suivante illustre le système FlexPod utilisé pour la configuration et la validation de la GATK. Nous avons utilisé "FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7 conception validée par Cisco (CVD)" pendant le processus de configuration.



Le diagramme suivant représente les détails du câblage FlexPod.



Le tableau suivant répertorie les composants matériels utilisés lors du test GATK en activant sur un FlexPod. Voici le "Matrice d'interopérabilité NetApp" (IMT) et "Liste de compatibilité matérielle Cisco (HCL)".

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1 ou 2	
	Les serveurs lames Cisco UCS	6 B200 M5	Chacun doté de 2 20 cœurs ou plus, de 2,7 GHz et de 128 Go de RAM

Calque	Famille de produits	Quantité et modèle	Détails
	Carte d'interface virtuelle Cisco UCS (VIC)	Cisco UCS 1440	Voir la
	2 interconnexions de fabric Cisco UCS	6332	-
Le réseau	Commutateurs Cisco Nexus	2 x Cisco Nexus 9332	-
Réseau de stockage	Réseau IP pour l'accès au stockage via les protocoles SMB/CIFS, NFS ou iSCSI	Mêmes commutateurs réseau que ci-dessus	-
	Accès au stockage via FC	2 x Cisco MDS 9148S	-
Stockage	Système de stockage 100 % Flash NetApp AFF A700	1 Cluster	Cluster à deux nœuds
	Tiroir disque	Un tiroir disque DS224C ou NS224	Plein avec 24 disques
	SSD	24, 1,2 To ou plus	-

Ce tableau répertorie le logiciel de l'infrastructure.

Logiciel	Famille de produits	Version ou version	Détails
Divers	Linux	RHEL 8.3	-
	Répertoires de base	Windows Server 2012 R2 (64 bits)	-
	NetApp ONTAP	ONTAP 9.8 ou version ultérieure	-
	Fabric Interconnect Cisco UCS	Cisco UCS Manager 4.1 ou version ultérieure	-
	Switchs Cisco Ethernet 3000 ou 9000	Pour la série 9000, 7.0(3)I7(7) ou ultérieure pour la série 3000, 9.2(4) ou ultérieure	-
	Cisco FC : Cisco MDS 9132T	8.4(1a) ou ultérieure	-
	Hyperviseur	VMware vSphere ESXi 7.0	-
Stockage	Système de gestion de l'hyperviseur	VMware vCenter Server 7.0 (vCSA) ou version ultérieure	-
Le réseau	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	-

Logiciel	Famille de produits	Version ou version	Détails
	NetApp SnapCenter	SnapCenter 4.3 ou version ultérieure	-
	Cisco UCS Manager	4.1(3c) ou ultérieure	
Hyperviseur	VMware ESXi		
Gestion	Système de gestion de l'hyperviseur VMware vCenter Server 7.0 (vCSA) ou version ultérieure		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	
	NetApp SnapCenter	SnapCenter 4.3 ou version ultérieure	
	Cisco UCS Manager	4.1(3c) ou ultérieure	

"Suivant: Génomique - Configuration et exécution de la GATK."

Génomique - configuration et exécution de la GATK

"Précédent : composants matériels et logiciels de l'infrastructure de la solution."

Selon l'Institut national de recherche sur le génome humain ("NHGRI"), « la génomique est l'étude de tous les gènes d'une personne (le génome), y compris les interactions entre ces gènes et avec l'environnement d'une personne. "

Selon le "NHGRI", "L'acide désoxyribonucléique (ADN) est le composé chimique qui contient les instructions nécessaires pour développer et diriger les activités de presque tous les organismes vivants. Les molécules d'ADN sont faites de deux torons couplés, souvent appelés « hélice double ». « L'ensemble complet d'ADN d'un organisme est appelé son génome. »

Le séquençage est le processus de détermination de l'ordre exact des bases dans un brin d'ADN. L'un des types de séquençage les plus courants utilisés aujourd'hui est appelé séquençage par synthèse. Cette technique utilise l'émission de signaux fluorescents pour commander les bases. Les chercheurs peuvent utiliser le séquençage de l'ADN pour rechercher des variations génétiques et des mutations susceptibles de jouer un rôle dans le développement ou la progression d'une maladie alors qu'une personne est encore au stade embryonnaire.

De l'identification de l'échantillon à la variante, de l'annotation et de la prédiction

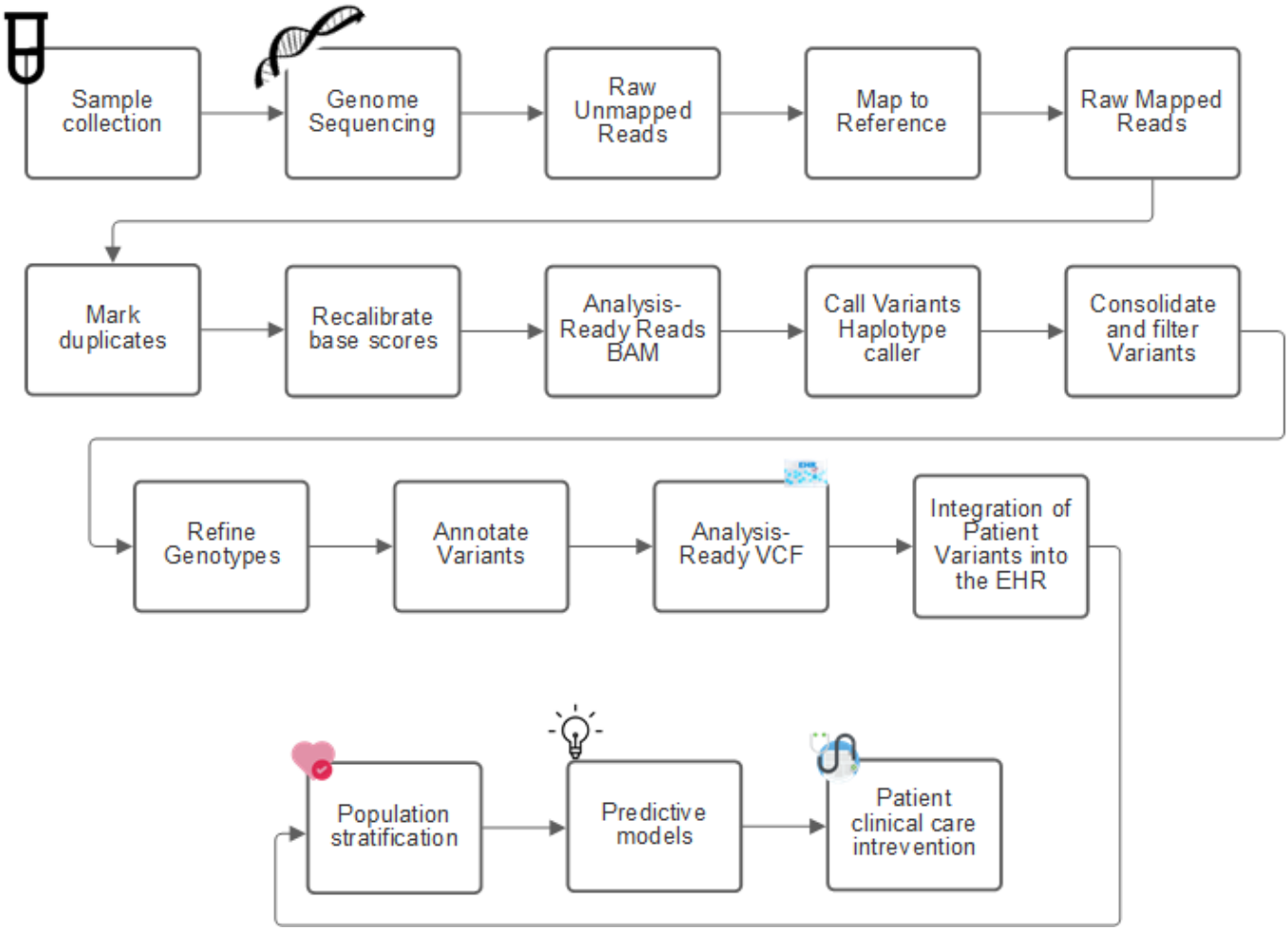
À un niveau élevé, la génomique peut être classée comme suit. Cette liste n'est pas exhaustive :

1. Prélèvement d'échantillons.
2. "Séquençage du génome" utilisation d'un séquenceur pour générer les données brutes.
3. Prétraitement. Par exemple : "déduplication" à l'aide de "Picard".
4. Analyse génomique.
    a. Mappage sur un génome de référence.

b. "Variante" Identification et annotation effectuées généralement à l'aide de la GATK et d'outils similaires.

5. Intégration au système de dossier médical électronique (EHR).
6. "Stratification de la population" et l'identification de la variation génétique entre la localisation géographique et le milieu ethnique.
7. "Modèles prédictifs" utilisant un polymorphisme significatif de nucléotide unique.
8. "Validation".

La figure suivante montre le processus de l'échantillonnage à l'identification de variante, à l'annotation et à la prédiction.



Le projet sur le génome humain a été achevé en avril 2003 et le projet a réalisé une simulation de très haute qualité de la séquence du génome humain disponible dans le domaine public. Ce génome de référence a initié une explosion de la recherche et du développement de capacités en génomique. Pratiquement chaque affection humaine a une signature dans les gènes de cet homme. Jusqu'à récemment, les médecins utilisaient les gènes pour prédire et déterminer les anomalies congénitales comme l'anémie falciforme, qui est causée par un certain modèle d'héritage causé par un changement dans un gène unique. Le Trésor des données mises à disposition par le projet du génome humain a conduit à l'avènement de l'état actuel des capacités en génomique.

La génomique offre de nombreux avantages. Voici quelques avantages dans le domaine de la santé et des sciences de la vie :

- Un meilleur diagnostic sur le lieu des soins

- Meilleur pronostic
- Médecine de précision
- Plans de traitement personnalisés
- Une meilleure surveillance des maladies
- Réduction des événements indésirables
- Amélioration de l'accès aux thérapies
- Amélioration de la surveillance des maladies
- Participation efficace aux essais cliniques et meilleure sélection des patients pour les essais cliniques basés sur les génotypes.

La génomique est une "bête à quatre têtes," compte tenu des besoins de calcul tout au long du cycle de vie d'un dataset : acquisition, stockage, distribution et analyse.

Boîte à outils d'analyse génomique (GATK)

La GATK a été développée comme plate-forme de science des données à l' "Institut étendu". GATK est un ensemble d'outils open source qui permettent l'analyse du génome, en particulier la découverte de variantes, l'identification, l'annotation et le génotypage. L'un des avantages de GATK est que l'ensemble d'outils et/ou de commandes peut être enchaîné pour former un workflow complet. Voici les principaux défis que le large institut doit relever :

- Comprendre les causes profondes et les mécanismes biologiques des maladies.
- Identifier les interventions thérapeutiques qui agissent à la cause fondamentale d'une maladie.
- Comprendre la ligne visuelle des variantes au fonctionnement dans la physiologie humaine.
- Création de normes et de règles "frameworks" pour la représentation, le stockage, l'analyse, la sécurité, etc. des données génomiques.
- Normaliser et socialiser les bases de données d'agrégation de génome interopérables (gnomAD).
- Surveillance, diagnostic et traitement basés sur des génomes pour le compte de patients avec plus de précision.
- Aider à mettre en œuvre des outils qui prédisent les maladies bien avant que les symptômes apparaissent.
- Créer et donner les moyens à une communauté de collaborateurs transdisciplinaires pour aider à s'attaquer aux problèmes les plus difficiles et les plus importants de la biomédecine.

Selon la GATK et le large institute, le séquençage du génome doit être considéré comme un protocole dans un laboratoire de pathologie. Chaque tâche est bien documentée, optimisée, reproductible et cohérente dans l'ensemble des échantillons et des expériences. Voici un ensemble de mesures recommandées par le large Institute pour plus d'informations, voir "Site web de GATK".

Définition FlexPod

La validation d'un workload génomique inclut une configuration complète d'une plateforme d'infrastructure FlexPod. La plateforme FlexPod est extrêmement disponible et peut évoluer indépendamment. Ainsi, vous pouvez faire évoluer indépendamment le réseau, le stockage et les ressources de calcul, par exemple. Nous avons utilisé le guide de conception validée Cisco suivant comme document d'architecture de référence pour configurer l'environnement FlexPod : "FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7". Découvrez les points forts de la configuration de la plateforme FlexPod suivante :

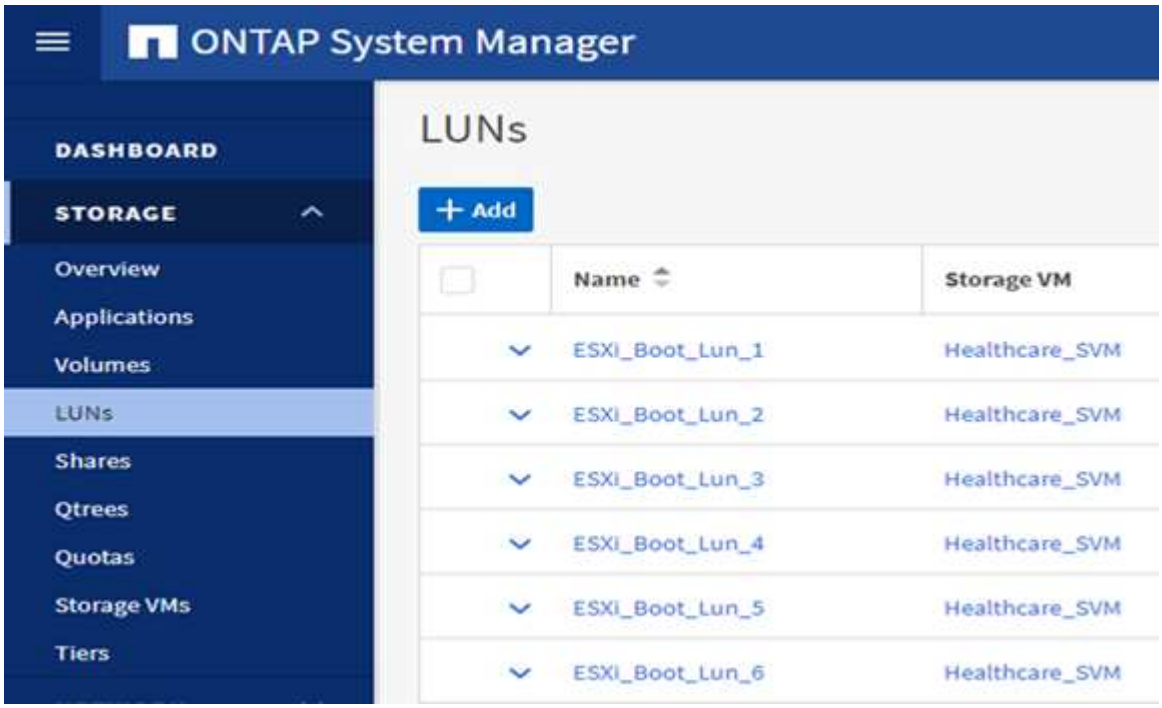
Pour effectuer la configuration du laboratoire FlexPod, procédez comme suit :

1. La configuration et la validation du laboratoire FlexPod utilisent les réservations IP4 et les VLAN suivants.

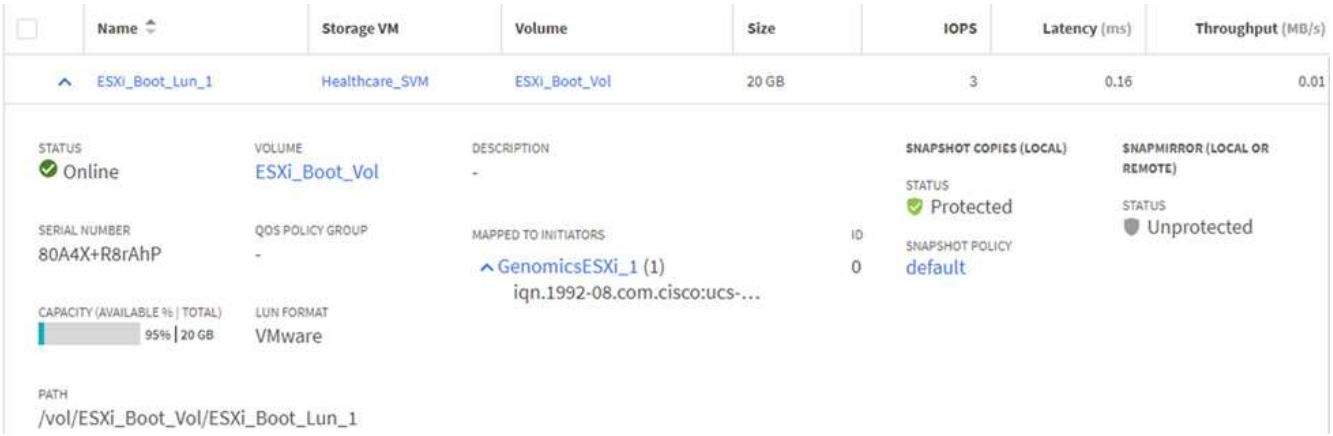
IP Reservations

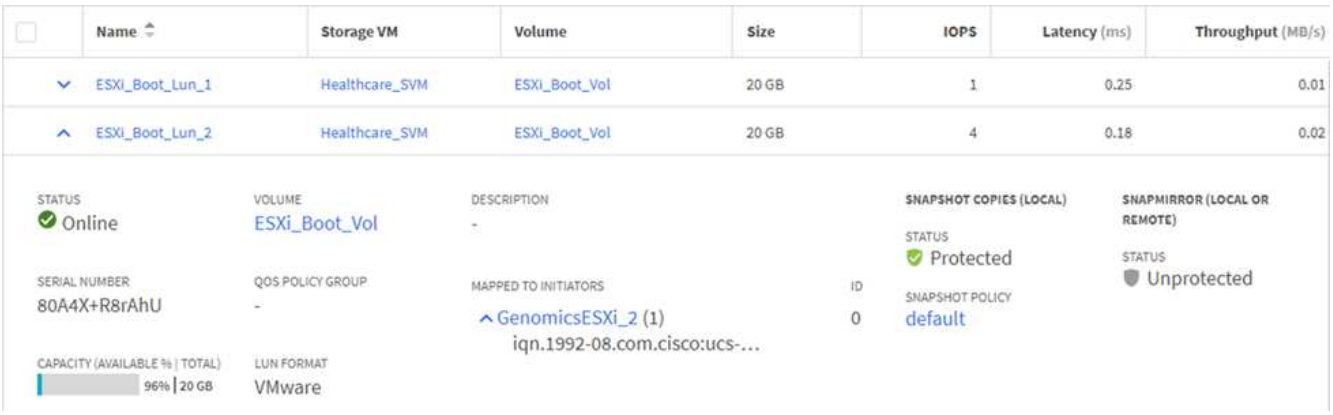
VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. Configuration des LUN de démarrage iSCSI sur le SVM ONTAP



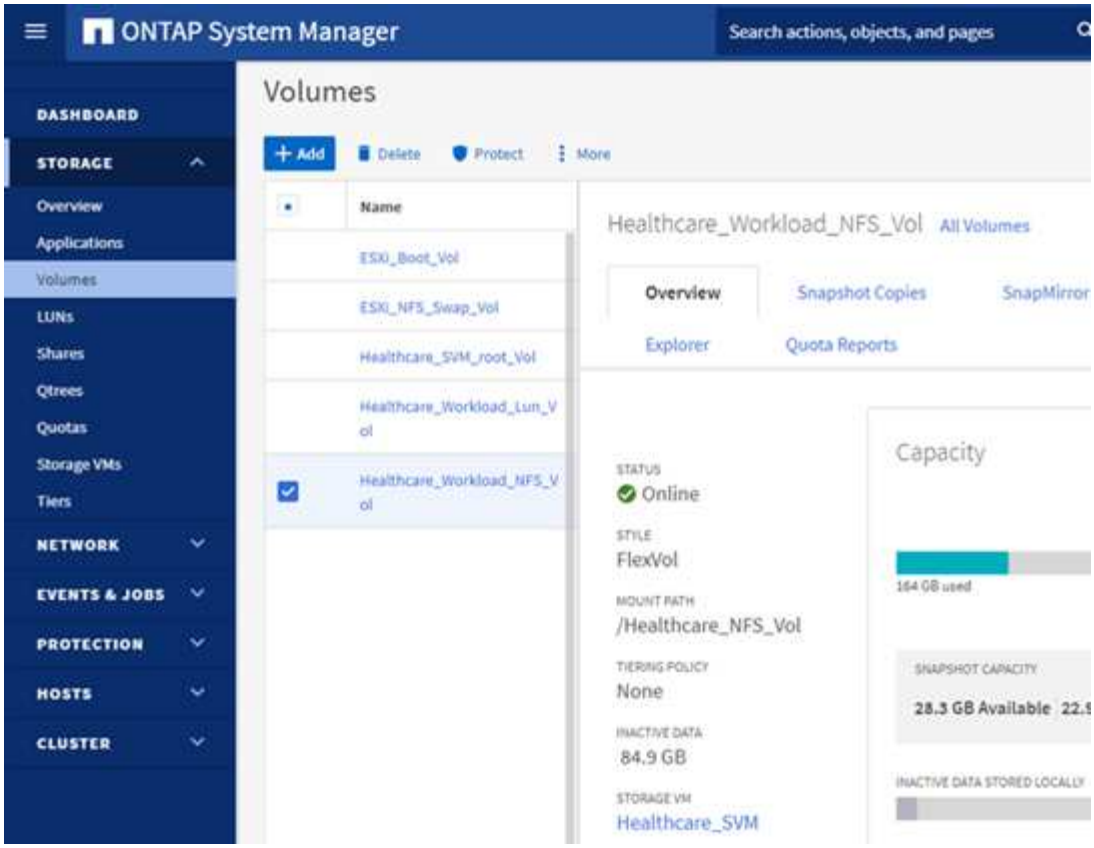
3. Mapper les LUN sur des groupes initiateurs iSCSI.



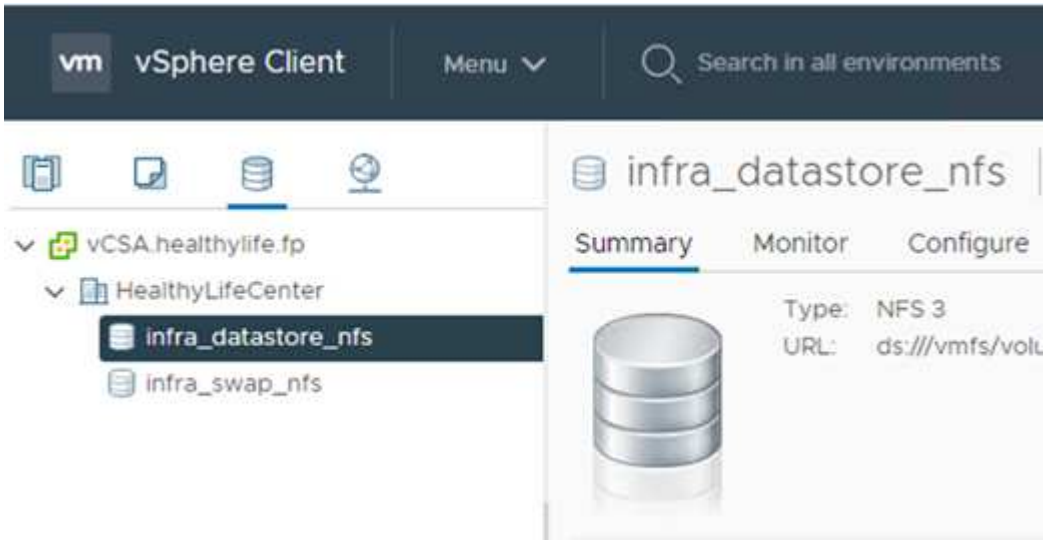


4. Installez vSphere 7.0 avec le démarrage iSCSI.
5. Enregistrez les hôtes ESXi avec vCenter.

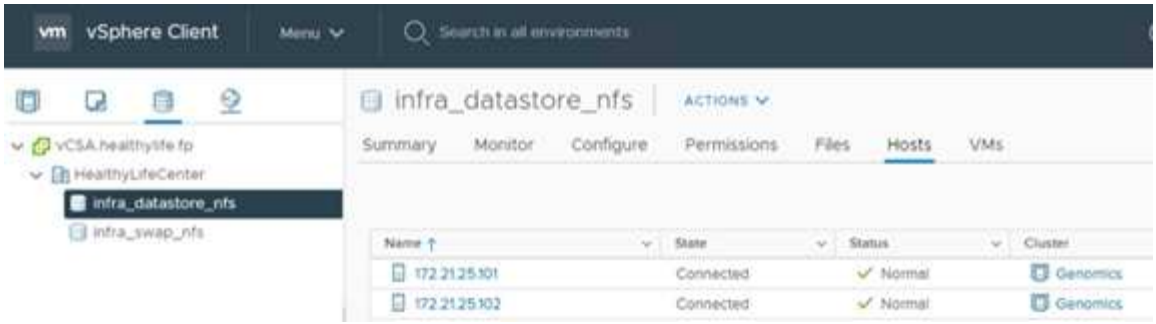
6. Provisionner un datastore NFS `infra_datastore_nfs` Sur le stockage ONTAP.



7. Ajoutez le datastore au vCenter.



8. À l'aide de vCenter, ajoutez un datastore NFS aux hôtes ESXi.



9. A l'aide de vCenter, créez une machine virtuelle Red Hat Enterprise Linux (RHEL) 8.3 pour exécuter GATK.
10. Un datastore NFS est présenté à la machine virtuelle et monté sur `/mnt/genomics`, Qui est utilisé pour stocker les exécutables GATK, les scripts, les fichiers de carte d'alignement binaire (BAM), les fichiers de référence, les fichiers d'index, les fichiers de dictionnaire et les fichiers de sortie pour les appels de variantes.

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb               308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

Configuration et exécution de la GATK

Installez les prérequis suivants sur la VM RedHat Enterprise 8.3 Linux :

- Java 8 ou SDK 1.8 ou version ultérieure
- Télécharger GATK 4.2.0.0 depuis le large Institute "Site GitHub". Les données de séquence du génome sont généralement stockées sous la forme d'une série de colonnes ASCII délimitées par des tabulations. Cependant, l'espace ASCII est trop important pour être stocké. Par conséquent, un nouveau standard évolué appelé fichier BAM (*.bam). Un fichier BAM stocke les données de séquence sous forme compressée, indexée et binaire. Nous "téléchargé" Un ensemble de fichiers BAM disponibles publiquement pour l'exécution GATK à partir de l' "domaine public". Nous avons également téléchargé des fichiers d'index (*.bai), des fichiers de dictionnaire (*. dict) et les fichiers de données de référence (*. fasta) du même domaine public.

Après le téléchargement, le kit d'outils GATK dispose d'un fichier jar et d'un ensemble de scripts de support.

- `gatk-package-4.2.0.0-local.jar` exécutable
- `gatk` fichier de script.

Nous avons téléchargé les fichiers BAM et les fichiers d'index, de dictionnaire et de génome de référence correspondants pour une famille composée de fichiers de père, mère et fils *.bam.

Moteur Cromwell

Cromwell est un moteur open-source axé sur les flux de travail scientifiques qui permet la gestion des flux de travail. Le moteur Cromwell peut fonctionner en deux "modes", Mode serveur ou mode d'exécution d'un seul flux de travail. Le comportement du moteur Cromwell peut être contrôlé à l'aide du "Fichier de configuration du moteur Cromwell".

- **Le mode serveur.** active "RESTful" Exécution de flux de travail dans le moteur Cromwell.

- **Mode d'exécution.** le mode d'exécution est le mieux adapté à l'exécution de flux de travail uniques dans Cromwell, "réf" Pour obtenir un ensemble complet d'options disponibles en mode Run.

Nous utilisons le moteur Cromwell pour exécuter les flux de travail et les pipelines à grande échelle. Le moteur Cromwell est convivial "langage de description de workflow" Langage de script basé sur WDL. Cromwell prend également en charge une deuxième norme de script de flux de travail appelée langage de flux de travail commun (CWL). Tout au long de ce rapport technique, nous avons utilisé WDL. À l'origine, le WDL a été développé par le large institut pour les pipelines d'analyse du génome. L'utilisation des workflows WDL peut être mise en œuvre à l'aide de plusieurs stratégies, notamment :

- **Chaînage linéaire.** comme le nom l'indique, la sortie de la tâche #1 est envoyée à la tâche #2 comme entrée.
- **Multi-in/out.** Ceci est similaire à la chaînage linéaire dans le fait que chaque tâche peut avoir plusieurs sorties envoyées en entrée aux tâches suivantes.
- **Scatter-rassembler.** il s'agit de l'une des stratégies d'intégration des applications d'entreprise les plus puissantes disponibles, surtout lorsqu'elle est utilisée dans une architecture basée sur des événements. Chaque tâche s'exécute de façon dissociée, et le résultat de chaque tâche est consolidé dans le résultat final.

Il existe trois étapes lorsque WDL est utilisé pour faire fonctionner GATK en mode autonome :

1. Valider la syntaxe à l'aide de `womtool.jar`.

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. Générer des entrées JSON.

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. Exécutez le flux de travail à l'aide du moteur Cromwell et `Cromwell.jar`.

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

Le GATK peut être exécuté à l'aide de plusieurs méthodes; ce document explore trois de ces méthodes.

Exécution de GATK à l'aide du fichier jar

Examinons l'exécution d'un pipeline d'appel variante unique à l'aide de l'appelant variant en haplotype.

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

Dans cette méthode d'exécution, nous utilisons le fichier JAR d'exécution locale GATK, une seule commande Java pour appeler le fichier jar, et nous transmettons plusieurs paramètres à la commande.

1. Ce paramètre indique que nous invoons le `HaplotypeCaller` variante du pipeline appelant.
2. `-- input` Spécifie le fichier BAM en entrée.
3. `--output` spécifie le fichier de sortie de variante dans le format d'appel de variante (*.vcf) ("réf").
4. Avec le `--reference` paramètre, nous sommes en passe de passer un génome de référence.

Une fois exécuté, les détails de sortie se trouvent dans la section "Sortie pour l'exécution de GATK à l'aide du fichier jar."

Exécution de GATK à l'aide du script ./gatk

La trousse à outils GATK peut être exécutée à l'aide de l' `./gatk` script. Examinons la commande suivante :

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

Nous transmettons plusieurs paramètres à la commande.

- Ce paramètre indique que nous invoons le `HaplotypeCaller` variante du pipeline appelant.
- `-I` Spécifie le fichier BAM en entrée.
- `-O` spécifie le fichier de sortie de variante dans le format d'appel de variante (*.vcf) ("réf").
- Avec le `-R` paramètre, nous sommes en passe de passer un génome de référence.

Une fois exécuté, les détails de sortie se trouvent dans la section

Exécution de la GATK à l'aide du moteur Cromwell

Nous utilisons le moteur Cromwell pour gérer l'exécution GATK. Examinons la ligne de commande et ses paramètres.

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

Ici, nous invoquons la commande Java en passant le `-jar` paramètre pour indiquer que nous avons l'intention d'exécuter un fichier jar, par exemple, `Cromwell-65.jar`. Le paramètre suivant a réussi (`run`) Indique que le moteur Cromwell fonctionne en mode RUN, l'autre option possible est le mode serveur. Le paramètre suivant est `*.wdl` Que le mode Exécuter doit utiliser pour exécuter les pipelines. Le paramètre suivant est l'ensemble des paramètres d'entrée des flux de travail exécutés.

Voici le contenu du `ghplo.wdl` type de fichier :

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

Voici le fichier JSON correspondant avec les entrées du moteur Cromwell.

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Veuillez noter que Cromwell utilise une base de données in-memory pour l'exécution. Une fois exécuté, le journal de sortie est visible dans la section "Sortie pour l'exécution de la GATK à l'aide du moteur Cromwell."

Pour un ensemble complet d'étapes sur la façon d'exécuter GATK, voir "Documentation GATK".

"Suivant : sortie pour l'exécution de GATK à l'aide du fichier jar."

Sortie pour l'exécution de GATK à l'aide du fichier jar

"Précédent : génomique - Configuration et exécution de la GATK."

L'exécution de GATK à l'aide du fichier jar a produit la sortie d'échantillon suivante.

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
```

```
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
```

```
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

Notez que le fichier de sortie se trouve à l'emplacement spécifié après l'exécution.

Sortie pour l'exécution de GATK à l'aide du script ./gatk

"Précédent : sortie pour l'exécution de GATK à l'aide du fichier jar."

L'exécution de GATK à l'aide de l' `./gatk` le script a produit l'exemple de sortie suivant.

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
```

```
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
```

```
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

Notez que le fichier de sortie se trouve à l'emplacement spécifié après l'exécution.

"Suivant : sortie pour l'exécution de la GATK à l'aide du moteur Cromwell."

Sortie pour l'exécution de la GATK à l'aide du moteur Cromwell

L'exécution de la GATK à l'aide du moteur Cromwell a produit la sortie d'échantillon suivante.

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
```

```
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
```

```
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
```

```
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
```

```
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"Suivant : configuration du GPU."

Configuration des GPU

"Précédent : sortie pour l'exécution de la GATK à l'aide du moteur Cromwell."

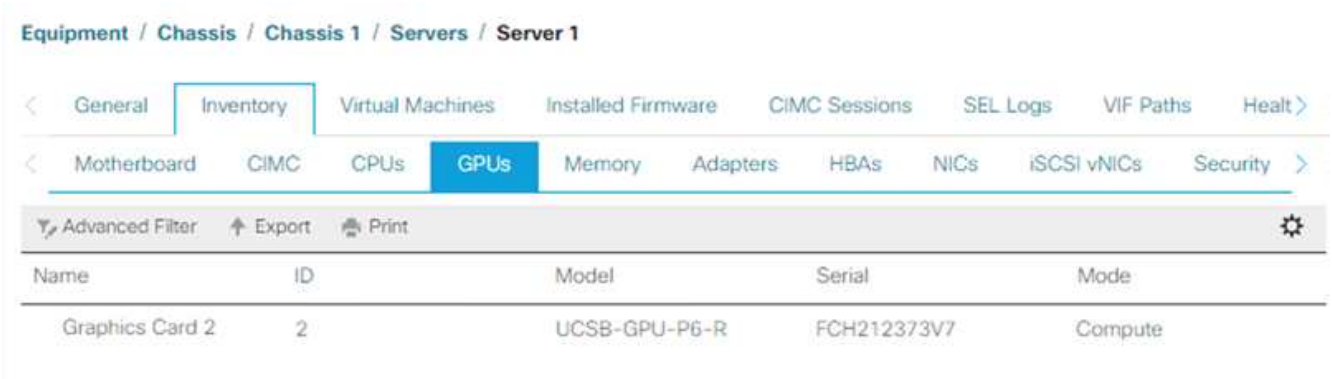
Au moment de la publication, l'outil GATK n'a pas de prise en charge native de l'exécution basée sur GPU sur site. La configuration et les conseils suivants permettent aux lecteurs de comprendre à quel point il est simple d'utiliser FlexPod avec un GPU NVIDIA Tesla P6 monté à l'arrière au moyen d'une carte mezzanine PCIe pour le GATK.

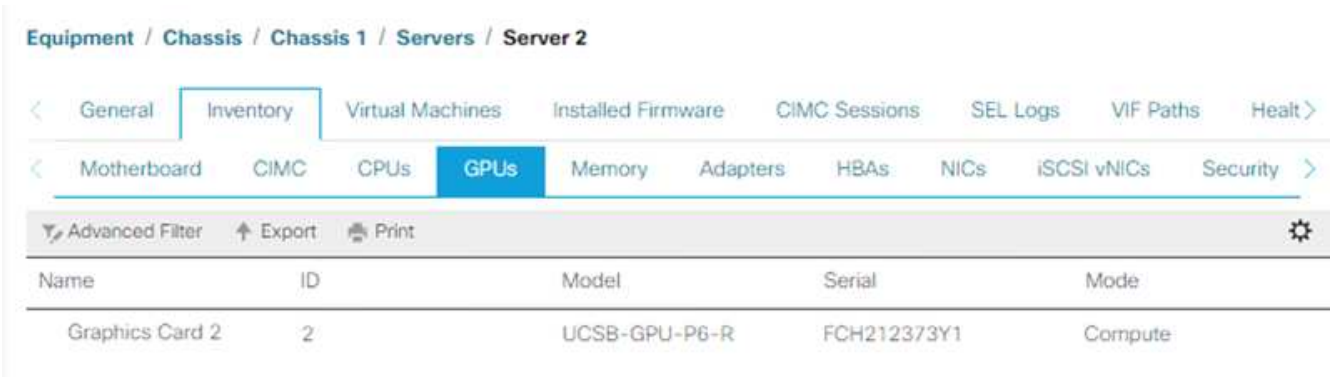
Nous avons utilisé le CVD suivant pour l'architecture de référence et le guide des meilleures pratiques pour configurer l'environnement FlexPod afin que nous puissions exécuter des applications utilisant des GPU.

- "FlexPod Datacenter pour l'IA/ML avec Cisco UCS 480 ML pour le deep learning"

Voici un ensemble de messages clés à retenir lors de cette configuration :

1. Nous avons utilisé un processeur graphique PCIe NVIDIA Tesla P6 dans un slot mezzanine des serveurs UCS B200 M5.





2. Pour cette configuration, nous nous sommes inscrits sur le portail partenaires NVIDIA et avons obtenu une

licence d'évaluation (également appelée droit) pour pouvoir utiliser les GPU en mode de calcul.

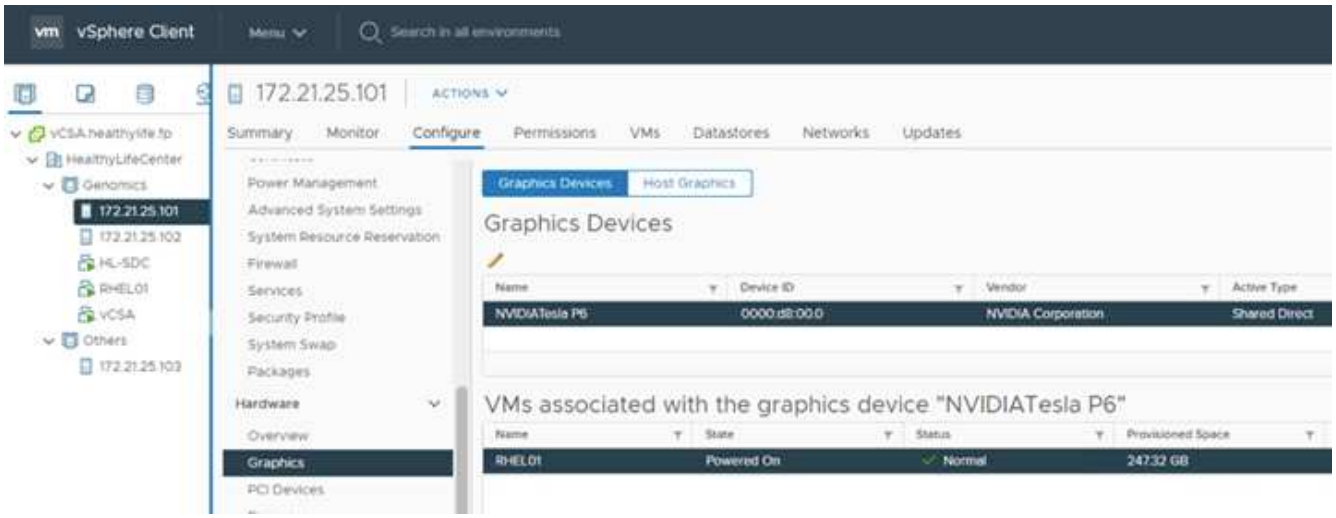
3. Nous avons téléchargé le logiciel NVIDIA vGPU requis du site Web dédié aux partenaires NVIDIA.
4. Nous avons téléchargé le droit `*.bin` Fichier du site Web partenaire de NVIDIA.
5. Nous avons installé un serveur de licences NVIDIA vGPU et ajouté les droits au serveur de licences à l'aide de `*.bin` Fichier téléchargé du site partenaire NVIDIA.
6. Veillez à choisir la version correcte du logiciel NVIDIA vGPU pour votre déploiement sur le portail partenaires NVIDIA. Pour cette configuration, nous avons utilisé la version 460.73.02 du pilote.
7. Cette commande installe le "NVIDIA vGPU Manager" Dans ESXi.

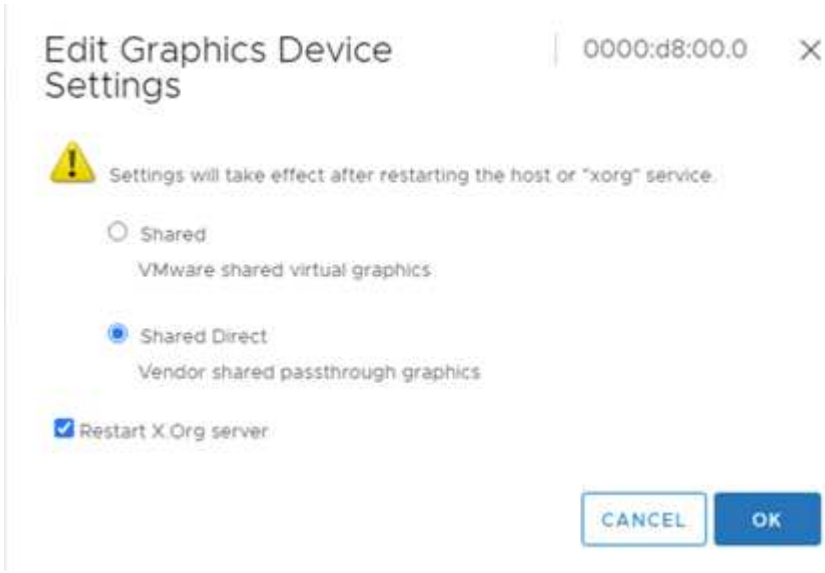
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. Après le redémarrage du serveur ESXi, exécutez la commande suivante pour valider l'installation et vérifier l'état des GPU.

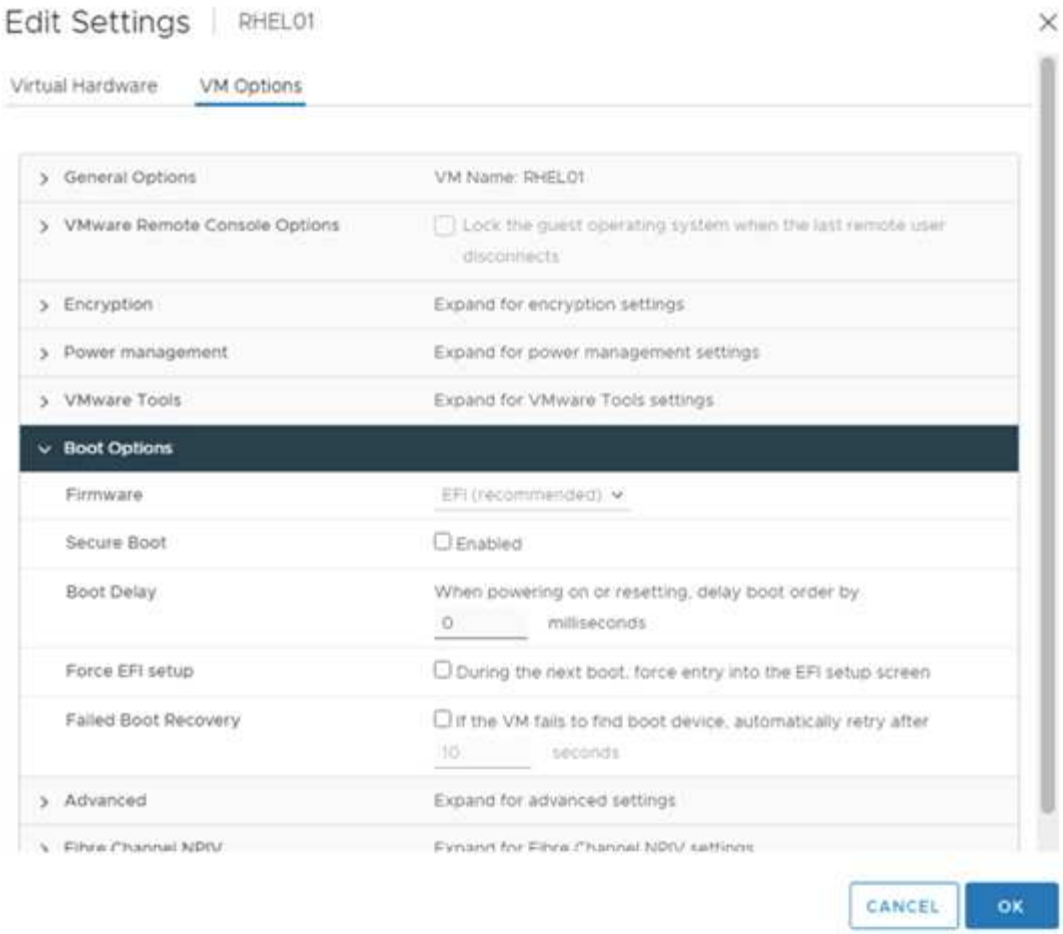
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. À l'aide de vCenter, "configurer" Les paramètres du périphérique graphique sur « Shared Direct ».





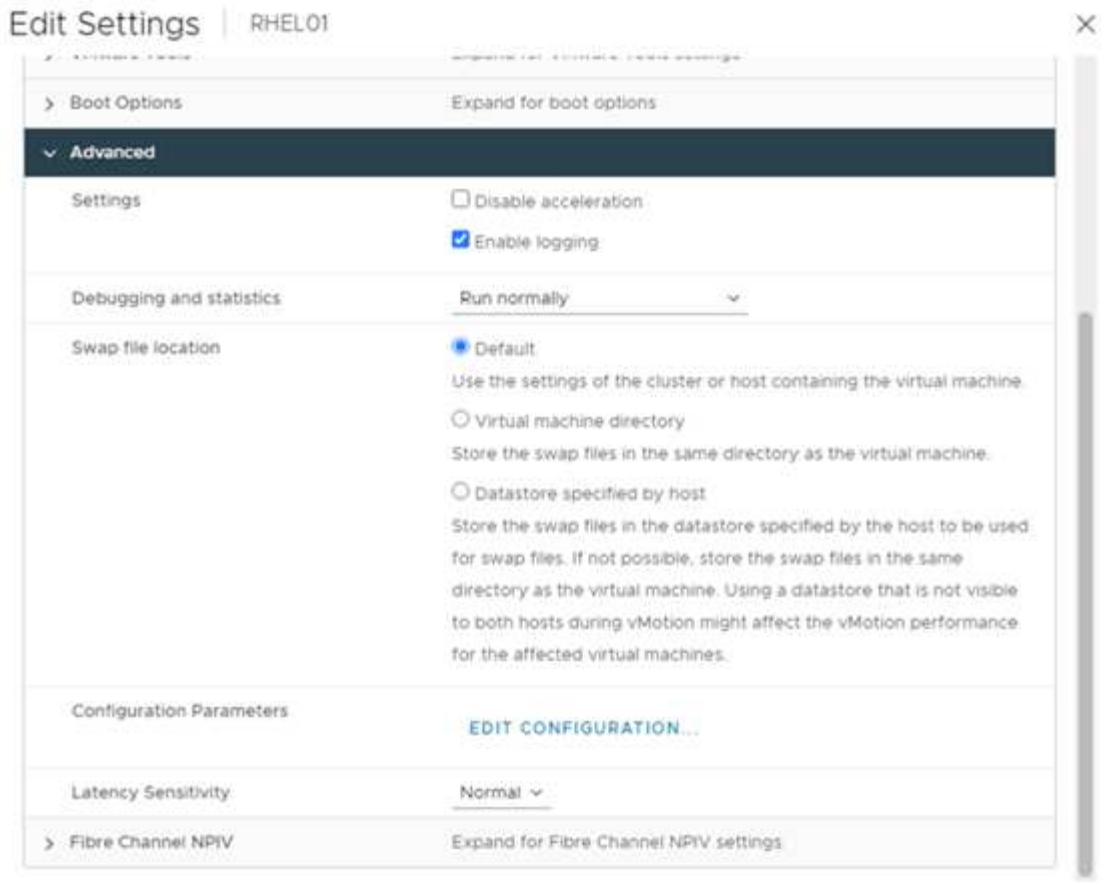
10. Assurez-vous que le démarrage sécurisé est désactivé pour la machine virtuelle RedHat.
11. Assurez-vous que le micrologiciel des options de démarrage VM est défini sur EFI ("réf").

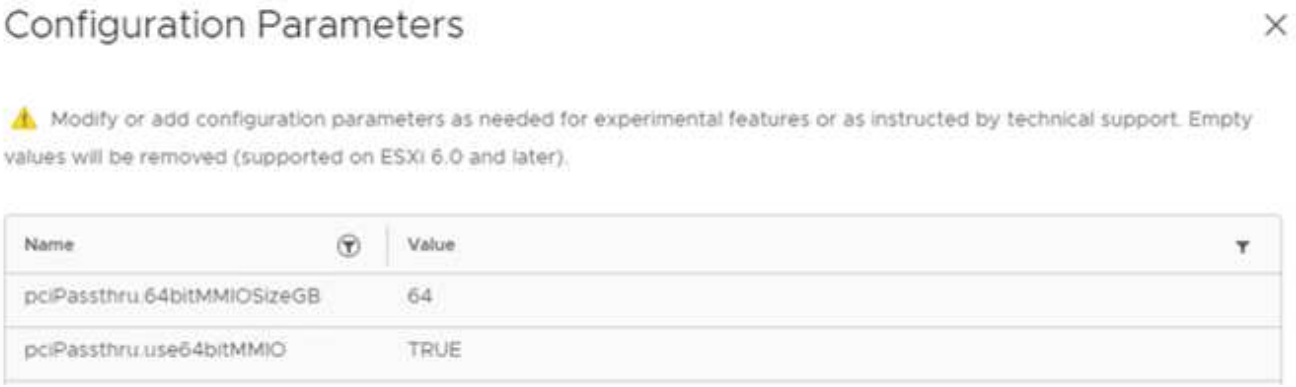


12. Assurez-vous que les PARAMÈTRES suivants sont ajoutés à VM Options Advanced Edit Configuration. La valeur du `pciPassthru.64bitMMIOSizeGB` Le paramètre dépend de la mémoire du GPU et du nombre de GPU affectés à la machine virtuelle. Par exemple :

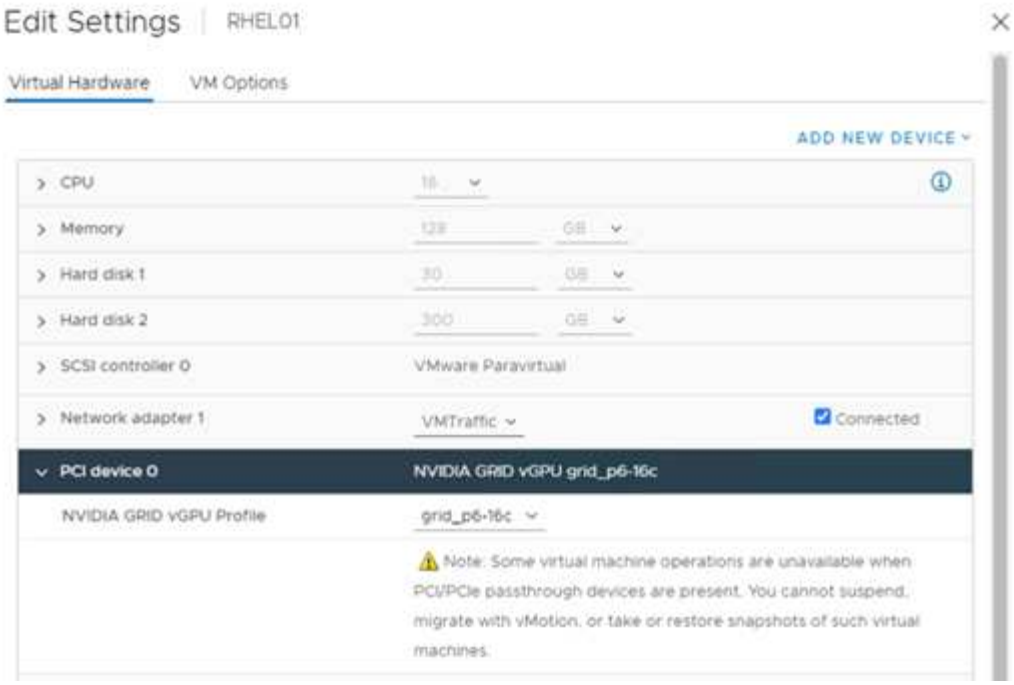
    a. Si une machine virtuelle est affectée à 4 GPU V100 de 32 Go, la valeur doit être 128.

    b. Si une machine virtuelle est affectée à 4 processeurs graphiques P6 de 16 Go, cette valeur doit être 64.





13. Lorsque vous ajoutez des vGPU en tant que nouveau périphérique PCI à la machine virtuelle dans vCenter, veillez à sélectionner NVIDIA GRID vGPU comme type de périphérique PCI.
14. Choisissez le profil GPU correct qui suites le GPU utilisé, la mémoire GPU et son usage : par exemple, les graphiques plutôt que le calcul.



15. Sur la VM RedHat Linux, les pilotes NVIDIA peuvent être installés en exécutant la commande suivante :

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. Vérifiez que le profil vGPU correct est signalé en exécutant la commande suivante :

```
[root@genomics1 genomics]# nvidia-smi -query-gpu=gpu_name
-format=csv,noheader -id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. Après le redémarrage, vérifiez que le NVIDIA vGPU correct est signalé avec les versions du pilote.

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. Assurez-vous que l'adresse IP du serveur de licences est configurée sur la machine virtuelle dans le fichier de configuration de la grille vGPU.
    a. Copier le modèle.

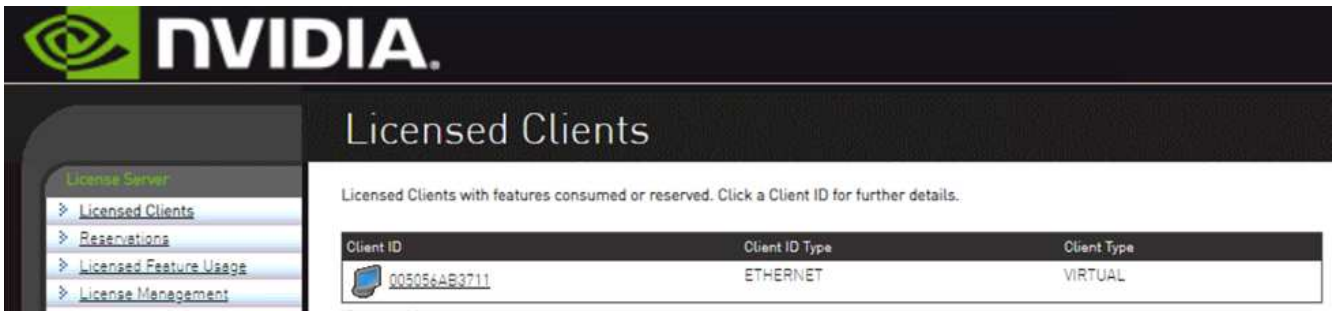
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. Modifiez le fichier `/etc/nvidia/rid.conf`, Ajoutez l'adresse IP du serveur de licences et définissez le type de fonction sur 1.

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. Après avoir redémarré la VM, vous devriez voir une entrée sous clients sous Licence dans le serveur de licences comme indiqué ci-dessous.



20. Se reporter à la section Configuration des solutions pour plus d'informations sur le téléchargement des logiciels GATK et Cromwell.
21. Une fois que la GATK peut utiliser des GPU sur site, le langage de description du workflow `*. wdl` possède les attributs d'exécution comme indiqué ci-dessous.

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"Suivant: Conclusion."

Conclusion

"Précédent : configuration du GPU."

De nombreuses organisations du secteur de la santé à travers le monde ont choisi FlexPod comme plateforme commune. FlexPod vous permet de déployer des capacités médicales en toute confiance. FlexPod avec NetApp ONTAP est fourni de série avec la capacité d'implémenter un ensemble de protocoles de pointe, clé en main. Quelle que soit l'origine de la demande d'exécution de la génomique d'un patient donné, une plateforme FlexPod assure l'interopérabilité, l'accessibilité, la disponibilité et l'évolutivité.

Lorsqu'elle est standardisée sur une plate-forme FlexPod, la culture de l'innovation devient contagieuse.

Où trouver des informations complémentaires

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

- FlexPod Datacenter pour l'IA/ML avec Cisco UCS 480 ML pour le deep learning

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- Centre de documentation ONTAP 9

  "http://docs.netapp.com"

- Agile et efficace : FlexPod favorise la modernisation des data centers

  "https://www.flexpod.com/idc-white-paper/"

- L'IA dans le domaine de la santé

  "https://www.netapp.com/us/media/na-369.pdf"

- FlexPod pour le secteur de la santé facilite votre transformation

  "https://flexpod.com/solutions/verticals/healthcare/"

- FlexPod de Cisco et NetApp

  "https://flexpod.com/"

- IA et analytique pour le secteur de la santé (NetApp)

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- Des choix d'infrastructure intelligents pour le secteur de la santé favorisent la réussite

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- FlexPod Datacenter avec ONTAP 9.8, ONTAP Storage Connector for Cisco Intersight et Cisco Intersight Managed mode.

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- FlexPod Datacenter avec Red Hat Enterprise Linux OpenStack Platform

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Novembre 2021	Version initiale.

FlexPod pour MEDITECH : Guide de dimensionnement

Tr-4774 : FlexPod pour MEDITECH : dimensionnement directionnel

Brandon Agee, John Duignan, NetApp Mike Brennan, Jon Ebmeir, Cisco

En partenariat avec : 

Ce rapport fournit des conseils sur le dimensionnement des FlexPod pour l'environnement logiciel applicatif MEDITECH EHR.

Objectif

Les systèmes FlexPod peuvent être déployés pour héberger les services MEDITECH, 6.x, 5.x et MAGIC. Les serveurs FlexPod qui hébergent la couche applicative MEDITECH fournissent une plateforme intégrée et fiable, et haute performance. La plateforme intégrée FlexPod est déployée rapidement par des partenaires revendeurs FlexPod compétents et est prise en charge par les centres de support technique Cisco et NetApp.

Le dimensionnement repose sur les informations contenues dans la proposition de configuration matérielle du MEDITECH et dans le document de tâche MEDITECH. L'objectif est de déterminer la taille optimale des composants d'infrastructure de calcul, de réseau et de stockage.

Le "Présentation de la charge de travail MEDITECH" La section décrit les types de charges de travail de calcul et de stockage disponibles dans les environnements MEDITECH.

Le "Spécifications techniques pour les petites, moyennes et grandes architectures" La section fournit un exemple de nomenclature pour les différentes architectures de stockage décrites dans la section. Les configurations indiquées ne sont que des instructions générales. Dimensionnez toujours les systèmes à l'aide des outils de dimensionnement en fonction de la charge de travail et ajustez les configurations en fonction de ces paramètres.

Avantages globaux de la solution

L'exécution d'un environnement MEDITECH sur l'architecture FlexPod peut aider les établissements de santé à améliorer leur productivité et à réduire leurs dépenses d'investissement et d'exploitation. Grâce à son partenariat stratégique, FlexPod fournit une infrastructure convergée prévalidée, rigoureusement testée et rigoureusement. Il est spécialement conçu pour fournir des performances prévisibles avec une faible latence du système et une haute disponibilité. Cette approche accélère les temps de réponse pour les utilisateurs du système DME MEDITECH.

La solution FlexPod de Cisco et NetApp répond aux besoins des systèmes MEDITECH grâce à ses performances élevées, modulaires, prévalidées, convergées et virtualisées plateforme efficace, évolutive et économique. FlexPod Datacenter avec MEDITECH offre plusieurs avantages spécifiques au secteur de la

santé :

- **Architecture modulaire**. FlexPod répond aux divers besoins de l'architecture modulaire MEDITECH avec des systèmes FlexPod personnalisés pour chaque charge de travail. Tous les composants sont connectés via une structure de gestion du stockage et des serveurs en cluster, et ils utilisent un ensemble d'outils de gestion cohésif.
- **Opérations simplifiées et coûts réduits**. En remplaçant leurs plateformes par une ressource partagée plus efficace et évolutive, qui prend en charge les médecins où qu'ils soient, vous éliminez les dépenses et la complexité des plateformes existantes. Cette solution optimise l'utilisation des ressources pour un retour sur investissement plus important.
- **Déploiement plus rapide de l'infrastructure**. Avec la conception intégrée de FlexPod Datacenter avec MEDITECH, les entreprises peuvent déployer et exécuter la nouvelle infrastructure rapidement et facilement, aussi bien pour les data centers sur site que distants.
- **Architecture scale-out**. Vous pouvez faire évoluer vos systèmes SAN et NAS de quelques téraoctets à plusieurs dizaines de pétaoctets sans reconfigurer vos applications en cours d'exécution.
- * Continuité de l'activité*. Vous pouvez effectuer les opérations de maintenance du système de stockage, de renouvellement du matériel et de mise à niveau des logiciels sans interrompre votre activité.
- **Colocation sécurisée**. Cet avantage répond aux besoins accrus des serveurs virtualisés et de l'infrastructure de stockage partagé, ce qui permet la colocation sécurisée des informations spécifiques aux sites. Cet avantage est important si vous hébergez plusieurs instances de bases de données et de logiciels.
- **Optimisation des ressources regroupées**. Cet avantage peut vous permettre de réduire la quantité de contrôleurs de stockage et de serveurs physiques, d'équilibrer la charge applicative, d'optimiser l'utilisation et d'améliorer simultanément les performances.
- **Qualité de service (QoS).** FlexPod offre la qualité de service (QoS) sur l'ensemble de la pile. Les règles de QoS leaders du marché permettent des niveaux de service différenciés dans un environnement partagé. Ces règles permettent d'obtenir des performances optimales pour les charges de travail et d'isoler et de contrôler les applications non contrôlées.
- **Efficacité du stockage**. Vous pouvez réduire vos coûts de stockage grâce à l'efficacité du stockage NetApp 7:1.
- **Agilité**. Les outils de gestion, d'orchestration et d'automatisation des flux de travail proposés par les systèmes FlexPod lui permettent d'être bien plus réactifs face aux demandes des entreprises. Allant de la sauvegarde MEDITECH au provisionnement d'environnements de test et de formation en passant par la réplication des bases de données d'analytique pour les initiatives de gestion de la santé des populations.
- * Productivité*. Déployez et faites évoluer cette solution pour offrir à un médecin une expérience utilisateur optimale.
- **Data Fabric**. L'architecture NetApp Data Fabric offre un maillage sur l'ensemble des sites, des emplacements physiques et des applications, NetApp Data Fabric est conçu pour un monde centré sur la donnée. Les données sont créées et utilisées dans divers emplacements et sont souvent partagées avec des applications et des infrastructures. Data Fabric offre un moyen de gérer des données cohérentes et intégrées. En outre, il contrôle davantage la donnée et simplifie une INFRASTRUCTURE IT toujours plus complexe.

Portée

Ce document concerne les environnements qui utilisent Cisco UCS et les systèmes de stockage ONTAP NetApp. Il fournit des exemples d'architectures de référence pour l'hébergement MEDITECH.

Elle ne couvre pas :

- Conseils détaillés sur le dimensionnement à l'aide de NetApp System Performance Modeler (SPM) ou d'autres outils de dimensionnement NetApp.
- Dimensionnement pour les charges de travail non productifs

Public

Ce document est destiné aux ingénieurs système partenaires et NetApp, ainsi qu'au personnel des services professionnels NetApp. NetApp suppose que le lecteur connaît bien les concepts de dimensionnement du stockage et du calcul, ainsi que la connaissance technique de Cisco UCS et des systèmes de stockage NetApp.

Documentation associée

Les rapports techniques et autres documents suivants sont pertinents pour ce rapport technique. Ils constituent un ensemble complet de documents requis pour le dimensionnement, la conception et le déploiement d'MEDITECH sur l'infrastructure FlexPod.

- "Tr-4753 : Guide de déploiement de FlexPod Datacenter pour MEDITECH"
- "Tr-4190 : directives de dimensionnement NetApp pour les environnements MEDITECH"
- "Tr-4319 : directives de déploiement NetApp pour les environnements MEDITECH"

> Vous devez disposer d'identifiants de connexion pour accéder à certains de ces rapports sur le Field Portal NetApp.

Présentation de la charge de travail MEDITECH

Cette section décrit les types de charges de travail de calcul et de stockage que les environnements MEDITECH peuvent trouver.

MEDITECH et charges de travail de sauvegarde

Lorsque vous dimensionnez les systèmes de stockage NetApp pour les environnements MEDITECH, il est nécessaire d'examiner à la fois le workload de production MEDITECH et le workload de sauvegarde.

Hôte MEDITECH
Un hôte MEDITECH est un serveur de base de données. Cet hôte est également appelé serveur de fichiers MEDITECH (pour la plate-forme ÉTENDUE, 6.x ou C/S 5.x) ou UNE machine MAGIC (pour la plate-forme MAGIC). Ce document utilise l'hôte du terme MEDITECH pour faire référence au serveur de fichiers MEDITECH et à une machine MAGIC.

Les sections qui suivent décrivent les caractéristiques d'E/S et les exigences de performance de ces deux charges de travail.

Charge de travail MEDITECH

Dans l'environnement MEDITECH, plusieurs serveurs qui exécutent le logiciel MEDITECH effectuent différentes tâches sous forme de système intégré appelé système MEDITECH. Pour en savoir plus sur le système MEDITECH, consultez la documentation du MEDITECH :

- Pour les environnements de production MEDITECH, consultez la documentation appropriée pour déterminer le nombre d'hôtes MEDITECH et la capacité de stockage qui doit être incluse dans le

dimensionnement du système de stockage NetApp.

- Pour les nouveaux environnements MEDITECH, consultez le document de proposition de configuration matérielle. Pour les environnements MEDITECH existants, consultez le document des tâches d'évaluation du matériel. La tâche d'évaluation matérielle est associée à un ticket MEDITECH. Les clients peuvent demander l'un ou l'autre de ces documents MEDITECH.

Vous pouvez faire évoluer le système MEDITECH pour accroître la capacité et les performances en ajoutant des hôtes. Chaque hôte a besoin d'une capacité de stockage pour ses fichiers de base de données et d'applications. Le stockage disponible pour chaque hôte MEDITECH doit également prendre en charge les E/S générées par l'hôte. Pour les environnements MEDITECH, une LUN est disponible pour chaque hôte et elle prend en charge les besoins de stockage des applications et des bases de données de cet hôte. Le type de catégorie MEDITECH et le type de plateforme que vous déployez déterminent les caractéristiques de charge de travail de chaque hôte MEDITECH et, par conséquent, du système dans son ensemble.

Catégories MEDITECH

MEDITECH associe la taille du déploiement à des numéros de catégorie allant de 1 à 6. La catégorie 1 représente les plus petits déploiements MEDITECH : cette catégorie 6 est celle qui est la plus importante. Les caractéristiques de l'application MEDITECH associées à chaque catégorie incluent notamment des indicateurs de mesure :

- Nombre de lits d'hôpital
- Patients hospitalisés par an
- Patients externes par an
- Visites en salle d'urgence par an
- Examens par an
- Prescriptions d'hospitalisation par jour
- Prescriptions ambulatoires par jour

Pour en savoir plus sur les catégories MEDITECH, consultez la fiche de référence des catégories MEDITECH. Cette fiche peut être obtenue du client MEDITECH ou avec le programme d'installation du système MEDITECH.

Plateformes MEDITECH

MEDITECH possède quatre plateformes :

- ÉTENDUE
- MEDITECH 6.x
- Client/serveur 5.x (C/S 5.x)
- MAGIE

Pour les plates-formes MEDITECH, 6.x et C/S 5.x, les caractéristiques d'E/S de chaque hôte sont définies comme étant aléatoires à 100 % avec une taille de demande de 4,000. Pour la plateforme MEDITECH MAGIC, les caractéristiques d'E/S de chaque hôte sont définies comme étant aléatoires à 100 % avec une taille de demande de 8,000 ou 16,000. Selon MEDITECH, le volume des demandes d'un déploiement de production MAGIC est de 8,000 ou 16,000.

Le rapport entre les lectures et les écritures varie en fonction de la plateforme déployée. MEDITECH estime la proportion moyenne de lectures et d'écritures, puis les exprime sous forme de pourcentages. MEDITECH estime également la valeur moyenne des IOPS requises pour chaque hôte MEDITECH sur une plateforme

MEDITECH particulière. Le tableau ci-dessous résume les caractéristiques des E/S spécifiques à la plateforme fournies par MEDITECH.

Catégorie MEDITECH	Plateforme MEDITECH	Pourcentage moyen de lecture aléatoire	Pourcentage moyen d'écriture aléatoire	IOPS moyennes durables par hôte MEDITECH
1	ÉTENDUE, 6.x	20	80	750
2-6	ÉTENDUE	20	80	750
	6.x	20	80	750
	C/S 5.x	40	60	600
	MAGIE	90	10	400

Dans un système MEDITECH, le niveau d'IOPS moyen de chaque hôte doit être égal aux valeurs d'IOPS définies dans le tableau ci-dessus. Pour déterminer le dimensionnement correct du stockage basé sur chaque plateforme, les valeurs d'IOPS spécifiées dans le tableau ci-dessus sont utilisées dans le cadre de la méthodologie de dimensionnement décrite dans le "Spécifications techniques pour les petites, moyennes et grandes architectures" section.

MEDITECH nécessite une latence moyenne en écriture aléatoire inférieure à 1 ms pour chaque hôte. Cependant, les augmentations temporaires de la latence d'écriture jusqu'à 2 ms durant les tâches de sauvegarde et de réaffectation sont considérées comme acceptables. MEDITECH nécessite également une latence en lecture aléatoire moyenne inférieure à 7 ms pour les hôtes de catégorie 1 et inférieure à 5 ms pour les hôtes de catégorie 2. Ces exigences de latence s'appliquent à chaque hôte, quelle que soit la plateforme MEDITECH utilisée.

Le tableau ci-dessous récapitule les caractéristiques d'E/S que vous devez prendre en compte pour le dimensionnement du stockage NetApp pour les charges de travail MEDITECH.

Paramètre	Catégorie MEDITECH	ÉTENDUE	MEDITECH 6.x	C/S 5.x	MAGIE
Taille de la requête	1-6	4K	4K	4K	8K ou 16K
Aléatoires et séquentielles		100 % aléatoire	100 % aléatoire	100 % aléatoire	100 % aléatoire
IOPS moyennes en continu	1	750	750	S/O	S/O
	2-6	750	750	600	400
Ratio lecture/écriture	1-6	20 % en lecture, 80 % en écriture	20 % en lecture, 80 % en écriture	40 % en lecture, 60 % en écriture	90 % en lecture, 10 % en écriture
Latence d'écriture		< 1 ms.	< 1 ms.	< 1 ms.	< 1 ms.
Latence d'écriture de pic temporaire	1-6	<2 ms.	<2 ms.	<2 ms.	<2 ms.
Latence en lecture	1	<7 ms	<7 ms	S/O	S/O
	2-6	<5 ms.	<5 ms.	<5 ms.	<5 ms.

LES hôtes MEDITECH des catégories 3 à 6 ont les mêmes caractéristiques d'E/S que les catégories 2. Pour les catégories MEDITECH 2 à 6, le nombre d'hôtes déployés dans chaque catégorie est différent.

La baie de stockage NetApp doit être dimensionnée pour répondre aux exigences de performances décrites aux sections précédentes. Outre la charge de travail de production MEDITECH, le système de stockage NetApp doit être en mesure d'assurer et de maintenir les objectifs de performance fixés pour les opérations de sauvegarde, comme décrit dans la section suivante.

Description de la charge de travail de sauvegarde

Le logiciel de sauvegarde certifié MEDITECH sauvegarde les LUN utilisées par chaque hôte MEDITECH d'un système MEDITECH. Pour que les sauvegardes soient cohérentes avec les applications, le logiciel de sauvegarde arrête le système MEDITECH et interrompt les demandes d'E/S au disque. Lorsque le système est mis en veille, le logiciel de sauvegarde émet une commande vers le système de stockage NetApp pour créer une copie NetApp Snapshot des volumes contenant les LUN. Ensuite, le logiciel de sauvegarde arrête le système MEDITECH, qui permet de continuer les demandes d'E/S de production vers la base de données. Le logiciel crée un volume NetApp FlexClone basé sur la copie Snapshot. Ce volume est utilisé par la source de sauvegarde pendant que les demandes d'E/S de production se poursuivent sur les volumes parents qui hébergent les LUN.

La charge de travail générée par le logiciel de sauvegarde s'effectue à partir de la lecture séquentielle des LUN résidant sur les volumes FlexClone. La charge de travail est définie en tant que charge de travail en lecture séquentielle à 100 % avec une taille de requête de 64,000. Pour la charge de travail de production MEDITECH, le critère de performance est de maintenir les IOPS requises et les niveaux de latence de lecture et d'écriture associés. Toutefois, pour la charge de travail de sauvegarde, l'attention porte sur le débit de données global (Mbit/s) généré au cours de l'opération de sauvegarde. Les sauvegardes LUN DE MEDITECH doivent être effectuées dans une fenêtre de sauvegarde de huit heures, mais NetApp recommande de réaliser la sauvegarde de toutes les LUN MEDITECH en six heures ou moins. Comme le but d'effectuer une sauvegarde en moins de six heures est de limiter les événements : une augmentation non planifiée de la charge de travail MEDITECH, les opérations d'arrière-plan NetApp ONTAP et une croissance du volume des données au fil du temps. L'un de ces événements peut entraîner un temps de sauvegarde supplémentaire. Quelle que soit la quantité de données applicatives stockées, le logiciel de sauvegarde effectue une sauvegarde complète au niveau des blocs de l'intégralité du LUN pour chaque hôte MEDITECH.

Calculez le débit de lecture séquentielle requis pour terminer la sauvegarde dans cette fenêtre en fonction des autres facteurs impliqués :

- La durée de sauvegarde souhaitée
- Nombre de LUN
- Taille de chaque LUN à sauvegarder

Par exemple, pour un environnement MEDITECH à 50 hôtes dont la taille de LUN de chaque hôte est de 200 Go, la capacité totale de LUN à sauvegarder est de 10 To.

Pour sauvegarder 10 To de données en huit heures, le débit suivant est requis :

- = (10 x 10^6)Mo (8 x 3,600)s
- = 347.2MBps

Toutefois, pour prendre en compte les événements non planifiés, une fenêtre de sauvegarde prudente de 5.5 heures est sélectionnée pour bénéficier d'une marge au-delà des six heures recommandées.

Pour sauvegarder 10 To de données en huit heures, le débit suivant est requis :

- = (10 x 10^6)Mo (5.5 x 3,600)s
- = 500 Mbit/s.

Avec un débit de 500 Mbit/s, la sauvegarde peut être effectuée dans un délai de 5.5 heures, sans problème dans un délai de 8 heures.

Le tableau ci-dessous résume les caractéristiques d'E/S de la charge de travail de sauvegarde à utiliser pour la taille du système de stockage.

Paramètre	Toutes les plateformes
Taille de la requête	64 KO
Aléatoires et séquentielles	100 % séquentiel
Ratio lecture/écriture	100 % lecture
Débit moyen	Dépend du nombre d'hôtes MEDITECH et de la taille de chaque LUN : la sauvegarde doit s'effectuer dans un délai de 8 heures.
Durée de sauvegarde requise	8 heures

Architecture de référence Cisco UCS pour MEDITECH

L'architecture pour MEDITECH sur FlexPod est basée sur les conseils des clients MEDITECH, Cisco et NetApp et l'expérience du partenaire et elle est établie avec les clients MEDITECH de toutes les tailles. L'architecture est adaptable et applique les bonnes pratiques pour MEDITECH, selon la stratégie de data Center du client : petite ou grande, centralisée, distribuée ou mutualisée.

Pour déployer MEDITECH, Cisco a conçu les architectures de référence Cisco UCS et qui s'alignent directement avec les meilleures pratiques du MEDITECH. Cisco UCS propose une solution étroitement intégrée qui offre des performances élevées, une haute disponibilité, une fiabilité et une évolutivité élevées afin de prendre en charge les cabinets médicaux et les systèmes hospitaliers disposant de plusieurs milliers de lits.

Spécifications techniques des petites, moyennes et grandes architectures

Cette section présente un exemple de nomenclature pour des architectures de stockage de différentes tailles.

Nomenclature pour les petites, moyennes et grandes architectures.

La conception du système FlexPod est une infrastructure flexible qui englobe de nombreux composants et versions logicielles différents. Utiliser "Tr-4036 : spécifications techniques de FlexPod" Pour faciliter l'assemblage d'une configuration FlexPod valide. Les configurations du tableau ci-dessous représentent les exigences minimales pour FlexPod et ne sont qu'un exemple. La configuration peut être étendue pour chaque famille de produits, selon les besoins pour différents environnements et cas d'utilisation.

Pour cet exercice de dimensionnement, petit correspond à un environnement MEDITECH de catégorie 3, moyen à une catégorie 5 et grand à une catégorie 6.

	Petit	Moyen	Grand
Plateforme	Une paire haute disponibilité du système de stockage 100 % Flash NetApp AFF A220	Une paire haute disponibilité NetApp AFF A220	Une paire haute disponibilité de systèmes de stockage 100 % Flash NetApp AFF A300
Tiroirs disques	9 To x 3,8 To	13 To x 3,8 To	19 To x 3,8 To
Taille de la base DE données MEDITECH	3TO-12 TO	17 TO	> 30 TO
IOPS DE MEDITECH	<22,000 000 IOPS	> 25,000 IOPS	> 32,000 IOPS
IOPS total	22000	27000	35000
Brut	34,2 TO	49,4 TO	68,4 TO
Capacité exploitable	18,53 Tio	27,96 Tio	33,82 Tio
Capacité réelle (efficacité du stockage 2:1)	55,6 Tio	83,89Tio	101,47 Tio

Certains environnements client peuvent exécuter plusieurs charges de travail de production MEDITECH simultanément ou avec des besoins en IOPS plus élevés. Dans de tels cas, contactez l'équipe NetApp en charge des comptes pour dimensionner les systèmes de stockage en fonction des IOPS et de la capacité requises. Vous devez être en mesure de déterminer la plateforme adaptée aux charges de travail. Par exemple, les entreprises exécutent efficacement plusieurs environnements MEDITECH sur une paire haute disponibilité du système de stockage 100 % Flash AFF de NetApp.

Le tableau suivant présente les logiciels standard requis pour les configurations MEDITECH.

Logiciel	Famille de produits	Version ou version	Détails
Stockage	ONTAP	ONTAP 9.4 - disponibilité générale (GA)	
Le réseau	Interconnexions de fabric Cisco UCS	Cisco UCSM 4.x	Version actuelle recommandée
	Commutateurs Ethernet Cisco Nexus	7.0(3)I7(6)	Version actuelle recommandée
	Cisco FC : Cisco MDS 9132T	8.3(2)	Version actuelle recommandée
Hyperviseur	Hyperviseur	VMware vSphere ESXi 6.7	
	Machines virtuelles (VM)	Windows 2016	

Logiciel	Famille de produits	Version ou version	Détails
Gestion	Système de gestion de l'hyperviseur	VMware vCenter Server 6.7 U1 (VCSA)	
	NetApp Virtual Storage Console (VSC)	VSC 7.0P1	
	NetApp SnapCenter	SnapCenter 4.0	
	Cisco UCS Manager	4.x	

Le tableau suivant présente un petit exemple de configuration (catégorie 3) : composants d'infrastructure.

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1	Prend en charge jusqu'à huit lames demi-largeur ou quatre lames pleine largeur. Ajout de châssis à mesure que les besoins en serveurs augmentent.
	Modules d'E/S de châssis Cisco	2 x 2208	Ports uplink 8 Go x 10 Go
	Les serveurs lames Cisco UCS	4 x B200 M5	Chacun avec 2 x 14 cœurs, une vitesse d'horloge de 2,6 GHz ou plus et BIOS 3.2 384 Go (3#)
	Cartes d'interface virtuelle Cisco UCS	4 x UCS 1440	Pilote FC FNIC de VMware ESXi : 1.6.0.47 pilote Ethernet ENIC VMware ESXi : 1.0.27.0 (voir matrice d'interopérabilité :
	2 interconnexions de fabric Cisco UCS (FI)	2 X UCS 6454 FI	Fabric Interconnect de 4e génération prenant en charge les protocoles Ethernet 10/25 Gb et FC 32 Gb
Le réseau	Commutateurs Ethernet Cisco	2 x Nexus 9336c-FX2	1 GO, 10 GO, 25 GO, 40 GO, 100 GO
Réseau de stockage	Réseau IP Nexus 9k pour stockage BLOB		Châssis FI et UCS
	FC : CISCO MDS 9132T		Deux commutateurs Cisco 9132T

Calque	Famille de produits	Quantité et modèle	Détails
Stockage	Système de stockage 100 % Flash NetApp AFF A300	1 paire HA	Cluster à 2 nœuds pour toutes les charges de travail MEDITECH (serveur de fichiers, image Server, SQL Server, VMware, etc.)
	Tiroir disque DS224C	1 tiroir disque DS224C	
	Disque SSD	9 x 3,8 To	

Le tableau suivant présente un exemple de configuration moyenne (catégorie 5) – composants d'infrastructure

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1	Prend en charge jusqu'à huit lames demi-largeur ou quatre lames pleine largeur. Ajout de châssis à mesure que les besoins en serveurs augmentent.
	Modules d'E/S de châssis Cisco	2 x 2208	Ports uplink 8 Go x 10 Go
	Les serveurs lames Cisco UCS	6 x B200 M5	Chacun avec 2 x 16 cœurs, une vitesse d'horloge de 2,5 GHz/ou plus, et 384 Go ou plus de mémoire BIOS 3.2 (3#)
	Carte d'interface virtuelle Cisco UCS (VIC)	6 x UCS 1440 VICS	Pilote FC FNIC de VMware ESXi : 1.6.0.47 pilote Ethernet ENIC VMware ESXi : 1.0.27.0 (voir matrice d'interopérabilité :)
	2 interconnexions de fabric Cisco UCS (FI)	2 X UCS 6454 FI	Fabric Interconnect de 4e génération prenant en charge les protocoles Ethernet 10 Gb/25 Gb et FC 32 Gb
Le réseau	Commutateurs Ethernet Cisco	2 x Nexus 9336c-FX2	1 GO, 10 GO, 25 GO, 40 GO, 100 GO
Réseau de stockage	Réseau IP Nexus 9k pour stockage BLOB		
	FC : CISCO MDS 9132T		Deux commutateurs Cisco 9132T

Calque	Famille de produits	Quantité et modèle	Détails
Stockage	Système de stockage 100 % Flash AFF A220 NetApp	2 paire HA	Cluster à 2 nœuds pour toutes les charges de travail MEDITECH (serveur de fichiers, image Server, SQL Server, VMware, etc.)
	Tiroir disque DS224C	1 tiroir disque DS224C	
	SSD	13 x 3,8 To	

Le tableau suivant présente un grand exemple de configuration (catégorie 6) – composants d'infrastructure.

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1	
	Modules d'E/S de châssis Cisco	2 x 2208	8 ports de liaison ascendante 10 Go
	Les serveurs lames Cisco UCS	8 x B200 M5	Chacun avec 2 x 24 cœurs, 2,7 GHz et 768 Go de BIOS 3.2 (3#)
	Carte d'interface virtuelle Cisco UCS (VIC)	8 x UCS 1440 VICS	Pilote FC FNIC de VMware ESXi : 1.6.0.47 pilote Ethernet ENIC VMware ESXi : 1.0.27.0 (consultez la matrice d'interopérabilité :
	2 interconnexions de fabric Cisco UCS (FI)	2 X UCS 6454 FI	Fabric Interconnect de 4e génération prenant en charge les protocoles Ethernet 10 Gb/25 Gb et FC 32 Gb
Le réseau	Commutateurs Ethernet Cisco	2 x Nexus 9336c-FX2	2 x Cisco Nexus 9332PQ1, 10 Go, 25 Go, 40 Go, 100 Go
Réseau de stockage	IP Network N9k pour le stockage BLOB		
	FC : CISCO MDS 9132T		Deux commutateurs Cisco 9132T
Stockage	AFF A300	1 paire HA	Cluster à 2 nœuds pour toutes les charges de travail MEDITECH (serveur de fichiers, image Server, SQL Server, VMware, etc.)
	Tiroir disque DS224C	1 tiroir disque DS224C	
	SSD	19 x 3,8 To	

Ces configurations constituent un point de départ pour les conseils de dimensionnement. Certains environnements client peuvent avoir plusieurs charges de travail de production MEDITECH et non-MEDITECH exécutées simultanément, ou elles peuvent avoir des exigences d'IOPS plus élevées. En collaboration avec l'équipe de gestion de compte NetApp, vous devez dimensionner les systèmes de stockage en fonction des IOPS, des charges de travail et de la capacité requises pour déterminer la plateforme la mieux adaptée aux charges de travail.

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce document, consultez ces documents ou sites web :

- Conception validée FlexPod Datacenter avec FC Cisco.

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Directives de déploiement NetApp pour les environnements MEDITECH.

  "https://fieldportal.netapp.com/content/248456" (Identifiant NetApp requis)

- Directives de dimensionnement pour les environnements MEDITECH.

  "www.netapp.com/us/media/tr-4190.pdf"

- Déploiement de FlexPod Datacenter pour Epic EHR

  "www.netapp.com/us/media/tr-4693.pdf"

- Zone de conception FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- FlexPod DC avec stockage FC (commutateurs MDS) et NetApp AFF, vSphere 6.5U1 et Cisco UCS Manager

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Cisco Healthcare

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

Remerciements

Les personnes suivantes ont contribué à la rédaction et à la création de ce guide.

- Brandon Agee, Ingénieur marketing et technique, NetApp
- John Duignan, architecte de solutions – Santé, NetApp
- Ketan Mota, responsable produits, NetApp
- Jon Ebmeier, architecte de solutions techniques, Cisco Systems, Inc
- Mike Brennan, responsable produits, Cisco Systems, Inc

Guide de déploiement de FlexPod Datacenter pour MEDITECH

Tr-4753 : Guide de déploiement de FlexPod Datacenter pour MEDITECH

Brandon Agee et John Duignan, NetApp Mike Brennan et Jon Ebmeier, Cisco

En partenariat avec : 

Avantages globaux de la solution

En exécutant un environnement MEDITECH sur le socle architectural de FlexPod, votre organisme de santé peut s'attendre à une amélioration de la productivité du personnel et une réduction des dépenses d'investissement et d'exploitation. FlexPod Datacenter pour MEDITECH offre plusieurs avantages et caractéristiques spécifiques au secteur de la santé :

- **Opérations simplifiées et coûts réduits.** éliminez les dépenses et la complexité des plates-formes existantes en les remplaçant par une ressource partagée plus efficace et évolutive qui peut aider les cliniciens où qu'ils soient. Profitez également d'une utilisation améliorée des ressources et d'un meilleur retour sur investissement.
- **Déploiement plus rapide de l'infrastructure.** Qu'il s'agisse d'un centre de données existant ou d'un emplacement distant, avec la conception intégrée et testée de FlexPod Datacenter, votre nouvelle infrastructure peut être opérationnelle plus rapidement et sans effort.
- **Stockage certifié.** le logiciel de gestion des données NetApp ONTAP avec MEDITECH offre une fiabilité exceptionnelle et un fournisseur de stockage testé et certifié. MEDITECH ne certifie pas d'autres composants d'infrastructure.
- **Évolutivité horizontale.** évolution des systèmes SAN et NAS de téraoctets (To) à des dizaines de pétaoctets (po) sans reconfigurer les applications en cours d'exécution.
- * Continuité de l'activité.* effectuez la maintenance du stockage, les opérations de renouvellement du matériel et les mises à niveau FlexPod sans interrompre l'activité.
- **Colocation sécurisée.** prendre en charge les besoins accrus de l'infrastructure partagée de stockage et de serveur virtualisé, ce qui permet une colocation sécurisée des informations spécifiques à votre installation, particulièrement si votre système héberge plusieurs instances de bases de données et de logiciels.
- **Optimisation des ressources regroupées.** aide à réduire le nombre de contrôleurs de stockage et de serveurs physiques, équilibrer la charge de travail et optimiser l'utilisation tout en améliorant les performances.
- **Qualité de service (QoS).** FlexPod offre la qualité de service sur l'ensemble de la pile. Les meilleures règles de qualité de service du réseau, du calcul et du stockage du secteur garantissent des niveaux de service différenciés dans un environnement partagé. Ces règles permettent d'obtenir des performances optimales pour les charges de travail et d'isoler et de contrôler les applications non contrôlées.
- **Efficacité du stockage.** Réduisez les coûts de stockage avec "La garantie d'efficacité du stockage NetApp 7:1" .
- **Agile.** grâce aux outils de gestion, d'orchestration et d'automatisation de flux de travail les plus performants du secteur fournis par les systèmes FlexPod, votre équipe INFORMATIQUE peut être beaucoup plus réactive aux demandes de l'entreprise. Allant de la sauvegarde MEDITECH au

provisionnement d'environnements de test et de formation et aux réplications de bases de données d'analytique pour les initiatives de gestion de la santé des populations.

- * Productivité accrue.* déployez et faites évoluer rapidement cette solution pour des expériences cliniques optimales pour les utilisateurs finaux.
- **NetApp Data Fabric**.* l'architecture NetApp Data Fabric offre un maillage sur l'ensemble des sites, des emplacements physiques et des applications, NetApp Data Fabric est conçu pour un monde centré sur la donnée. Les données étant créées et exploitées dans divers emplacements, et souvent, vous devez les exploiter et les partager avec d'autres sites, applications et infrastructures. Vous devez disposer d'un moyen de gérer des données cohérent et intégré. Data Fabric est une méthode de gestion qui aide À maîtriser ET à simplifier une INFRASTRUCTURE IT toujours plus complexe.

FlexPod

Nouvelle approche d'infrastructure pour les DME MEDITECH

Les organismes de soins de santé comme la vôtre sont confrontés à une pression considérable pour optimiser les avantages offerts par les investissements conséquents qu'apporte les dossiers médicaux électroniques MEDITECH de pointe. Lorsque les clients conçoivent leurs data centers pour les solutions MEDITECH, ils identifient souvent les objectifs et l'architecture de leur data Center :

- Haute disponibilité des applications MEDITECH
- Hautes performances
- Il est facile d'implémenter MEDITECH dans le data Center
- Agilité et évolutivité pour accompagner la croissance des nouvelles applications ou versions MEDITECH
- Aspect économique
- Alignement avec les recommandations du MEDITECH et les plateformes cibles
- Facilité de gestion, stabilité et support
- Protection robuste des données, sauvegarde, restauration et continuité de l'activité

Les utilisateurs MEDITECH transforment les entreprises et s'adaptent aux modèles de remboursement et aux modèles réduits. Le défi est de fournir l'infrastructure MEDITECH requise dans un modèle de prestation IT plus efficace et plus agile.

Valeur d'une infrastructure convergée prévalidée

Parce qu'il est une exigence fondamentale pour fournir des performances prévisibles et une haute disponibilité des systèmes à faible latence, MEDITECH est prescriptive dans les exigences matérielles de ses clients.

FlexPod est une infrastructure convergée prévalidée et rigoureusement testée par le partenariat stratégique de Cisco et de NetApp. Il est conçu spécialement pour fournir des performances prévisibles avec une faible latence du système et une haute disponibilité. Cette approche donne lieu à la conformité MEDITECH et au délai de réponse optimal pour les utilisateurs du système MEDITECH.

La solution FlexPod de Cisco et NetApp répond aux exigences des systèmes MEDITECH grâce aux services et aux technologies haute performance, modulaires, prévalidées, convergées et virtualisées. plateforme efficace, évolutive et économique. Il offre les avantages suivants :

- **Architecture modulaire.** FlexPod répond aux besoins variés de l'architecture modulaire MEDITECH avec des plateformes FlexPod spécialement configurées pour chaque charge de travail spécifique. Tous les composants sont connectés via un serveur en cluster, une structure de gestion du stockage et un ensemble d'outils de gestion cohésif.

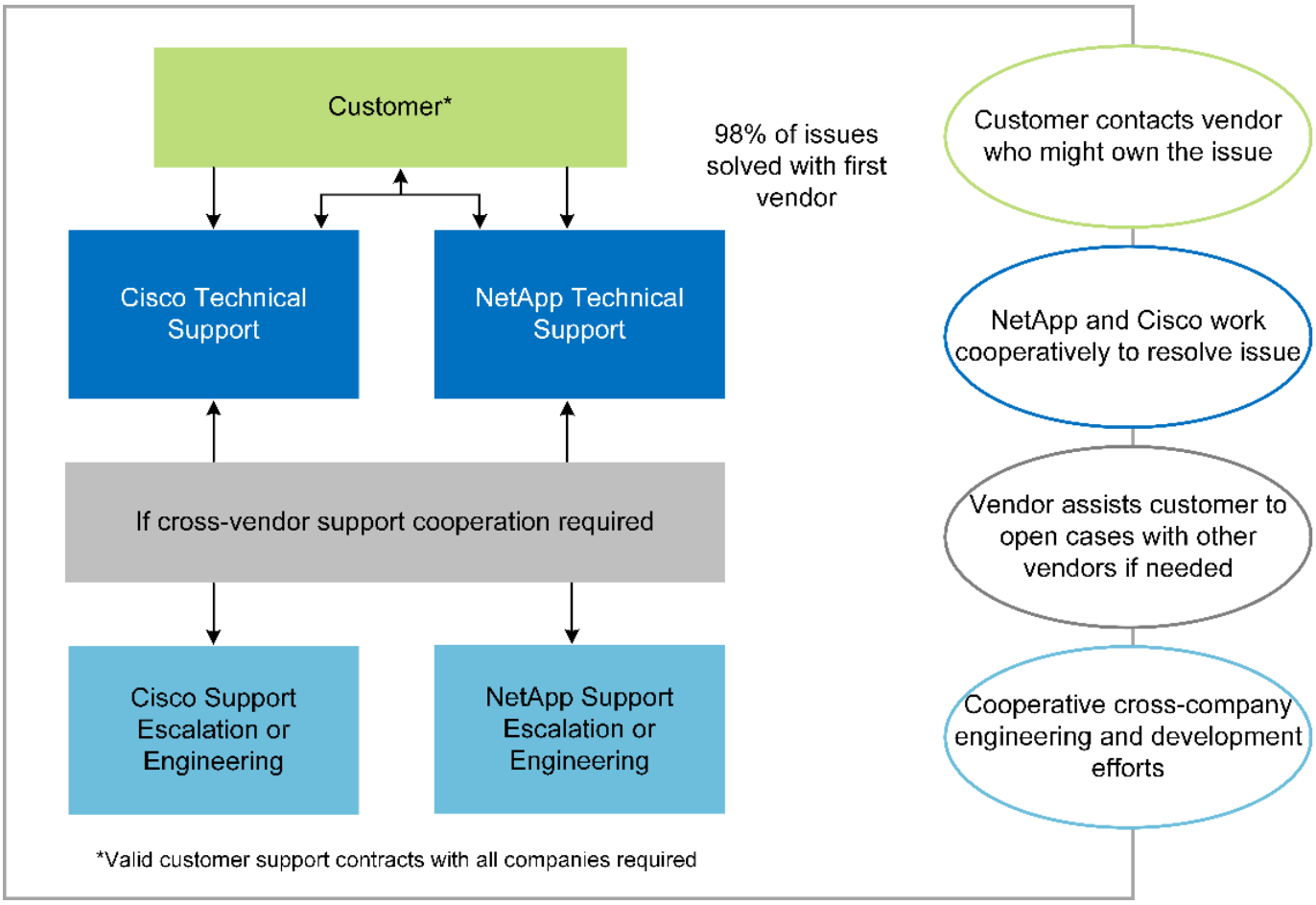
- **Les technologies de pointe à chaque niveau de la pile convergée.** Cisco, NetApp, VMware et Microsoft Windows sont toutes les entreprises classées en première ou 2e position par analystes du secteur dans leurs catégories respectives de serveurs, de réseaux, de stockage et de systèmes d'exploitation.
- * Protection de l'investissement avec UNE INFRASTRUCTURE IT flexible et standardisée* l'architecture de référence FlexPod anticipe les nouvelles versions et mises à jour de produit, avec des tests d'interopérabilité rigoureux en cours pour tenir compte des technologies futures dès qu'elles sont disponibles.
- **Déploiement éprouvé pour une large gamme d'environnements.** solution prétestée et validée avec les principaux hyperviseurs, systèmes d'exploitation, applications et logiciels d'infrastructure, FlexPod a été installé dans plusieurs entreprises clientes MEDITECH.

Architecture FlexPod éprouvée et support coopératif

FlexPod est une solution de data Center éprouvée. Grâce à son infrastructure partagée flexible, elle évolue facilement pour prendre en charge les besoins croissants des charges de travail sans compromettre la performance. En exploitant l'architecture FlexPod, cette solution permet de bénéficier de tous les avantages de FlexPod, notamment :

- **Performances pour répondre aux exigences de la charge de travail MEDITECH** selon les exigences de votre proposition de configuration matérielle MEDITECH, différentes plateformes ONTAP peuvent être déployées pour répondre à vos besoins en E/S et en latence.
- **Évolutivité permettant de faire face facilement à la croissance des données cliniques** évolution dynamique des machines virtuelles, des serveurs et de la capacité de stockage à la demande, sans limites traditionnelles.
- **Efficacité améliorée.** réduire à la fois le temps d'administration et le coût total de possession grâce à une infrastructure virtualisée convergée, qui est plus facile à gérer et qui stocke les données plus efficacement tout en augmentant les performances du logiciel MEDITECH.
- **Réduction des risques.** minimiser les interruptions d'activité grâce à une plateforme prévalidée basée sur une architecture définie qui élimine les approximations de déploiement et permet l'optimisation continue de la charge de travail.
- **Support coopératif FlexPod.** NetApp et Cisco ont mis en place un modèle de support coopératif, solide, évolutif et flexible, pour répondre aux exigences de support uniques de l'infrastructure convergée FlexPod. Ce modèle tire parti de l'expérience, des ressources et de l'expertise de NetApp et de Cisco pour simplifier l'identification et la résolution de votre problème dans le cadre du support FlexPod, et ce, quelle que soit l'origine du problème. Grâce au modèle de support coopératif FlexPod, votre système FlexPod fonctionne efficacement et bénéficie des toutes dernières technologies, et vous travaillez avec une équipe expérimentée pour résoudre les problèmes d'intégration.

  Le support coopératif FlexPod est essentiel pour les organismes de santé qui exécutent des applications stratégiques, telles que MEDITECH sur l'infrastructure convergée FlexPod. La figure suivante illustre le modèle de support coopératif FlexPod.



Outre ces avantages, chaque composant de la pile FlexPod Datacenter avec MEDITECH offre des avantages spécifiques aux workflows EHR.

Cisco Unified Computing System

Un système intégrant automatiquement et autonome, Cisco Unified Computing System (Cisco UCS) se compose d'un domaine de gestion unique interconnecté à une infrastructure d'E/S unifiée. Pour que l'infrastructure puisse fournir des informations stratégiques aux patients et offrir une disponibilité maximale, Cisco UCS pour les environnements MEDITECH a été aligné avec les recommandations d'infrastructure et les meilleures pratiques du secteur.

Les fondations de l'architecture MEDITECH sur Cisco UCS sont la technologie Cisco UCS et la gestion des systèmes intégrée, les processeurs Intel Xeon et la virtualisation des serveurs. Ces technologies intégrées répondent aux défis des data centers et vous aident à les atteindre pour le design des data centers MEDITECH. Cisco UCS unifie la gestion des réseaux LAN, SAN et systèmes dans une seule liaison simplifiée pour les serveurs rack, les serveurs lames et les VM. Cisco UCS est une architecture d'E/S de bout en bout qui intègre la structure unifiée Cisco et la technologie FEX (Fabric Extender) pour connecter tous les composants du système Cisco UCS à l'aide d'une structure réseau unique et d'une couche réseau unique.

Le système peut être déployé en tant qu'unité logique unique ou multiple pour les intégrer et les faire évoluer au sein de plusieurs châssis lames, serveurs en rack, racks et data centers. Le système met en œuvre une architecture radicalement simplifiée qui élimine les multiples périphériques redondants qui peuplent les châssis et les serveurs rack traditionnels des serveurs lame. Dans les systèmes traditionnels, les périphériques redondants, tels que les adaptateurs Ethernet et FC, ainsi que les modules de gestion de châssis, se traduit par plusieurs couches de complexité. Cisco UCS comprend une paire redondante de Cisco UCS Fabric Interconnect (fournis) qui offre un point de gestion unique et un point de contrôle unique pour l'ensemble du trafic d'E/S.

Cisco UCS utilise des profils de service pour s'assurer que les serveurs virtuels de l'infrastructure Cisco UCS sont correctement configurés. Les profils de service sont composés de règles de réseau, de stockage et de calcul qui sont créées une fois par des experts techniques dans chaque discipline. Les profils de service incluent des informations stratégiques sur l'identité du serveur telles que l'adressage LAN et SAN, les configurations d'E/S, les versions de micrologiciel, l'ordre de démarrage, le réseau local virtuel (VLAN), le port physique et les stratégies de qualité de service. Il est possible de créer et d'associer des profils de service de façon dynamique avec n'importe quel serveur physique du système en quelques minutes, et non plus en plusieurs heures ou jours. L'association des profils de service avec des serveurs physiques se fait sous forme d'une opération simple et unique, qui permet la migration d'identités entre les serveurs de l'environnement sans nécessiter de modification de la configuration physique. Il facilite le provisionnement rapide sans système d'exploitation de remplacements des serveurs obsolètes.

L'utilisation de profils de service permet de s'assurer que les serveurs sont configurés de manière cohérente dans toute l'entreprise. Lorsque plusieurs domaines de gestion Cisco UCS sont utilisés, Cisco UCS Central peut utiliser des profils de services globaux pour synchroniser les informations de configuration et de stratégie entre les domaines. Si la maintenance doit être effectuée dans un domaine, l'infrastructure virtuelle peut être migrée vers un autre domaine. Cette approche permet de garantir que même lorsqu'un seul domaine est hors ligne, les applications continuent à fonctionner avec une haute disponibilité.

Pour démontrer qu'il répond aux exigences de configuration des serveurs, Cisco UCS a été énormément testé avec MEDITECH sur une période de plusieurs années. Cisco UCS est une plateforme de serveur prise en charge, répertoriée sur le site de support du système de ressources produit MEDITECH.

La mise en réseau Cisco

Les commutateurs Cisco Nexus et les directeurs multicouches Cisco MDS offrent une connectivité haute performance et une consolidation SAN. Les réseaux de stockage multiprotocoles Cisco réduisent les risques en offrant flexibilité et options : FC, Fibre Connection (FICON), FC over Ethernet (FCoE), SCSI over IP (iSCSI) et FC over IP (FCIP).

Les commutateurs Cisco Nexus offrent l'un des ensembles de fonctionnalités réseau de data centers les plus complets au sein d'une plateforme unique. Elles offrent de hautes performances et une densité élevée aussi bien pour les cœurs des data centers que des campus. Ils offrent également un ensemble complet de fonctionnalités pour les déploiements d'agrégation de data Center, de bout en bout et d'interconnexion de data Center dans une plateforme modulaire extrêmement résiliente.

Cisco UCS intègre des ressources de calcul autour de commutateurs Cisco Nexus et une structure d'E/S unifiée qui identifie et gère différents types de trafic réseau. Ce trafic inclut les E/S du stockage, le trafic des postes de travail en continu, la gestion et l'accès aux applications cliniques et professionnelles. Avantages :

- **Évolutivité de l'infrastructure.** virtualisation, alimentation et refroidissement efficaces, évolutivité du cloud avec automatisation, haute densité et hautes performances, tous ces éléments prennent en charge la croissance efficace du data Center.
- **Continuité opérationnelle.** la conception intègre le matériel, les fonctionnalités logicielles NX-OS et la gestion pour prendre en charge les environnements sans temps d'indisponibilité.
- **QoS des réseaux et des ordinateurs.** Cisco fournit une classe de service (CoS) et une qualité de service basées sur des stratégies sur le réseau, le stockage et le calcul pour des performances optimales des applications stratégiques.
- * Flexibilité des transports.* adopter progressivement de nouvelles technologies de mise en réseau avec une solution économique.

Ensemble, Cisco UCS avec des switchs Cisco Nexus et des directeurs multicouches Cisco MDS offre une solution optimale de connectivité réseau, de calcul et SAN pour MEDITECH.

NetApp ONTAP

Le stockage NetApp qui exécute le logiciel ONTAP réduit vos coûts de stockage globaux, tout en offrant les temps de réponse en lecture et écriture à faible latence et les IOPS nécessaires aux charges de travail MEDITECH. ONTAP prend en charge à la fois les configurations 100 % Flash et hybrides pour créer une plateforme de stockage optimale qui répond aux exigences du MEDITECH. Les systèmes NetApp à accélération Flash ont reçu la validation et la certification MEDITECH : il vous offre, en tant que client MEDITECH, les performances et la réactivité qui sont essentielles aux opérations MEDITECH sensibles à la latence. La création de plusieurs domaines de défaillance dans un seul cluster permet aux systèmes NetApp d'isoler les environnements de production hors production. Les systèmes NetApp permettent également de réduire les problèmes de performance avec un niveau minimal de performance garantie pour les charges de travail avec la QoS ONTAP.

L'architecture scale-out du logiciel ONTAP s'adapte en toute flexibilité à diverses charges de travail d'E/S. Les architectures ONTAP permettent généralement d'atteindre le débit et la faible latence nécessaires aux applications cliniques tout en proposant une architecture scale-out modulaire. Les nœuds NetApp AFF peuvent être associés dans le même cluster scale-out avec des nœuds de stockage hybride (HDD et Flash) qui sont adaptés au stockage de datasets volumineux à haut débit. Outre une solution de sauvegarde approuvée par MEDITECH, vous pouvez cloner, répliquer et sauvegarder votre environnement MEDITECH depuis un système de stockage SSD (Solid-State Drive) coûteux et le stockage HDD plus économique sur d'autres nœuds. Cette approche rencontre, voire dépasse, les directives MEDITECH pour le clonage et la sauvegarde des pools de production basés sur le SAN.

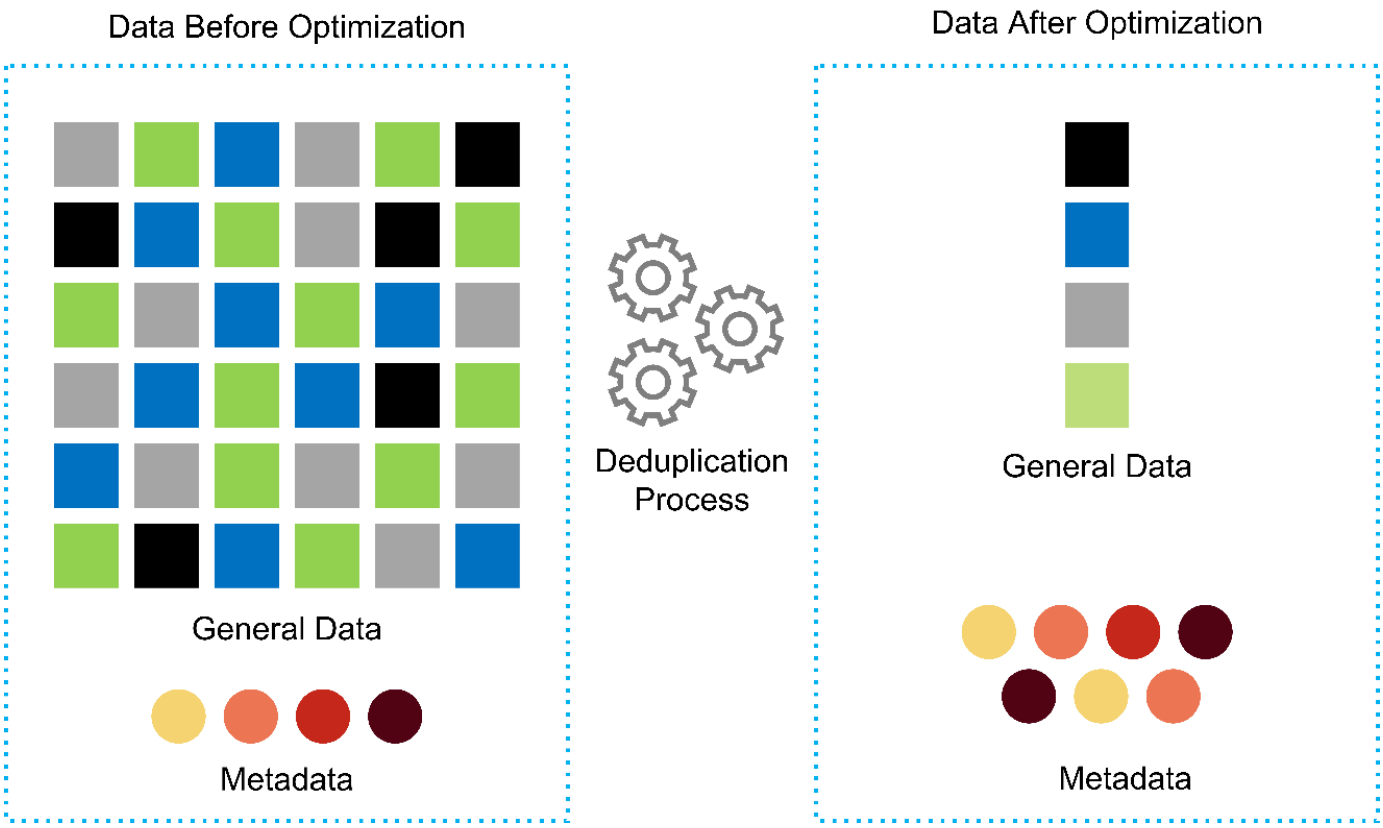
De nombreuses fonctionnalités ONTAP sont particulièrement utiles pour les environnements MEDITECH : simplification de la gestion, amélioration de la disponibilité et de l'automatisation et réduction du volume total de stockage requis. Avantages de ces fonctionnalités :

- **Performances exceptionnelles.** la solution NetApp AFF partage l'architecture de stockage unifié, le logiciel ONTAP, l'interface de gestion, les services de données complets et les fonctionnalités avancées des autres gammes de produits FAS de NetApp. Cette association innovante des supports 100 % Flash avec les systèmes ONTAP offre la faible latence prévisible et les IOPS élevées des systèmes de stockage 100 % Flash, associées à la qualité de logiciel ONTAP optimale.
- **Efficacité du stockage.** réduisez les besoins en capacité totale grâce à la déduplication, à la technologie de réplication des données NetApp FlexClone, à la compression à la volée, à la compaction, à la réplication fine, au provisionnement fin et déduplication dans l'agrégat.

  La déduplication NetApp offre une déduplication au niveau des blocs dans un volume NetApp FlexVol ou dans un composant de données. La déduplication supprime les blocs dupliqués pour ne stocker que les blocs uniques du volume FlexVol ou du composant de données.

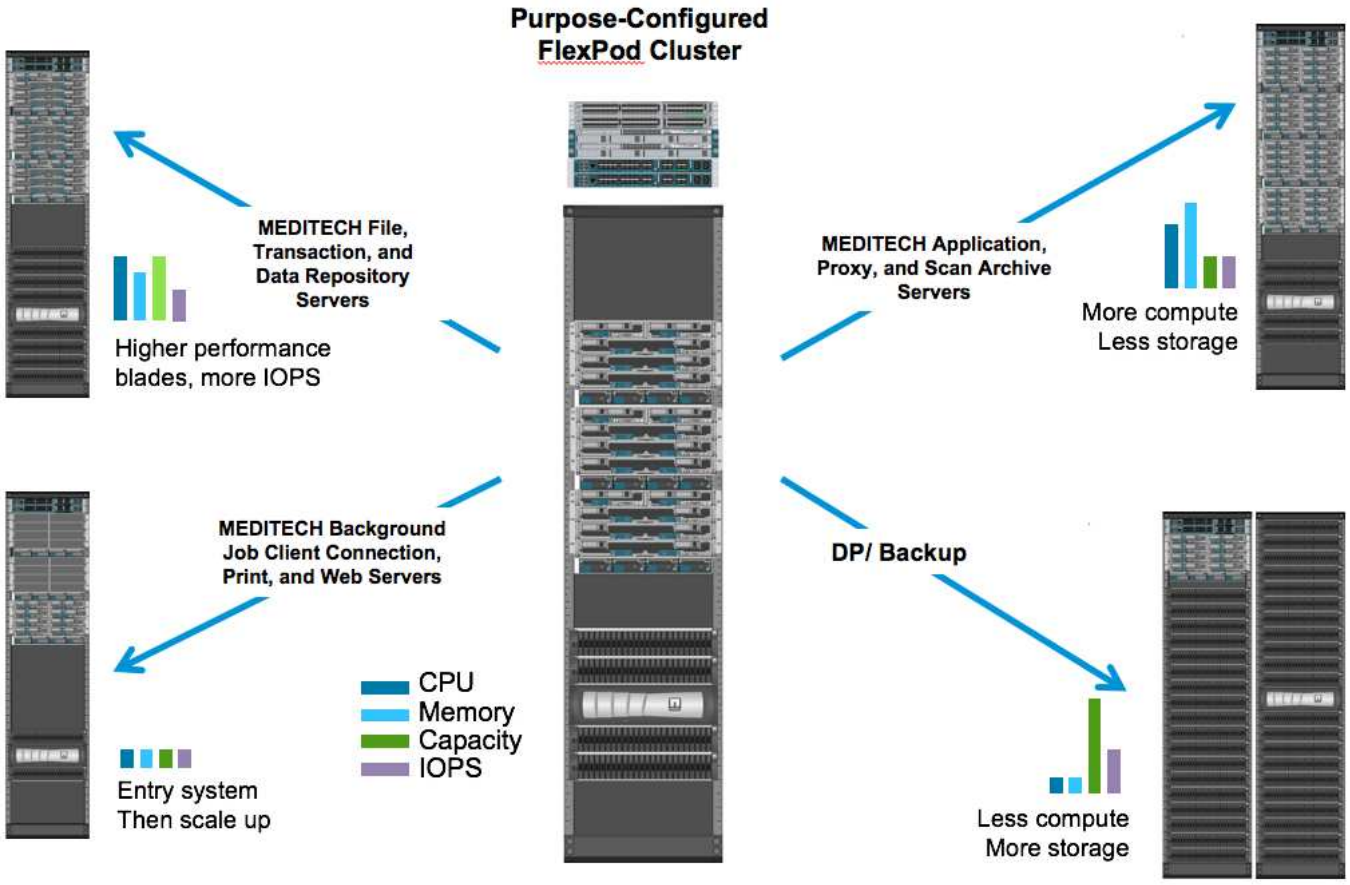
  La déduplication fonctionne avec un niveau de granularité élevé et s'exécute sur le système de fichier actif du volume FlexVol ou du composant de données. La déduplication est transparente pour les applications. Vous pouvez donc l'utiliser pour dédupliquer des données provenant de toute application qui utilise le système NetApp. Vous pouvez exécuter la déduplication des volumes comme processus à la volée (depuis la version ONTAP 8.3.2). Vous pouvez également l'exécuter en arrière-plan sous la forme d'un processus que vous pouvez configurer pour s'exécuter automatiquement, de manière à être planifiée ou manuellement via l'interface de ligne de commande, NetApp ONTAP System Manager ou NetApp Active IQ Unified Manager.

  La figure suivante illustre le fonctionnement optimal de la déduplication NetApp.



- **Clonage compact.** la fonctionnalité FlexClone vous permet de créer presque instantanément des clones pour prendre en charge l'actualisation de l'environnement de sauvegarde et de test. Ces clones consomment davantage d'espace de stockage uniquement lorsque des modifications sont apportées.
- **Technologies NetApp Snapshot et SnapMirror.** ONTAP peut créer des copies Snapshot compactes des LUN (Logical Unit Numbers) utilisées par l'hôte MEDITECH. Dans le cas de déploiements sur deux sites, vous pouvez implémenter le logiciel SnapMirror pour améliorer la réplication des données et la résilience.
- **Protection intégrée des données.** les fonctionnalités de protection complète des données et de reprise après incident vous aident à protéger les données stratégiques et à assurer une reprise après incident.
- **Continuité de l'activité.** vous pouvez effectuer des mises à niveau et des opérations de maintenance sans mettre les données hors ligne.
- **QoS et QoS adaptative (AQoS).** la qualité de service du stockage vous permet de limiter les charges de travail dominantes potentielles. Plus important encore, la QoS peut garantir des performances minimales pour les charges de travail stratégiques telles que la production MEDITECH. En limitant les conflits, la qualité de services NetApp peut réduire les problèmes de performance. AQoS fonctionne avec des groupes de règles prédéfinis que vous pouvez appliquer directement à un volume. Ces groupes de règles peuvent automatiquement adapter une taille maximale ou au sol par volume, ce qui conserve un rapport d'IOPS de quelques téraoctets et de plusieurs gigaoctets en fonction de la taille du volume modifié.
- **NetApp Data Fabric**. NetApp Data Fabric simplifie et intègre la gestion des données dans les environnements cloud et sur site afin d'accélérer la transformation digitale. Elles offrent des services et des applications de gestion de données intégrés et cohérents pour la visibilité, l'exploitation, l'accès, le contrôle ainsi que la protection et la sécurité, NetApp est intégré avec Amazon Web Services (AWS), Azure, Google Cloud Platform et les clouds IBM Cloud pour vous offrir un large choix.

La figure suivante illustre l'architecture FlexPod pour les charges de travail MEDITECH.



Présentation DE MEDITECH

Medical information Technology, Inc., communément appelé MEDITECH, est une entreprise de logiciel basée au Massachusetts qui fournit des systèmes d'information aux organismes de santé. MEDITECH fournit un système de DME conçu pour stocker et organiser les dernières données patient et fournir les données au personnel clinique. Les données patient comprennent, sans s'y limiter, les données démographiques; les antécédents médicaux; les médicaments; les résultats des tests de laboratoire; images de radiologie ; et informations personnelles telles que l'âge, la taille et le poids.

Il va au-delà du périmètre de ce document et couvre l'éventail étendu des fonctions prises en charge par le logiciel MEDITECH. L'annexe A fournit plus d'informations sur ces vastes ensembles de fonctions MEDITECH. Les applications MEDITECH nécessitent plusieurs machines virtuelles pour prendre en charge ces fonctions. Pour déployer ces applications, consultez les recommandations du MEDITECH.

Pour chaque déploiement, du point de vue des systèmes de stockage, tous les systèmes logiciels MEDITECH nécessitent une base de données distribuée axée sur les patients. MEDITECH possède sa propre base de données propriétaire, qui utilise le système d'exploitation Windows.

Bridgehead et CommVault sont les deux applications logicielles de sauvegarde certifiées par NetApp et MEDITECH. Ce document ne couvre pas le déploiement de ces applications de sauvegarde.

L'objectif principal de ce document est de permettre à la pile FlexPod (serveurs et stockage) de répondre aux exigences de performances de la base de données MEDITECH et aux exigences de sauvegarde dans l'environnement EHR.

Conçu spécialement pour les charges de travail MEDITECH spécifiques

MEDITECH ne revende pas de matériel de serveur, de réseau ou de stockage, d'hyperviseurs ou de systèmes d'exploitation mais elle a des exigences spécifiques pour chaque composant de la pile d'infrastructure. C'est pourquoi Cisco et NetApp ont travaillé ensemble pour tester et permettre à FlexPod Datacenter d'être configuré, déployé et pris en charge pour répondre aux besoins de l'environnement de production MEDITECH des clients tels que vous.

Catégories MEDITECH

MEDITECH associe la taille du déploiement à un numéro de catégorie compris entre 1 et 6. La catégorie 1 représente les plus petits déploiements MEDITECH, et la catégorie 6 représente les plus grands déploiements MEDITECH.

Pour plus d'informations sur les caractéristiques d'E/S et les besoins en performances d'un hôte MEDITECH dans chaque catégorie, consultez le site NetApp "Tr-4190 : directives de dimensionnement NetApp pour les environnements MEDITECH".

Plateforme MEDITECH

La plate-forme MEDITECH expanse est la dernière version du logiciel EHR de l'entreprise. Les anciennes plateformes MEDITECH sont client/serveur 5.x et MAGIC. Cette section décrit la plateforme MEDITECH (avec étendue, 6.x, C/S 5.x et MAGIC), concernant l'hôte MEDITECH et ses besoins en stockage.

Pour toutes les plateformes MEDITECH précédentes, plusieurs serveurs exécutent le logiciel MEDITECH pour effectuer différentes tâches. La figure précédente représente un système MEDITECH standard, avec les hôtes MEDITECH qui sont utilisés en tant que serveurs de base de données applicative et d'autres serveurs MEDITECH. Les autres serveurs MEDITECH sont notamment l'application de référentiel de données, l'application d'analyse et d'archivage et les clients de travail en arrière-plan. Pour obtenir la liste complète des autres serveurs MEDITECH, reportez-vous aux documents « proposition de configuration matérielle » (pour les nouveaux déploiements) et « tâche d'évaluation matérielle » (pour les déploiements existants). Ces documents peuvent être obtenu auprès de MEDITECH par l'intégrateur système MEDITECH ou auprès de votre responsable de compte technique MEDITECH.

Hôte DE MEDITECH

Un hôte MEDITECH est un serveur de base de données. Cet hôte est également appelé serveur de fichiers MEDITECH (pour la plate-forme étendue, 6.x ou C/S 5.x) ou COMME une machine MAGIC (pour la plate-forme MAGIC). Ce document utilise l'hôte du terme MEDITECH pour faire référence au serveur de fichiers MEDITECH ou à une machine MAGIC.

LES hôtes MEDITECH peuvent être des serveurs ou des machines virtuelles physiques exécutés sur le système d'exploitation Microsoft Windows Server. Les hôtes MEDITECH sont le plus souvent déployés sur le terrain en tant que machines virtuelles Windows qui s'exécutent sur un serveur VMware ESXi. À ce jour, VMware est le seul hyperviseur pris en charge par MEDITECH. Un hôte MEDITECH stocke son programme, son dictionnaire et ses fichiers de données sur un lecteur Microsoft Windows (par exemple, le lecteur E) du système Windows.

Dans un environnement virtuel, un lecteur Windows E réside sur un LUN relié à la machine virtuelle par le biais d'un RDM (Raw Device Mapping) en mode de compatibilité physique. L'utilisation des fichiers VMDK (Virtual machine Disk) comme lecteur Windows E dans ce scénario n'est pas prise en charge par MEDITECH.

Caractéristiques en E/S de la charge de travail hôte MEDITECH

Les caractéristiques d'E/S de chaque hôte MEDITECH et du système dans son ensemble dépendent de la

plateforme MEDITECH que vous déployez. Toutes les plateformes MEDITECH (étendue, 6.x, C/S 5.x et MAGIC) génèrent des workloads qui sont 100 % aléatoires.

La plateforme d'étendue MEDITECH génère le workload le plus exigeants. En effet, elle présente le plus grand pourcentage d'opérations d'écriture et d'IOPS globales par hôte, suivi par 6.x, C/S 5.x et les plateformes MAGIC.

Pour plus de détails sur les descriptions des charges de travail de MEDITECH, voir "Tr-4190 : directives de dimensionnement NetApp pour les environnements MEDITECH".

Réseau de stockage

MEDITECH nécessite l'utilisation du protocole FC pour le trafic de données entre le système NetApp FAS ou AFF et les hôtes MEDITECH de toutes les catégories.

Présentation du stockage pour un hôte MEDITECH

Chaque hôte MEDITECH utilise deux disques Windows :

- **Lecteur C.** ce lecteur stocke le système d'exploitation Windows Server et les fichiers d'application hôte MEDITECH.
- **Lecteur E.** l'hôte MEDITECH stocke son programme, son dictionnaire et ses fichiers de données sur le lecteur E du système d'exploitation Windows Server. Le disque E est une LUN mappée à partir du système FAS ou AFF de NetApp via le protocole FC. MEDITECH nécessite l'utilisation du protocole FC afin de répondre aux exigences en termes d'IOPS et de latence de lecture et d'écriture de l'hôte MEDITECH.

nomenclature établie des volumes et des LUN

MEDITECH nécessite l'utilisation d'une convention de nommage spécifique pour toutes les LUN.

Avant de déployer tout système de stockage, vérifiez la proposition de configuration matérielle MEDITECH afin de confirmer la convention de nom des LUN. La sauvegarde MEDITECH s'appuie sur la convention de nom des volumes et des LUN pour identifier correctement les LUN à sauvegarder.

Outils de gestion et fonctionnalités d'automatisation complets

Cisco UCS et Cisco UCS Manager

Cisco s'articule autour de trois éléments clés pour offrir une infrastructure de data Center de pointe : simplification, sécurité et évolutivité. Associé à la modularité de plateforme, le logiciel Cisco UCS Manager procure une plateforme de virtualisation des postes de travail simplifiée, sécurisée et évolutive :

- **Simplifié.** Cisco UCS offre une nouvelle approche radicale de l'informatique standard et fournit le cœur de l'infrastructure de centre de données pour toutes les charges de travail. Cisco UCS offre de nombreuses fonctionnalités et avantages, notamment une réduction du nombre de serveurs nécessaires et du nombre de câbles utilisés par serveur. Une autre fonctionnalité importante est la possibilité de déployer ou de reprovisionner rapidement des serveurs via des profils de service Cisco UCS. Le nombre de serveurs et de câbles à gérer, ainsi que le provisionnement rationalisé des charges de travail applicatives et de serveurs simplifient les opérations. Les profils de service Cisco UCS Manager permettent de provisionner une quantité de serveurs lames et en rack en quelques minutes. Les profils de service Cisco UCS éliminent les runbooks d'intégration de serveurs tout en éliminant les écarts de configuration. Cette approche accélère le temps consacré à la productivité des utilisateurs finaux, améliore la souplesse de l'entreprise et permet l'allocation des ressources INFORMATIQUES à d'autres tâches.

  Cisco UCS Manager automatise de nombreuses opérations courantes et sujettes aux erreurs des data

centers, telles que la configuration et le provisionnement de l'infrastructure d'accès au serveur, au réseau et au stockage. De plus, les serveurs lames Cisco UCS B-Series et les serveurs en rack C-Series avec un encombrement important de mémoire assurent une densité élevée pour les utilisateurs d'applications, ce qui réduit les exigences de l'infrastructure de serveurs.

La simplification conduit à un déploiement d'infrastructure MEDITECH plus rapide et efficace.

- **Secure.** bien que les machines virtuelles soient intrinsèquement plus sécurisées que leurs prédécesseurs physiques, elles présentent de nouveaux défis en matière de sécurité. Les serveurs web et d'applications stratégiques qui utilisent une infrastructure commune telle que les postes de travail virtuels courent désormais un risque plus élevé de menaces de sécurité. Le trafic entre les VM représente désormais un élément de sécurité important que les responsables INFORMATIQUES doivent traiter, en particulier dans les environnements dynamiques dans lesquels les VM, via VMware vMotion, déplacent dans l'infrastructure de serveurs.

  Par conséquent, la virtualisation augmente considérablement la sensibilisation au niveau des machines virtuelles aux règles et à la sécurité, notamment étant donné la nature dynamique et fluide de la mobilité des machines virtuelles au sein d'une infrastructure informatique étendue. La facilité avec laquelle les nouveaux postes de travail virtuels peuvent proliférer accroît l'importance d'une infrastructure réseau et de sécurité orientée virtualisation. L'infrastructure de data Center Cisco (Cisco UCS, Cisco MDS et gamme de solutions Cisco Nexus) pour la virtualisation des postes de travail offre une sécurité renforcée au niveau du data Center, du réseau et des postes de travail, avec une sécurité complète depuis le poste de travail vers l'hyperviseur. La segmentation des postes de travail virtuels, des stratégies et de l'administration intégrant la cohérence avec les machines virtuelles, ainsi que la sécurité réseau sur l'ensemble de l'infrastructure LAN et WAN.

- **Évolutif.** la croissance des solutions de virtualisation est inévitable. Une solution doit donc être capable d'évoluer de manière prévisible avec cette croissance. Les solutions de virtualisation Cisco prennent en charge une forte densité d'ordinateurs virtuels (VM par serveur). De plus, plus le nombre de serveurs peut évoluer en s'appuyant sur des performances quasi linéaires. L'infrastructure de data Center Cisco offre une plateforme flexible pour la croissance et améliore la souplesse commerciale. Les profils de service Cisco UCS Manager permettent un provisionnement d'hôte à la demande et facilitent le déploiement de centaines d'hôtes car celui-ci doit être déployé des dizaines.

  Les serveurs Cisco UCS offrent des performances et une évolutivité quasi linéaires. Cisco UCS met en œuvre la technologie de mémoire étendue brevetée Cisco, qui offre un grand format de mémoire avec moins de sockets (avec une évolutivité jusqu'à 1 To de mémoire avec des serveurs à 2 et 4 sockets). Grâce à la technologie Unified Fabric comme élément de base, la bande passante agrégée des serveurs Cisco UCS Server peut évoluer jusqu'à 80 Gbit/s par serveur. En outre, Cisco UCS Fabric Interconnect peut produire 2 Tbit/s à un taux de ligne inférieur. Cette fonctionnalité permet d'éviter les goulets d'étranglement en E/S de la virtualisation des postes de travail et la mémoire. Cisco UCS, grâce à son architecture réseau unifiée basée sur la structure hautes performances à faible latence, prend en charge des volumes importants de trafic de postes de travail virtuels, notamment le trafic vidéo et de communication haute résolution. De plus, grâce aux solutions de virtualisation FlexPod, ONTAP garantit la disponibilité des données et des performances optimales lors des « boot storms » et « login storms ».

  Les conceptions d'infrastructures de data Center Cisco UCS, Cisco MDS et Cisco Nexus fournissent une excellente plateforme à plus forte croissance. Vous bénéficiez d'une évolutivité transparente des ressources de serveur, de réseau et de stockage pour prendre en charge la virtualisation des postes de travail, les applications de data Center et le cloud computing.

Serveur VMware vCenter

VMware vCenter Server constitue une plateforme centralisée pour la gestion des environnements MEDITECH : votre entreprise du secteur de la santé peut automatiser et fournir une infrastructure virtuelle en toute

confiance :

- **Déploiement simple.** déployez rapidement et facilement vCenter Server à l'aide d'une appliance virtuelle.
- **Contrôle et visibilité centralisés.** administrer l'ensemble de l'infrastructure VMware vSphere à partir d'un emplacement unique.
- **Optimisation proactive.** allouer et optimiser les ressources pour une efficacité maximale.
- **Gestion.** utilisez des plug-ins et des outils puissants pour simplifier la gestion et étendre le contrôle.

Virtual Storage Console pour VMware vSphere

Virtual Storage Console (VSC), le fournisseur vSphere API for Storage Awareness (VASA) et l'appliance VMware Storage Replication adapter (SRA) pour VMware vSphere de NetApp constituent une seule appliance virtuelle. La suite de produits inclut SRA et VASA Provider comme plug-in vCenter Server, qui permet de gérer de bout en bout le cycle de vie des machines virtuelles dans les environnements VMware qui utilisent des systèmes de stockage NetApp.

L'appliance virtuelle pour VSC, VASA Provider et SRA s'intègre facilement avec le client Web VMware vSphere et vous permet d'utiliser les services SSO. Dans un environnement comportant plusieurs instances VMware vCenter Server, chaque instance vCenter Server à gérer doit disposer de sa propre instance enregistrée de VSC. La page du tableau de bord VSC vous permet de consulter rapidement l'état global de vos datastores et machines virtuelles.

Grâce au déploiement de l'appliance virtuelle pour VSC, VASA Provider et SRA, vous pouvez effectuer les tâches suivantes :

- **Utilisez VSC pour déployer et gérer le stockage et configurer l'hôte ESXi.** vous pouvez utiliser VSC pour ajouter des informations d'identification, supprimer des informations d'identification, attribuer des informations d'identification et configurer des autorisations pour les contrôleurs de stockage dans votre environnement VMware. De plus, vous pouvez gérer des serveurs ESXi connectés aux systèmes de stockage NetApp. En quelques clics, vous pouvez définir les valeurs recommandées pour les délais d'expiration des hôtes, le NAS et les chemins d'accès multiples pour tous les hôtes. Vous pouvez également afficher les détails du stockage et collecter des informations de diagnostic.
- **Utilisez VASA Provider pour créer des profils de capacité de stockage et définir des alarmes.** VASA Provider pour ONTAP est enregistré avec VSC lorsque vous activez l'extension VASA Provider. Vous pouvez créer et utiliser des profils de capacité de stockage et des datastores virtuels. Vous pouvez également définir des alarmes pour vous alerter lorsque les seuils des volumes et des agrégats sont presque pleins. Il est possible de surveiller les performances des VMDK et des machines virtuelles qui sont créées sur des datastores virtuels.
- **Utilisez SRA pour la reprise après sinistre.** vous pouvez utiliser SRA pour configurer les sites protégés et de reprise dans votre environnement pour la reprise après sinistre en cas de panne.

NetApp OnCommand Insight et ONTAP

NetApp OnCommand Insight intègre la gestion de l'infrastructure à la chaîne de livraison des services MEDITECH. Cette approche permet à votre établissement de santé de mieux contrôler, automatiser et analyser votre infrastructure de stockage, de réseau et de calcul. Optimisez votre infrastructure actuelle afin d'en tirer le meilleur parti, tout en simplifiant les prises de décision en termes d'achat. Elle réduit également les risques associés aux migrations technologiques complexes. Aucun agent n'étant nécessaire, l'installation est simple et sans perturbation. Les périphériques de stockage et SAN sont continuellement découverts et des informations détaillées sont recueillies pour offrir une totale visibilité de l'ensemble de votre environnement de stockage. Vous pouvez identifier rapidement les actifs mal utilisés, déréglés, sous-employés ou orphelins, puis les récupérer pour alimenter l'extension future. OnCommand Insight peut vous aider à :

- * Optimiser les ressources existantes.* identifier les actifs mal utilisés, sous-employés ou orphelins en utilisant les meilleures pratiques établies pour éviter les problèmes et respecter les niveaux de service.
- * Prendre de meilleures décisions.* les données en temps réel permettent de résoudre plus rapidement les problèmes de capacité afin de planifier avec précision les futurs achats, d'éviter les surinvestissements et de reporter les dépenses d'investissement.
- **Accélérer les initiatives INFORMATIQUES.** mieux comprendre vos environnements virtuels pour vous aider à gérer les risques, réduire les temps d'arrêt et accélérer le déploiement du cloud.

Design

L'architecture de FlexPod pour MEDITECH est basée sur les conseils d'MEDITECH, de Cisco et de NetApp et de l'expérience du partenaire qui équipe avec les clients MEDITECH de toutes les tailles. L'architecture est adaptable et applique les bonnes pratiques pour MEDITECH, selon la stratégie de votre data Center, la taille de votre entreprise et si votre système est centralisé, distribué ou mutualisé.

L'architecture de stockage appropriée peut être déterminée par la taille globale avec le nombre total d'IOPS. La performance seule n'est pas le seul facteur et vous pouvez décider d'utiliser un plus grand nombre de nœuds en fonction des exigences supplémentaires des clients. Le stockage NetApp présente l'avantage de faciliter et d'assurer une évolutivité verticale du cluster sans interruption, en fonction de l'évolution de vos besoins. Vous pouvez également supprimer des nœuds du cluster sans interruption pour reconvertir les équipements ou procéder à des mises à jour d'équipements.

Voici quelques-uns des avantages de l'architecture de stockage NetApp ONTAP :

- **Évolutivité horizontale et verticale simple et sans interruption.** vous pouvez mettre à niveau, ajouter ou supprimer des disques et des nœuds à l'aide de la continuité de l'activité ONTAP. Vous pouvez commencer avec quatre nœuds et passer à six nœuds, ou effectuer une mise à niveau vers des contrôleurs plus volumineux sans interruption.
- **Fonctionnalités d'efficacité du stockage** réduisez vos besoins en capacité totale grâce à la déduplication, NetApp FlexClone, la compression à la volée, la compaction à la volée, la réplication fine, le provisionnement fin et la déduplication d'agrégat. La fonctionnalité FlexClone vous permet de créer presque instantanément des clones pour prendre en charge les mises à jour de l'environnement de sauvegarde et de test. Ces clones consomment davantage d'espace de stockage uniquement lorsque des modifications sont apportées.
- **Serveur de base de données shadow de reprise après sinistre.** le serveur de base de données shadow de reprise après sinistre fait partie de votre stratégie de continuité de l'activité (utilisé pour prendre en charge la fonctionnalité de stockage en lecture seule et potentiellement configuré pour être une instance de lecture/écriture de stockage). Par conséquent, le placement et le dimensionnement du troisième système de stockage sont généralement identiques à ceux de votre système de stockage de base de données de production.
- **Cohérence de la base de données (nécessite un certain degré d'considération).** si vous utilisez des copies de sauvegarde NetApp SnapMirror en relation avec la continuité de l'activité, voir "Tr-3446 : Guide des meilleures pratiques et présentation du mode asynchrone de SnapMirror".

Disposition du stockage

Agrégats dédiés pour les hôtes MEDITECH

Pour répondre aux besoins haute performance et haute disponibilité du MEDITECH, il est important de concevoir correctement l'infrastructure de stockage et d'isoler la charge de travail de production de l'hôte

MEDITECH dans le système de stockage dédié et haute performance.

Un agrégat dédié doit être provisionné sur chaque contrôleur de stockage pour stocker le programme, le dictionnaire et les fichiers de données des hôtes MEDITECH. Afin d'éliminer tout risque que d'autres charges de travail utilisent les mêmes disques et d'affecter les performances, aucun autre stockage n'est provisionné à partir de ces agrégats.

> Le stockage que vous provisionnez pour les autres serveurs MEDITECH ne doit pas être placé sur l'agrégat dédié des LUN qui sont utilisées par les hôtes MEDITECH. Le stockage des autres serveurs MEDITECH doit être placé sur un agrégat distinct. Les besoins en stockage des autres serveurs MEDITECH sont disponibles dans les documents « proposition de configuration matérielle » (pour les nouveaux déploiements) et « tâche d'évaluation du matériel » (pour les déploiements existants). Ces documents peuvent être obtenu auprès de MEDITECH par l'intégrateur système MEDITECH ou auprès de votre responsable de compte technique MEDITECH. Les ingénieurs solutions NetApp peuvent contacter l'équipe MEDITECH Independent Software Vendor (éditeur de logiciels indépendant) de NetApp pour faciliter la configuration du dimensionnement du stockage et de son application.

Répartir les charges de travail hôte MEDITECH de façon homogène entre tous les contrôleurs de stockage

Les systèmes NetApp FAS et AFF sont déployés sous forme d'une ou de plusieurs paires haute disponibilité. NetApp vous recommande d'étendre l'étendue MEDITECH et les charges de travail 6.x de manière homogène entre chaque contrôleur de stockage afin d'appliquer les ressources de calcul, de réseau et de mise en cache à chaque contrôleur de stockage.

Utilisez les recommandations suivantes pour répartir uniformément les charges de travail MEDITECH sur chaque contrôleur de stockage :

- Si vous connaissez les IOPS de chaque hôte MEDITECH, vous pouvez étendre l'étendue MEDITECH et les charges de travail 6.x de manière homogène entre tous les contrôleurs de stockage. Ils confirment que chaque contrôleur gère un nombre similaire d'IOPS depuis les hôtes MEDITECH.
- Si vous ne connaissez pas les IOPS de chaque hôte MEDITECH, vous pouvez encore étendre l'étendue MEDITECH et les charges de travail 6.x de façon homogène entre tous les contrôleurs de stockage. Cette tâche doit être effectuée en confirmant que la capacité des agrégats pour les hôtes MEDITECH est répartie de façon homogène entre tous les contrôleurs de stockage. Le nombre de disques est donc le même pour tous les agrégats de données dédiés aux hôtes MEDITECH.
- Utilisez des types de disques similaires et des groupes RAID identiques pour créer les agrégats de stockage des deux contrôleurs en vue de répartir les charges de travail de manière homogène. Avant de créer l'agrégat de stockage, contactez un intégrateur NetApp Certified.

> Selon MEDITECH, deux hôtes du système MEDITECH génèrent plus d'IOPS que le reste des hôtes. Les LUN de ces deux hôtes doivent être placées sur des contrôleurs de stockage distincts. Vous devez identifier ces deux hôtes avec l'aide de l'équipe MEDITECH avant de déployer votre système.

Placement du stockage

Stockage de base de données pour les hôtes MEDITECH

Le stockage de base de données d'un hôte MEDITECH est présenté sous forme d'un bloc (c'est-à-dire une LUN) avec le système NetApp FAS et AFF. Le LUN est généralement monté sur le système d'exploitation Windows en tant que lecteur E.

Autres stockages

Le système d'exploitation hôte MEDITECH et l'application de base de données génèrent généralement une quantité considérable d'IOPS pour le stockage. Le provisionnement du stockage pour les machines virtuelles hôtes MEDITECH et leurs fichiers VMDK, si nécessaire, est considéré comme indépendant du stockage requis pour répondre aux seuils de performances MEDITECH.

Le stockage provisionné pour les autres serveurs MEDITECH ne doit pas être placé sur l'agrégat dédié des LUN que les hôtes MEDITECH utilisent. Placer le stockage des autres serveurs MEDITECH sur un agrégat distinct.

Configuration du contrôleur de stockage

Haute disponibilité

Pour limiter les conséquences de la défaillance du contrôleur et pour permettre des mises à niveau sans interruption du système de stockage, il est conseillé de configurer votre système de stockage avec des contrôleurs en mode haute disponibilité.

Dans le cas de la configuration de paires de contrôleurs haute disponibilité, les tiroirs disques doivent être connectés aux contrôleurs par plusieurs chemins. Cette connexion améliore la résilience du stockage en offrant une protection contre la défaillance d'un chemin unique, et améliore la cohérence des performances en cas de basculement du contrôleur.

Performances de stockage lors du basculement du contrôleur de stockage

Pour les systèmes de stockage configurés avec des contrôleurs dans une paire haute disponibilité, dans le éventualité peu probable d'une panne de contrôleur, le contrôleur partenaire prend le relais des charges de travail et des ressources de stockage du contrôleur défaillant. Il est important de contacter le client pour déterminer les exigences de performance à respecter en cas de défaillance du contrôleur et pour dimensionner le système en conséquence.

Basculement assisté par matériel

NetApp vous recommande d'activer la fonctionnalité de basculement assisté par matériel sur les deux contrôleurs de stockage.

Le basculement assisté par matériel est conçu pour réduire au maximum le temps de basculement du contrôleur de stockage. Il permet au module LAN distant ou au module processeur de service d'un contrôleur d'avertir son partenaire d'une défaillance de contrôleur plus rapidement qu'un déclencheur de délai d'impulsion peut, ce qui réduit le temps nécessaire au basculement. La fonctionnalité hardware-Assisted Takeover est activée par défaut pour les contrôleurs de stockage dans une configuration haute disponibilité.

Pour plus d'informations sur le basculement assisté par matériel, consultez le "Centre de documentation ONTAP 9".

Type de disque

Pour prendre en charge les exigences de faible latence de lecture des charges de travail MEDITECH, NetApp recommande d'utiliser un disque SSD haute performance pour les agrégats des systèmes AFF dédiés aux hôtes MEDITECH.

NetApp AFF

NetApp offre des baies AFF hautes performances pour gérer les charges de travail MEDITECH qui exigent un

débit élevé et des modèles d'accès aux données et une latence faible. Pour les charges de travail MEDITECH, les baies AFF offrent des avantages en termes de performance par rapport aux systèmes qui sont basés sur les HDD. L'association de la technologie Flash et de la gestion des données d'entreprise présente certains avantages dans trois domaines principaux : les performances, la disponibilité et l'efficacité du stockage.

Outils et services de support NetApp

NetApp propose un ensemble complet d'outils et de services de support. L'outil NetApp AutoSupport doit être activé et configuré sur les systèmes NetApp AFF/FAS pour signaler la défaillance matérielle ou les erreurs de configuration du système. Appeler le service d'alerte de support de NetApp pour résoudre rapidement tout problème. NetApp Active IQ est une application web qui utilise des informations de vos systèmes NetApp qu'AutoSupport lui envoie. Son objectif est de vous aider à améliorer votre disponibilité, efficacité et vis performances grâce à une vision proactive et prédictive.

Déploiement et configuration

Présentation

Vous trouverez dans ce document des conseils sur le stockage NetApp pour le déploiement de FlexPod les éléments suivants :

- Les environnements qui utilisent ONTAP
- Environnements utilisant des serveurs lames et en rack Cisco UCS

Ce document ne couvre pas :

- Déploiement détaillé de l'environnement de data Center FlexPod

  Pour plus d'informations, voir "Conception validée FlexPod Datacenter avec FC Cisco" (CVD).

- Présentation des environnements logiciels MEDITECH, des architectures de référence et des conseils sur les meilleures pratiques d'intégration.

  Pour plus d'informations, voir "Tr-4300i : Guide des meilleures pratiques des systèmes de stockage 100 % Flash et FAS pour les environnements MEDITECH" (Identifiant NetApp requis).

- Exigences quantitatives en termes de performances et conseils de dimensionnement.

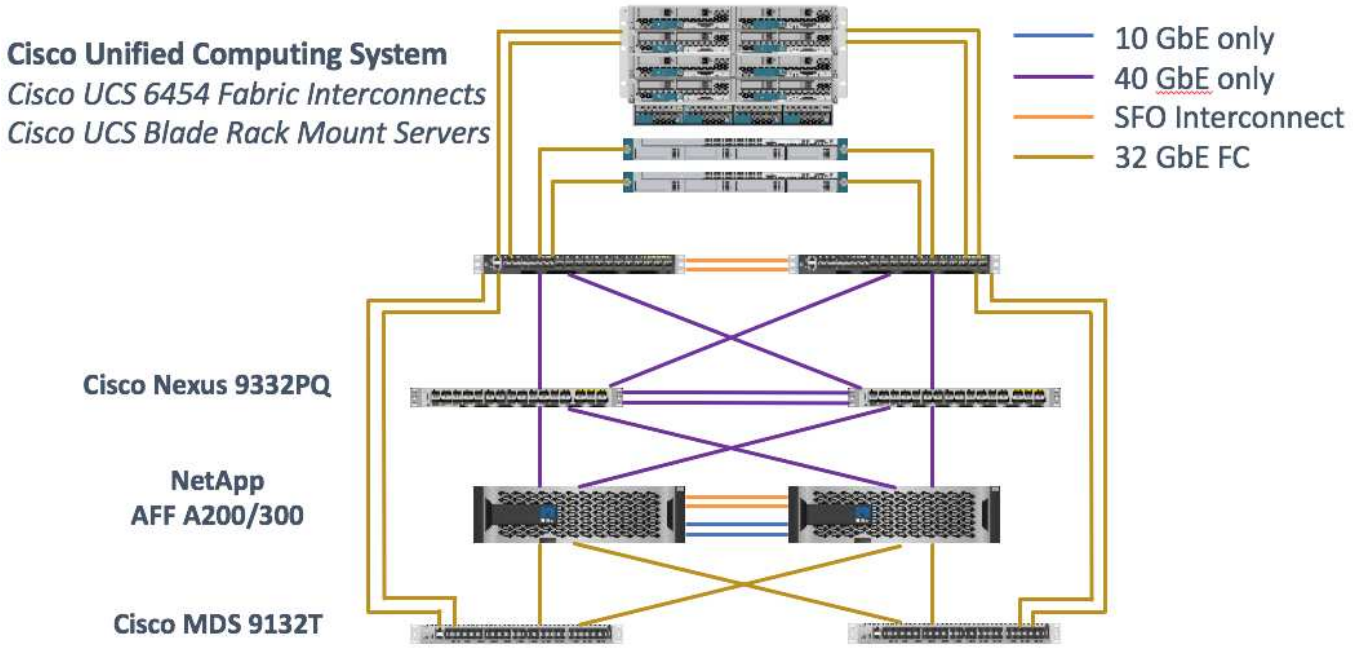
  Pour plus d'informations, voir "Tr-4190 : directives de dimensionnement NetApp pour les environnements MEDITECH".

- Utilisation des technologies NetApp SnapMirror pour répondre aux exigences de sauvegarde et de reprise d'activité.
- Conseils génériques sur le déploiement de stockage NetApp.

Cette section fournit un exemple de configuration avec les meilleures pratiques de déploiement d'infrastructure et répertorie les différents composants matériels et logiciels de l'infrastructure et les versions que vous pouvez utiliser.

Schéma de câblage

La figure suivante illustre le diagramme de topologie FC 32 Gb/40 GbE pour un déploiement MEDITECH.



Utilisez toujours le "Matrice d'interopérabilité (IMT)" pour vérifier que toutes les versions des logiciels et des firmwares sont prises en charge. Le tableau de la section "Modules ET composants MEDITECH" les composants matériels et logiciels de l'infrastructure utilisés pour les tests des solutions sont répertoriés dans le.

"Next : configuration de l'infrastructure de base."

Configuration de l'infrastructure de base

Connectivité réseau

Les connexions réseau suivantes doivent être en place avant de configurer l'infrastructure :

- L'agrégation de liens qui utilise des canaux de port et des canaux de port virtuels (VPC) est utilisée dans tout l'ensemble, ce qui permet d'obtenir une bande passante et une haute disponibilité plus élevées :
  - Le VPC est utilisé entre les commutateurs Cisco FI et Cisco Nexus.
  - Chaque serveur dispose de cartes réseau virtuelles (vNIC) qui offrent une connectivité redondante à la structure unifiée. Le basculement de carte réseau est utilisé entre les interfaces de redondance.
  - Chaque serveur dispose d'adaptateurs de bus hôte virtuels (vHBA) avec connectivité redondante à la structure unifiée.
- Le SYSTÈME Cisco UCS FI est configuré en mode hôte final comme recommandé, pour l'épinglage dynamique des vNIC sur les commutateurs de liaison ascendante.

Connectivité du stockage

Les connexions de stockage suivantes doivent être en place avant de configurer l'infrastructure :

- Groupes d'interfaces des ports de stockage (ifgroups, VPC)
- Lien 10 Gb vers le commutateur N9K-A
- Liaison 10 Gb pour le commutateur N9K-B.
- Gestion intrabande (liaison active-passive) :

    - Liaison 1 Go au commutateur de gestion N9K-A
    - Liaison 1 Go au commutateur de gestion N9K-B.
- Connectivité FC 32 Gb de bout en bout via des switchs Cisco MDS ; segmentation à un seul initiateur configurée
- Le démarrage SAN FC pour obtenir un calcul sans état ; les serveurs sont démarrés à partir de LUN dans le volume de démarrage hébergé sur le cluster de stockage AFF
- Toutes les charges de travail MEDITECH sont hébergées sur les LUN FC et réparties entre les nœuds du contrôleur de stockage

Logiciel hôte

Le logiciel suivant doit être installé :

- ESXi est installé sur les serveurs lames Cisco UCS
- VMware vCenter installé et configuré (avec tous les hôtes enregistrés dans vCenter)
- VSC a été installé et enregistré dans VMware vCenter
- Cluster NetApp configuré

"Suivant : configuration du serveur lame et des commutateurs Cisco UCS."

Configuration des serveurs lames et des switchs Cisco UCS

Le logiciel FlexPod pour MEDITECH est conçu avec une tolérance aux pannes à tous les niveaux. Le système ne présente aucun point de défaillance unique. Pour des performances optimales, Cisco recommande l'utilisation de serveurs lames de rechange à chaud.

Ce document présente des recommandations générales sur la configuration de base d'un environnement FlexPod pour le logiciel MEDITECH. Dans cette section, nous présentons des étapes générales incluant quelques exemples pour préparer l'élément de plateforme de calcul Cisco UCS de la configuration FlexPod. Vous devez préalablement bénéficier de ces conseils : la configuration FlexPod est mise en rack, alimentée et câblée conformément aux instructions du "FlexPod Datacenter avec stockage Fibre Channel via VMware vSphere 6.5 Update 1, baies NetApp AFF A-Series, et Cisco UCS Manager 3.2"CVD.

Configuration de commutateurs Cisco Nexus

La solution déploie une paire de commutateurs Ethernet Cisco Nexus 9300 Series tolérante aux pannes. Vous devez raccorder ces commutateurs comme décrit dans le "Schéma de câblage" section. La configuration Cisco Nexus assure que les flux de trafic Ethernet sont optimisés pour l'application MEDITECH.

1. Après avoir terminé la configuration initiale et la gestion des licences, exécutez les commandes suivantes pour définir les paramètres de configuration globale sur les deux commutateurs :

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. Créez les VLAN pour la solution sur chaque commutateur en utilisant le mode de configuration globale :

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. Créez l'interface de distribution NTP (Network Time Protocol), les canaux de port, les paramètres de canal de port et les descriptions de port pour le dépannage conformément à "FlexPod Datacenter avec stockage Fibre Channel via VMware vSphere 6.5 Update 1, baies NetApp AFF A-Series, et Cisco UCS Manager 3.2"CVD.

Configuration Cisco MDS 9132T

Les switchs FC Cisco MDS 9100 Series offrent une connectivité FC 32 Gb redondante entre les contrôleurs NetApp AFF A200 ou AFF A300 et la structure de calcul Cisco UCS. Vous devez brancher les câbles comme décrit dans le "Schéma de câblage" section.

1. À partir des consoles de chaque commutateur MDS, exécutez les commandes suivantes pour activer les fonctionnalités requises pour la solution :

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. Configurez les ports, les canaux de port et les descriptions individuels conformément à la section de configuration du commutateur Cisco MDS de FlexPod dans "Conception validée FlexPod Datacenter avec FC Cisco".

3. Pour créer les réseaux SAN virtuels (VSAN) nécessaires à la solution, effectuez les opérations suivantes en mode de configuration globale :
   a. Pour le commutateur Fabric-A MDS, exécutez les commandes suivantes :

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

   Les numéros de canal de port des deux dernières lignes de la commande ont été créés lorsque les ports, les canaux de port et les descriptions individuels ont été configurés à l'aide du document de référence.

   b. Pour le commutateur MDS Fabric-B, exécutez les commandes suivantes :

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

   Les numéros de canal de port des deux dernières lignes de la commande ont été créés lorsque les ports, les canaux de port et les descriptions individuels ont été configurés à l'aide du document de référence.

4. Pour chaque commutateur FC, créez des noms d'alias de périphérique qui rendent l'identification de chaque périphérique intuitive pour les opérations en cours en utilisant les détails du document de référence.
5. Enfin, créez les zones FC en utilisant les noms d'alias de périphérique créés à l'étape 4 pour chaque commutateur MDS comme suit :
   a. Pour le commutateur Fabric-A MDS, exécutez les commandes suivantes :

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. Pour le commutateur MDS Fabric-B, exécutez les commandes suivantes :

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Conseils de configuration du système Cisco UCS

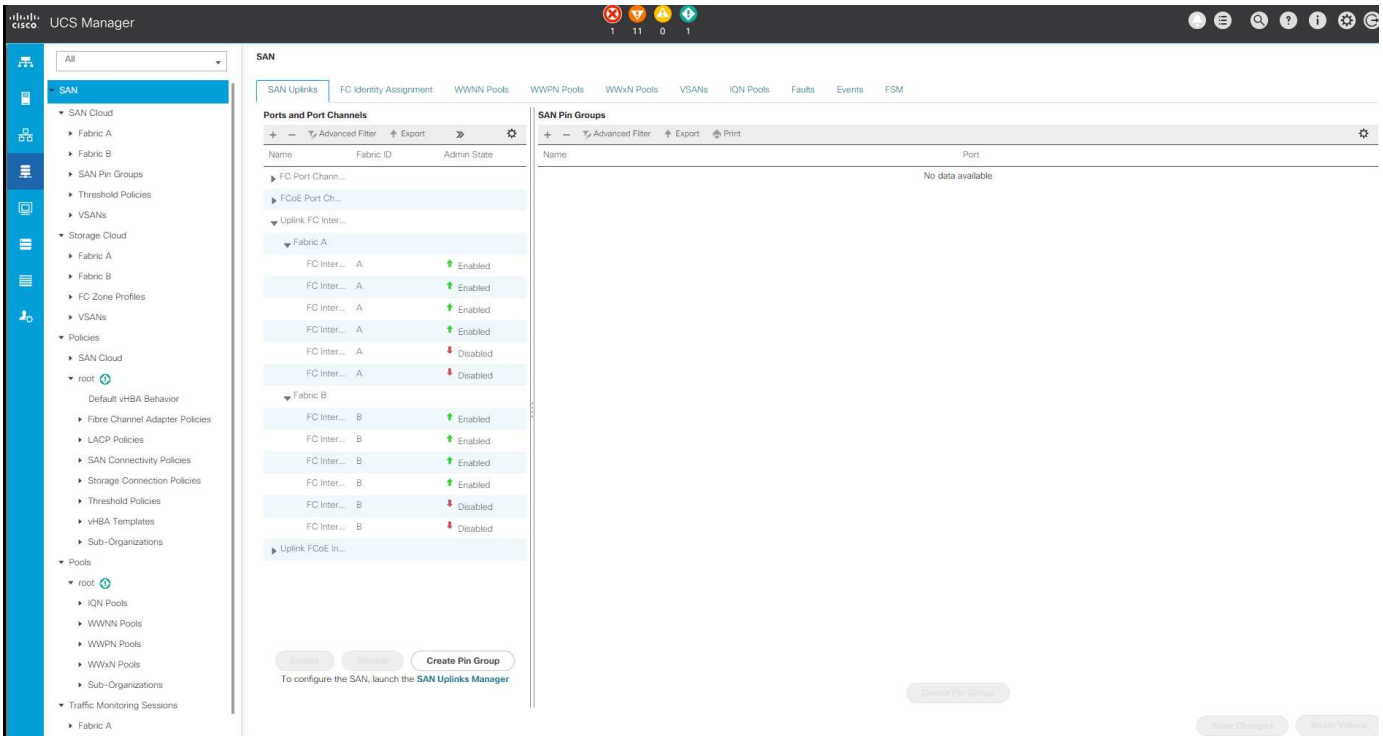
Grâce à Cisco UCS, vous pouvez compter sur les experts du réseau, du stockage et des ressources de calcul qui peuvent créer des règles et des modèles sur mesure de l'environnement en fonction de vos besoins. Une

fois créées, ces règles et modèles peuvent être combinés en profils de service qui assurent un déploiement cohérent, reproductible, fiable et rapide des serveurs lames et en rack Cisco.

Cisco UCS propose trois méthodes pour gérer un système Cisco UCS, appelé domaine :

- Interface graphique Cisco UCS Manager HTML5
- Interface de ligne de commandes Cisco UCS
- Cisco UCS Central pour les environnements multidomaines

La figure suivante présente un exemple d'écran du nœud SAN de Cisco UCS Manager.



Pour les déploiements de plus grande envergure, des domaines Cisco UCS indépendants peuvent être créés pour une meilleure tolérance aux pannes au niveau des composants fonctionnels MEDITECH majeurs.

Dans le cas de designs hautement tolérants aux pannes avec deux ou plusieurs data centers, Cisco UCS Central joue un rôle clé dans la définition des règles globales et des profils de service globaux pour la cohérence entre les hôtes dans toute l'entreprise.

Pour configurer la plateforme de calcul Cisco UCS, procédez comme suit. Effectuez ces procédures après l'installation des serveurs lames Cisco UCS B200 M5 dans le châssis lame Cisco UCS 5108 AC. Vous devez également répondre aux exigences de câblage décrites dans le "Schéma de câblage" section.

1. Mettez à niveau le firmware de Cisco UCS Manager vers la version 3.2(2f) ou ultérieure.
2. Configurez les fonctions de génération de rapports, les fonctionnalités d'appel à distance Cisco et les paramètres NTP pour le domaine.
3. Configurez les ports de serveur et de liaison montante de chaque interconnexion de structure.
4. Modifiez la stratégie de découverte du châssis.
5. Créer les pools d'adresses pour la gestion hors bande, les identifiants uniques universels (UUID), l'adresse MAC, les serveurs, le nom de nœud mondial (WWNN) et le nom de port mondial (WWPN).

6. Créez les canaux de port de liaison montante Ethernet et FC et les VSAN.
7. Créer des stratégies pour la connectivité SAN, le contrôle réseau, la qualification des pools de serveurs, le contrôle de l'alimentation, le BIOS serveur, et maintenance par défaut.
8. Créez des modèles vNIC et vHBA.
9. Créer des règles de démarrage vMedia et FC.
10. Créez des modèles de profil de service et des profils de service pour chaque élément de plateforme MEDITECH.
11. Associez les profils de service aux serveurs lames appropriés.

Pour connaître les étapes détaillées de configuration de chaque élément clé des profils de service Cisco UCS pour FlexPod, consultez le "FlexPod Datacenter avec stockage Fibre Channel via VMware vSphere 6.5 Update 1, baies NetApp AFF A-Series, et Cisco UCS Manager 3.2"Document CVD.

"Suivant : meilleures pratiques en matière de configuration VMware ESXi."

Meilleures pratiques de configuration ESXi

Pour la configuration côté hôte ESXi, configurez les hôtes VMware comme vous exécuteraient toute charge de travail de base de données d'entreprise :

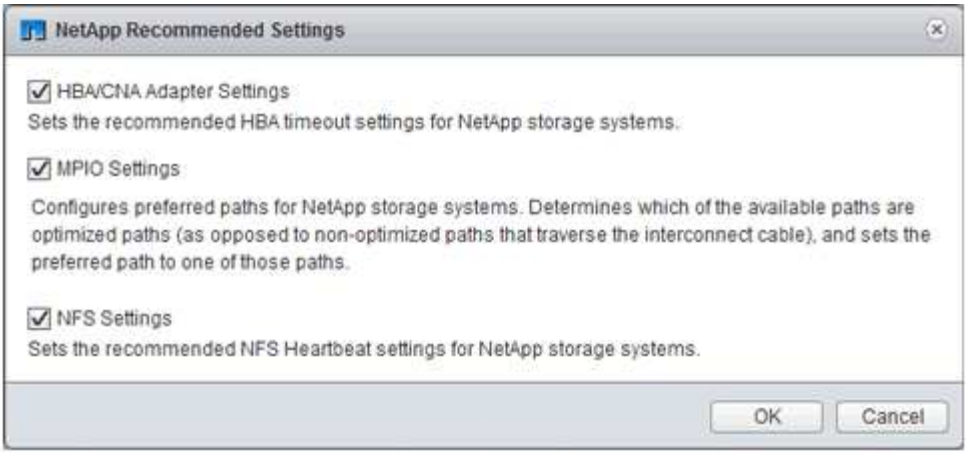
- VSC for VMware vSphere vérifie et définit les paramètres de chemins d'accès multiples de l'hôte ESXi ainsi que les paramètres de délai d'expiration de l'adaptateur HBA qui fonctionnent mieux avec les systèmes de stockage NetApp. Les valeurs des jeux de VSC sont basées sur des tests internes rigoureux menés par NetApp.
- Pour des performances de stockage optimales, envisagez l'utilisation de matériel de stockage prenant en charge VAAI (VMware vStorage APIs - Array Integration). Le plug-in NetApp pour VAAI est une bibliothèque logicielle qui intègre les bibliothèques de disques virtuels VMware installées sur l'hôte ESXi. Le package VMware VAAI permet de décharger certaines tâches des hôtes physiques vers la baie de stockage.

  Vous pouvez effectuer des tâches telles que le provisionnement fin et l'accélération matérielle au niveau de la baie afin de réduire la charge de travail sur les hôtes ESXi. La fonctionnalité de déchargement de copies et de réservation d'espace améliorent les performances des opérations VSC. Vous pouvez télécharger le pack d'installation du plug-in et obtenir les instructions d'installation du plug-in sur le site de support NetApp.

  La console VSC définit les délais d'expiration des hôtes ESXi, les paramètres de chemins d'accès multiples, et les paramètres d'expiration des HBA, ainsi que d'autres valeurs pour des performances optimales et un basculement réussi des contrôleurs de stockage NetApp. Voici la procédure à suivre :

  a. Sur la page d'accueil du client Web VMware vSphere, sélectionnez vCenter > hosts.
  b. Cliquez avec le bouton droit sur un hôte, puis sélectionnez actions > NetApp VSC > définir les valeurs recommandées.
  c. Dans la boîte de dialogue Paramètres recommandés par NetApp, sélectionnez les valeurs qui conviennent le mieux à votre système.

     Les valeurs standard recommandées sont définies par défaut.



a. Cliquez sur OK.

"Suivant : configuration NetApp."

Configuration NetApp

Les solutions de stockage NetApp déployées pour les environnements logiciels MEDITECH utilisent des contrôleurs de stockage et une configuration de paires haute disponibilité. Le stockage doit être présenté des deux contrôleurs aux serveurs de base de données MEDITECH via le protocole FC. La configuration présente le stockage des deux contrôleurs afin d'équilibrer uniformément la charge applicative pendant le fonctionnement normal.

Configuration ONTAP

Cette section décrit un exemple de procédures de déploiement et de provisionnement qui utilisent les commandes ONTAP appropriées. L'accent est mis sur le provisionnement du stockage pour implémenter l'infrastructure de stockage recommandée par NetApp, qui utilise une paire de contrôleurs haute disponibilité. L'un des principaux avantages de ONTAP est la possibilité d'évoluer horizontalement sans perturber les paires haute disponibilité existantes.

Licences ONTAP

Une fois que vous avez configuré les contrôleurs de stockage, appliquez les licences pour activer les fonctionnalités de ONTAP recommandées par NetApp. Les licences pour les charges de travail MEDITECH sont : FC, CIFS et NetApp Snapshot, SnapRestore, FlexClone et Et aux technologies SnapMirror.

Pour configurer les licences, ouvrez NetApp ONTAP System Manager, accédez à Configuration-Licenses, puis ajoutez les licences appropriées.

Vous pouvez également exécuter la commande suivante pour ajouter des licences à l'aide de l'interface de ligne de commande :

```
license add -license-code <code>
```

Configuration AutoSupport

L'outil NetApp AutoSupport envoie à NetApp des informations récapitulatives sur le support en HTTPS. Pour configurer AutoSupport, lancer les commandes ONTAP suivantes :

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

Configuration hardware-Assisted Takeover

Sur chaque nœud, activez le basculement assisté par matériel pour réduire le temps nécessaire au lancement d'un basculement dans l'éventualité peu probable d'une défaillance de contrôleur. Pour configurer le basculement assisté par matériel, procédez comme suit :

1. Exécutez la commande ONTAP suivante sur xxx.

   Définissez l'option d'adresse du partenaire sur l'adresse IP du port de gestion pour `prod1-01`.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. Exécutez la commande ONTAP suivante sur xxx :

   Définissez l'option d'adresse du partenaire sur l'adresse IP du port de gestion pour `cluster1-02`.

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. Exécutez la commande ONTAP suivante pour activer le basculement assisté par matériel sur les deux `prod1-01` et le `prod1-02` Paire de contrôleurs HAUTE DISPONIBILITÉ.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"Next : configuration de l'agrégat."

Configuration d'agrégat

NetApp RAID DP

NetApp recommande la technologie NetApp RAID DP en tant que type RAID pour tous les agrégats d'un système NetApp FAS ou AFF, y compris les agrégats NetApp Flash Pool réguliers. La documentation DE MEDITECH peut préciser l'utilisation du RAID 10, mais MEDITECH a approuvé l'utilisation de RAID DP.

Taille et nombre de groupes RAID

La taille du groupe RAID par défaut est 16. Cette taille peut être ou non optimale pour les agrégats pour les hôtes MEDITECH de votre site. Pour connaître le nombre de disques que NetApp recommande d'utiliser au sein d'un groupe RAID, reportez-vous à la section "NetApp TR-3838 : Guide de configuration du sous-système de stockage".

La taille du groupe RAID est importante pour l'extension du stockage car NetApp recommande d'ajouter des disques à un agrégat avec un ou plusieurs groupes de disques identiques à la taille du groupe RAID. Le nombre de groupes RAID dépend du nombre de disques de données et de la taille du groupe RAID. Pour déterminer le nombre de disques de données nécessaires, utilisez l'outil de dimensionnement NetApp System Performance Modeler (SPM). Une fois le nombre de disques de données déterminé, ajustez la taille du groupe RAID afin de réduire le nombre de disques de parité dans la plage recommandée pour la taille de groupe RAID par type de disque.

Pour en savoir plus sur l'utilisation de l'outil de dimensionnement SPM pour les environnements MEDITECH, consultez le site "NetApp TR-4190 : Guide de dimensionnement des environnements MEDITECH".

Considérations relatives à l'extension du stockage

Lorsque vous développez des agrégats avec plus de disques, ajoutez les disques des groupes qui sont égaux à la taille du groupe RAID de l'agrégat. La mise en œuvre de cette approche permet d'assurer la cohérence des performances dans l'ensemble de l'agrégat.

Par exemple, pour ajouter du stockage à un agrégat créé avec une taille de groupe RAID de 20, le nombre de disques que NetApp recommande d'ajouter est un ou plusieurs groupes de 20 disques. Vous devez donc ajouter 20, 40, 60, etc., des disques.

Une fois les agrégats créés, vous pouvez améliorer les performances en exécutant des tâches de réaffectation sur les volumes ou l'agrégat concernés, afin de répartir les bandes de données existantes sur les nouveaux disques. Cette action est utile, notamment si l'agrégat existant était presque plein.

> Nous vous conseillons de planifier la réaffectation du planning pendant les heures hors production, car cette tâche consomme énormément de ressources de processeur et de disques.

Pour plus d'informations sur l'utilisation de la fonctionnalité reallocation après une extension d'agrégat, reportez-vous à la section "NetApp TR-3929 : Guide des meilleures pratiques de réaffectation".

Copies Snapshot au niveau de l'agrégat

Définissez la réserve NetApp Snapshot de niveau de l'agrégat sur zéro et désactivez la planification Snapshot de l'agrégat par défaut. Supprimez, si possible, des copies Snapshot au niveau des agrégats préexistantes.

"Suivant : configuration de l'ordinateur virtuel de stockage."

Configuration des serveurs virtuels de stockage

Cette section se rapporte au déploiement sur ONTAP 8.3 et versions ultérieures.

Un SVM (Storage Virtual machine) est également appelé vServer dans l'API ONTAP et dans l'interface de ligne de commande de ONTAP.

SVM pour les LUN hôtes MEDITECH

Il est conseillé de créer un SVM dédié par cluster de stockage ONTAP pour posséder et gérer les agrégats contenant les LUN des hôtes MEDITECH.

Paramètre de codage du langage SVM

NetApp vous recommande de définir le codage du langage pour tous les SVM. Si aucun paramètre de codage de langue n'est spécifié au moment de la création du SVM, le paramètre de codage de langue par défaut est utilisé. Le paramètre de codage de langue par défaut est .UTF-8 pour ONTAP. Une fois le codage de langue défini, vous ne pouvez pas modifier par la suite la langue d'un SVM avec Infinite Volume.

Les volumes associés à la SVM héritent du paramètre de codage du langage SVM, sauf si vous spécifiez explicitement un autre paramètre lors de la création des volumes. Pour permettre certaines opérations de fonctionner, vous devez utiliser le paramètre de codage de langue de manière cohérente dans tous les volumes de votre site. Par exemple, SnapMirror nécessite que les SVM source et destination aient le même paramètre de codage du langage.

"Suivant : configuration de volume."

Configuration de volume

Provisionnement de volume

Les volumes MEDITECH dédiés aux hôtes MEDITECH peuvent être avec un provisionnement fin ou non fin.

Copies Snapshot par défaut au niveau des volumes

Les copies Snapshot sont créées dans le cadre du workflow de sauvegarde. Chaque copie Snapshot peut être utilisée pour accéder aux données stockées dans les LUN MEDITECH à différents moments. La solution de sauvegarde approuvée par MEDITECH crée des volumes FlexClone à provisionnement fin et basés sur ces copies Snapshot afin de fournir des copies instantanées des LUN MEDITECH. L'environnement MEDITECH est intégré avec une solution logicielle de sauvegarde et Par conséquent, NetApp recommande de désactiver le planning de copies Snapshot par défaut sur chaque volume NetApp FlexVol qui constitue les LUN de base de données de production MEDITECH.

Important : les volumes FlexClone partagent l'espace du volume de données parent. Il est donc essentiel que le volume dispose d'un espace suffisant pour les LUN de données MEDITECH et les volumes FlexClone créés par les serveurs de sauvegarde. Les volumes FlexClone n'occupent pas plus d'espace que les volumes de données. S'il y a des suppressions considérables sur les LUN MEDITECH dans un court moment, les volumes de clonage peuvent croître.

Nombre de volumes par agrégat

Pour un système NetApp FAS qui utilise la mise en cache Flash Pool ou NetApp Flash cache, NetApp recommande de provisionner au moins trois volumes par agrégat dédiés au stockage du programme MEDITECH, du dictionnaire et des fichiers de données.

Pour les systèmes AFF, NetApp recommande de dédier quatre volumes ou plus par agrégat pour stocker le programme MEDITECH, le dictionnaire et les fichiers de données.

Planification des réaffectations au niveau des volumes

La disposition des données du stockage s'avère moins optimale au fil du temps, en particulier lorsqu'elle est utilisée par des charges de travail exigeantes en écriture, telles que les plateformes MEDITECH, 6.x et C/S 5.x. Au fil du temps, cette situation peut augmenter la latence des lectures séquentielles, ce qui allonge le délai de la sauvegarde. Une disposition ou une fragmentation des données incorrectes peuvent également affecter la latence d'écriture. Cette fonctionnalité optimise la disposition des données sur disque en vue d'améliorer les latences en écriture et l'accès en lecture séquentielle. L'amélioration de la disposition du stockage permet d'effectuer la sauvegarde dans la fenêtre de temps allouée de 8 heures.

Et des meilleures pratiques
Au moins, NetApp vous recommande de mettre en œuvre une planification hebdomadaire de réaffectation des volumes pour exécuter les opérations de réaffectation pendant les temps d'indisponibilité de la maintenance alloués ou durant les heures creuses sur le site de production. NetApp vous recommande fortement d'exécuter la tâche de réaffectation sur un volume à la fois par contrôleur.

Pour plus d'informations sur la définition d'une planification appropriée de réaffectation de volumes pour le stockage de votre base de données de production, reportez-vous à la section 3.12 du "NetApp TR-3929 : Guide des meilleures pratiques de réaffectation". Cette section vous indique également comment créer un programme de réaffectation hebdomadaire pour un site occupé.

"Suivant : configuration de LUN."

Configuration du LUN

Le nombre d'hôtes MEDITECH dans votre environnement détermine le nombre de LUN qui sont créées avec le système NetApp FAS et AFF. La proposition de configuration matérielle spécifie la taille de chaque LUN.

Provisionnement de LUN

Les LUN MEDITECH dédiées aux hôtes MEDITECH peuvent être provisionnées très lourd ou léger.

Type de système d'exploitation LUN

Pour aligner correctement les LUN qui sont créées, vous devez définir correctement le type de système d'exploitation pour les LUN. Un mauvais alignement des LUN entraîne une surcharge d'opérations d'écriture inutile et l'erreur d'alignement des LUN est coûteuse.

Le serveur hôte MEDITECH s'exécute en général dans l'environnement Windows Server virtualisé et utilise l'hyperviseur VMware vSphere. Le serveur hôte peut également être exécuté dans l'environnement Windows Server sur un serveur bare-Metal. Pour déterminer la valeur correcte du type de système d'exploitation à définir, reportez-vous à la section « LUN Create » du "Commandes clustered Data ONTAP 8.3 : référence manuelle des pages".

Taille de la LUN

Pour déterminer la taille des LUN pour chaque hôte MEDITECH, consultez le document proposition de configuration matérielle (nouveau déploiement) et le document tâche d'évaluation du matériel (déploiement existant) du MEDITECH.

Présentation de LUN

MEDITECH nécessite que le stockage des fichiers de programme, de dictionnaire et de données soit présenté aux hôtes MEDITECH sous forme de LUN à l'aide du protocole FC. Dans l'environnement virtuel VMware, les LUN sont présentées aux serveurs VMware ESXi qui hébergent les hôtes MEDITECH. Ensuite, chaque LUN présentée au serveur VMware ESXi est mappée à chaque machine virtuelle hôte MEDITECH en utilisant RDM en mode de compatibilité physique.

Vous devez présenter les LUN aux hôtes MEDITCH en utilisant les conventions de dénomination des LUN appropriées. Par exemple, pour faciliter l'administration, vous devez présenter la LUN `MTFS01E` À l'hôte MEDITECH `mt-host-01`.

Pour consulter la proposition de configuration matérielle MEDITECH, contactez le programme d'installation du système de sauvegarde et MEDITECH afin de définir une convention de nommage des LUN utilisées par les hôtes MEDITECH.

Voici un exemple de nom de LUN MEDITECH `MTFS05E`, dans laquelle:

- `MTFS` Indique le serveur de fichiers MEDITECH (pour l'hôte MEDITECH).
- `05` indique le numéro d'hôte 5.
- `E` Indique le lecteur Windows E.

"Suivant : configuration du groupe initiateur."

Configuration du groupe initiateur

Lorsque vous utilisez FC en tant que protocole de réseau de données, vous créez deux groupes initiateurs sur chaque contrôleur de stockage. Le premier groupe initiateur contient les WWPN des cartes d'interface hôte FC sur les serveurs VMware ESXi qui hébergent les VM hôte MEDITECH (igroup pour MEDITECH).

Vous devez définir le type de système d'exploitation MEDITECH igroup en fonction de la configuration de l'environnement. Par exemple :

- Utilisez le type de système d'exploitation igroup `Windows` Pour les applications installées sur du matériel serveur bare-Metal dans un environnement Windows Server.
- Utilisez le type de système d'exploitation igroup `VMware` Destinée aux applications virtualisées à l'aide de l'hyperviseur VMware vSphere.

> Il se peut que le type de système d'exploitation d'un groupe initiateur soit différent du type de système d'exploitation d'une LUN. Par exemple, pour les hôtes MEDITECH virtualisés, vous devez définir le type de système d'exploitation du groupe initiateur sur `VMware`. Pour les LUN utilisées par les hôtes MEDITECH virtualisés, il est recommandé de définir le type de système d'exploitation sur `Windows 2008 or later`. Utilisez ce paramètre car le système d'exploitation hôte MEDITECH est Windows Server 2008 R2 64 bits Enterprise Edition.

Pour déterminer la valeur correcte pour le type de système d'exploitation, reportez-vous aux sections "LUN igroup Create" et "LUN Create" dans le "Commandes clustered Data ONTAP 8.2 : référence manuelle des pages".

"Suivant : mappages de LUN."

Mappages de LUN

Les mappages de LUN pour les hôtes MEDITECH sont établis lors de la création des LUN.

Modules ET composants MEDITECH

L'application MEDITECH couvre plusieurs modules et composants. Le tableau suivant répertorie les fonctions couvertes par ces modules. Pour plus d'informations sur la configuration et le déploiement de ces modules, consultez la documentation MEDITECH.

Fonction	Type
Connectivité	• Serveur Web • Serveur d'applications en direct (WI – intégration Web) • Test du serveur d'applications (WI) • Serveur d'authentification SAML (WI) • Serveur proxy SAML (WI) • Serveur de base de données
Infrastructures	• Serveur de fichiers • Client de travail en arrière-plan • Serveur de connexion • Serveur de transactions
Numérisation et archivage	• Serveur d'images
Référentiel de données	• Serveur SQL
Analyses commerciales et cliniques	• Serveur d'intelligence dynamique (BCA) • Serveur d'intelligence de test (BCA) • Serveur de base de données (BCA)
Soins à domicile	• Solution pour sites distants • Connectivité • Infrastructures • Impression • Périphériques de terrain • Numérisation • Exigences relatives au site hébergé • Configuration du pare-feu

Fonction	Type
Assistance	• Client de travail en arrière-plan (licences d'accès client)
Terminaux d'utilisateurs	• Tablettes • Périphériques fixes
Impression	• Serveur d'impression en réseau direct (requis ; peut déjà exister) • Test du serveur d'impression réseau (requis ; peut déjà exister)
Exigences tierces	• First Databank (FDB) MedKnowledge Framework version 4.3

Remerciements

Les personnes suivantes ont contribué à la création de ce guide.

- Brandon Agee, Ingénieur marketing et technique, NetApp
- Atul Bhalodia, Ingénieur marketing et technique, NetApp
- Ketan Mota, responsable produits senior, NetApp
- John Duignan, architecte de solutions – Santé, NetApp
- Jon Ebmeier, Cisco
- Mike Brennan, Cisco

Où trouver des informations complémentaires

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

Zone de conception FlexPod

- "Zone de conception FlexPod"
- "FlexPod Data Center avec stockage FC (commutateurs MDS) et NetApp AFF, vSphere 6.5U1 et Cisco UCS Manager"

Rapports techniques NetApp

- "Tr-3929 : Guide des meilleures pratiques de réaffectation"
- "Tr-3987 : plug-in Snap Creator Framework pour InterSystems caché"
- "Tr-4300i : Guide des meilleures pratiques des systèmes de stockage 100 % Flash et FAS pour les environnements MEDITECH"
- "Tr-4017 : meilleures pratiques relatives à SAN FC"

- "Tr-3446 : Guide des meilleures pratiques et présentation du mode asynchrone de SnapMirror"

Documentation ONTAP

- "Documentation produit NetApp"
- "Virtual Storage Console (VSC) pour la documentation vSphere"
- "Centre de documentation ONTAP 9":
  - "Guide FC Express pour ESXi"
- "Documentation All ONTAP 9.3":
  - "Guide de configuration logicielle"
  - "Guide d'alimentation des disques et des agrégats"
  - "Guide d'administration DU SAN"
  - "Guide de configuration SAN"
  - "Guide de configuration FC pour Windows Express"
  - "Guide d'installation de la solution AFF optimisée pour SAN FC"
  - "Guide de configuration haute disponibilité"
  - "Guide de gestion du stockage logique"
  - "Guide d'alimentation de gestion des performances"
  - "Guide d'alimentation de la configuration SMB/CIFS"
  - "Référence SMB/CIFS"
  - "Guide d'alimentation de la protection des données"
  - "Guide de protection, de sauvegarde sur bandes et de restauration des données"
  - "Guide d'alimentation du cryptage NetApp"
  - "Guide de gestion de réseaux"
  - "Commandes : Manuel de référence des pages pour ONTAP 9.3"

Guides Cisco Nexus, MDS, Cisco UCS et Cisco UCS Manager

- "Présentation des serveurs Cisco UCS"
- "Présentation des serveurs lames Cisco UCS"
- "Fiche technique Cisco UCS B200 M5"
- "Présentation de Cisco UCS Manager"
- "Offre groupée d'infrastructure Cisco UCS Manager 3.2(3a)" (Autorisation Cisco.com requise)
- "Commutateurs de plateforme Cisco Nexus 9300"
- "Commutateur Cisco MDS 9132T FC"

FlexPod pour l'imagerie médicale

Tr-4865 : FlexPod pour l'imagerie médicale

Jaya Kishore Esanakula et Atul Bhalodia, NetApp

L’imagerie médicale représente 70 % de toutes les données générées par les organismes de santé. Les modalités numériques continuent à évoluer et de nouvelles modalités émergent. Il est donc de plus en plus important de données. Par exemple, la transition d’une pathologie analogique à une pathologie numérique augmentera considérablement la taille des images à un rythme qui mettra en place toutes les stratégies de gestion des données actuellement en place.

Le COVID-19 a clairement redéfini la transformation digitale, selon une récente "rapport", Le COVID-19 a accéléré le commerce digital de 5 ans. L’innovation technologique tirée par les dépanneurs change radicalement la façon dont nous nous occupons de notre quotidien. Ce changement de technologie va réviser de nombreux aspects essentiels de notre vie, y compris les soins de santé.

Les soins de santé devraient subir un changement majeur dans les années à venir. La COVID accélère l’innovation dans le domaine de la santé qui propulsera le secteur d’au moins plusieurs années. Au cœur de ce changement se trouve la nécessité de rendre les soins de santé plus flexibles dans la gestion des pandémies en étant plus abordables, disponibles et accessibles, sans compromettre la fiabilité.

Au cœur de ce changement dans le domaine de la santé se trouve une plateforme bien conçue. L’un des indicateurs clés permettant de mesurer la plate-forme est la facilité avec laquelle les changements de plate-forme peuvent être mis en œuvre. La rapidité est la nouvelle évolutivité et la protection des données ne peut pas être compromise. Certaines des données les plus critiques au monde sont créées et utilisées par les systèmes cliniques qui prennent en charge les cliniciens. NetApp a mis à disposition les données stratégiques pour les soins aux patients là où les médecins en ont besoin, sur site, dans le cloud ou dans un environnement hybride. Les environnements multicloud hybrides sont la pointe de l’architecture IT.

Le domaine de la santé tel que nous le savons, il s’agit en effet de fournisseurs (médecins, infirmières, radiologues, techniciens en appareils médicaux, etc.) et de patients. Alors que nous rapprochons de la problématique des patients et des fournisseurs, il est donc plus important que la plateforme sous-jacente soit disponible lorsque les fournisseurs et les patients en ont besoin. La plateforme doit être à la fois efficace et économique à long terme. Dans leurs efforts pour réduire encore davantage les coûts des soins aux patients, "Organismes de soins responsables" (ACOS) serait doté d’une plate-forme efficace.

En matière de systèmes d’information sur la santé utilisés par les organismes de santé, la question de la construction par rapport à l’achat a tendance à avoir une seule réponse : l’achat. Cela peut être pour de nombreuses raisons subjectives. Les décisions d’achat prises au fil des ans peuvent créer des systèmes d’information hétérogènes. Chaque système présente un ensemble spécifique de besoins pour la plateforme sur laquelle il est déployé. Le problème le plus significatif concerne l’ensemble vaste et diversifié de protocoles de stockage et de niveaux de performances requis par les systèmes d’information. La standardisation de la plateforme et l’efficacité opérationnelle optimale constituent donc un défi considérable. Les établissements de santé ne peuvent pas se concentrer sur des problèmes stratégiques, car leur attention est répartie entre des besoins opérationnels triviaux comme le vaste ensemble de plateformes qui requièrent un ensemble diversifié de compétences et, par conséquent, la conservation des PME.

Les défis peuvent être classés dans les catégories suivantes :

- Besoins de stockage hétérogène
- Silos départementaux
- La complexité opérationnelle
- Connectivité cloud
- Cybersécurité
- L’intelligence artificielle et le deep learning

Avec FlexPod, vous disposez d'une plateforme unique qui prend en charge les protocoles FC, FCoE, iSCSI, NFS/pNFS, SMB/CIFS, etc., à partir d'une plateforme unique. Les personnes, les processus et la technologie sont partie de l'ADN de FlexPod conçu et développé. La qualité de service adaptative FlexPod contribue à éliminer les silos organisationnels en prenant en charge plusieurs systèmes cliniques stratégiques sur la même plateforme FlexPod sous-jacente. FlexPod est certifié FedRAMP et FIPS 140-2. Par ailleurs, les établissements de santé sont confrontés à des opportunités telles que l'intelligence artificielle et le deep learning. FlexPod et NetApp répondent à ces problématiques et rendent les données disponibles là où elles sont nécessaires sur site ou dans un environnement multicloud hybride via une plateforme standardisée. Pour en savoir plus et connaître les témoignages clients d'une série, consultez "FlexPod Santé".

Les systèmes PACS et les informations d'imagerie médicale classiques sont dotés de l'ensemble des fonctionnalités suivantes :

- Réception et inscription
- Planification
- Imagerie
- Transcription
- Gestion
- Échange de données
- Archivage d'images
- Visualisation d'images pour la capture et la lecture d'images pour les techniciens et la visualisation d'images pour les cliniciens

En ce qui concerne l'imagerie, le secteur de la santé tente de relever les défis cliniques suivants :

- Adoption plus large de "le traitement du langage naturel" (NLP) assistants de techniciens et de médecins pour la lecture d'images. Le service de radiologie peut bénéficier de la reconnaissance vocale pour transcrire des rapports. Le profil NLP peut être utilisé pour identifier et anonymiser le dossier d'un patient, en particulier les balises DICOM intégrées à l'image DICOM. Les capacités NLP nécessitent des plates-formes hautes performances avec des temps de réponse à faible latence pour le traitement d'images. La qualité de service de FlexPod fournit non seulement une performance et des performances, mais elle fournit également des prévisions de capacité mature pour soutenir la croissance future.
- Une adoption plus large des voies et protocoles cliniques normalisés par les ACO et les organismes de santé communautaire. Historiquement, les voies cliniques ont été utilisées comme un ensemble statique de lignes directrices plutôt qu'un workflow intégré qui guide les décisions cliniques. Grâce aux progrès réalisés en matière de NLP et de traitement d'images, les balises DICOM dans les images peuvent être intégrées dans les voies cliniques, car elles permettent de prendre des décisions cliniques. C'est pourquoi ces processus nécessitent des performances élevées, une faible latence et un débit élevé en provenance des systèmes de stockage et de la plateforme d'infrastructure sous-jacente.
- Les modèles DE ML qui s'appuient sur des réseaux neuronaux convolutifs permettent d'automatiser en temps réel les capacités de traitement d'images et nécessitent donc une infrastructure compatible avec les GPU. FlexPod propose des composants de calcul de processeur et de processeur graphique intégrés au même système, et les processeurs et GPU peuvent évoluer indépendamment les uns des autres.
- Si les balises DICOM sont utilisées comme des faits dans les conseils cliniques sur les meilleures pratiques, le système doit effectuer davantage de lectures d'artefacts DICOM avec une faible latence et un débit élevé.
- Lors de l'évaluation des images, la collaboration en temps réel entre radiologues au sein de l'entreprise a besoin d'un traitement graphique haute performance sur leurs périphériques de calcul. NetApp propose des solutions VDI leaders spécialement conçues et éprouvées pour des utilisations graphiques haut de gamme. Vous trouverez plus d'informations "ici".

- La gestion des images et des médias au sein des organisations de santé ACO peut utiliser une plate-forme unique, quel que soit le système d'enregistrement de l'image, en utilisant des protocoles tels que l'imagerie numérique et les communications en médecine ("DICOM") Et accès Web aux objets DICOM persistants ("WAD")
- Échange d'informations de santé ("HIE") comprend les images incorporées dans les messages.
- Les modalités mobiles, telles que les dispositifs de numérisation sans fil portables (par exemple, les échographes portables de poche connectés à un téléphone), nécessitent une infrastructure réseau robuste avec sécurité, fiabilité et latence de niveau DoD à la périphérie, au cœur et dans le Cloud. "Une Data Fabric NetApp" cette possibilité pour les entreprises est évolutive.
- Les nouvelles modalités ont des besoins de stockage exponentiels, par exemple. Par exemple, les tomographies ou les IRM nécessitent quelques centaines de Mo par modalité. Cependant, la taille des images de pathologie digitale (y compris l'imagerie plein diaporama) peut être de quelques Go. FlexPod est conçu avec "performances, fiabilité et évolutivité sont des caractéristiques fondamentales".

Une plateforme de système d'imagerie médicale bien conçue est au cœur de l'innovation. L'architecture FlexPod offre des fonctionnalités flexibles de calcul et de stockage, avec une efficacité du stockage inégalée.

Avantages globaux de la solution

En exécutant un environnement applicatif d'imagerie sur une base architecturale FlexPod, votre établissement de santé peut améliorer la productivité du personnel et diminuer les dépenses d'investissement et d'exploitation. FlexPod propose une solution convergée, prévalidée et rigoureusement testée, conçue et conçue pour fournir des performances prévisibles à faible latence et une haute disponibilité. Cette approche permet d'obtenir des niveaux de confort élevés et, au final, des temps de réponse optimaux pour les utilisateurs du système d'imagerie médicale.

Différents composants du système d'imagerie peuvent nécessiter le stockage des données dans les systèmes de fichiers SMB/CIFS, NFS, Ext4 ou NTFS. Ce critère signifie que l'infrastructure doit assurer l'accès aux données via les protocoles NFS, SMB/CIFS et SAN. Un seul système de stockage NetApp peut prendre en charge les protocoles NFS, SMB/CIFS et SAN, ce qui évite d'avoir recours à la pratique héritée de systèmes de stockage spécifiques au protocole.

L'infrastructure FlexPod est une plateforme modulaire, convergée, virtualisée, évolutive (scale-out et scale-up) et économique. Avec la plateforme FlexPod, vous pouvez faire évoluer indépendamment les ressources de calcul, de réseau et de stockage pour accélérer le déploiement de vos applications. En outre, l'architecture modulaire garantit la continuité de l'activité, même lors des activités de mise à niveau et d'évolutivité horizontale du système.

FlexPod offre plusieurs avantages spécifiques au secteur de l'imagerie médicale :

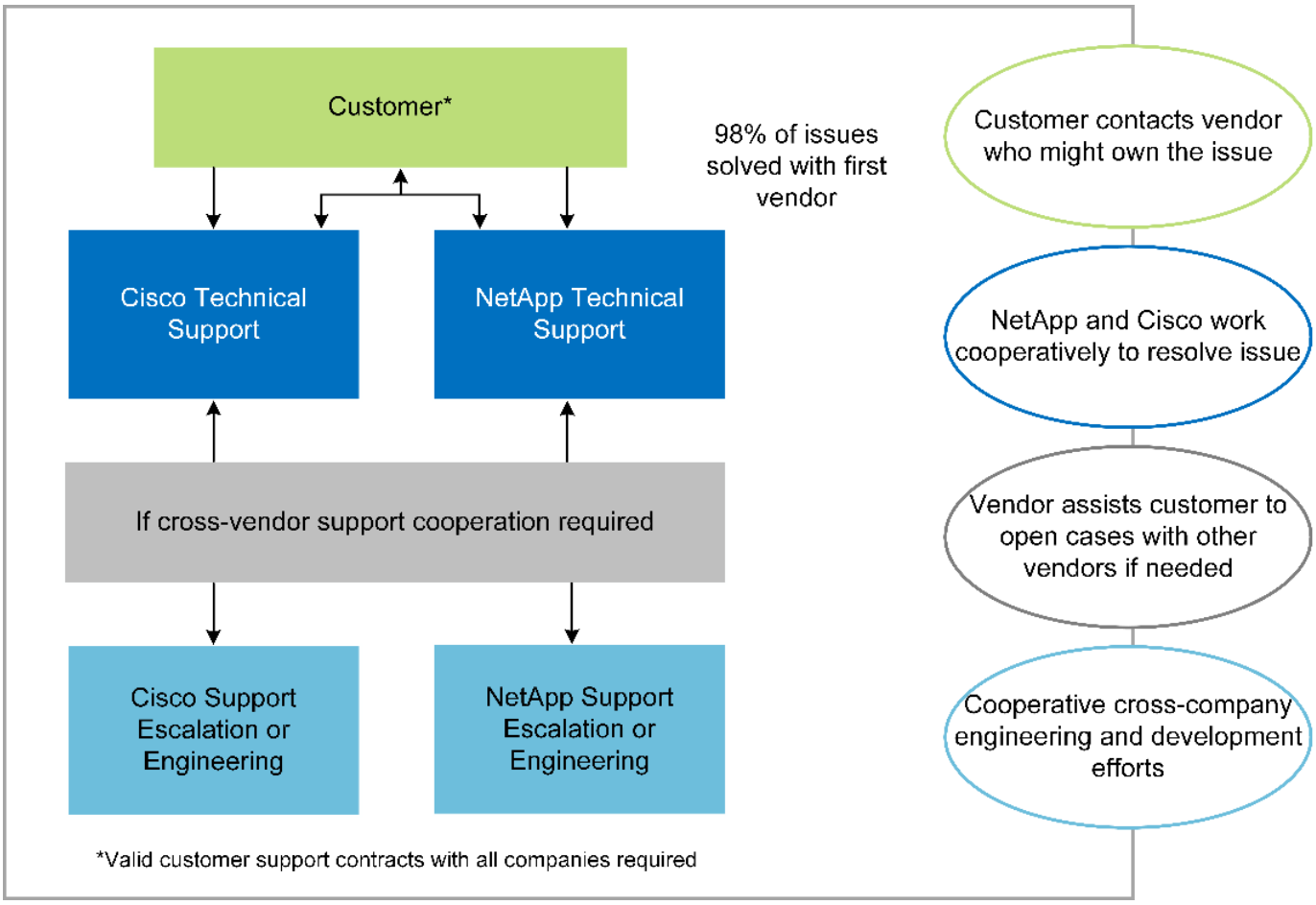
- **La performance du système à faible latence.** le temps du radiologue est une ressource à forte valeur ajoutée, et l'utilisation efficace du temps du radiologue est primordiale. L'attente d'images ou de vidéos à charger peut contribuer à l'épuisement professionnel des médecins et affecter l'efficacité du personnel soignant ainsi que la sécurité des patients.
- **Architecture modulaire.** les composants FlexPod sont connectés via un serveur en cluster, une structure de gestion du stockage et des outils de gestion cohérents. Avec l'augmentation du nombre d'études réalisées chaque année par les installations d'imagerie, l'infrastructure sous-jacente doit évoluer en conséquence. FlexPod permet de faire évoluer indépendamment les ressources de calcul, de stockage et de réseau.
- **Déploiement plus rapide de l'infrastructure.** que ce soit dans un centre de données existant ou un emplacement distant, la conception intégrée et testée de FlexPod Datacenter avec imagerie médicale vous permet de mettre la nouvelle infrastructure en service plus rapidement et sans effort.

- **Déploiement accéléré d'applications.** Une architecture prévalidée réduit le temps d'intégration de la mise en œuvre et les risques pour n'importe quelle charge de travail, et la technologie NetApp automatise le déploiement de l'infrastructure. Que vous utilisiez la solution pour le déploiement initial d'images médicales, pour le renouvellement du matériel ou pour l'extension, vous pouvez déplacer davantage de ressources sur la valeur commerciale du projet.
- **Opérations simplifiées et coûts réduits.** vous pouvez éliminer les dépenses et la complexité des plates-formes propriétaires existantes en les remplaçant par une ressource partagée plus efficace et évolutive qui peut répondre aux besoins dynamiques de votre charge de travail. Cette solution améliore l'utilisation des ressources d'infrastructure et améliore le retour sur investissement.
- **Architecture scale-out** vous pouvez faire évoluer vos systèmes SAN et NAS de quelques téraoctets à plusieurs dizaines de pétaoctets sans reconfigurer vos applications en cours d'exécution.
- **Continuité d'activité** vous pouvez effectuer la maintenance du stockage, des opérations de renouvellement du matériel et des mises à niveau logicielles sans interrompre votre activité.
- **Colocation sécurisée.** cet avantage prend en charge les besoins accrus de l'infrastructure partagée de stockage et de serveurs virtualisés, ce qui permet une colocation sécurisée des informations spécifiques aux installations, particulièrement si vous hébergez plusieurs instances de bases de données et de logiciels.
- **Optimisation des ressources regroupées.** cet avantage peut vous aider à réduire le nombre de contrôleurs de stockage et de serveurs physiques, équilibrer les charges de travail et optimiser l'utilisation tout en améliorant les performances.
- **Qualité de service (QoS).** FlexPod offre la qualité de service sur l'ensemble de la pile. Ces règles de QoS leaders du secteur garantissent des niveaux de service différenciés dans un environnement partagé. Ces règles aident à optimiser les performances des charges de travail et à isoler et contrôler les applications non contrôlées.
- **Prise en charge des contrats de niveau de service de niveau de stockage en utilisant la QoS.** vous n'avez pas besoin de déployer des systèmes de stockage différents pour les différents niveaux de stockage requis par un environnement d'imagerie médicale en général. Un cluster de stockage unique avec plusieurs volumes NetApp FlexVol dotés de règles de qualité de service spécifiques aux différents tiers peut servir cet objectif. Avec cette approche, l'infrastructure de stockage peut être partagée par la capacité de s'adapter de manière dynamique à l'évolution des besoins d'un niveau de stockage particulier. La solution NetApp AFF peut prendre en charge différents niveaux de service pour les tiers de stockage en permettant à la QoS au niveau du volume FlexVol, ce qui évite d'avoir recours à différents systèmes de stockage pour différents tiers de stockage pour l'application.
- * Efficacité de stockage.* les images médicales sont généralement pré-compressées par l'application d'imagerie à la compression sans perte jpeg2k qui est autour de 2.5:1. Cependant, il s'agit d'une application d'imagerie et d'un fournisseur spécifique. Dans des environnements applicatifs d'imagerie plus volumineux (plus de 1 po), 5 à 10 % d'économies de stockage sont possibles et vous pouvez réduire les coûts de stockage grâce aux fonctionnalités d'efficacité du stockage de NetApp. Collaborez avec vos fournisseurs d'applications d'imagerie et votre expert NetApp pour bénéficier d'une efficacité du stockage optimale pour votre système d'imagerie médicale.
- **Agilité.** grâce aux outils de gestion, d'orchestration et d'automatisation de flux de travail de pointe proposés par les systèmes FlexPod, votre équipe INFORMATIQUE peut être beaucoup plus réactive aux demandes de l'entreprise. Ces demandes peuvent aller de la sauvegarde d'imagerie médicale au provisionnement d'environnements de test et de formation supplémentaires à la réplication de bases de données d'analytique pour les initiatives de gestion de la santé des populations.
- **Productivité plus élevée.** vous pouvez déployer et adapter rapidement cette solution pour des expériences cliniques optimales pour les utilisateurs finaux.
- **Data Fabric** votre Data Fabric optimisé par NetApp offre un maillage sur l'ensemble des sites, des emplacements physiques et des applications, Votre Data Fabric optimisée par NetApp est conçue pour un

monde centré sur la donnée. Les données étant créées et exploitées dans divers emplacements et, la plupart du temps, partagées avec d'autres sites, applications et infrastructures, Il est donc primordial pour vous de disposer d'un mode de gestion cohérent et intégré. Avec cette solution, vous disposez d'une méthode de gestion des données qui aide votre équipe INFORMATIQUE à maîtriser et à simplifier une INFRASTRUCTURE IT toujours plus complexe.

- **FabricPool.** NetApp ONTAP FabricPool contribue à réduire les coûts de stockage sans compromettre les performances, l'efficacité, la sécurité ni la protection. FabricPool est transparent pour les applications d'entreprise et capitalise sur l'efficacité du cloud en réduisant le TCO du stockage sans devoir repenser l'architecture de l'infrastructure applicative. FlexPod bénéficie des fonctionnalités de hiérarchisation du stockage de FabricPool pour une utilisation plus efficace du stockage Flash ONTAP. Pour plus d'informations, voir "FlexPod avec FabricPool".
- **Sécurité FlexPod.** La sécurité est à la base même de FlexPod. Ces dernières années, les attaques par ransomware sont devenues une menace importante, Les ransomwares sont des programmes malveillants basés sur la crypto-virologie, l'utilisation de la cryptographie pour créer des logiciels malveillants. Ce programme malveillant peut utiliser à la fois un cryptage symétrique et asymétrique pour verrouiller les données d'une victime et exiger une rançon afin de fournir la clé de chiffrement des données. Pour découvrir comment FlexPod contribue à réduire les menaces telles que les ransomware, consultez "La solution aux attaques par ransomware". Les composants d'infrastructure FlexPod sont également "(FIPS) 140-2" conformes à la norme fédérale de traitement des informations.
- **Support coopératif FlexPod.** NetApp et Cisco ont mis en place le modèle de support coopératif FlexPod, un modèle de support solide, évolutif et flexible, afin de répondre aux exigences de support uniques de l'infrastructure convergée FlexPod. Ce modèle tire parti de l'expérience, des ressources et de l'expertise de NetApp et de Cisco pour simplifier l'identification et la résolution de votre problème dans le cadre du support FlexPod, et ce, quelle que soit l'origine du problème. Le modèle de support coopératif FlexPod permet de s'assurer que votre système FlexPod fonctionne correctement et qu'il bénéficie des toutes dernières technologies, tout en fournissant une équipe expérimentée pour résoudre les problèmes d'intégration.

  Le support coopératif FlexPod a un atout précieux si votre établissement de santé exécute des applications stratégiques. L'illustration ci-dessous présente le modèle de support coopératif FlexPod.



Portée

Ce document présente les caractéristiques techniques des systèmes Cisco UCS (Unified Computing System) et de l'infrastructure FlexPod basée sur ONTAP de NetApp pour héberger cette solution d'imagerie médicale.

Public

Ce document est destiné aux leaders techniques du secteur de la santé, aux ingénieurs solutions partenaires Cisco et NetApp et aux équipes des services professionnels. NetApp suppose que le lecteur connaît bien les concepts de dimensionnement du stockage et du calcul, ainsi que la connaissance technique du système d'imagerie médicale, de Cisco UCS et des systèmes de stockage NetApp.

Application d'imagerie médicale

Une application classique d'imagerie médicale est composée d'une suite d'applications qui, ensemble, constituent une solution d'imagerie haute performance pour les organismes de santé de toutes tailles.

Au cœur de la suite de produits se trouvent les capacités cliniques suivantes :

- Référentiel d'imagerie d'entreprise
- Prend en charge les sources d'images traditionnelles telles que la radiologie et la cardiologie. Prend également en charge d'autres domaines de soins tels que l'ophtalmologie, la dermatologie, la coloscopie et d'autres objets d'imagerie médicale tels que des photos et des vidéos.
- "Système d'archivage et de communication d'images" (PACS), qui est un moyen informatisé de remplacer les rôles du film radiologique classique

- VNA (Enterprise Imaging Vendor Neutral Archive) :
  - Consolidation évolutive des documents DICOM et non DICOM
  - Système d'imagerie médicale centralisé
  - Prise en charge de la synchronisation des documents et de l'intégrité des données entre plusieurs (PACs) de l'entreprise
  - Gestion du cycle de vie des documents par un système expert basé sur des règles qui exploite les métadonnées des documents, telles que :
  - Type de modalité
  - Âge de l'étude
  - Âge du patient (actuel et au moment de la capture de l'image)
  - Point d'intégration unique à l'intérieur et à l'extérieur (HIE) de l'entreprise :
  - Lien de document contextuel
  - HL7 (Health Level Seven International), DICOM et WADO
  - Capacité d'archivage indépendante du stockage
- Intégration à d'autres systèmes d'information médicale utilisant HL7 et des liens contextuels :
  - Permet aux DME d'implémenter des liens directs vers les images des patients à partir des dossiers médicaux, des flux de travail d'imagerie, etc.
  - Permet d'intégrer l'historique des images de soins longitudinaux d'un patient dans les DME.
- Flux de travail de technologue en radiologie
- Visualiseurs d'entreprise à encombrement nul pour un affichage d'images depuis n'importe quel périphérique compatible, quel que soit le lieu où
- Outils analytiques qui exploitent les données rétrospectives et en temps réel :
  - Création de rapports de conformité
  - Rapports opérationnels
  - Rapports de contrôle qualité et d'assurance qualité

Taille de l'organisation de soins de santé et dimensionnement de la plate-forme

Les organismes de soins de santé peuvent être classés de façon générale en utilisant des méthodes normalisées qui aident les programmes tels que l'ACO. Une de ces classifications utilise le concept de réseau clinique intégré (CIN). Un groupe d'hôpitaux peut être appelé un CIN s'ils collaborent et respectent des protocoles cliniques et des voies d'accès éprouvés afin d'améliorer la valeur des soins et de réduire les coûts des patients. Les hôpitaux au sein d'un CIN ont des contrôles et des pratiques en place pour intégrer des médecins qui suivent les valeurs fondamentales du CIN. Traditionnellement, un réseau de prestation intégré (RDI) a été limité aux hôpitaux et aux groupes de médecins. Un CIN traverse les frontières traditionnelles de l'IDN, et un CIN peut encore faire partie d'un ACO. Selon les principes d'un CIN, les organismes de santé peuvent être classés en petits, moyens et grands.

Les petits organismes de santé

Une organisation de soins de santé est petite si elle ne comprend qu'un seul hôpital avec des cliniques ambulatoires et un service d'hospitalisation, mais elle ne fait pas partie d'un CIN. Les médecins travaillent en tant que soignants et coordonnent les soins aux patients pendant un continuum de soins. Ces petites organisations comprennent généralement des installations gérées par des médecins. Ils peuvent ou non offrir des soins d'urgence et de traumatologie comme soins intégrés pour le patient. En règle générale, un petit

établissement de santé réalise environ 40 250,000 études d'imagerie clinique par an. Les centres d'imagerie sont considérés comme des petites organisations de santé et fournissent des services d'imagerie. Certains fournissent également des services de dictée radiologique à d'autres organisations.

Moyennes entreprises de santé

Un organisme de santé considéré comme de taille moyenne s'il comprend plusieurs systèmes hospitaliers avec des organisations ciblées, par exemple :

- Cliniques de soins pour adultes et hôpitaux hospitalisés pour adultes
- Services de main-d'œuvre et de livraison
- Cliniques de garde d'enfants et hôpitaux pour enfants hospitalisés
- Un centre de traitement du cancer
- Services d'urgence pour adultes
- Services d'urgence pour enfants
- Un bureau de médecine familiale et de soins primaires
- Un centre de soins de traumatologie pour adultes
- Un centre de soins de traumatologie pour enfants

Dans un organisme de santé de taille moyenne, les médecins suivent les principes d'un CIN et agissent comme une seule unité. Les hôpitaux ont des fonctions distinctes de facturation à l'hôpital, au médecin et à la pharmacie. Les hôpitaux peuvent être associés à des instituts de recherche universitaire et effectuer des recherches et des essais cliniques interventionnels. Un organisme de santé de taille moyenne réalise jusqu'à 500,000 études d'imagerie clinique par an.

Les grandes structures de santé

Une organisation de soins de santé est considérée comme importante si elle comprend les caractéristiques d'une organisation de soins de santé de taille moyenne et offre à la communauté des capacités cliniques de taille moyenne dans plusieurs sites géographiques.

Une grande organisation de soins de santé remplit généralement les fonctions suivantes :

- Dispose d'un bureau central pour gérer l'ensemble des fonctions
- Participe à des coentreprises avec d'autres hôpitaux
- Négocie chaque année les taux avec les organismes payeurs
- Négocie les taux de payeur par état et par région
- Participe à des programmes d'utilisation significative (MU)
- Effectuer des recherches cliniques de pointe dans les cohortes de santé de la population en utilisant des outils normalisés de gestion de la santé de la population (PHM)
- Réalise jusqu'à un million d'études d'imagerie clinique chaque année

Certains grands établissements de santé qui participent à un CIN disposent également de fonctionnalités de lecture d'imagerie basées sur l'IA. En général, ces entreprises réalisent chaque année un à deux millions d'études en imagerie clinique.

Avant d'étudier la façon dont ces entreprises de taille différente se traduisent en un système FlexPod de taille optimale, vous devez comprendre les différents composants de FlexPod et les différentes fonctionnalités d'un système FlexPod.

FlexPod

Cisco Unified Computing System

Cisco UCS se compose d'un seul domaine de gestion interconnecté avec une infrastructure d'E/S unifiée. Cisco UCS pour les environnements d'imagerie médicale a été conforme aux recommandations et aux bonnes pratiques de NetApp en matière d'infrastructure des systèmes d'imagerie médicale. Ainsi, l'infrastructure peut fournir des informations médicales critiques avec une disponibilité maximale.

La technologie de calcul de l'imagerie médicale d'entreprise repose sur la technologie Cisco UCS, avec ses fonctions de gestion des systèmes intégrées, ses processeurs Intel Xeon et sa virtualisation des serveurs. Ces technologies intégrées répondent aux problématiques des data centers et vous permettent de respecter vos objectifs en matière de conception de data Center avec un système d'imagerie médicale classique. Cisco UCS unifie la gestion des réseaux LAN, SAN et systèmes dans une seule liaison simplifiée pour les serveurs rack, les serveurs lames et les machines virtuelles. Cisco UCS comprend une paire redondante d'interconnexions de fabric Cisco UCS qui assure un point de gestion unique et un point de contrôle unique pour tout le trafic d'E/S.

Cisco UCS utilise des profils de service, de sorte que les serveurs virtuels de l'infrastructure Cisco UCS soient configurés correctement et de façon cohérente. Les profils de service incluent des informations stratégiques sur l'identité du serveur, telles que l'adressage LAN et SAN, les configurations d'E/S, les versions de micrologiciel, l'ordre de démarrage, le réseau local virtuel (VLAN), le port physique et les stratégies de qualité de service. Les profils de service peuvent être créés et associés dynamiquement à n'importe quel serveur physique du système en quelques minutes, et non plus en quelques heures ou jours. L'association des profils de service avec des serveurs physiques s'effectue sous la forme d'une opération simple et unique qui permet de migrer les identités entre les serveurs de l'environnement sans nécessiter de modification de la configuration physique. Il facilite également le provisionnement rapide, sans système d'exploitation, des remplacements des serveurs défaillants.

L'utilisation des profils de service permet de confirmer que les serveurs sont configurés de manière cohérente dans toute l'entreprise. Lors de l'utilisation de plusieurs domaines de gestion Cisco UCS, Cisco UCS Central peut utiliser des profils de service globaux pour synchroniser les informations de configuration et de stratégie entre les domaines. Si la maintenance doit être effectuée dans un domaine, l'infrastructure virtuelle peut être migrée vers un autre domaine. Avec cette approche, même lorsqu'un seul domaine est hors ligne, les applications continuent à fonctionner avec une haute disponibilité.

Cisco UCS est une solution nouvelle génération pour l'informatique basée sur des serveurs lames et en rack. Le système comprend une structure en réseau unifiée 40 GbE à faible latence et sans perte, équipée de serveurs x86 de grande qualité. Il s'agit d'une plate-forme intégrée, évolutive et multi-châssis dans laquelle toutes les ressources participent à un domaine de gestion unifié. Cisco UCS accélère la prestation de nouveaux services de façon simple, fiable et sécurisée grâce à une prise en charge du provisionnement et de la migration de bout en bout pour les systèmes virtualisés et non virtualisés. Cisco UCS offre les fonctionnalités suivantes :

- Gestion complète
- Simplification radicale
- Hautes performances

Cisco UCS comprend les composants suivants :

- **Compute.** le système est basé sur une toute nouvelle classe de système informatique qui intègre des serveurs lames et montés en rack basés sur la famille de processeurs évolutifs Intel Xeon.
- **Réseau.** le système est intégré dans une structure de réseau unifiée à faible latence et sans perte de 40 Gbits/s. Cette base consolide actuellement les réseaux LAN, SAN et les réseaux de calcul hautes

performances, qui sont dédiés aux réseaux distincts. La structure unifiée réduit les coûts en diminuant le nombre d'adaptateurs, de commutateurs et de câbles réseau ainsi que les besoins en alimentation et en climatisation.

- **Virtualisation.** le système libère tout le potentiel de la virtualisation en améliorant l'évolutivité, les performances et le contrôle opérationnel des environnements virtuels. Les fonctionnalités Cisco de sécurité, d'application de règles et de diagnostic sont maintenant étendues sous forme d'environnements virtualisés afin de mieux répondre aux exigences commerciales en constante évolution.
- **Accès au stockage.** le système fournit un accès consolidé au stockage SAN et au stockage NAS sur la structure unifiée. C'est également un système idéal pour le SDS. En combinant les avantages d'une structure unique pour gérer les serveurs de calcul et de stockage dans une seule fenêtre, la qualité de service peut être mise en œuvre si nécessaire pour injecter une accélération des E/S dans le système. De plus, les administrateurs de vos serveurs peuvent pré-attribuer des règles d'accès au stockage aux ressources de stockage, ce qui simplifie la connectivité et la gestion du stockage et vous permet d'accroître la productivité. Outre le stockage externe, les serveurs rack et lames sont dotés d'un stockage interne accessible via des contrôleurs RAID matériels intégrés. En configurant la règle de configuration du disque et du profil de stockage dans Cisco UCS Manager, les besoins en stockage du système d'exploitation hôte et des données applicatives sont satisfaits par les groupes RAID définis par l'utilisateur. Il en résulte une haute disponibilité et des performances supérieures.
- **Gestion.** le système intègre de façon unique tous les composants système afin que l'ensemble de la solution puisse être géré comme une entité unique par Cisco UCS Manager. Pour gérer toutes les configurations et opérations du système, Cisco UCS Manager dispose d'une interface graphique intuitive, d'une interface de ligne de commandes et d'un puissant module de bibliothèque de scripts pour Microsoft Windows PowerShell basé sur une API robuste.

Le système Unified Computing System de Cisco fusionne la mise en réseau de la couche d'accès et les serveurs. Ce système serveur nouvelle génération hautes performances offre à votre datacenter un haut niveau d'agilité et d'évolutivité des charges de travail.

Cisco UCS Manager

Cisco UCS Manager offre une gestion unifiée et intégrée de tous les composants logiciels et matériels dans Cisco UCS. Grâce à une technologie de connexion unique, UCS Manager gère, contrôle et gère plusieurs châssis pour des milliers de machines virtuelles. Grâce à une interface graphique intuitive, une interface de ligne de commandes ou une API XML, vos administrateurs utilisent le logiciel pour gérer tout le système Cisco UCS en tant qu'entité logique unique. Cisco UCS Manager réside sur une paire de Cisco UCS 6300 Series Fabric Interconnect qui utilisent une configuration en cluster de secours actif-actif pour une haute disponibilité.

Cisco UCS Manager propose une interface de gestion unifiée intégrée qui intègre vos serveurs, votre réseau et votre système de stockage. Cisco UCS Manager effectue une détection automatique pour détecter l'inventaire, gérer et provisionner les composants système que vous ajoutez ou modifiez. Il offre un ensemble complet d'API XML pour une intégration tierce et expose 9,000 points d'intégration. Cette solution facilite également le développement personnalisé pour l'automatisation, l'orchestration et permet d'atteindre de nouveaux niveaux de visibilité et de contrôle sur le système.

Les profils de services bénéficient des environnements virtualisés et non virtualisés. Ils permettent d'augmenter la mobilité des serveurs non virtualisés, par exemple lors du déplacement des charges de travail d'un serveur à un autre ou lorsque vous mettez un serveur hors ligne pour maintenance ou mise à niveau. Vous pouvez également utiliser des profils en association avec des clusters de virtualisation afin de mettre facilement en ligne de nouvelles ressources, en complétant la mobilité existante des machines virtuelles.

Pour plus d'informations sur Cisco UCS Manager, consultez le "Page produit Cisco UCS Manager".

Atouts de Cisco UCS

Cisco Unified Computing System révolutionne la gestion des serveurs dans le data Center. Découvrez les atouts uniques de Cisco UCS et Cisco UCS Manager :

- **Gestion intégrée.** dans Cisco UCS, les serveurs sont gérés par le micrologiciel intégré dans les interconnexions de fabric, ce qui élimine la nécessité pour les périphériques physiques ou virtuels externes de les gérer.
- **Structure unifiée.** dans Cisco UCS, des châssis de serveur lame ou des serveurs rack aux interconnexions de structure, un seul câble Ethernet est utilisé pour le trafic LAN, SAN et de gestion. Ces e/S convergées réduisent le nombre de câbles, de SFP et d'adaptateurs requis, et diminuent ainsi vos dépenses d'investissement et d'exploitation pour la solution globale.
- **AutoDiscovery.** en insérant simplement le serveur lame dans le châssis ou en connectant les serveurs rack aux interconnexions de structure, la découverte et l'inventaire des ressources de calcul se produisent automatiquement sans aucune intervention de gestion. L'association de la structure unifiée et de la détection automatique rend possible l'architecture à un seul câble de Cisco UCS. Ses capacités de calcul peuvent donc être étendues facilement tout en conservant la connectivité externe existante aux réseaux LAN, SAN et de gestion.
- **Classification de ressources basée sur des règles.** lorsqu'une ressource de calcul est découverte par Cisco UCS Manager, elle peut être classée automatiquement dans un pool de ressources donné en fonction des règles que vous avez définies. Cette fonctionnalité est utile dans le cloud computing mutualisé.
- **Gestion combinée des serveurs rack et lame.** Cisco UCS Manager peut gérer des serveurs lame B-Series et des serveurs rack C-Series sous le même domaine Cisco UCS. Grâce à cette fonctionnalité et aux ressources de calcul sans état, les ressources de calcul sont totalement indépendantes des facteurs physiques.
- **Architecture de gestion basée sur des modèles.** l'architecture et la base de données de gestion de Cisco UCS Manager sont basées sur des modèles et des données. L'API XML ouverte fournie pour fonctionner sur le modèle de gestion permet une intégration simple et évolutive de Cisco UCS Manager avec d'autres systèmes de gestion.
- **Stratégies, pools et modèles.** l'approche de gestion de Cisco UCS Manager est basée sur la définition de règles, de pools et de modèles au lieu d'une configuration encombrée. Elle offre une approche simple, flexible et axée sur les données pour la gestion des ressources de calcul, de réseau et de stockage.
- **Intégrité référentielle non imposée.** dans Cisco UCS Manager, un profil de service, un profil de port ou des règles peut faire référence à d'autres stratégies ou à d'autres ressources logiques avec une intégrité référentielle desserrée. Une stratégie référencée ne peut pas exister au moment de la création de la stratégie de référence, mais une stratégie référencée peut être supprimée même si d'autres politiques le font. Cette fonctionnalité permet à différents experts de travailler indépendamment les uns des autres. Vous bénéficiez d'une grande flexibilité en permettant à différents experts, dont le réseau, le stockage, la sécurité, les serveurs et la virtualisation, de travailler ensemble pour accomplir une tâche complexe.
- **Résolution des règles.** dans Cisco UCS Manager, vous pouvez créer une arborescence de hiérarchie d'unités organisationnelles qui reproduit les locataires réels et les relations organisationnelles. Vous pouvez définir diverses stratégies, pools et modèles à différents niveaux de votre hiérarchie organisationnelle. Une règle faisant référence à une autre règle par nom est résolue dans la hiérarchie organisationnelle avec la correspondance de stratégie la plus proche. Si aucune stratégie avec un nom spécifique n'est trouvée dans la hiérarchie de l'organisation racine, une stratégie spéciale nommée "default" est recherchée. Cette pratique de résolution de règles rend possible des API de gestion conviviales et offre une grande flexibilité aux propriétaires des différentes entreprises.
- **Profils de service et calcul sans état.** Un profil de service est une représentation logique d'un serveur, qui comporte ses différentes identités et stratégies. Vous pouvez attribuer ce serveur logique à n'importe quelle ressource de calcul physique, à condition qu'il réponde aux besoins en ressources. Le calcul sans

état permet d'acheter un serveur en quelques minutes, contre plusieurs jours auparavant dans les anciens systèmes de gestion de serveurs.

- **Prise en charge de la colocation intégrée.** la combinaison de règles, de pools, de modèles, d'une intégrité référentielle libre, de la résolution des règles dans la hiérarchie organisationnelle et d'une approche basée sur les profils de service pour les ressources de calcul rend Cisco UCS Manager intrinsèquement convivial pour les environnements mutualisés qui sont généralement observés dans les clouds privés et publics.
- **Mémoire étendue** le serveur lame Cisco UCS B200 M5 pour entreprise étend les capacités de la gamme Cisco Unified Computing System en un format lame demi-largeur. Le système Cisco UCS B200 M5 exploite la puissance des derniers processeurs évolutifs Intel Xeon avec jusqu'à 3 To de RAM. Cette fonctionnalité permet de disposer du rapport machine virtuelle/serveur physique que de nombreux déploiements nécessitent ou permet à certaines architectures de prendre en charge d'importantes opérations de mémoire, comme le Big Data.
- **Réseau orienté virtualisation.** la technologie Cisco Virtual machine Fabric Extender (VM-FEX) rend la couche réseau d'accès consciente de la virtualisation des hôtes. Cette prise en charge évite la pollution des domaines de calcul et de réseau grâce à la virtualisation lorsqu'un réseau virtuel est géré par des profils de port définis par l'équipe d'administration réseau. VM-FEX décharge également le CPU de l'hyperviseur en effectuant une commutation au niveau matériel, ce qui permet au CPU de l'hyperviseur d'effectuer davantage de tâches liées à la virtualisation. Pour simplifier la gestion du cloud, la technologie VM-FEX est parfaitement intégrée à VMware vCenter, Linux Kernel-based Virtual machine (KVM) et Microsoft Hyper-V SR-IOV.
- **QoS simplifiée** même si les protocoles FC et Ethernet sont convergés dans Cisco UCS, la prise en charge intégrée de la qualité de service et l'Ethernet sans perte rendent cela transparent. En représentant toutes les classes de système dans un panneau d'interface graphique, la QoS réseau est simplifiée dans Cisco UCS Manager.

Commutateurs Cisco Nexus IP et MDS

Les commutateurs Cisco Nexus et les directeurs multicouches Cisco MDS vous offrent une connectivité haute performance et une consolidation SAN. Les réseaux de stockage multiprotocoles Cisco vous aident à réduire les risques en vous offrant la flexibilité et les options suivantes : FC, Fibre Connection (FICON), FC over Ethernet (FCoE), iSCSI et FC over IP (FCIP).

Les commutateurs Cisco Nexus offrent l'un des ensembles de fonctionnalités réseau de data centers les plus complets au sein d'une plateforme unique. Elles offrent de hautes performances et une densité élevée aussi bien pour le data Center que pour le cœur du campus. Ils offrent également un ensemble complet de fonctionnalités pour les déploiements d'agrégation de data Center, de bout en bout et d'interconnexion de data Center dans une plateforme modulaire extrêmement résiliente.

Cisco UCS intègre des ressources de calcul avec des switchs Cisco Nexus et une structure unifiée qui identifie et gère différents types de trafic réseau. Ce trafic inclut les E/S du stockage, le trafic des postes de travail en continu, la gestion et l'accès aux applications cliniques et professionnelles. Vous bénéficiez des fonctionnalités suivantes :

- **Évolutivité de l'infrastructure.** virtualisation, alimentation et refroidissement efficaces, évolutivité du cloud avec automatisation, haute densité et performances, tous ces éléments prennent en charge la croissance efficace du data Center.
- **Continuité opérationnelle.** la conception intègre le matériel, les fonctionnalités logicielles Cisco NX-OS et la gestion pour prendre en charge les environnements sans temps d'indisponibilité.
- **La flexibilité du transport.** vous pouvez adopter progressivement de nouvelles technologies de mise en réseau avec cette solution économique.

Ensemble, Cisco UCS avec switchs Cisco Nexus et directeurs multicouches MDS offre une solution de calcul, de réseau et de connectivité SAN pour un système d'imagerie médicale d'entreprise.

Stockage 100 % Flash NetApp

Une solution de stockage NetApp exécutant le logiciel ONTAP réduit vos coûts de stockage globaux, tout en offrant des temps de réponse de lecture et d'écriture à faible latence et des IOPS élevées nécessaires aux workloads du système d'imagerie médicale. Pour créer un système de stockage optimal adapté à des exigences système d'imagerie médicale standard, ONTAP prend en charge à la fois les configurations 100 % Flash et hybrides. Le stockage Flash NetApp offre aux clients des systèmes d'imagerie médicale tels que vous les composants clés de performance et de réactivité pour prendre en charge les opérations de leur système d'imagerie médicale sensibles à la latence. Avec la création de plusieurs domaines de défaillance dans un seul cluster, la technologie NetApp peut également isoler vos environnements de production de vos environnements non productifs. De plus, en garantissant que la performance du système ne descend pas en dessous d'un certain niveau pour les charges de travail avec la QoS minimale de ONTAP, nous réduisent les problèmes de performance pour votre système.

L'architecture scale-out du logiciel ONTAP s'adapte en toute flexibilité à vos diverses charges de travail d'E/S. Les architectures ONTAP permettent généralement d'atteindre le débit et la faible latence nécessaires aux applications cliniques et de fournir une architecture scale-out modulaire. Les nœuds NetApp AFF peuvent être associés dans le même cluster scale-out avec des nœuds de stockage hybrides (HDD et Flash), adaptés au stockage de datasets volumineux à haut débit. Vous pouvez cloner, répliquer et sauvegarder votre environnement de système d'imagerie médicale à partir d'un stockage SSD coûteux vers un stockage HDD plus économique sur d'autres nœuds. Grâce au stockage NetApp compatible cloud et à une Data Fabric fournie par NetApp, vous pouvez sauvegarder vos données dans un stockage objet sur site ou dans le cloud.

Pour l'imagerie médicale, ONTAP a été validé par la plupart des principaux systèmes d'imagerie médicale. Cela signifie qu'il a été testé pour fournir des performances rapides et fiables pour l'imagerie médicale. De plus, les fonctionnalités suivantes simplifient la gestion, optimisent la disponibilité et l'automatisation, et réduisent le volume total de stockage nécessaire.

- **Performances exceptionnelles.** la solution NetApp AFF partage la même architecture de stockage unifié, le logiciel ONTAP, une interface de gestion, des services de données complets et des fonctionnalités avancées, que les autres gammes de produits NetApp FAS. Cette combinaison innovante de supports 100 % Flash avec les systèmes ONTAP vous offre la faible latence prévisible et les IOPS élevées des systèmes de stockage 100 % Flash, grâce au logiciel ONTAP leader du secteur.
- **Efficacité du stockage.** vous pouvez réduire vos besoins en capacité totale en collaboration avec votre PME NetApp pour comprendre comment cela a appliqué votre système d'imagerie médicale spécifique.
- **Clonage compact.** avec la fonctionnalité FlexClone, votre système peut créer presque instantanément des clones pour prendre en charge l'actualisation de l'environnement de sauvegarde et de test. Ces clones ne consomment de l'espace de stockage supplémentaire que lorsque des modifications sont apportées.
- **Protection intégrée des données.** les fonctionnalités de protection complète des données et de reprise après sinistre vous aident à protéger vos données stratégiques et à assurer une reprise après incident.
- **Continuité de l'activité.** vous pouvez effectuer des mises à niveau et des opérations de maintenance sans mettre les données hors ligne.
- **QoS.** la QoS du stockage vous aide à limiter les charges de travail dominantes potentielles. Plus important encore, la QoS crée une garantie de performance minimale qui ne passera pas un niveau minimal pour les charges de travail stratégiques, comme l'environnement de production d'un système d'imagerie médicale. En limitant les conflits, la qualité de services de NetApp peut également réduire les problèmes de performance.
- **Data Fabric** pour accélérer la transformation digitale, votre Data Fabric NetApp simplifie et intègre la gestion des données dans les environnements cloud et sur site. Elles offrent des services et des

applications de gestion de données intégrés et cohérents pour améliorer la visibilité, l'exploitation, l'accès, le contrôle ainsi que la protection et la sécurité des données. NetApp est intégré avec de grands clouds publics, tels qu'AWS, Azure, Google Cloud et IBM Cloud vous offre un large choix.

Virtualisation de l'hôte : VMware vSphere

Les architectures FlexPod sont validées avec VMware vSphere 6.x, la plateforme de virtualisation leader du marché. VMware ESXi 6.x est utilisé pour déployer et exécuter les machines virtuelles. VCenter Server Appliance 6.x est utilisé pour gérer les hôtes et les machines virtuelles ESXi. Plusieurs hôtes ESXi qui s'exécutent sur des serveurs lames Cisco UCS B200 M5 sont utilisés pour former un cluster VMware ESXi. Le cluster VMware ESXi regroupe les ressources de calcul, de mémoire et de réseau à partir de tous les nœuds de cluster, et fournit une plateforme résiliente aux machines virtuelles exécutées sur le cluster. Les fonctionnalités du cluster VMware ESXi, la haute disponibilité vSphere et Distributed Resource Scheduler (DRS) contribuent toutes à la tolérance du cluster vSphere pour résister aux défaillances et contribuent à la distribution des ressources entre les hôtes VMware ESXi.

Le plug-in de stockage NetApp et le plug-in Cisco UCS s'intègrent à VMware vCenter pour assurer les flux de travail opérationnels de vos ressources de stockage et de calcul requises.

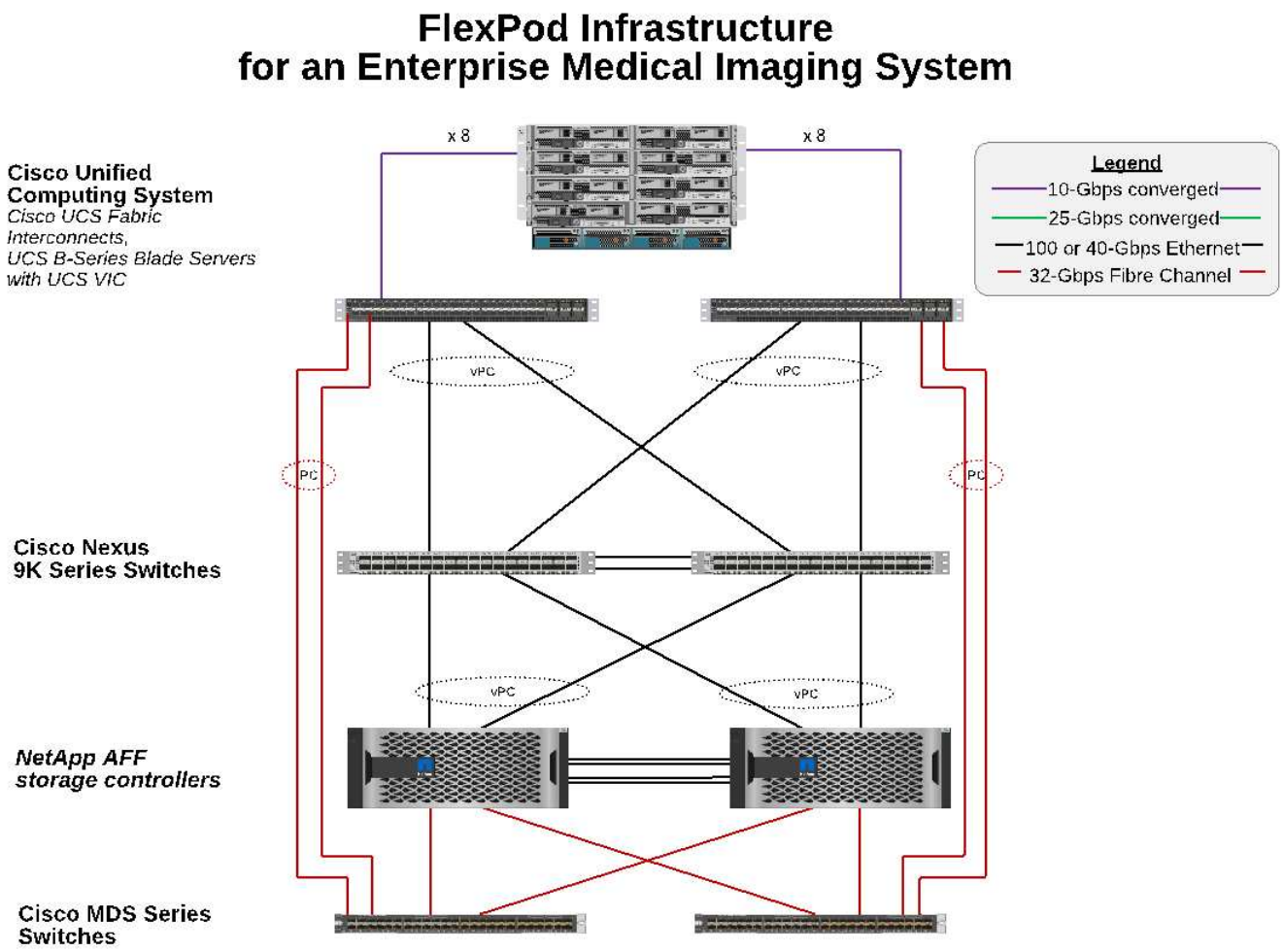
Le cluster VMware ESXi et vCenter Server vous offrent une plateforme centralisée pour le déploiement d'environnements d'imagerie médicale dans des VM. Votre établissement de santé peut bénéficier de tous les avantages d'une infrastructure virtuelle de pointe en toute confiance, notamment :

- **Déploiement simple.** déployez rapidement et facilement vCenter Server à l'aide d'une appliance virtuelle.
- **Contrôle et visibilité centralisés.** administrer l'ensemble de l'infrastructure vSphere à partir d'un emplacement unique.
- **Optimisation proactive.** allouer, optimiser et migrer les ressources pour une efficacité maximale.
- **Gestion.** utilisez des plug-ins et des outils puissants pour simplifier la gestion et étendre le contrôle.

Architecture

L'architecture FlexPod est conçue pour assurer une haute disponibilité si un composant ou une liaison échoue dans l'ensemble de la pile de calcul, de réseau et de stockage. Plusieurs chemins réseau pour l'accès client et au stockage permettent l'équilibrage de la charge et l'utilisation optimale des ressources.

La figure suivante montre la topologie FC 16 Gbit/s/Ethernet 40 Gbit/s (40 GbE) pour le déploiement de la solution de système d'imagerie médicale.



Architecture du stockage

Utilisez les instructions d'architecture de stockage de cette section pour configurer l'infrastructure de stockage d'un système d'imagerie médicale d'entreprise.

Niveaux de stockage

En général, un environnement d'imagerie médicale d'entreprise se compose de plusieurs tiers de stockage. Chaque Tier présente des exigences spécifiques en matière de performances et de protocoles de stockage. Le stockage NetApp prend en charge diverses technologies RAID ; plus d'informations sont disponibles "ici". Découvrez comment les systèmes de stockage NetApp AFF répondent aux besoins des différents tiers de stockage du système d'imagerie :

- **Stockage de performances (niveau 1).** ce niveau offre des performances élevées et une redondance élevée pour les bases de données, les disques OS, les datastores VMFS (Virtual machine File System) VMware, etc. Comme configuré dans ONTAP, les E/S de blocs sont transférées via fibre optique vers une baie de stockage partagé du SSD. La latence minimale est de 1 ms à 3 ms avec un pic occasionnel de 5 ms. Ce niveau de stockage est généralement utilisé pour le cache de stockage à court terme, généralement entre 6 et 12 mois de stockage d'images pour un accès rapide aux images DICOM en ligne. Ce niveau offre des performances élevées et une redondance élevée pour les caches d'images, la sauvegarde des bases de données, etc. Les baies 100 % Flash de NetApp offrent une latence inférieure à la milliseconde pour une bande passante continue, ce qui est bien inférieur aux délais d'intervention attendus dans un environnement d'imagerie médicale classique. NetApp ONTAP prend en charge à la fois

RAID-TEC (RAID triple parité pour gérer les trois défaillances de disques) et RAID DP (RAID double parité pour gérer les deux défaillances de disques).

- **Stockage d'archives (niveau 2).** ce niveau est utilisé pour un accès aux fichiers standard optimisé en termes de coût, un stockage RAID 5 ou RAID 6 pour des volumes plus importants et un archivage à long terme à moindre coût/performance. NetApp ONTAP prend en charge à la fois RAID-TEC (RAID triple parité pour gérer les trois défaillances de disques) et RAID DP (RAID double parité pour gérer les deux défaillances de disques). Avec NetApp FAS dans FlexPod, vous pouvez utiliser les E/S des applications d'imagerie via NFS/SMB vers une baie de disques SAS. Les systèmes NetApp FAS offrent une latence d'environ 10 ms pour une bande passante continue, ce qui est bien inférieur aux temps de service attendus pour le niveau de stockage 2 dans un environnement d'imagerie médicale d'entreprise.

L'archivage dans le cloud dans un environnement de cloud hybride peut être utilisé à des fins d'archivage vers un fournisseur de stockage de cloud public utilisant des protocoles S3 ou similaires. Avec la technologie NetApp SnapMirror, vous pouvez répliquer les données d'imagerie depuis des baies 100 % Flash ou FAS vers des baies de stockage sur disque plus lentes ou vers Cloud Volumes ONTAP pour AWS, Azure ou Google Cloud.

Avec ses fonctionnalités de réplication des données, NetApp SnapMirror protège votre système d'imagerie médicale grâce à la réplication unifiée des données. Gérez plus simplement la protection des données dans l'environnement Data Fabric grâce à une réplication multiplateforme, du Flash au disque et au cloud :

- Déplacez les données de manière fluide et efficace entre les systèmes de stockage NetApp pour la sauvegarde et la reprise d'activité avec le même volume cible et le même flux d'E/S.
- Basculez vers un volume secondaire. Restaurez vos données à partir d'une copie Snapshot générée à un point dans le temps sur le système de stockage secondaire.
- Protégez vos workloads stratégiques avec une réplication synchrone sans perte de données (RPO=0).
- Diminuez le trafic réseau Et l'empreinte du stockage grâce à une meilleure efficacité opérationnelle.
- Réduisez le trafic réseau en déplaçant uniquement les blocs de données modifiés.
- Conservez les avantages de l'efficacité du stockage sur les systèmes principaux pendant le déplacement, notamment la déduplication, la compression et la compaction.
- Bénéficiez de fonctionnalités d'efficacité à la volée supplémentaires avec la compression réseau.

Plus d'informations sont disponibles "ici".

Le tableau ci-dessous répertorie chaque niveau qu'un système d'imagerie médicale classique nécessite pour une latence spécifique et les caractéristiques de performances de débit.

Niveau de stockage	De formation	Recommandation NetApp
1	Latence comprise entre 1 et 5 ms avec un débit de 35 et 500 Mbit/s.	Avec une latence inférieure à 1 ms, la paire haute disponibilité AFF A300, avec deux tiroirs disques, peut atteindre un débit d'environ 1,6 Gbit/s. AFF
2	Archivage sur site	FAS avec une latence jusqu'à 30 ms.
	Archivage dans le cloud	Réplication de SnapMirror vers Cloud Volumes ONTAP ou archivage des sauvegardes avec le logiciel NetApp StorageGRID

Connectivité réseau du stockage

Structure FC

- La structure FC est destinée aux E/S des systèmes d'exploitation hôte, du calcul au stockage.
- Deux structures FC (Fabric A et Fabric B) sont respectivement connectées aux structures Cisco UCS Fabric A et UCS Fabric B.
- Un serveur SVM (Storage Virtual machine) avec deux interfaces logiques FC (LIF) se trouve sur chaque nœud de contrôleur. Sur chaque nœud, une LIF est connectée à Fabric A et l'autre est connectée à Fabric B.
- La connectivité de bout en bout FC 16 Gbit/s s'effectue via les commutateurs Cisco MDS. Un initiateur unique, plusieurs ports cibles et un zoning sont tous configurés.
- Un démarrage SAN FC est utilisé pour créer un calcul sans état. Les serveurs sont démarrés à partir de LUN dans le volume de démarrage hébergé sur le cluster de stockage AFF.

Réseau IP pour l'accès au stockage sur iSCSI, NFS et SMB/CIFS

- Deux LIF iSCSI se trouvent au SVM sur chaque nœud de contrôleur. Sur chaque nœud, une LIF est connectée à l'environnement Fabric A, et le second est relié à l'environnement Fabric B.
- Deux LIF de données NAS se trouvent au SVM sur chaque nœud de contrôleur. Sur chaque nœud, une LIF est connectée à l'environnement Fabric A, et le second est relié à l'environnement Fabric B.
- Groupes d'interfaces de ports de stockage (canal de port virtuel [VPC]) pour une liaison 10 Gbits/s vers le commutateur N9k-A et pour une liaison 10 Gbits/s vers le commutateur N9k-B.
- Charge de travail dans les systèmes de fichiers Ext4 ou NTFS, de la machine virtuelle au stockage :
  - Protocole iSCSI sur IP.
- VM hébergées dans le datastore NFS :
  - Les E/S du système d'exploitation de machine virtuelle passent par plusieurs chemins Ethernet via des commutateurs Nexus.

Gestion dans la bande (liaison active/passive)

- Liaison 1 Gbit/s au commutateur de gestion N9k-A, et liaison 1 Gbit/s au commutateur de gestion N9k-B.

Sauvegarde et restauration

Le data Center FlexPod repose sur une baie de stockage gérée par le logiciel de gestion des données NetApp ONTAP. Le logiciel ONTAP a évolué au fil des 20 ans pour fournir de nombreuses fonctionnalités de gestion des données pour les VM, les bases de données Oracle, les partages de fichiers SMB/CIFS et NFS. Elle propose également une technologie de protection telle que la technologie NetApp Snapshot, SnapMirror et la technologie de réplication des données NetApp FlexClone. Le logiciel NetApp SnapCenter dispose d'un serveur et d'un client GUI afin d'utiliser les fonctionnalités ONTAP Snapshot, SnapRestore et FlexClone pour les machines virtuelles, les partages de fichiers SMB/CIFS, NFS et la sauvegarde et la restauration de bases de données Oracle.

Utilisation du logiciel NetApp SnapCenter "breveté" Technologie Snapshot permettant de créer instantanément une sauvegarde d'une machine virtuelle entière ou d'une base de données Oracle sur un volume de stockage NetApp. Par rapport à Oracle Recovery Manager (RMAN), les copies Snapshot ne nécessitent pas de copie de sauvegarde de base complète, car elles ne sont pas stockées comme copies physiques des blocs. Les copies Snapshot sont stockées sous forme de pointeurs vers les blocs de stockage tels qu'ils existaient dans le système de fichiers ONTAP WAFL au moment de la création des copies Snapshot. Du fait de cette relation

physique étroite, les copies Snapshot sont conservées sur la même baie de stockage que les données d'origine. Il est également possible de créer des copies Snapshot au niveau des fichiers afin de vous donner un contrôle plus granulaire pour la sauvegarde.

La technologie Snapshot est basée sur une technique de redirection sur écriture. Initialement, il contient uniquement des pointeurs de métadonnées et ne consomme pas beaucoup d'espace tant que les premières données ne sont pas modifiées dans un bloc de stockage. Si un bloc existant est verrouillé par une copie Snapshot, un nouveau bloc est écrit par le système de fichiers ONTAP WAFL en tant que copie active. Cette approche évite les doubles-écritures qui se produisent avec la technique de changement sur écriture.

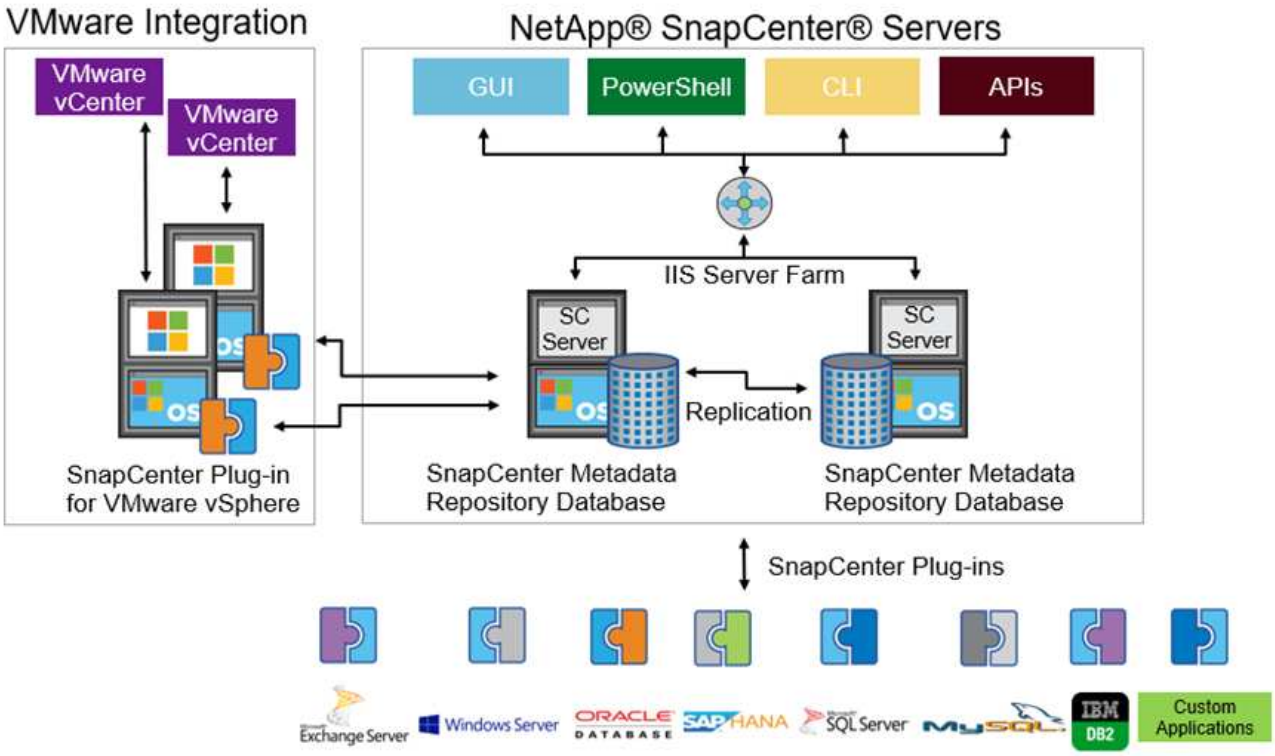
Pour la sauvegarde de bases de données Oracle, les copies Snapshot permettent un gain de temps considérable. Par exemple, une sauvegarde effectuée 26 avec RMAN à elle seule peut prendre moins de 2 minutes à l'aide du logiciel SnapCenter.

En outre, étant donné que la restauration des données ne copie aucun bloc de données, il est possible de restaurer instantanément une copie de sauvegarde Snapshot en fonction des pointeurs vers les images de blocs Snapshot cohérentes au niveau des applications. Le clonage SnapCenter crée une copie séparée des pointeurs de métadonnées sur une copie Snapshot existante, et monte la nouvelle copie sur un hôte cible. Ce processus est également rapide et efficace en termes de stockage.

Le tableau suivant récapitule les principales différences entre Oracle RMAN et le logiciel NetApp SnapCenter.

	Sauvegarde	**Restaurer**	**Clonage**	**Sauvegarde complète nécessaire**	**Utilisation de l'espace**	**Copie hors site**
RMAN	Lentes	Lentes	Lentes	Oui.	Élevée	Oui.
SnapCenter	Rapides	Rapides	Rapides	Non	Faible	Oui.

La figure suivante présente l'architecture SnapCenter.



Les configurations NetApp MetroCluster sont utilisées par des milliers d'entreprises à travers le monde pour offrir une haute disponibilité et une continuité de l'activité sans aucune perte de données au sein du data Center et au-delà. MetroCluster est une fonctionnalité gratuite du logiciel ONTAP qui met en miroir les données et la configuration de manière synchrone entre deux clusters ONTAP dans des emplacements distincts ou dans des domaines de défaillance. MetroCluster fournit un stockage disponible en continu pour les applications en gérant automatiquement deux objectifs : zéro objectif de point de restauration (RPO) en réalisant une mise en miroir synchrone des données écrites sur le cluster. Objectif de délai de restauration (RTO) proche de zéro en mettant en miroir la configuration et en automatisant l'accès aux données sur le second site. MetroCluster offre une mise en miroir simple et automatique des données et de la configuration entre les deux clusters indépendants situés sur les deux sites. Le stockage étant provisionné dans un cluster, il est automatiquement mis en miroir sur le second cluster sur le second site. La technologie NetApp SyncMirror offre une copie complète de toutes les données avec un RPO nul. , Par conséquent, les charges de travail d'un site peuvent basculer à tout moment vers le site opposé et continuer à transmettre des données sans perte de données. Vous trouverez plus d'informations "ici".

Mise en réseau

Une paire de commutateurs Cisco Nexus fournit des chemins redondants pour le trafic IP du calcul au stockage, et pour les clients externes du visualiseur d'images du système d'imagerie médicale :

- L'agrégation de liens qui utilise des canaux de port et des VPC est utilisée dans tout l'ensemble, ce qui permet d'obtenir une bande passante plus élevée et une haute disponibilité :
  - VPC est utilisé entre la baie de stockage NetApp et les commutateurs Cisco Nexus.
  - Le VPC est utilisé entre les Fabric Interconnect Cisco UCS et les commutateurs Cisco Nexus.
  - Chaque serveur dispose de cartes réseau virtuelles (vNIC) qui offrent une connectivité redondante à la structure unifiée. Le basculement de carte réseau est utilisé entre les interconnexions de fabric pour la redondance.
  - Chaque serveur dispose d'adaptateurs de bus hôte virtuels (vHBA) avec connectivité redondante à la

structure unifiée.

- Les interconnexions de fabric Cisco UCS sont configurées en mode hôte final comme recommandé, pour l'épinglage dynamique des cartes réseau vNIC sur les commutateurs uplink.
- Un réseau de stockage FC est fourni par une paire de commutateurs Cisco MDS.

Calcul - Cisco Unified Computing System

Deux structures Cisco UCS via des interconnexions de fabric différentes fournissent deux domaines à défaillance. Chaque structure est connectée aux commutateurs de réseau IP et à différents commutateurs de mise en réseau FC.

Nous avons créé des profils de service identiques pour chaque serveur lame Cisco UCS conformément aux meilleures pratiques de FlexPod pour exécuter VMware ESXi. Chaque profil de service doit disposer des composants suivants :

- Deux vNIC (une sur chaque structure) pour le trafic NFS, SMB/CIFS et client ou de gestion
- Autres VLAN nécessaires aux vNIC pour NFS, SMB/CIFS et le trafic client ou de gestion
- Deux vNIC (une sur chaque structure) pour le trafic iSCSI
- Deux HBA FC de stockage (une sur chaque structure) pour le trafic FC vers le stockage
- Démarrage SAN

Virtualisation

Le cluster hôte VMware ESXi exécute les VM charges de travail. Le cluster comprend des instances ESXi exécutées sur des serveurs lames Cisco UCS.

Chaque hôte ESXi comprend les composants réseau suivants :

- Démarrage SAN via FC ou iSCSI
- Démarrer des LUN sur un système de stockage NetApp (dans un FlexVol dédié pour le démarrage du système d'exploitation)
- Deux vmnics (Cisco UCS vNIC) pour NFS, SMB/CIFS ou le trafic de gestion
- Deux HBA de stockage (Cisco UCS FC vHBA) pour le trafic FC vers le stockage
- Commutateur standard ou commutateur virtuel distribué (selon les besoins)
- Datastore NFS pour les VM de workloads
- Gestion, réseau de trafic client et groupes de ports du réseau de stockage pour les VM
- Adaptateur réseau pour la gestion, le trafic client et l'accès au stockage (NFS, iSCSI ou SMB/CIFS) pour chaque machine virtuelle
- VMware DRS activé
- Chemins d'accès multiples natifs activés pour les chemins FC ou iSCSI vers le stockage
- Les snapshots VMware pour machine virtuelle sont désactivés
- Déploiement de NetApp SnapCenter pour les sauvegardes de machines virtuelles

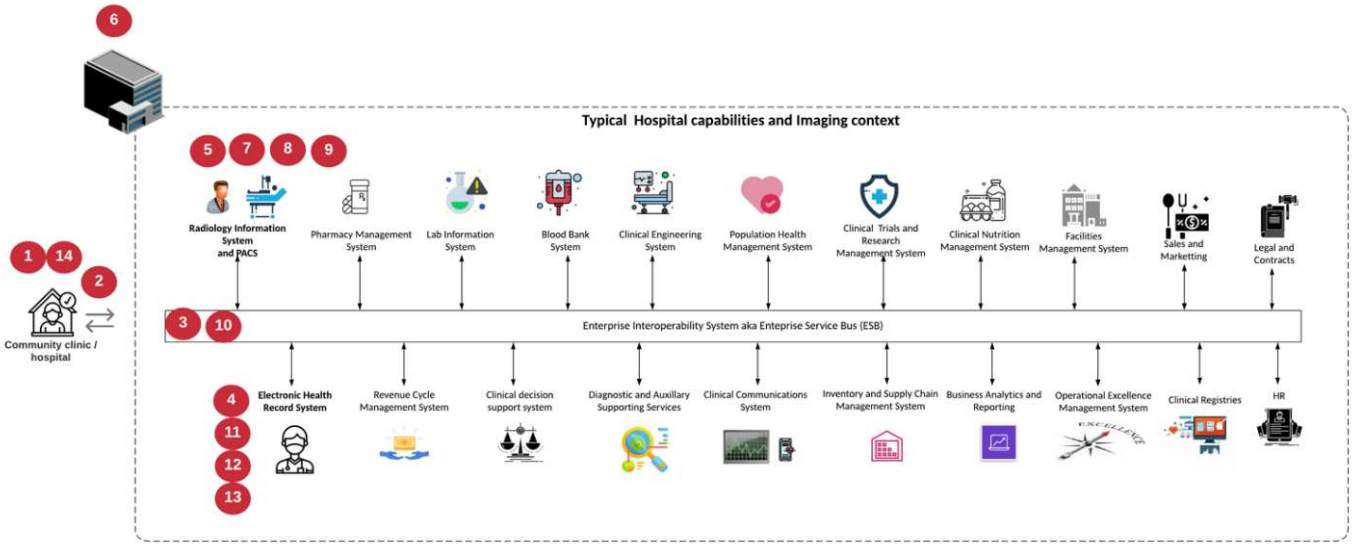
Architecture du système d'imagerie médicale

Dans les organismes de santé, les systèmes d'imagerie médicale sont des applications stratégiques. Ils sont parfaitement intégrés aux flux de travail cliniques, qui commencent dès le début de l'inscription des patients et

se terminent par les activités de facturation au cours du cycle de revenus.

Le schéma suivant présente les différents systèmes impliqués dans un grand hôpital typique ; ce schéma est conçu pour fournir un contexte architectural à un système d'imagerie médicale avant d'effectuer un zoom sur les composants architecturaux d'un système d'imagerie médicale classique. Les flux de travail varient considérablement, sont propres aux hôpitaux et à l'utilisation.

La figure ci-dessous illustre le système d'imagerie médicale dans le contexte d'un patient, d'une clinique communautaire et d'un grand hôpital.



1. Le patient visite la clinique communautaire avec des symptômes. Au cours de la consultation, le médecin de la communauté place une prescription d'imagerie envoyée à l'hôpital plus large sous la forme d'un message de prescription HL7.
2. Le système EHR du médecin de la communauté envoie le message HL7 Order/ORD au grand hôpital.
3. Le système d'interopérabilité de l'entreprise (également appelé bus de service d'entreprise [ESB]) traite le message de commande et envoie le message de commande au système EHR.
4. L'EHR traite le message de commande. Si aucun dossier patient n'existe, un nouveau dossier patient est créé.
5. L'EHR envoie une commande d'imagerie au système d'imagerie médicale.
6. Le patient appelle le grand hôpital pour un rendez-vous d'imagerie.
7. La réception d'imagerie et le bureau d'enregistrement programment le patient pour un rendez-vous d'imagerie à l'aide d'un système de radiologie ou d'un système similaire.
8. Le patient arrive pour le rendez-vous d'imagerie et les images ou la vidéo sont créées et envoyées au PACS.
9. Le radiologue lit les images et annote les images dans le PACS à l'aide d'un visualiseur de diagnostic graphique haut de gamme/GPU. Certains systèmes d'imagerie sont dotés de fonctionnalités d'amélioration de l'efficacité basées sur l'intelligence artificielle (IA) intégrées aux workflows d'imagerie.
10. Les résultats de l'ordre des images sont envoyés au DSE sous la forme d'un message HL7 ORU de résultats de prescription via le ESB.
11. L'EHR traite les résultats de la prescription dans le dossier du patient, place l'image miniature avec un lien contextuel vers l'image DICOM réelle. Les médecins peuvent lancer le visualiseur de diagnostic si une image de résolution plus élevée est nécessaire à partir de l'EHR.

12. Le médecin examine l'image et saisit les notes du médecin dans le dossier du patient. Le médecin pourrait utiliser le système d'aide à la décision clinique pour améliorer le processus d'examen et aider à diagnostiquer correctement le patient.
13. Le système EHR envoie ensuite les résultats de la commande sous la forme d'un message de résultats de la commande à l'hôpital communautaire. À ce stade, si l'hôpital communautaire pouvait recevoir l'image complète, alors l'image est envoyée via WADO ou DICOM.
14. Le médecin de la communauté effectue le diagnostic et fournit les prochaines étapes au patient.

Un système d'imagerie médicale classique utilise une architecture à plusieurs niveaux. Le composant central d'un système d'imagerie médicale est un serveur d'applications pour héberger divers composants d'application. Les serveurs d'applications classiques sont basés sur Java Runtime ou C# .Net CLR. La plupart des solutions d'imagerie médicale d'entreprise utilisent une base de données Oracle Server, MS SQL Server ou Sybase comme base de données primaire. En outre, certains systèmes d'imagerie médicale utilisent des bases de données pour l'accélération du contenu et la mise en cache sur une région géographique. Certains systèmes d'imagerie médicale d'entreprise utilisent également des bases de données NoSQL comme MongoDB, Redis, etc. En conjonction avec des serveurs d'intégration d'entreprise pour les interfaces ou API DICOM.

Un système d'imagerie médicale standard permet d'accéder aux images de deux groupes d'utilisateurs distincts : le diagnostique utilisateur/radiologue, le médecin ou le médecin traitant de l'imagerie.

En général, les radiologues utilisent des visionneuses de diagnostic haut de gamme compatibles avec des graphiques exécutées sur des postes de travail graphiques et de calcul haut de gamme qui sont physiques ou font partie d'une infrastructure de postes de travail virtuels. Si vous êtes sur le point de démarrer votre transition vers l'infrastructure de postes de travail virtuels, vous trouverez plus d'informations "ici" .

Lorsque l'ouragan Katrina a détruit deux des principaux hôpitaux d'enseignement de la Louisiane, les dirigeants se sont réunis et ont construit un système de dossiers médicaux électroniques résilient qui comprenait plus de 3000 000 bureaux virtuels en un temps record. Vous trouverez des informations supplémentaires sur les cas d'utilisation de l'architecture de référence et les bundles de référence FlexPod "ici".

Les médecins accèdent aux images de deux façons principales :

- **Accès basé sur le Web.** qui est généralement utilisé par les systèmes EHR pour intégrer les images PACS comme des liens contextuels dans le dossier médical électronique (EMR) du patient, et des liens qui peuvent être placés dans les flux de travail d'imagerie, les flux de travail de procédure, les flux de travail de notes de progression, etc. Les liens Web sont également utilisés pour fournir un accès aux images aux patients via les portails des patients. L'accès basé sur le Web utilise un modèle technologique appelé liens contextuels. Les liens contextuels peuvent être des liens statiques/URI vers le support DICOM directement ou des liens/URI générés dynamiquement à l'aide de macros personnalisées.
- * Client lourd.* certains systèmes médicaux d'entreprise vous permettent également d'utiliser une approche basée sur un client lourd pour visualiser les images. Vous pouvez lancer un client lourd à partir de l'EMR du patient ou en tant qu'application autonome.

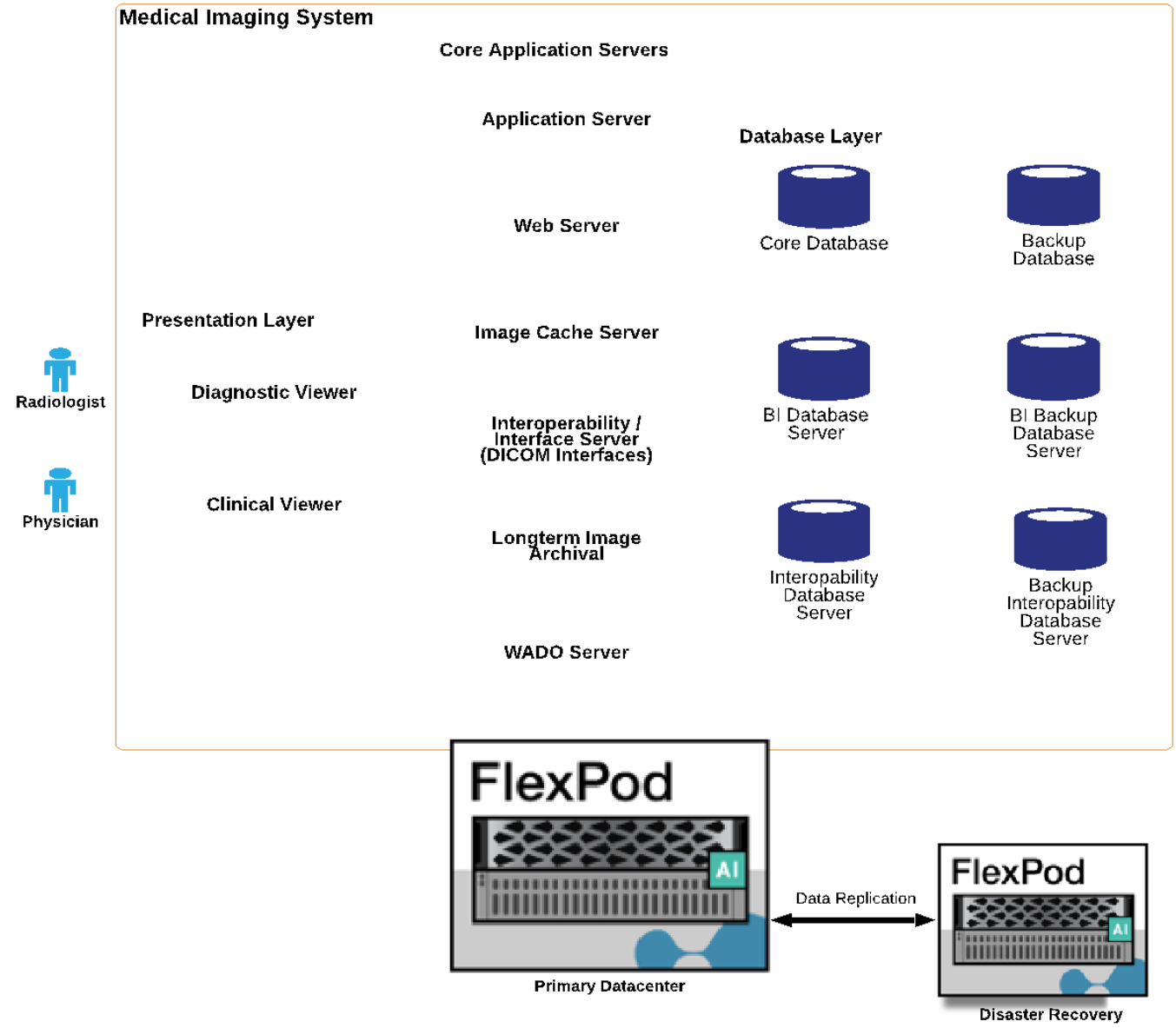
Le système d'imagerie médicale peut offrir un accès à l'image à une communauté de médecins ou à des médecins participants au CIN. Les systèmes d'imagerie médicale classiques incluent des composants qui assurent l'interopérabilité des images avec d'autres systèmes INFORMATIQUES de santé au sein et en dehors de votre établissement de santé. Les médecins de la communauté peuvent soit accéder aux images via une application Web, soit exploiter une plate-forme d'échange d'images pour l'interopérabilité des images. Les plates-formes d'échange d'images utilisent généralement WADO ou DICOM comme protocole d'échange d'images sous-jacent.

Les systèmes d'imagerie médicale peuvent également prendre en charge les centres médicaux universitaires

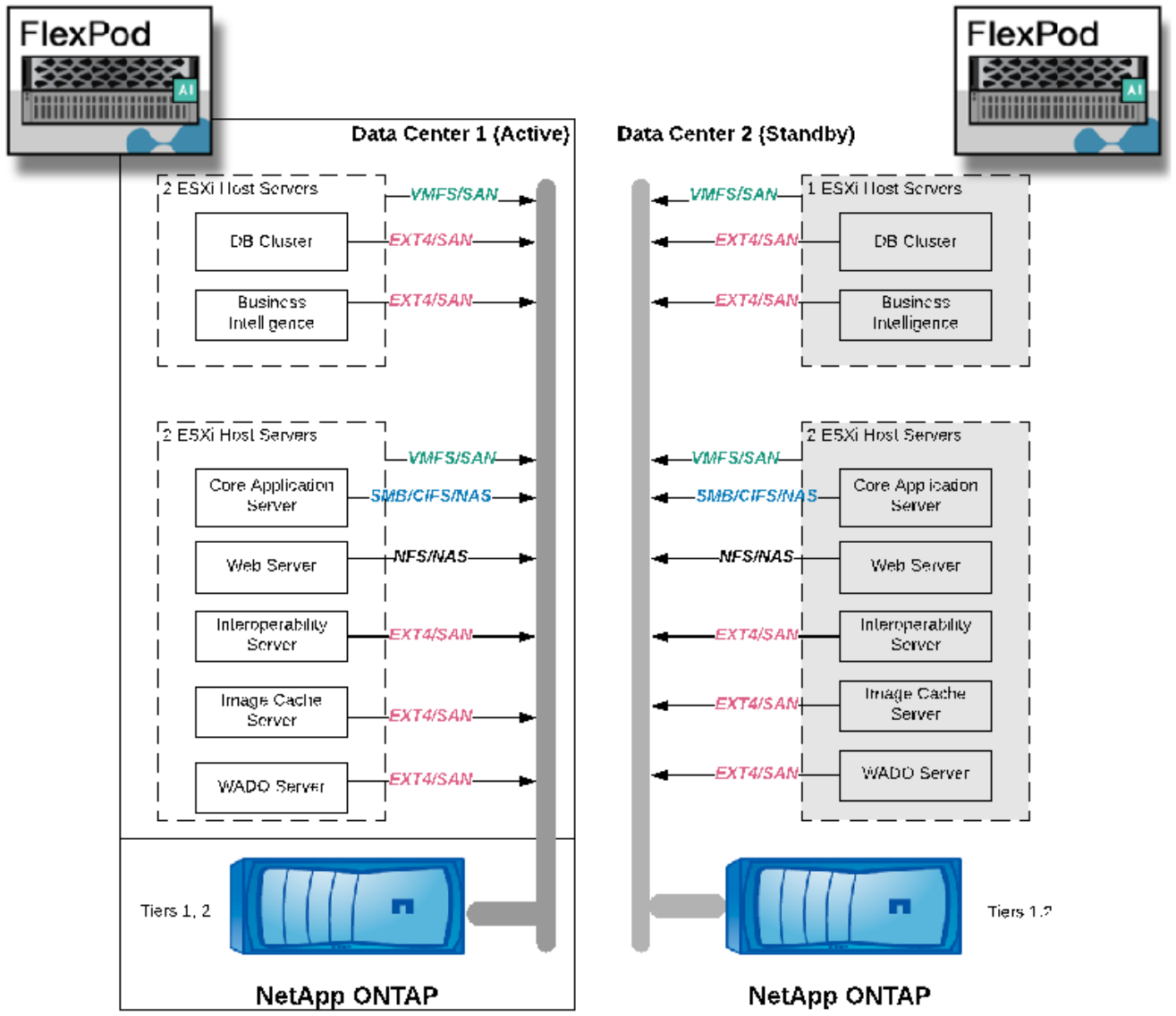
qui requièrent des systèmes PACS ou d'imagerie pour les utiliser en classe. Pour soutenir les activités universitaires, un système d'imagerie médicale classique peut disposer des capacités d'un système PACS dans un format plus compact ou dans un environnement d'imagerie uniquement pédagogique. Les systèmes d'archivage neutre typiques des fournisseurs et certains systèmes d'imagerie médicale de classe entreprise offrent des fonctionnalités de morphing d'étiquette d'image DICOM pour anonymiser les images utilisées à des fins d'enseignement. La morphing de tags permet à l'organisation de santé d'échanger des images DICOM entre des systèmes d'imagerie médicale de différents fournisseurs de manière neutre. De plus, la morphing de tags permet aux systèmes d'imagerie médicale de mettre en œuvre une fonctionnalité d'archivage neutre, à l'échelle de l'entreprise, pour les images médicales.

Les systèmes d'imagerie médicale commencent à "Capacités de calcul basées sur les GPU" améliorer les workflows humains en pré-traitant les images pour une efficacité accrue. Les systèmes d'imagerie médicale courants exploitent les meilleures fonctionnalités d'efficacité du stockage NetApp du secteur. Les systèmes d'imagerie médicale d'entreprise utilisent généralement RMAN pour les activités de sauvegarde, de restauration et de restauration. Pour améliorer les performances et réduire le temps nécessaire à la création des sauvegardes, la technologie Snapshot est disponible pour les opérations de sauvegarde et la technologie SnapMirror pour la réplication.

La figure ci-dessous présente les composants d'application logique dans une vue architecturale superposée.



La figure ci-dessous présente les composants de l’application physique.



Les composants d'application logique exigent que l'infrastructure prend en charge un ensemble varié de protocoles et de systèmes de fichiers. Le logiciel NetApp ONTAP prend en charge un ensemble de protocoles et de systèmes de fichiers leaders sur le marché.

Le tableau ci-dessous répertorie les composants de l'application, les protocoles de stockage et les exigences relatives au système de fichiers.

Composant d'application	SAN/NAS	Type de système de fichiers	Niveau de stockage	Type de réplication
Base de données de production de l'hôte VMware	rencontre locale	SAN	VMFS	Niveau 1
Client supplémentaire	Base de données de production de l'hôte VMware	REP	SAN	VMFS

Composant d'application	SAN/NAS	Type de système de fichiers	Niveau de stockage	Type de réplication
Niveau 1	Client supplémentaire	Application de production hôte VMware	rencontre locale	SAN
VMFS	Niveau 1	Client supplémentaire	Application de production hôte VMware	REP
SAN	VMFS	Niveau 1	Client supplémentaire	Serveur de base de données central
SAN	Ext4	Niveau 1	Client supplémentaire	Serveur de base de données de sauvegarde
SAN	Ext4	Niveau 1	Aucune	Serveur de cache d'images
NAS	SMB/CIFS	Niveau 1	Aucune	Serveur d'archivage
NAS	SMB/CIFS	Niveau 2	Client supplémentaire	Serveur Web
NAS	SMB/CIFS	Niveau 1	Aucune	Serveur WODO
SAN	NFS	Niveau 1	Client supplémentaire	Serveur de veille stratégique
SAN	NTFS	Niveau 1	Client supplémentaire	Sauvegarde de veille stratégique
SAN	NTFS	Niveau 1	Client supplémentaire	Serveur d'interopérabilité
SAN	Ext4	Niveau 1	Client supplémentaire	Serveur de base de données d'interopérabilité

Composants matériels et logiciels de l'infrastructure de la solution

Les tableaux ci-après répertorient les composants matériels et logiciels, respectivement, de l'infrastructure FlexPod pour le système d'imagerie médicale.

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1 ou 2	En fonction du nombre de lames nécessaires pour prendre en charge le nombre d'études annuelles
	Les serveurs lames Cisco UCS	B200 M5	Le nombre de lames basé sur le nombre d'études annuelles avec 2 x 20 cœurs ou plus, 2,7 GHz et 128 Go de RAM
	Carte d'interface virtuelle Cisco UCS (VIC)	Cisco UCS 1440	Voir la
	2 interconnexions de fabric Cisco UCS	6454 ou ultérieure	–
Le réseau	Commutateurs Cisco Nexus	2 gammes Cisco Nexus 3000 ou 9000	–
Réseau de stockage	Réseau IP pour l'accès au stockage via les protocoles SMB/CIFS, NFS ou iSCSI	Mêmes commutateurs réseau que ci-dessus	–
	Accès au stockage via FC	2 x Cisco MDS 9132T	–
Stockage	Système de stockage 100 % Flash NetApp AFF A400	1 paire HA ou plus	Cluster avec deux nœuds ou plus
	Tiroir disque	1 ou plus de tiroirs disques DS224C ou NS224	Plein avec 24 disques
	SSD	Pour 24, 1,2 To ou plus	–

Logiciel	Famille de produits	Version ou version	Détails
Système d'imagerie médicale d'entreprise			
	Serveur de base de données MS SQL ou Oracle	Comme le suggère le fournisseur du système d'imagerie médicale	
	Pas de bases de données SQL comme MongoDB Server	Comme le suggère le fournisseur du système d'imagerie médicale	
	Serveurs d'applications	Comme le suggère le fournisseur du système d'imagerie médicale	
	Serveur d'intégration (MS BizTalk, MuleSoft, Rhapsody, TIBCO)	Comme le suggère le fournisseur du système d'imagerie médicale	
	VM	Linux (64 bits)	
	VM	Windows Server (64 bits)	
Stockage	ONTAP	ONTAP 9.7 ou version ultérieure	
Le réseau	Fabric Interconnect Cisco UCS	Cisco UCS Manager 4.1 ou version ultérieure	
	Commutateurs Ethernet Cisco	9.2(3)I7(2) ou ultérieure	
	Cisco FC : Cisco MDS 9132T	8.4(2) ou ultérieure	
Hyperviseur	Hyperviseur	VMware vSphere ESXi 6.7 U2 ou version ultérieure	
Gestion	Système de gestion de l'hyperviseur	VMware vCenter Server 6.7 U1 (vCSA) ou ultérieure	
	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	
	SnapCenter	SnapCenter 4.3 ou version ultérieure	

Dimensionnement de la solution

Dimensionnement du stockage

Cette section décrit le nombre d'études et les exigences d'infrastructure correspondantes.

Les besoins en stockage répertoriés dans le tableau suivant supposent que les données existantes valent 1 an et que la croissance prévue pour un an d'étude dans le système primaire (niveau 1, 2). Les besoins en stockage supplémentaires liés à la croissance prévue d'au 3-delà des 2 premières années sont répertoriés séparément.

	Petit	Moyen	Grand
Études annuelles	<250 000 études	250 000 à 500 000 études	500 000 à 1 million d'études
Stockage de niveau 1			
IOPS (moyenne)	1,5 K À 5 KO	DE 5 000 À 15 000 TR/MIN	15 000 À 40 000
IOPS (pic)	5 000	20K	65 000
Débit	50–100 Mbit/s	50–150 Mbit/s	100–300 Mbit/s.
Data Center de capacité 1 (1 an de données anciennes et 1 an de nouvelle étude)	70 TO	140 TO	260 TO
Data Center de capacité 1 (besoin supplémentaire de 4 ans pour la nouvelle étude)	25 TO	45 TO	80 TO
Data Center de capacité 2 (1 an de données anciennes et 1 an de nouvelle étude)	45 TO	110TO	165 TO
Data Center de capacité 2 (besoin supplémentaire de 4 ans pour une nouvelle étude)	25 TO	45 TO	80 TO
Stockage de niveau 2			
IOPS (moyenne)	1 000	2K	3K
Data Center de capacité 1	320 TO	800 TO	2000 TO

Dimensionnement des ressources de calcul

Le tableau ci-dessous répertorie les exigences de calcul des systèmes d'imagerie médicale de petite, moyenne et grande taille.

	Petit	Moyen	Grand
Études annuelles	<250 000 études	250 000 à 500 000 études	500 000 à 1 million d'études
Data Center 1			
Nombre de VM	21	27	35
Nombre total de processeurs virtuels (CPU virtuels)	56	124	220
Mémoire totale requise	225GO	450 GO	900 GO

	Petit	Moyen	Grand
Spécifications du serveur physique (lames) (1 vCPU :=1 cœur)	4 serveurs avec 20 cœurs et 192 Go de RAM chacun	8 serveurs avec 20 cœurs et 128 Go de RAM chacun	14 serveurs avec 20 cœurs et 128 Go de RAM chacun
Data Center 2			
Nombre de VM	15	17	22
Nombre total de vCPU	42	72	140
Mémoire totale requise	179 GO	243GB	513 GO
Spécifications des serveurs physiques (lames) (1 CPU virtuel = 1 cœur)	3 serveurs avec 20 cœurs et 168 Go de RAM chacun	6 serveurs avec 20 cœurs et 128 Go de RAM chacun	8 serveurs avec 24 cœurs et 128 Go de RAM chacun

Mise en réseau et dimensionnement de l'infrastructure Cisco UCS

Le tableau ci-dessous répertorie les exigences de l'infrastructure réseau et Cisco UCS pour les systèmes d'imagerie médicale de petite, moyenne et grande taille.

	Petit	Moyen	Grand
Data Center 1			
Nombre de ports du nœud de stockage	2 adaptateurs réseau convergés (CNA) ; 2 CNA	2 CNA ; 2 CNA	2 CNA ; 2 CNA
Ports switchs réseau IP (Cisco Nexus 9000)	commutateur 48 ports	commutateur 48 ports	commutateur 48 ports
Commutateur FC (Cisco MDS)	commutateur 32 ports	commutateur 32 ports	commutateur 48 ports
Nombre de châssis Cisco UCS	1 x 5108	1 x 5108	2 x 5108
Fabric Interconnect Cisco UCS	2 x 6332	2 x 6332	2 x 6332
Data Center 2			
Nombre de châssis Cisco UCS	1 x 5108	1 x 5108	1 x 5108
Fabric Interconnect Cisco UCS	2 x 6332	2 x 6332	2 x 6332
Nombre de ports du nœud de stockage	2 CNA ; 2 CNA	2 CNA ; 2 CNA	2 CNA ; 2 CNA
Ports switchs réseau IP (Cisco Nexus 9000)	commutateur 48 ports	commutateur 48 ports	commutateur 48 ports
Commutateur FC (Cisco MDS)	commutateur 32 ports	commutateur 32 ports	commutateur 48 ports

Et des meilleures pratiques

Meilleures pratiques de stockage

Haute disponibilité

La conception du cluster de stockage NetApp garantit une haute disponibilité à tous les niveaux :

- Nœuds de cluster
- Connectivité du stockage interne
- RAID TEC, capable de gérer trois pannes de disque
- RAID DP pouvant supporter deux défaillances de disque
- Connectivité physique à deux réseaux physiques à partir de chaque nœud
- Plusieurs chemins de données vers les LUN et les volumes de stockage

Colocation sécurisée

Les SVM NetApp fournissent une infrastructure de baies de stockage virtuelles pour séparer votre domaine de sécurité, vos règles et votre réseau virtuel. NetApp recommande de créer des SVM distincts pour chaque organisation de locataires qui héberge les données sur le cluster de stockage.

Meilleures pratiques stockage NetApp

Prenez en compte les meilleures pratiques de stockage NetApp suivantes :

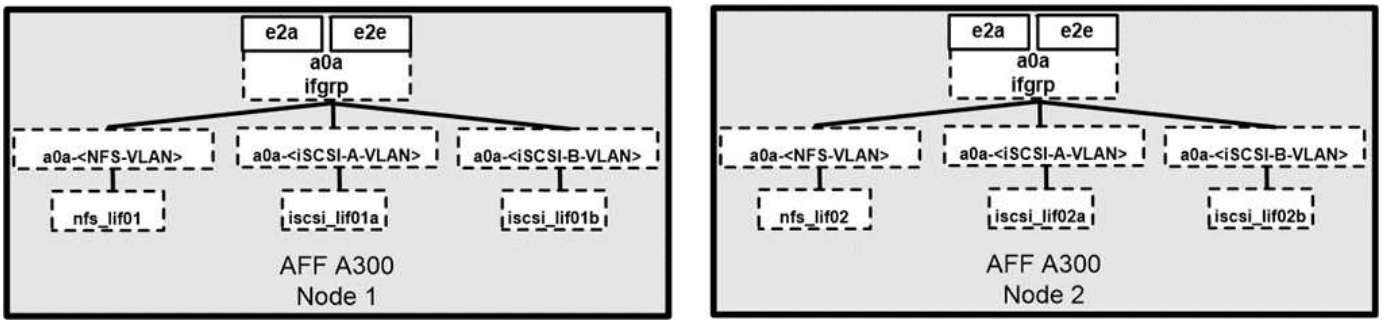
- Activez toujours la technologie NetApp AutoSupport, qui envoie à NetApp des informations récapitulatives sur le support via HTTPS.
- Pour optimiser la disponibilité et la mobilité, assurez-vous qu'une LIF est créée pour chaque SVM sur chaque nœud du cluster NetApp ONTAP. L'ALUA (Asymmetric Logical Unit Access) est utilisé pour analyser les chemins et identifier les chemins optimisés (directs) actifs au lieu de chemins non optimisés actifs. ALUA est utilisé pour les configurations FC ou FCoE et iSCSI.
- Un volume contenant uniquement des LUN n'a pas besoin d'être monté en interne, ni de chemin de jonction.
- Si vous utilisez le protocole CHAP (Challenge-Handshake Authentication Protocol) dans ESXi pour l'authentification de la cible, vous devez également le configurer dans ONTAP. Utiliser l'interface de ligne de commande (`vserver iscsi security create`) Ou NetApp ONTAP System Manager (modifiez la sécurité de l'initiateur sous Storage > SVM > Paramètres SVM > protocoles > iSCSI).

Démarrage SAN

NetApp recommande d'implémenter un démarrage SAN pour les serveurs Cisco UCS dans la solution de data Center FlexPod. Cette étape permet de sécuriser le système d'exploitation en toute sécurité grâce au système de stockage NetApp AFF, offrant ainsi de meilleures performances. La conception décrite dans cette solution utilise un démarrage SAN iSCSI.

Lors du démarrage SAN iSCSI, chaque serveur Cisco UCS est affecté à deux vNIC iSCSI (une pour chaque structure SAN), qui fournissent une connectivité redondante sur tout le réseau de stockage. Les ports de stockage dans cet exemple, e2a et e2e, qui sont connectés aux commutateurs Cisco Nexus, sont regroupés pour former un port logique appelé groupe d'interface (ifgrp) (dans cet exemple, a0A). Les VLAN iSCSI sont créés sur le groupe initiateur et les LIF iSCSI sont créées sur des groupes de ports iSCSI (dans cet exemple, a0A-<iSCSI-A-VLAN>). Le LUN de démarrage iSCSI est exposé aux serveurs via la LIF iSCSI en utilisant des

igroups. Cette approche permet uniquement au serveur autorisé d'accéder à la LUN de démarrage. Pour disposition des ports et LIF, voir la figure ci-dessous.



Contrairement aux interfaces réseau NAS, les interfaces réseau SAN ne sont pas configurées pour basculer en cas de défaillance. En revanche, si une interface réseau n'est plus disponible, l'hôte choisit un nouveau chemin optimisé vers une interface réseau disponible. ALUA, une norme prise en charge par NetApp, fournit des informations sur les cibles SCSI, qui permet à un hôte d'identifier le meilleur chemin d'accès au stockage.

Efficacité du stockage et provisionnement fin

NetApp s'est leader de l'innovation en matière d'efficacité du stockage, avec notamment la première déduplication pour les workloads primaires et la compaction des données à la volée qui améliore la compression et stocke les fichiers et E/S de petite taille. ONTAP prend en charge la déduplication à la volée et en arrière-plan, ainsi que la compression à la volée et en arrière-plan.

Pour bénéficier des avantages de la déduplication dans un environnement de blocs, les LUN doivent être à provisionnement fin. Bien que la LUN soit toujours visible par l'administrateur de vos machines virtuelles en prenant la capacité provisionnée, les économies de déduplication sont renvoyées vers le volume pour qu'il soit utilisé pour d'autres besoins. NetApp recommande de déployer ces LUN dans des volumes FlexVol également à provisionnement fin avec une capacité deux fois supérieure à la taille de la LUN. Lorsque vous déployez la LUN de cette manière, le volume FlexVol agit simplement comme un quota. Le stockage utilisé par la LUN est signalé dans le volume FlexVol et son agrégat de contenant.

Pour des économies de déduplication maximales, envisagez de planifier la déduplication en arrière-plan. Cependant, ces processus utilisent des ressources système lorsqu'ils sont en cours d'exécution. Dans l'idéal, il est préférable de les planifier pendant les heures moins actives (par exemple pendant les week-ends) ou de les exécuter plus fréquemment pour réduire la quantité de données modifiées à traiter. La déduplication automatique en arrière-plan sur les systèmes AFF a beaucoup moins d'impact sur les activités prioritaires. La compression en arrière-plan (pour les systèmes sur disque dur) consomme également des ressources. Vous devez donc l'envisager uniquement pour les charges de travail secondaires dont les besoins de performances sont limités.

Qualité de service

Les systèmes qui exécutent le logiciel ONTAP peuvent utiliser la fonctionnalité de qualité de services du stockage ONTAP pour limiter le débit en mégabits par seconde (Mbit/s) et limiter les IOPS pour différents objets de stockage tels que les fichiers, les LUN, les volumes, ou des SVM entiers. La QoS adaptative sert à définir un seuil et un plafond (QoS minimale) d'IOPS, qui s'ajustent dynamiquement en fonction de la capacité du datastore et de l'espace utilisé.

Les limites de débit permettent de contrôler les charges de travail inconnues ou de test avant un déploiement pour confirmer qu'elles n'affectent pas les autres charges de travail. Vous pouvez également utiliser ces limites pour contraindre une charge de travail dominante après son identification. Des niveaux minimaux de service basés sur des IOPS sont également pris en charge afin d'assurer des performances prévisibles pour les objets SAN d'ONTAP.

Avec un datastore NFS, une politique de qualité de services peut s'appliquer à tout le volume FlexVol ou à chaque fichier VMDK (Virtual machine Disk) de celui-ci. Avec les datastores VMFS (CSV (Cluster Shared volumes [CSV] dans Hyper-V) qui utilisent des LUN ONTAP, vous pouvez appliquer les règles de QoS au volume FlexVol qui contient les LUN ou aux LUN individuels. Toutefois, comme ONTAP ne connaît pas le VMFS, vous ne pouvez pas appliquer les règles de QoS à des fichiers VMDK individuels. Si vous utilisez les volumes virtuels VMware (VVol) avec VSC 7.1 ou version ultérieure, vous pouvez définir une QoS maximale sur des machines virtuelles individuelles à l'aide du profil de capacité de stockage.

Pour affecter une politique de QoS à une LUN, y compris VMFS ou CSV, vous pouvez obtenir le SVM ONTAP (affiché en tant que `Vserver`), chemin LUN et numéro de série dans le menu Storage Systems de la page d'accueil de VSC. Sélectionner le système de stockage (SVM), puis objets associés > SAN. Utilisez cette approche lorsque vous spécifiez la QoS en utilisant l'un des outils ONTAP.

Vous pouvez définir la limite de débit maximal QoS sur un objet en Mbit/s et en IOPS. Si vous utilisez les deux, la première limite atteinte est appliquée par ONTAP. Une charge de travail peut contenir plusieurs objets et une règle de QoS peut être appliquée à un ou plusieurs workloads. Lorsque vous appliquez une règle à plusieurs charges de travail, la limite totale de la règle est partagée par vos charges de travail. Les objets imbriqués ne sont pas pris en charge (par exemple, pour un fichier au sein d'un volume, ils ne peuvent pas chacun avoir leur propre stratégie). La valeur minimale de qualité de service peut être définie uniquement en IOPS.

Disposition du stockage

Cette section décrit les meilleures pratiques pour l'organisation des LUN, des volumes et des agrégats sur le stockage.

LUN de stockage

Pour des performances, une gestion et une sauvegarde optimales, NetApp recommande les meilleures pratiques suivantes en matière de conception des LUN :

- Créez un LUN distinct pour stocker les données de base de données et les fichiers journaux.
- Créez un LUN distinct pour chaque instance afin de stocker les sauvegardes des journaux de bases de données Oracle. Les LUN peuvent faire partie du même volume.
- Provisionner les LUN avec provisionnement fin (désactivez l'option réservation d'espace) pour les fichiers de base de données et les fichiers journaux.
- Toutes les données d'imagerie sont hébergées dans des LUN FC. Créez ces LUN dans les volumes FlexVol répartis sur les agrégats qui appartiennent à différents nœuds de contrôleur de stockage.

Pour placer les LUN dans un volume de stockage, suivez les instructions de la section suivante.

Volumes de stockage

Pour des performances et une gestion optimales, NetApp recommande les meilleures pratiques suivantes en matière de conception de volumes :

- Isolez les bases de données avec des requêtes exigeantes en E/S sur des volumes de stockage distincts
- Les fichiers de données peuvent être placés sur un seul LUN ou un volume, mais plusieurs volumes/LUN sont recommandés pour un débit plus élevé.
- Le parallélisme des E/S peut être atteint en utilisant n'importe quel système de fichiers pris en charge lorsque plusieurs LUN sont utilisées.
- Placement des fichiers de base de données et des journaux de transactions sur des volumes distincts pour une restauration plus granulaire.

- Envisagez d’utiliser des attributs de volume tels que la taille automatique, la réserve Snapshot, la QoS, etc.

64 bits

Les agrégats sont les conteneurs de stockage principaux pour les configurations de stockage NetApp et contiennent un ou plusieurs groupes RAID composés à la fois des disques de données et des disques de parité.

NetApp a effectué différents tests de caractérisation des charges de travail d’E/S à l’aide d’agrégats partagés et dédiés contenant des fichiers de données et des fichiers journaux de transactions séparés. Les tests montrent qu’un grand agrégat intégrant davantage de groupes et de disques RAID (disques durs ou SSD) optimise et améliore les performances du stockage, et qu’il est plus facile pour les administrateurs de gérer pour deux raisons :

- L’un des grands agrégats rend les capacités d’E/S de tous les disques disponibles pour tous les fichiers.
- Un seul grand agrégat permet d’optimiser l’utilisation de l’espace disque.

Pour une reprise après incident efficace, NetApp vous recommande de placer la réplique asynchrone sur un agrégat faisant partie d’un cluster de stockage distinct dans votre site de reprise après incident et d’utiliser la technologie SnapMirror pour répliquer du contenu.

Pour des performances de stockage optimales, NetApp recommande de disposer d’au moins 10 % d’espace libre dans un agrégat.

Les conseils relatifs à la disposition des agrégats de stockage pour les systèmes AFF A300 (avec deux tiroirs disques de 24 disques) comprennent :

- Conserver deux disques de secours.
- Le partitionnement de disque avancé permet de créer trois partitions sur chaque disque : racine et données.
- Utiliser un total de 20 partitions de données et deux partitions de parité pour chaque agrégat.

Meilleures pratiques de sauvegarde

NetApp SnapCenter est utilisé pour les sauvegardes des machines virtuelles et des bases de données. NetApp recommande les meilleures pratiques de sauvegarde suivantes :

- Lorsque SnapCenter est déployé pour créer des copies Snapshot pour les sauvegardes, désactivez la planification Snapshot pour le FlexVol qui héberge les machines virtuelles et les données d’applications.
- Créez un FlexVol dédié pour les LUN de démarrage hôte.
- Utilisation d’une stratégie de sauvegarde similaire ou unique pour les machines virtuelles qui servent le même objectif.
- Utilisez une règle de sauvegarde similaire ou unique pour chaque type de charge de travail ; par exemple, utilisez une règle similaire pour toutes les charges de travail de base de données. Utilisez différentes règles pour les bases de données, les serveurs Web, les postes de travail virtuels pour les utilisateurs finaux, etc.
- Activer la vérification de la sauvegarde dans SnapCenter.
- Configurer l’archivage des copies de sauvegarde Snapshot sur la solution de sauvegarde NetApp SnapVault
- Configurer la conservation des sauvegardes sur le stockage primaire en fonction du planning d’archivage.

Bonnes pratiques en matière d'infrastructure

Meilleures pratiques en matière de mise en réseau

NetApp recommande les meilleures pratiques suivantes en matière de mise en réseau :

- Vérifiez que votre système inclut des cartes réseau physiques redondantes pour le trafic de production et de stockage.
- VLAN séparés pour le trafic iSCSI, NFS et SMB/CIFS entre le calcul et le stockage
- Assurez-vous que votre système comprend un VLAN dédié pour l'accès client au système d'imagerie médicale.

Vous trouverez des pratiques d'excellence réseau supplémentaires dans les guides de conception et de déploiement d'infrastructure FlexPod.

Calculer les bonnes pratiques

Recommandation NetApp :

- Vérifiez que chaque CPU virtuel spécifié est pris en charge par un cœur physique.

Meilleures pratiques de virtualisation

NetApp recommande les meilleures pratiques de virtualisation suivantes :

- Utilisez VMware vSphere 6 ou version ultérieure.
- Définissez le BIOS du serveur hôte ESXi et la couche OS sur Custom Controlled–High Performance.
- Création de sauvegardes pendant les heures creuses.

Bonnes pratiques pour les systèmes d'imagerie médicale

Consultez les bonnes pratiques suivantes et certaines exigences d'un système d'imagerie médicale classique :

- Ne pas surallouer la mémoire virtuelle.
- Assurez-vous que le nombre total de vCPU équivaut au nombre de CPU physiques.
- Si vous disposez d'un environnement étendu, des VLAN dédiés sont nécessaires.
- Configurer des VM de base de données avec des clusters haute disponibilité dédiés
- S'assurer que les VMDK du système d'exploitation des machines virtuelles sont hébergés dans un stockage de niveau 1 rapide.
- En collaboration avec le fournisseur de systèmes d'imagerie médicale, déterminez la meilleure approche pour préparer les modèles de VM afin d'accélérer le déploiement et la maintenance.
- Les réseaux de gestion, de stockage et de production nécessitent une ségrégation LAN pour la base de données, avec des VLAN isolés pour VMware vMotion.
- Utilisez la technologie de réplication NetApp basée sur la baie de stockage "SnapMirror", appelée plutôt que la réplication basée sur vSphere.
- Utilisez les technologies de sauvegarde qui tirent parti des API VMware ; les fenêtres de sauvegarde doivent être en dehors des heures de production normales.

Conclusion

En exécutant un environnement d'imagerie médicale sur FlexPod, votre organisme de santé s'attend à améliorer la productivité de ses équipes ainsi qu'à diminuer les dépenses d'investissement et d'exploitation. Grâce à son partenariat stratégique, FlexPod fournit une infrastructure convergée prévalidée et rigoureusement testée. Il est conçu spécialement pour fournir des performances prévisibles avec une faible latence du système et une haute disponibilité. Cette approche permet d'améliorer l'expérience utilisateur et de bénéficier d'un temps de réponse optimal pour les utilisateurs du système d'imagerie médicale.

Les différents composants d'un système d'imagerie médicale nécessitent le stockage des données dans les systèmes de fichiers SMB/CIFS, NFS, Ext4 et NTFS. Par conséquent, votre infrastructure doit fournir un accès aux données via les protocoles NFS, SMB/CIFS et SAN. Les systèmes de stockage NetApp prennent en charge ces protocoles à partir d'une baie de stockage unique.

La haute disponibilité, l'efficacité du stockage, les sauvegardes rapides planifiées basées sur des copies Snapshot, les opérations de restauration rapide, la réplication des données pour la reprise après incident et les fonctionnalités de l'infrastructure de stockage FlexPod proposent un système de gestion et de stockage des données leader du marché.

Informations supplémentaires

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

- Guide de conception de FlexPod Datacenter pour l'IA/ML avec Cisco UCS 480 ML pour le deep learning

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- Infrastructure de data Center FlexPod avec VMware vSphere 6.7 U1, Cisco UCS de 4e génération et systèmes NetApp AFF A-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_datacenter_vmware_netappaffa.html"

- Description de la solution FlexPod Datacenter Oracle Database Backup with SnapCenter

  "https://www.netapp.com/us/media/sb-3999.pdf"

- FlexPod Datacenter avec bases de données Oracle RAC sur Cisco UCS et NetApp AFF A-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- FlexPod Datacenter avec Oracle RAC sur Oracle Linux

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- FlexPod pour Microsoft SQL Server

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- FlexPod de Cisco et NetApp

  "https://flexpod.com/"

- "Solutions NetApp pour MongoDB" Description de la solution (identifiant NetApp requis)

  "https://fieldportal.netapp.com/content/734702"

- Tr-4700 : plug-in SnapCenter pour base de données Oracle

  "https://www.netapp.com/us/media/tr-4700.pdf"

- Documentation produit NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- Solutions FlexPod pour infrastructure de postes de travail virtuels (VDI)

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

Infrastructure de bureau virtuel

FlexPod Datacenter avec Citrix Virtual Apps & Desktops 1912 LTSR et VMware vSphere 7 jusqu'à 6 6000 postes

Jeff Nichols, Cisco Suresh Thoppay, NetApp Dre Jackson, NetApp

Ce document fournit l'architecture et la conception d'une infrastructure de postes de travail virtuels pour un maximum de 6000 utilisateurs finaux. La solution est virtualisée sur des serveurs lames Cisco UCS B200 M5 de cinquième génération en démarrant VMware vSphere 7.01 Update 1 via un SAN FC à partir de la baie de stockage AFF A400. Les postes de travail virtuels sont optimisés avec Citrix Provisioning Server 1912 LTSR et Citrix RDS/Citrix Virtual Apps & Desktops 1912 LTSR, avec un mélange de postes de travail partagés hébergés par RDS (6000), de postes de travail virtuels regroupés et/ou non persistants sous Windows 10 (5000), Et des postes de travail Windows 10 virtuels hébergés en permanence, provisionnés avec Citrix machine Creation Services (5000) pour prendre en charge le nombre d'utilisateurs. Le cas échéant, ce document fournit des recommandations sur les meilleures pratiques et des instructions de dimensionnement pour le déploiement de cette solution par les clients.

"FlexPod Datacenter avec Citrix Virtual Apps ; Desktops 1912 LTSR et VMware vSphere 7 jusqu'à 6 6000 postes"

FlexPod Datacenter avec VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 et NetApp ONTAP 9.6 pour un maximum de 6 6700 postes

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Ce document fournit un guide de design et une architecture de référence pour les charges de travail de 5000 à 6000 postes de travail ainsi que l'environnement d'end-user computing sur FlexPod Datacenter avec Cisco UCS et NetApp AFF A300 et le logiciel de gestion des données NetApp ONTAP. La solution comprend les sessions RDS sur serveur VMware Horizon Windows Server 2019, les postes de travail virtuels de clone permanent VMware Horizon Microsoft Windows 10 et les postes de travail virtuels Microsoft Windows 10 de clone instantané et non persistants VMware Horizon sur VMware vSphere 6.7U2

"FlexPod Datacenter avec VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 et NetApp ONTAP 9.6 pour un maximum de 6 6700 postes"

Visualisation graphique 3D avec Citrix et NVIDIA - Livre blanc

Ce document décrit les performances de Citrix XenDesktop sur Citrix XenServer avec les

cartes NVIDIA Tesla P4, P6 et P40 sur les serveurs Cisco UCS C240 M5 et B200 M5 avec SPECviewperf 13.

"Visualisation graphique 3D avec Citrix et NVIDIA - Livre blanc"

FlexPod Datacenter avec Citrix XenDesktop/XenApp 7.15 et VMware vSphere 6.5 Update 1 pour 6 6000 postes

Vadim Lebedev, Cisco Chris Rodriguez, NetApp

Ce document présente l'architecture de référence pour la conception d'applications et de postes de travail virtuels à l'aide de Citrix XenApp/XenDesktop 7.15 basé sur Cisco UCS avec FAS un système de stockage NetApp AFF A300 et la plateforme d'hyperviseur VMware vSphere ESXi 6.5.

L'environnement de la virtualisation des postes de travail et des applications évolue en permanence. Associés à l'infrastructure éprouvée FlexPod, les nouveaux serveurs lames Cisco UCS haute performance M5 et Cisco UCS Unified Fabric offrent AFF une plateforme plus compacte, plus puissante, plus fiable et plus efficace.

"FlexPod Datacenter avec Citrix XenDesktop/XenApp 7.15 et VMware vSphere 6.5 Update 1 pour 6 6000 postes"

FlexPod Datacenter avec VMware Horizon View 7.3 et VMware vSphere 6.5 Update 1 avec Cisco UCS Manager 3.2 pour 6 5000 postes

Ramesh Guduru, Cisco David Arnette, NetApp

Ce document fournit une architecture de référence, un guide de design et un déploiement pour un environnement d'end-user computing comprenant jusqu'à 5000 postes de charge de travail mixtes dans le data Center FlexPod avec Cisco UCS et le système de stockage NetApp FAS 100 % Flash (AFF) A300. Cette solution comprend des sessions hébergées sur serveur Remote Desktop Server basées sur VMware Horizon, des postes de travail virtuels Microsoft Windows 10 persistants de VMware Horizon et des postes de travail virtuels de clone instantané Microsoft Windows 10 non persistants sur VMware vSphere 6.5.

"FlexPod Datacenter avec VMware Horizon View 7.3 et VMware vSphere 6.5 Update 1 avec Cisco UCS Manager 3.2 pour 6 5000 postes"

FlexPod Datacenter avec VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 et NetApp ONTAP 9.6 pour un maximum de 6 6700 postes

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Ce document fournit un guide de design et une architecture de référence pour un

environnement d’end-user computing de 5000 à 6000 postes de travail sur FlexPod Datacenter avec Cisco UCS et NetApp AFF A300 et le logiciel de gestion des données NetApp ONTAP. La solution inclut les sessions RDS sur serveur VMware Horizon Windows Server 2019, les postes de travail virtuels persistants VMware Horizon, le clone complet de Microsoft Windows 10 et les postes de travail virtuels Microsoft Windows 10 non persistants et instantanés VMware Horizon sur VMware vSphere 6.7 U2.

"FlexPod Datacenter avec VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 et NetApp ONTAP 9.6 pour un maximum de 6 6700 postes"

Applications modernes

FlexPod Datacenter pour l'IA et LE ML associés à Cisco UCS 480 ML pour le deep learning - Design

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Dans ce document, nous proposons des informations de conception relatives à l'intégration de la plateforme Cisco UCS C480 ML M5 à la solution FlexPod Datacenter afin de proposer une approche unifiée qui unifie les fonctionnalités d'IA et DE ML dans l'infrastructure convergée. Les clients peuvent ainsi gérer les serveurs à l'aide de fonctionnalités combinées d'IA et DE ML et des outils familiers qu'ils utilisent pour gérer les systèmes FlexPod classiques. Ils peuvent ainsi réduire de manière significative les charges administratives et le coût de déploiement de la plateforme de deep learning. Le design présenté dans ce CVD inclut également d'autres plateformes Cisco UCS, comme le serveur C220 M5 avec deux processeurs graphiques NVIDIA T4 et le serveur C240 M5 équipé de deux cartes PCIe NVIDIA V100 32 Gb comme options supplémentaires pour gérer simultanément les charges de travail d'IA et DE ML.

"FlexPod Datacenter pour l'intelligence artificielle et LE MACHINE LEARNING associés à Cisco UCS 480 ML pour le deep learning - Design"

Déployez le plug-in NetApp Trident CSI sur la plateforme de conteneurs Cisco avec FlexPod

Ce document présente des procédures détaillées de déploiement du plug-in NetApp Trident Container Storage interface (CSI) sur un cluster locataire Kubernetes de la plateforme de conteneurs Cisco dans une solution FlexPod.

"Déployez le plug-in NetApp Trident CSI sur la plateforme de conteneurs Cisco avec FlexPod"

FlexPod Datacenter pour OpenShift Container Platform 4 : déploiement

Haseeb Niazi, Cisco Alan Cowles, NetApp

Red Hat OpenShift est une plateforme de conteneurs Kubernetes pour entreprise qui gère les déploiements de cloud hybride et multicloud. Red Hat OpenShift Container Platform comprend tous les éléments nécessaires pour le cloud hybride, les conteneurs d'entreprise, ainsi que le développement et les déploiements Kubernetes. Il comprend un système d'exploitation Linux haute performance, un service d'exécution de conteneurs, une mise en réseau, une surveillance, un registre de conteneurs, des solutions d'authentification et d'autorisation.

L'association de Red Hat OpenShift à la solution FlexPod Datacenter simplifie le déploiement et la gestion de

l'infrastructure de conteneurs. Les clients peuvent bénéficier d'une efficacité accrue, d'une meilleure protection des données, d'une réduction des risques et de la flexibilité nécessaire pour faire évoluer cette pile d'infrastructure haute disponibilité afin de répondre aux nouveaux besoins de l'entreprise. L'approche de solution convergée prévalidée permet aux entreprises d'atteindre la vitesse, la flexibilité et l'évolutivité requises pour toutes leurs initiatives de modernisation des applications et de transformation digitale.

"FlexPod Datacenter pour OpenShift Container Platform 4 : déploiement"

FlexPod Datacenter avec Docker Enterprise Edition pour la gestion de conteneurs

Muhammad Afzal, Cisco John George, Cisco Amit Borulkar, NetApp Uday Shetty, Docker

Docker est la plateforme de conteneurs logiciels leader du secteur pour les développeurs et les équipes IT qui peuvent créer, expédier et exécuter des applications distribuées partout. L'architecture de microservices étant en train de façonner la nouvelle génération D'IT, les entreprises qui investissent massivement dans des applications monolithiques voient en Docker une stratégie qui leur permet de moderniser leurs architectures applicatives et d'assurer la compétitivité et la rentabilité de leur entreprise. La conteneurisation offre l'agilité, le contrôle et la portabilité dont les développeurs et LES équipes IT ont besoin pour créer et déployer des applications dans n'importe quelle infrastructure. La plateforme Docker permet de créer facilement des applications distribuées dans un conteneur d'applications léger qui peut évoluer de manière dynamique, mais sans interruption. Ainsi, les applications sont portables dans les environnements de développement, de test et de production s'exécutant sur des machines physiques ou virtuelles localement, dans des data centers et sur les réseaux de différents fournisseurs de services cloud.

"FlexPod Datacenter avec Docker Enterprise Edition pour la gestion de conteneurs"

FlexPod Datacenter pour OpenShift Container Platform 4 : conception

Haseeb Niazi, Cisco Alan Cowles, NetApp

Cisco et NetApp se sont associés pour proposer une gamme de solutions FlexPod compatibles avec des plateformes de data Center stratégiques. La solution FlexPod propose une architecture intégrée qui intègre les meilleures pratiques en matière de calcul, de stockage et de conception réseau, réduisant ainsi les risques INFORMATIQUES en validant l'architecture intégrée pour assurer la compatibilité entre les différents composants. La solution répond également aux problématiques IT en fournissant des conseils de conception, des conseils de déploiement et un support documentés qui peuvent être utilisés à différentes étapes (planification, conception et implémentation) d'un déploiement.

"FlexPod Datacenter pour OpenShift Container Platform 4 : conception"

FlexPod Datacenter pour l’intelligence artificielle et LE MACHINE LEARNING associés à Cisco UCS 480 ML pour le deep learning - déploiement

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Ce document détaille le déploiement et propose des conseils concernant l’intégration de la plateforme Cisco UCS C480 ML M5 à la solution de data Center FlexPod afin de proposer une approche unifiée pour fournir des fonctionnalités d’IA et DE ML dans l’infrastructure convergée. Ce document présente également la configuration des processeurs graphiques NVIDIA sur les plateformes Cisco UCS C220 et C240. Pour une description détaillée de la conception des plateformes et technologies utilisées dans cette solution, reportez-vous au "FlexPod Datacenter pour une combinaison de l’IA et DU ML avec Cisco UCS 480 ML pour la conception du deep learning".

"FlexPod Datacenter pour l’intelligence artificielle et LE MACHINE LEARNING associés à Cisco UCS 480 ML pour le deep learning - déploiement"

Visualisation graphique 3D avec VMware et NVIDIA sur Cisco UCS - Livre blanc

Ce document décrit les performances de l’hyperviseur VMware ESXi et de VMware Horizon avec la solution NVIDIA Tesla P4, P6 et P40 sur serveurs rack Cisco UCS C240 M5 et serveurs lames B200 M5.

"Visualisation graphique 3D avec VMware et NVIDIA sur Cisco UCS - Livre blanc"

Visualisation graphique 3D avec Citrix et NVIDIA - Livre blanc

Ce document décrit les performances de Citrix XenDesktop sur Citrix XenServer avec les cartes NVIDIA Tesla P4, P6 et P40 sur les serveurs Cisco UCS C240 M5 et B200 M5 avec SPECviewperf 13.

"Visualisation graphique 3D avec Citrix et NVIDIA - Livre blanc"

FlexPod Express

Guide de design de FlexPod Express avec Cisco UCS C-Series et NetApp AFF C190

NVA-1139-DESIGN : FlexPod Express avec Cisco UCS C-Series et NetApp AFF C190 Series

Savita Kumari, NetApp

En partenariat avec : 

Les tendances du secteur témoignent d'une vaste transformation des data centers en infrastructure partagée et cloud computing. Les entreprises ont également besoin d'une solution simple et efficace pour leurs succursales et bureaux distants qui exploitent la technologie qu'elles connaissent bien dans leur data Center.

FlexPod Express est une architecture de data Center préconçue et conforme aux bonnes pratiques. Elle repose sur la plateforme Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus et les systèmes NetApp AFF. Les composants de FlexPod Express sont similaires à ceux de leurs homologues FlexPod Datacenter, ce qui favorise une gestion plus efficace de l'environnement de l'infrastructure INFORMATIQUE complète à petite échelle. Les plateformes FlexPod Datacenter et FlexPod Express sont optimales pour la virtualisation, et pour les systèmes d'exploitation sans système d'exploitation et les charges de travail d'entreprise.

"Suivant : résumé du programme."

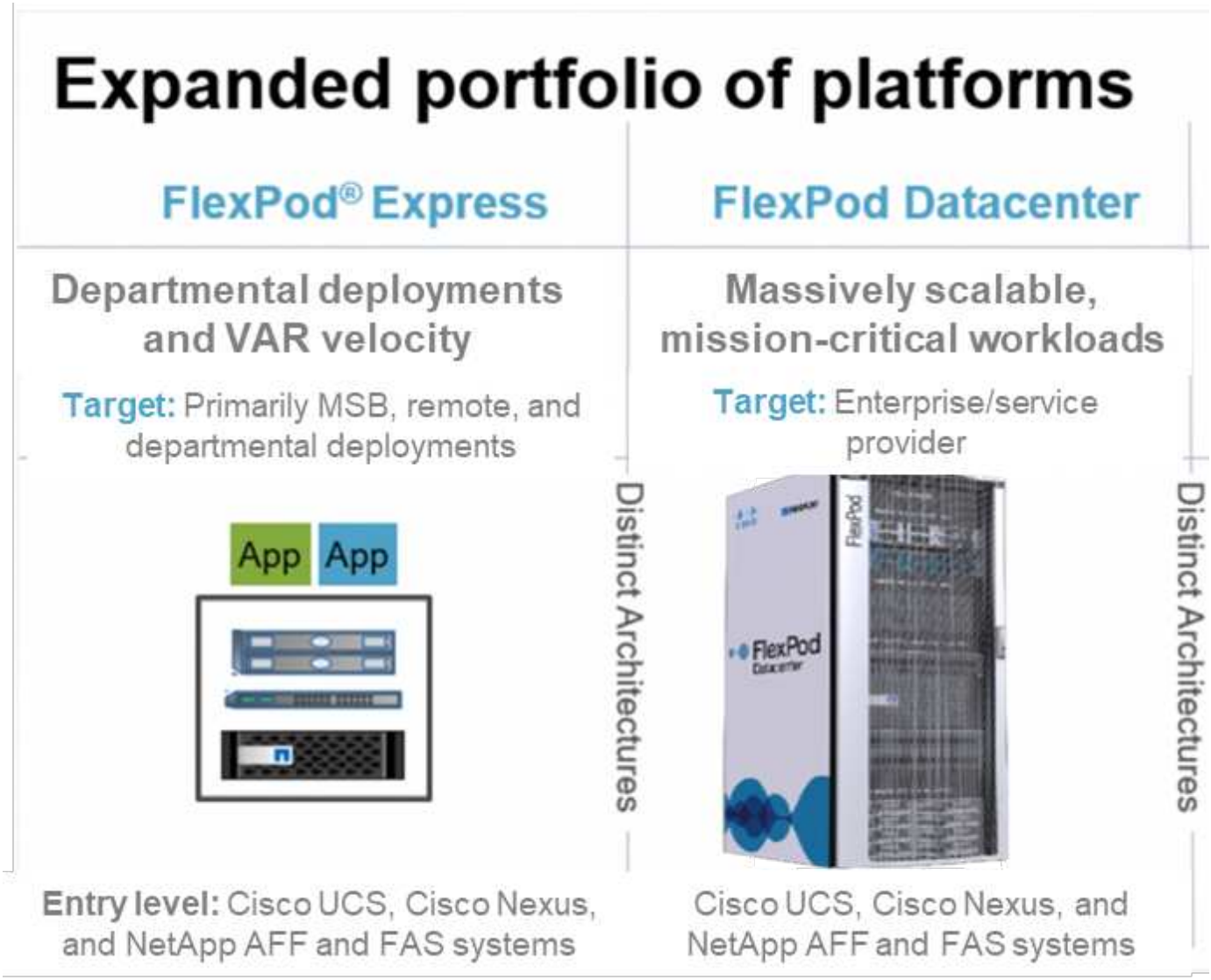
Récapitulatif du programme

Le portefeuille de solutions d'infrastructure convergée FlexPod

Les architectures de référence FlexPod sont fournies sous la forme de designs validés par Cisco (CVD) ou d'architectures vérifiées par NetApp (NVA). Les écarts basés sur les exigences des clients pour une CVD ou une NVA donnée sont autorisés si ces variations n'entraînent pas le déploiement de configurations non prises en charge.

Comme illustré dans la figure suivante, la gamme FlexPod inclut les solutions suivantes : FlexPod Express et FlexPod Datacenter.

- **FlexPod Express** est une solution d'entrée de gamme dotée des technologies de Cisco et de NetApp.
- **FlexPod Datacenter** offre une base polyvalente optimale pour diverses charges de travail et applications.



Programme d'architecture vérifiée NetApp

Le programme d'architecture vérifiée NetApp propose une architecture validée pour les solutions NetApp Une solution NVA offre les qualités suivantes :

- Testée en profondeur
- Normative par nature
- Réduction des risques de déploiement
- Accélérer la mise sur le marché ce guide détaille le design de FlexPod Express avec VMware vSphere.

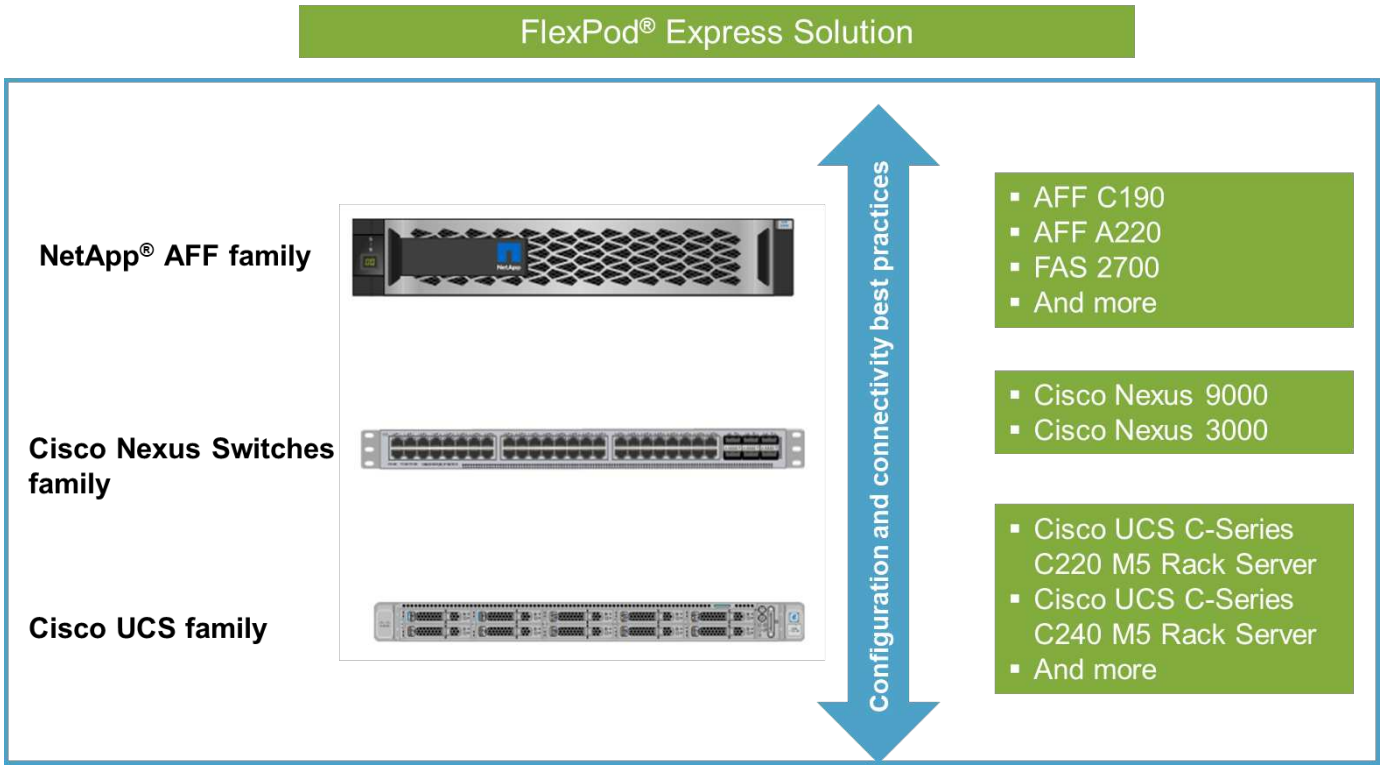
Cette conception tire également parti du tout nouveau système AFF C190, qui exécute le logiciel NetApp ONTAP 9.6, des switchs Cisco Nexus 31108 et des serveurs Cisco UCS C220 M5 comme nœuds d'hyperviseur.

Présentation de la solution

FlexPod Express est conçu pour exécuter des charges de travail de virtualisation mixtes. Elle est destinée aux bureaux distants, aux succursales et aux moyennes entreprises. Il convient également aux grandes entreprises qui souhaitent mettre en œuvre une solution dédiée pour un usage spécifique. Cette nouvelle solution pour FlexPod Express inclut de nouvelles technologies telles que NetApp ONTAP 9.6, le système

NetApp AFF C190 et VMware vSphere 6.7U2.

La figure suivante présente les composants matériels inclus dans la solution FlexPod Express.

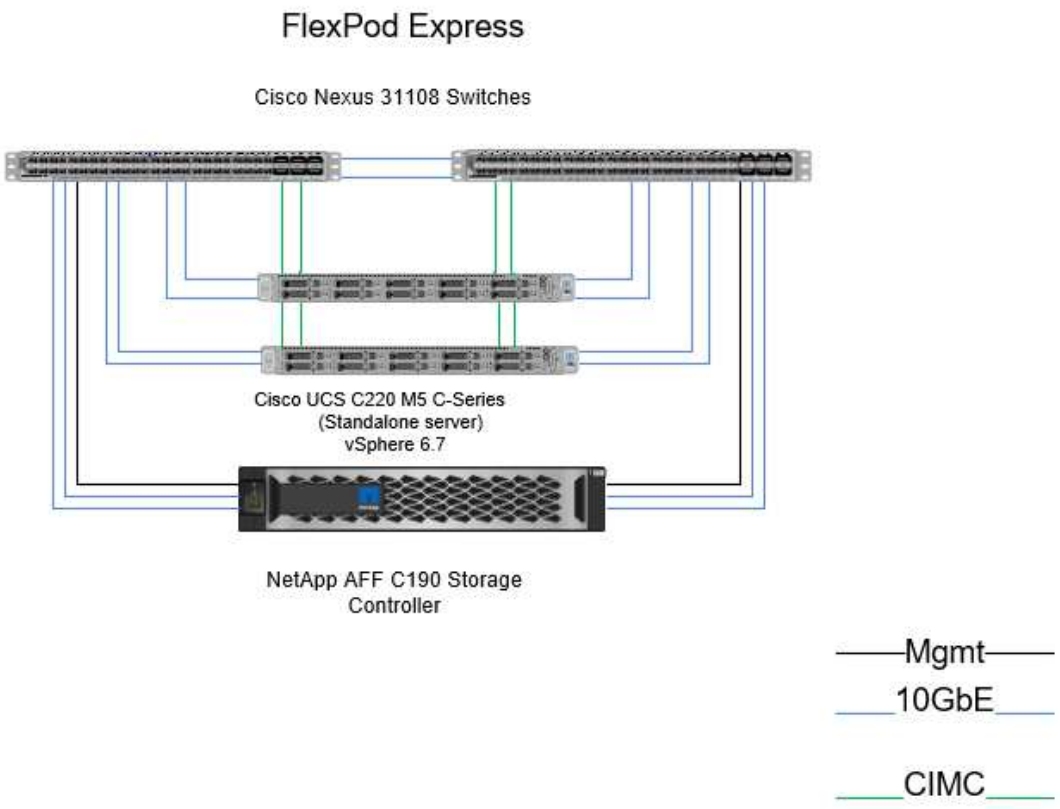


Public visé

Ce document est destiné à ceux qui souhaitent tirer parti d'une infrastructure conçue pour optimiser l'efficacité IT et favoriser l'innovation IT. Le public cible de ce document inclut, sans s'y limiter, les ingénieurs commerciaux, les consultants sur le terrain, le personnel des services professionnels, les responsables INFORMATIQUES, les ingénieurs partenaires et les clients.

Technologie de la solution

Cette solution tire parti des dernières technologies de NetApp, Cisco et VMware. Le nouveau système NetApp AFF C190, qui exécute le logiciel ONTAP 9.6, deux switchs Cisco Nexus 31108 et des serveurs rack Cisco UCS C220 M5 exécutant VMware vSphere 6.7U2. Cette solution validée, illustrée dans la figure suivante, utilise une technologie 10 Gigabit Ethernet (10GbE). Des conseils sont également fournis sur la manière d'évoluer en ajoutant deux nœuds d'hyperviseur à la fois afin que l'architecture FlexPod Express puisse s'adapter aux besoins commerciaux en constante évolution de l'entreprise.



"Ensuite, les exigences technologiques."

Exigences technologiques

FlexPod Express requiert une combinaison de composants matériels et logiciels qui dépend de l'hyperviseur et de la vitesse réseau sélectionnés. En outre, FlexPod Express dispose des composants matériels requis pour ajouter des nœuds d'hyperviseur au système par unités 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 changent, vous pouvez utiliser un hyperviseur différent sur le même matériel FlexPod Express.

Les composants matériels requis pour cette configuration FlexPod Express sont répertoriés dans le tableau suivant. Les composants matériels utilisés dans toute implémentation de cette solution peuvent varier en fonction des besoins du client.

Sous-jacent	Quantité
Cluster AFF C190 à 2 nœuds	1
Serveur Cisco UCS C220 M5	2
Commutateur Cisco Nexus 31108	2

Sous-jacent	Quantité
Cisco UCS Virtual interface Card (VIC) 1457 pour serveur en rack Cisco UCS C220 M5	2

Configuration logicielle requise

Les composants logiciels requis pour l'implémentation des architectures de la solution FlexPod Express sont répertoriés dans le tableau suivant.

Logiciel	Version	Détails
Contrôleur de gestion intégrée Cisco (CIMC)	4.0.4	Pour serveurs en rack C220 M5
Cisco NX-OS	7.0(3)I7(6)	Pour les commutateurs Cisco Nexus 31108
NetApp ONTAP	9.6	Pour les contrôleurs NetApp AFF C190

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

Logiciel	Version
Appliance VMware vCenter Server	6.7U2
VMware vSphere ESXi	6.7U2
Plug-in NetApp VAAI pour ESXi	1.1.2
NetApp Virtual Storage Console	9.6

"Suivant : choix de conception."

Choix de conception

Les technologies répertoriées dans cette section ont été choisies au cours de la phase de conception architecturale. Chaque technologie répond à un usage spécifique de la solution d'infrastructure FlexPod Express.

NetApp AFF C190 Series avec ONTAP 9.6

Cette solution tire parti de deux des derniers produits NetApp : le système NetApp AFF C190 et le logiciel ONTAP 9.6.

Système AFF C190

Ce groupe cible est les clients qui souhaitent moderniser leur infrastructure IT avec une technologie 100 % Flash à un prix abordable. Le système AFF C190 est fourni avec le nouveau ONTAP 9.6 et la licence pack Flash, ce qui signifie que les fonctions suivantes sont intégrées :

- CIFS, NFS, iSCSI et FCP
- Logiciel de réplication des données NetApp SnapMirror, logiciel de sauvegarde NetApp SnapVault, logiciel

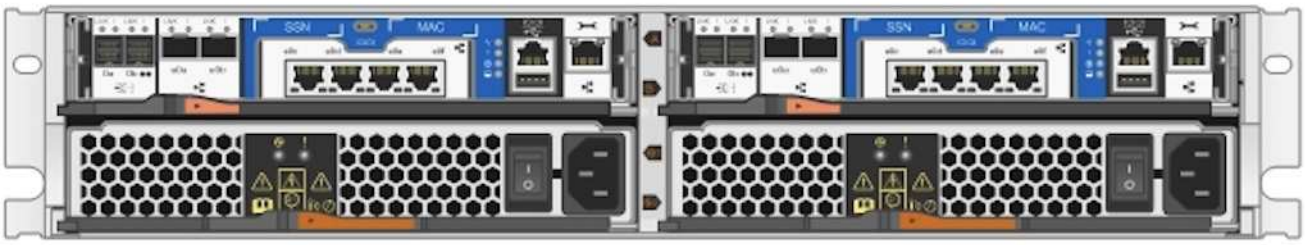
de restauration des données NetApp SnapRestore, suite logicielle de gestion du stockage NetApp SnapManager et logiciel NetApp SnapCenter

- Technologie FlexVol
- Déduplication, compression et compaction
- Provisionnement fin
- QoS du stockage
- Technologie NetApp RAID DP
- Technologie Snapshot de NetApp
- FabricPool

Les figures suivantes illustrent les deux options de connectivité hôte.

La figure suivante illustre les ports UTA 2 dans lesquels le module SFP+ peut être inséré.

La figure suivante illustre les ports 10GBASE-T pour la connexion via des câbles Ethernet RJ-45 traditionnels.



Pour l'option de port 10GBASE-T, vous devez disposer d'un commutateur uplink basé sur 10GBASE-T.

Le système AFF C190 est proposé exclusivement avec des SSD de 960 Go. Les extensions sont au choix en quatre étapes :

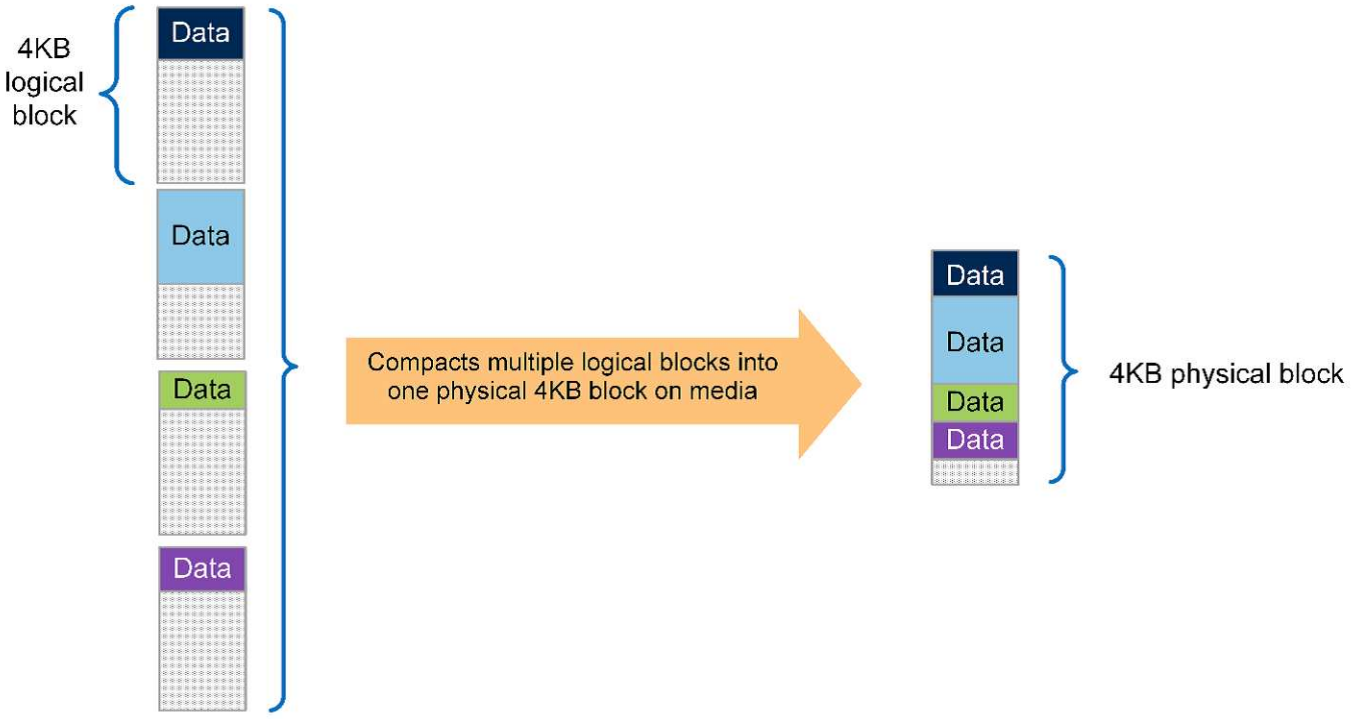
- 8 x 960 Go
- 12 x 960 Go
- 18 x 960 Go
- 24 x 960 Go

Pour obtenir des informations complètes sur le système matériel AFF C190, consultez la "Page dédiée aux baies 100 % Flash NetApp AFF C190".

Le logiciel ONTAP 9.6

Les systèmes NetApp AFF C190 utilisent le nouveau logiciel de gestion des données ONTAP 9.6. ONTAP 9.6 est le logiciel de gestion des données d'entreprise leader du secteur. Il allie une simplicité et une flexibilité inédites à de puissantes fonctionnalités de gestion des données, d'efficacité du stockage et d'intégration cloud.

ONTAP 9.6 propose plusieurs fonctionnalités particulièrement adaptées à la solution FlexPod Express. L'engagement de NetApp en faveur de l'efficacité du stockage est avant tout primordial, ce qui peut constituer l'une des fonctionnalités les plus importantes pour les déploiements de petite taille. ONTAP 9.6 propose les fonctionnalités d'efficacité du stockage de NetApp, telles que la déduplication, la compression, la compaction et le provisionnement fin. Le système WAFL de NetApp écrit toujours des blocs de 4 Ko. Par conséquent, la compaction combine plusieurs blocs dans un bloc de 4 Ko lorsque l'espace alloué des blocs de 4 Ko. La figure suivante illustre ce processus.



ONTAP 9.6 prend désormais en charge une taille de bloc de 512 octets en option pour les volumes NVMe. Cette fonctionnalité est très efficace avec le VMFS (Virtual machine File System) de VMware, qui utilise de manière native un bloc de 512 octets. Vous pouvez conserver la taille 4K par défaut ou définir la taille de bloc de 512 octets.

ONTAP 9.6 inclut d'autres améliorations :

- **NetApp Aggregate Encryption (NAE).** NAE attribue des clés au niveau de l'agrégat, en cryptant ainsi tous les volumes de l'agrégat. Cette fonctionnalité permet le chiffrement et la déduplication des volumes au niveau des agrégats.
- **Amélioration du volume NetApp ONTAP FlexGroup**. Dans ONTAP 9.6, vous pouvez facilement renommer un volume FlexGroup. Nul besoin de créer un nouveau volume pour migrer les données vers. La taille du volume peut également être réduite via ONTAP System Manager ou l'interface de ligne de commande.
- **Améliorations FabricPool.** ONTAP 9.6 a ajouté une prise en charge supplémentaire pour les magasins d'objets en tant que niveaux cloud. La prise en charge de Google Cloud et d'Alibaba Cloud Object Storage Service (OSS) a également été ajoutée à la liste. FabricPool prend en charge plusieurs magasins d'objets, notamment AWS S3, Azure Blob, le stockage objet IBM Cloud et le logiciel de stockage objet NetApp

StorageGRID.

- **Amélioration de SnapMirror.** dans ONTAP 9.6, une nouvelle relation de réplication de volume est chiffrée par défaut avant de quitter la baie source et déchiffrée à la destination SnapMirror.

Cisco Nexus 3000 Series

Le Cisco Nexus 31108PC-V est un switch Tor (Top of rack) basé sur SFP+ 10 Gbit/s avec 48 ports SFP+ et 6 ports QSFP28. Chaque port SFP+ peut fonctionner en 100 Mbit/s, 10 Gbit/s et chaque port QSFP28 peut fonctionner en mode natif 100 Gbit/s ou 40 Gbit/s, ou 4 Gbit/s, offrant des options de migration flexibles. Ce commutateur est un véritable commutateur sans PHY optimisé pour une faible latence et une faible consommation d'énergie.

La spécification Cisco Nexus 31108PC-V comprend les composants suivants :

- Capacité de commutation de 2,16 Tbit/s et vitesse de transfert allant jusqu'à 1,2 Tbit/s pour 31108PC-V.
- 48 ports SFP prennent en charge 1 et 10 ports Gigabit Ethernet (10GbE) ; 6 ports QSFP28 prennent en charge 4 ports 10 GbE ou 40 GbE chacun ou 100 GbE

La figure suivante illustre le commutateur Cisco Nexus 31108PC-V.

Pour plus d'informations sur les commutateurs Cisco Nexus 31108PC-V, reportez-vous à la section "Fiche technique des commutateurs Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL et 3172TQ-XL".

Cisco UCS C-Series

Le serveur en rack Cisco UCS C-Series a été choisi pour FlexPod Express, car ses nombreuses options de configuration le permettent d'être personnalisé pour des exigences spécifiques dans un déploiement FlexPod Express.

Les serveurs en rack Cisco UCS C-Series offrent une solution informatique unifiée dans un format standard afin de réduire le coût total de possession et d'accroître l'agilité.

Les serveurs en rack Cisco UCS C-Series offrent les avantages suivants :

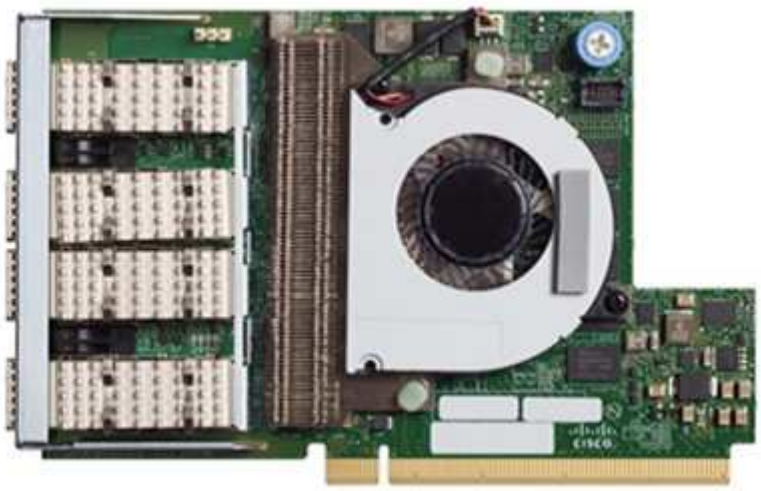
- Un point d'entrée indépendant des formats dans Cisco UCS
- Un déploiement simplifié et rapide des applications
- Extension des innovations et avantages de l'informatique unifiée aux serveurs rack
- Un plus grand choix pour les clients avec des avantages uniques dans un pack rack familier

Le serveur en rack Cisco UCS C220 M5, présenté dans la figure ci-dessus, est l'un des serveurs applicatifs et d'infrastructure d'entreprise polyvalents les plus polyvalents du marché. Il s'agit d'un serveur en rack à deux sockets haute densité qui offre des performances et une efficacité de pointe pour une large gamme de charges de travail, notamment pour la virtualisation, la collaboration et les applications sans système d'exploitation. Les serveurs en rack Cisco UCS C-Series peuvent être déployés en tant que serveurs autonomes ou en tant que partie intégrante de Cisco UCS afin de tirer parti des innovations de Cisco en matière d'informatique unifiée, qui contribuent à réduire le coût total de possession des clients et à accroître leur souplesse commerciale.

Pour plus d'informations sur les serveurs C220 M5, reportez-vous à la section "Fiche technique du serveur rack Cisco UCS C220 M5".

Connectivité Cisco UCS VIC 1457 pour serveurs en rack C220 M5

L'adaptateur Cisco UCS VIC 1457 illustré dans la figure suivante est une carte LAN modulaire à quatre ports Small Form-factor pluggable (SFP28) sur carte mère (mLOM) conçue pour la génération M5 de serveurs Cisco UCS C-Series. La carte supporte Ethernet 10/25 Gbit/s ou FCoE. La carte peut présenter à l'hôte des interfaces conformes aux normes PCIe, qui peuvent être configurées dynamiquement en tant que cartes réseau ou HBA.



Pour obtenir des informations complètes sur l'adaptateur Cisco UCS VIC 1457, consultez la page "Fiche technique sur la carte d'interface virtuelle Cisco UCS série 1400".

VMware vSphere 6.7U2

VMware vSphere 6.7U2 est l'une des options d'hyperviseur qui s'utilise avec FlexPod Express. VMware vSphere permet aux entreprises de réduire leur empreinte électrique et de climatisation tout en bénéficiant de la pleine capacité de calcul achetée. De plus, VMware vSphere permet une protection contre les défaillances matérielles (VMware High Availability ou VMware HA), ainsi qu'un équilibrage de la charge des ressources de calcul sur un cluster d'hôtes vSphere (VMware Distributed Resource Scheduler en mode maintenance ou VMware DRS-MM).

Comme il ne redémarre que le noyau, VMware vSphere 6.7U2 permet aux clients de démarrer rapidement, de charger vSphere ESXi sans redémarrer le matériel. Le client vSphere 6.7U2 (client basé sur HTML5) comporte de nouvelles améliorations telles que Developer Center avec Code Capture et API Explore. Avec la fonction de capture de code, vous pouvez enregistrer vos actions dans le client vSphere pour générer une sortie de code simple et utilisable. VSphere 6.7U2 contient également de nouvelles fonctionnalités telles que DRS en mode maintenance (DRS-MM).

VMware vSphere 6.7U2 offre les fonctionnalités suivantes :

- VMware dépecation du modèle de déploiement externe de VMware Platform Services Controller (PSC).

> À compter de la prochaine version majeure de vSphere, un PSC externe ne sera pas disponible.

- Prise en charge du nouveau protocole pour la sauvegarde et la restauration d'une appliance vCenter Server. Présentation de NFS et SMB comme choix de protocoles pris en charge, jusqu'à 7 au total (HTTP, HTTPS, FTP, FTPS, SCP, NFS et SMB) lors de la configuration d'un serveur vCenter dans le cadre d'opérations de sauvegarde ou de restauration basées sur des fichiers.
- Nouvelle fonctionnalité lors de l'utilisation de la bibliothèque de contenus. La synchronisation d'un modèle de VM natif entre les bibliothèques de contenu est désormais disponible lorsque vCenter Server est configuré pour le mode lié amélioré.
- Mettez à jour vers "Page des plug-ins clients".
- VMware vSphere Update Manager ajoute également des améliorations au client vSphere. Vous pouvez effectuer une vérification de conformité des liaisons et corriger les actions à partir d'un seul écran.

Pour en savoir plus sur VMware vSphere 6.7 U2, consultez le "Page du blog VMware vSphere".

Pour plus d'informations sur les mises à jour de VMware vCenter Server 6.7 U2, consultez le "Notes de version".

> Bien que cette solution ait été validée avec vSphere 6.7U2, elle prend en charge toute version vSphere qualifiée avec les autres composants par le "Matrice d'interopérabilité NetApp (IMT)". NetApp vous recommande de déployer la prochaine version de vSphere pour ses correctifs et ses fonctionnalités améliorées.

Architecture de démarrage

Les options prises en charge pour l'architecture de démarrage FlexPod Express sont les suivantes :

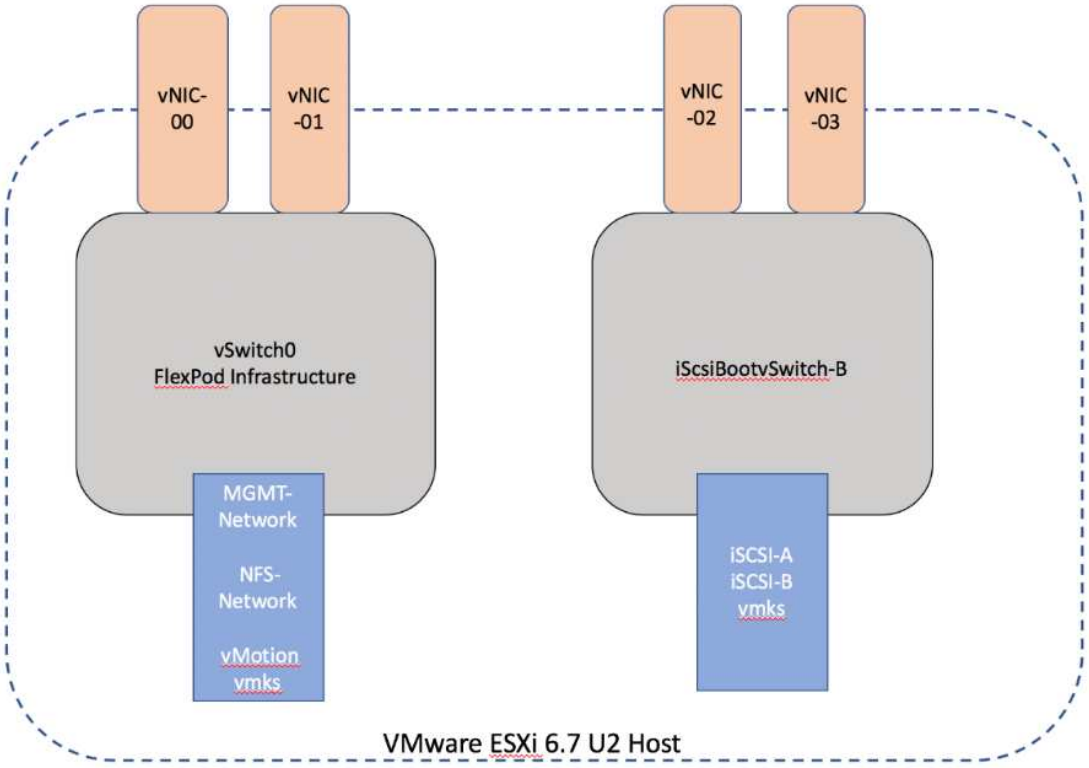
- LUN SAN iSCSI
- Carte SD Cisco FlexFlash
- Disque local

Le data Center FlexPod est démarré à partir des LUN iSCSI. La gestion de la solution est donc améliorée grâce au démarrage iSCSI pour FlexPod Express.

Disposition de la carte d'interface réseau virtuelle de l'hôte ESXi

La carte VIC 1457 de Cisco UCS est dotée de quatre ports physiques. Cette validation de la solution inclut ces quatre ports physiques lors de l'utilisation de l'hôte ESXi. Si vous disposez d'un nombre plus petit ou plus important de cartes réseau, vous pouvez avoir différents numéros VMNIC.

Dans une implémentation de démarrage iSCSI, le démarrage iSCSI nécessite des cartes d'interface réseau virtuelles (vNIC) distinctes pour le démarrage iSCSI. Ces vNIC utilisent le VLAN iSCSI de la structure appropriée comme VLAN natif et sont reliés aux vswitches de démarrage iSCSI, comme le montre la figure suivante.



"Suivant: Conclusion."

Conclusion

La conception validée de FlexPod Express est une solution simple et efficace qui utilise des composants de pointe. FlexPod Express peut être adapté à des besoins métier spécifiques en faisant évoluer la plateforme d'hyperviseur et en proposant des options. Les PME, les bureaux distants, les succursales et d'autres entreprises qui ont besoin de solutions dédiées ont été conçues pour l'FlexPod Express.

"Suivant : où trouver des informations supplémentaires ?"

Où trouver des informations complémentaires

Pour en savoir plus sur les informations fournies dans ce document, consultez ces documents et sites web :

- Centre de documentation du système AFF et FAS

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

- Page des ressources de documentation AFF

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

- Guide de déploiement de FlexPod Express avec VMware vSphere 6.7 et NetApp AFF C190 (en cours)

- Documentation NetApp

  "https://docs.netapp.com"

Guide de déploiement de FlexPod Express avec Cisco UCS C-Series et NetApp AFF C190

NVA-1142-DEPLOY : FlexPod Express avec Cisco UCS C-Series et NetApp AFF C190 Series - déploiement NVA

Savita Kumari, NetApp

Les tendances du secteur indiquent qu'une vaste transformation des data centers est en train de tendre vers l'infrastructure partagée et le cloud computing. Les entreprises ont également besoin d'une solution simple et efficace pour leurs succursales et bureaux distants qui exploitent les technologies qu'elles connaissent bien dans leur data Center.

FlexPod® Express est une architecture de data Center préconçue et conforme aux meilleures pratiques. Elle repose sur 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, et pour 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 peuvent être dimensionnées et optimisées pour prendre en charge de nombreux cas d'utilisation et besoins. 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 passer à la gestion d'FlexPod Datacenter à mesure que leur environnement se développe.

FlexPod Express constitue 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 d'infrastructure convergée FlexPod

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.

Le programme FlexPod comprend deux solutions : FlexPod Express et FlexPod Datacenter.

- **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.

Programme d'architecture vérifiée NetApp

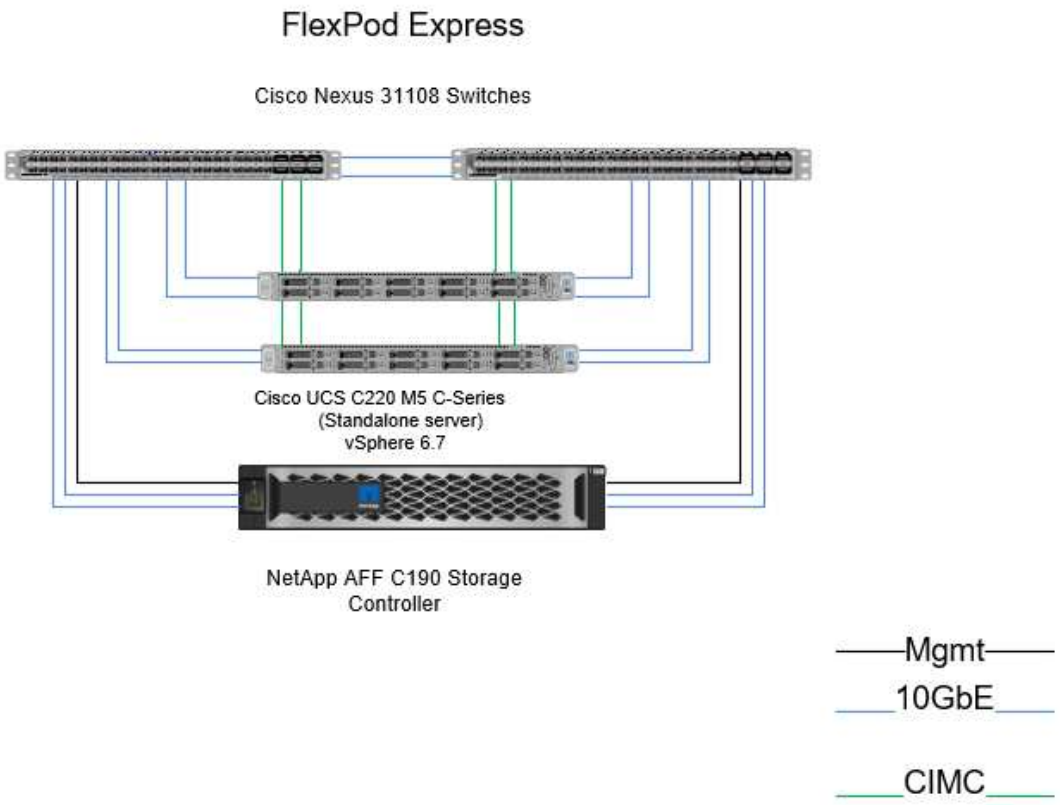
Le programme d'architecture vérifiée NetApp propose une architecture validée pour les solutions NetApp Une architecture vérifiée NetApp fournit une architecture de solution NetApp qui apporte les qualités suivantes :

- Tests approfondis
- Normative par nature
- Risques de déploiement minimisés
- Réduction du délai de mise sur le marché

Ce guide détaille la conception de FlexPod Express avec VMware vSphere. Cette conception utilise également le tout nouveau système AFF C190 (exécutant NetApp ONTAP® 9.6), le Cisco Nexus 31108 et les serveurs Cisco UCS C-Series C220 M5 comme nœuds d'hyperviseur.

Technologie de la solution

Cette solution tire parti des dernières technologies de NetApp, Cisco et VMware. Cette solution comprend le nouveau système NetApp AFF C190 exécutant ONTAP 9.6, deux switchs Cisco Nexus 31108 et des serveurs rack Cisco UCS C220 M5 exécutant VMware vSphere 6.7U2. Cette solution validée utilise une technologie 10GbE. Des recommandations sont également fournies quant à la manière de faire évoluer les capacités de calcul en ajoutant deux nœuds d'hyperviseur à la fois afin que l'architecture FlexPod Express puisse s'adapter aux besoins métier en constante évolution de l'entreprise.



Pour utiliser les quatre ports 10GbE physiques sur le VIC 1457 de manière efficace, créez deux liaisons supplémentaires entre chaque serveur et les commutateurs du rack supérieur.

Récapitulatif du cas d'utilisation

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

- Bureaux distants ou succursales
- Moyennes entreprises
- Les environnements qui nécessitent une solution dédiée et économique

FlexPod Express est parfaitement adapté aux charges de travail virtualisées et mixtes. Bien que cette solution ait été validée avec vSphere 6.7U2, elle prend en charge toute version vSphere qualifiée avec les autres composants par l'outil de matrice d'interopérabilité NetApp. NetApp recommande de déployer vSphere 6.7U2 pour ses correctifs et ses fonctionnalités améliorées, telles que :

- Prise en charge des nouveaux protocoles pour la sauvegarde et la restauration d'une appliance serveur vCenter, notamment HTTP, HTTPS, FTP, FTPS, SCP, NFS ET SMB.
- Nouvelle fonctionnalité lors de l'utilisation de la bibliothèque de contenus. La synchronisation des modèles VM natifs entre les bibliothèques de contenu est désormais disponible lorsque vCenter Server est configuré pour un mode lié amélioré.
- Une page de plug-in client mise à jour.
- Améliorations ajoutées dans vSphere Update Manager (VUM) et le client vSphere. Vous pouvez maintenant effectuer les actions de rattachement, de vérification de conformité et de correction, le tout à partir d'un seul écran.

Pour plus d'informations sur ce sujet, reportez-vous au "Page vSphere 6.7U2" et le "Notes de mise à jour de vCenter Server 6.7U2".

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 changent, vous pouvez utiliser un hyperviseur différent sur le même matériel FlexPod Express.

Les composants matériels requis pour la configuration et l'implémentation de FlexPod Express sont répertoriés dans le tableau suivant. Ils peuvent varier selon l'implémentation de la solution et les besoins du client.

Sous-jacent	Quantité
Cluster à deux nœuds AFF C190	1
Serveur Cisco C220 M5	2
Commutateur Cisco Nexus 31108PC-V.	2
Carte d'interface virtuelle Cisco UCS (VIC) 1457 pour serveur en rack Cisco UCS C220 M5	2

Ce tableau répertorie le matériel requis en plus de la configuration de base pour l'implémentation de la technologie 10GbE.

Sous-jacent	Quantité
Serveur Cisco UCS C220 M5	2
Cisco VIC 1457	2

Configuration logicielle requise

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

Logiciel	Version	Détails
Contrôleur de gestion intégrée Cisco (CIMC)	4.0.4	Pour les serveurs en rack Cisco UCS C220 M5
Pilote nenic Cisco	1.0.0.29	Pour les cartes d'interface VIC 1457
Cisco NX-OS	7.0(3)I7(6)	Pour les commutateurs Cisco Nexus 31108PC-V.
NetApp ONTAP	9.6	Pour les contrôleurs AFF C190

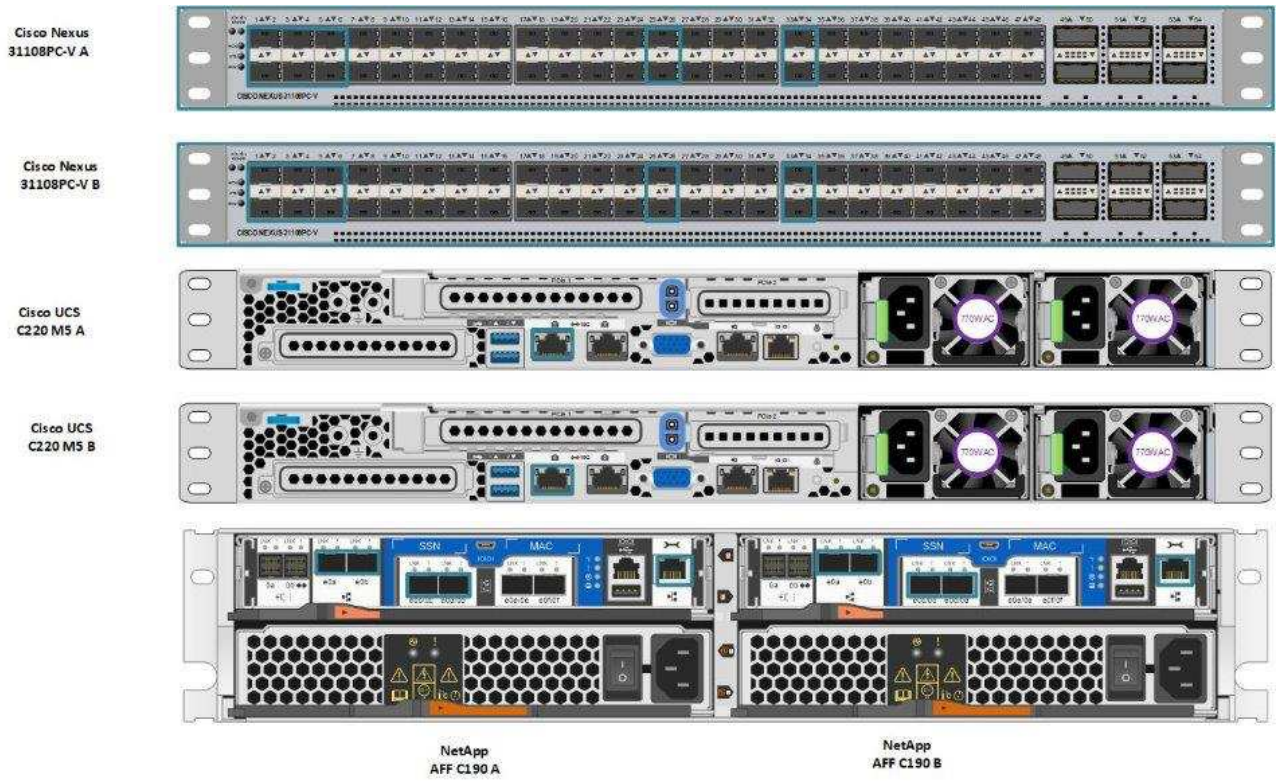
Ce tableau répertorie les logiciels requis pour toutes les implémentations VMware vSphere sur FlexPod Express.

Logiciel	Version
Appliance de serveur VMware vCenter	6.7U2
Hyperviseur VMware vSphere ESXi	6.7U2
Plug-in NetApp VAAI pour ESXi	1.1.2
NetApp VSC	9.6

Informations sur le câblage FlexPod Express

Cette validation de référence est câblée comme indiqué dans les figures et tableaux suivants.

Cette figure illustre le câblage de validation de référence.



Le tableau suivant répertorie les informations de câblage du commutateur Cisco Nexus 31108PC-V-A.

Périphérique local	Port local	Périphérique distant	Port distant
Commutateur Cisco Nexus 31108PC-V A	Eth1/1	Contrôleur A de stockage NetApp AFF C190	e0c
	Eth1/2	Contrôleur de stockage NetApp AFF C190 B	e0c
	Eth1/3	Serveur autonome Cisco UCS C220 C-Series A	MLOM0
	Eth1/4	Serveur autonome Cisco UCS C220 C-Series B	MLOM0
	Eth1/5	Serveur autonome Cisco UCS C220 C-Series A	MLOM1
	Eth1/6	Serveur autonome Cisco UCS C220 C-Series B	MLOM1
	Eth1/25	Commutateur Cisco Nexus 31108PC-V B	Eth1/25
	Eth1/26	Commutateur Cisco Nexus 31108PC-V B	Eth1/26
	Eth1/33	Contrôleur A de stockage NetApp AFF C190	E0M
	Eth1/34	Serveur autonome Cisco UCS C220 C-Series A	CIMC (FEX135/1/25)

Ce tableau répertorie les informations de câblage du commutateur Cisco Nexus 31108PC-V- B.

Périphérique local	Port local	Périphérique distant	Port distant
Commutateur Cisco Nexus 31108PC-V B	Eth1/1	Contrôleur A de stockage NetApp AFF C190	e0d
	Eth1/2	Contrôleur de stockage NetApp AFF C190 B	e0d
	Eth1/3	Serveur autonome Cisco UCS C220 C-Series A	MLOM2
	Eth1/4	Serveur autonome Cisco UCS C220 C-Series B	MLOM2
	Eth1/5	Serveur autonome Cisco UCS C220 C-Series A	MLOM3
	Eth1/6	Serveur autonome Cisco UCS C220 C-Series B	MLOM3
	Eth1/25	Commutateur Cisco Nexus 31108 A	Eth1/25
	Eth1/26	Commutateur Cisco Nexus 31108 A	Eth1/26
	Eth1/33	Contrôleur de stockage NetApp AFF C190 B	E0M
	Eth1/34	Serveur autonome Cisco UCS C220 C-Series B	CIMC (FEX135/1/26)

Ce tableau répertorie les informations de câblage du contrôleur de stockage NetApp AFF C190 A.

Périphérique local	Port local	Périphérique distant	Port distant
Contrôleur A de stockage NetApp AFF C190	e0a	Contrôleur de stockage NetApp AFF C190 B	e0a
	e0b	Contrôleur de stockage NetApp AFF C190 B	e0b
	e0c	Commutateur Cisco Nexus 31108PC-V A	Eth1/1
	e0d	Commutateur Cisco Nexus 31108PC-V B	Eth1/1
	E0M	Commutateur Cisco Nexus 31108PC-V A	Eth1/33

Ce tableau répertorie les informations de câblage du contrôleur de stockage B. AFF C190 de NetApp

Périphérique local	Port local	Périphérique distant	Port distant
Contrôleur de stockage NetApp AFF C190 B	e0a	Contrôleur A de stockage NetApp AFF C190	e0a
	e0b	Contrôleur A de stockage NetApp AFF C190	e0b
	e0c	Commutateur Cisco Nexus 31108PC-V A	Eth1/2
	e0d	Commutateur Cisco Nexus 31108PC-V B	Eth1/2
	E0M	Commutateur Cisco Nexus 31108PC-V B	Eth1/33

Procédures de déploiement

Présentation

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

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

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

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

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 suivant décrit les VLAN nécessaires au 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 VLAN	
VLAN de gestion	VLAN pour les interfaces de gestion	3437	VSwitch0

Nom du VLAN	Objectif VLAN	ID VLAN	
VLAN NFS	VLAN pour le trafic NFS	3438	VSwitch0
VLAN VMware vMotion	VLAN désigné pour le déplacement de machines virtuelles (VM) d'un hôte physique à un autre	3441	VSwitch0
VLAN trafic des VM	VLAN pour le trafic des applications des VM	3442	VSwitch0
ISCSI-A-VLAN	VLAN pour le trafic iSCSI sur la structure A	3439	VSwitch iSciBootvSwitch
ISCSI-B-VLAN	VLAN pour le trafic iSCSI sur la structure B	3440	VSwitch iSciBootvSwitch
VLAN natif	VLAN auquel des trames non marquées sont attribuées	2	

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).

Deux vswitches sont créés dans cette validation.

Le tableau suivant répertorie les vswitches de solution.

Nom du vSwitch	Adaptateurs actifs	Ports	MTU	Équilibrage de la charge
VSwitch0	Vmnic2 et vmnic4	par défaut (120)	9000	Route basée sur un hachage IP
VSwitch iSciBootvSwitch	Vmnic3, vmnic5	par défaut (120)	9000	Route basée sur l'ID de port virtuel d'origine.

La méthode de hachage IP d'équilibrage de charge nécessite une configuration correcte pour le commutateur physique sous-jacent à l'aide de SRC-DST-IP EtherChannel avec un canal de port statique (mode activé). En cas de connectivité intermittente due à une éventuelle mauvaise configuration du commutateur, arrêtez temporairement l'un des deux ports de liaison montante associés sur le commutateur Cisco pour restaurer la communication vers le port vmkernel de gestion ESXi tout en dépannant les paramètres du canal de port.

Le tableau suivant répertorie les machines virtuelles VMware créées.

Description de la machine virtuelle	Nom d'hôte
Serveur VMware vCenter	FlexPod-VCSA
Virtual Storage Console	FlexPod-VSC

Déployez Cisco Nexus 31108PC-V

Cette section décrit en détail la configuration du commutateur Cisco Nexus 331108PC-V utilisée dans un environnement FlexPod Express.

Configuration initiale du commutateur Cisco Nexus 31108PC-V.

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

> Cette procédure suppose que vous utilisez un Cisco Nexus 31108PC-V exécutant la version 7.0(3)I7(6) 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 sur les commutateurs 331108PC-V peuvent être connectées à un réseau de gestion existant, ou les interfaces mgmt0 des commutateurs 331108PC-V peuvent être connectées dans une configuration dos à dos. Cependant, ce lien ne peut pas être utilisé pour l'accès à une gestion externe, tel que le trafic SSH.

   > Dans ce guide de déploiement, les commutateurs FlexPod Express Cisco Nexus 31108PC-V sont connectés à un réseau de gestion existant.

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

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

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

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

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

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

Activez les fonctionnalités avancées

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

Dans le mode de configuration (config t), entrez les commandes suivantes pour définir la configuration d'équilibrage de charge du canal du port global sur le commutateur Cisco Nexus A et le commutateur B :

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

Configurer l'arborescence à ressources globales

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.

A partir du mode de configuration (config t), exécutez les commandes suivantes pour configurer les options de l'arborescence à ressources par défaut, y compris le type de port par défaut et le protecteur BPDU, sur le

commutateur Cisco Nexus A et le commutateur B :

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

Définissez 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.

Depuis le 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 B :

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

Configurez les descriptions des ports d'accès et de gestion

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

Dans le mode de configuration (config t) de chacun des commutateurs, entrez les descriptions de port suivantes pour la configuration grand format de FlexPod Express :

Commutateur Cisco Nexus A

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Commutateur Cisco Nexus B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

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.

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

Commutateur Cisco Nexus A

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

Commutateur Cisco Nexus B

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

Effectuez la configuration globale du canal du 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 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 `ping <<switch_A/B_mgmt0_ip_addr>>vrf` commande de gestion.

Depuis le 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-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

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
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configurez les canaux du port de stockage

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

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

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

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

2. Exécutez les commandes suivantes sur les commutateurs A et B pour configurer les canaux de port du contrôleur de stockage B :

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

Configurez les connexions du serveur

Les serveurs Cisco UCS sont dotés d'une carte d'interface virtuelle à quatre ports, VIC11457, utilisée pour le trafic de données et le démarrage du système d'exploitation ESXi via iSCSI. Ces interfaces sont configurées pour basculer les unes sur les autres, assurant ainsi une redondance supplémentaire au-delà d'une liaison unique. La diffusion de ces liaisons sur plusieurs commutateurs permet au serveur de survivre même à une défaillance complète du commutateur.

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

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

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

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

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Configurez les canaux de port du serveur

Exécutez les commandes suivantes sur le commutateur A et le commutateur B pour configurer les canaux de port pour le serveur A :

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

Exécutez les commandes suivantes sur le commutateur A et le commutateur B pour configurer les canaux de port pour le serveur B :

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

Une MTU de 9 9000 a été utilisée pour la validation de cette solution. Cependant, vous pouvez configurer une valeur différente pour la MTU adaptée aux exigences de votre application. Il est important de définir la même valeur MTU sur l'ensemble de la solution FlexPod. Des configurations MTU incorrectes entre les composants entraînent la perte de paquets et leur retransmission affecte les performances globales de la solution.

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

Se uplink dans une 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 31108 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 pour enregistrer la configuration sur chaque commutateur une fois la configuration terminée.

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

Procédure de déploiement du stockage NetApp (partie 1)

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

Installation de la gamme AFF C190 du contrôleur de stockage NetApp

NetApp Hardware Universe

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

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

Accédez au "HWU" application pour afficher les guides de configuration du système. Cliquez sur l'onglet contrôleurs pour afficher la compatibilité entre différentes versions du logiciel ONTAP et les appliances de stockage NetApp avec les spécifications souhaitées.

Vous pouvez également comparer les composants par appliance de stockage en cliquant sur Comparer les systèmes de stockage.

Conditions préalables au contrôleur AFF C190 Series
Pour planifier l'emplacement physique des systèmes de stockage, consultez le Hardware Universe NetApp. Reportez-vous aux sections suivantes : • Exigences électriques • Cordons d'alimentation pris en charge • Ports et câbles intégrés

Contrôleurs de stockage

Suivez les procédures d'installation physique des contrôleurs dans AFF "C190" Documentation :

NetApp ONTAP 9.6

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 d'installation du logiciel ONTAP 9.6.

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

Le tableau suivant présente des informations sur l'installation et la configuration de ONTAP 9.6.

Détail du cluster	Valeur des détails du cluster
Adresse IP du nœud de cluster A	<<var_NODEA_mgmt_ip>>
Masque de réseau du nœud de cluster A	<<var_NODEA_mgmt_mask>>
Passerelle de nœud de cluster A	<<var_NODEA_mgmt_Gateway>>
Nom du nœud de cluster A	<<var_NODEA>>
Adresse IP du nœud B du cluster	<<var_NodeB_mgmt_ip>>
Masque de réseau du nœud B du cluster	<<var_NodeB_mgmt_mask>>
Passerelle de nœud B du cluster	<<var_NodeB_mgmt_Gateway>>
Nom du nœud B du cluster	<<var_NodeB>>
URL ONTAP 9.6	<<var_url_boot_software>>
Nom du cluster	<<var_clustername>>
Adresse IP de gestion du cluster	<<var_clustermgmt_ip>>
Passerelle du cluster B	<<var_clustermgmt_gateway>>
Masque de réseau du cluster B.	\<<var_clustermgmt_mask>
Nom de domaine	<<nom_domaine_var>>
IP du serveur DNS (vous pouvez entrer plusieurs adresses)	<var_dns_server_ip
IP de serveur NTP (vous pouvez entrer plusieurs adresses)	<<var_ntp_server_ip>>

Configurez le nœud A

Pour configurer le nœud A, procédez comme suit :

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

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

   Laissez le système démarrer.

   ```
   autoboot
   ```

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

Si ONTAP 9.6 n'est pas la version du logiciel en cours de démarrage, procédez comme suit pour installer le nouveau logiciel. Si ONTAP 9.6 est la version en cours de démarrage, sélectionnez les options 8 et y pour redémarrer le nœud. Ensuite, passez à l'étape 14.

3. Pour installer un nouveau logiciel, sélectionnez l'option 7.
4. Entrez y pour effectuer une mise à niveau.
5. Sélectionnez e0M pour le port réseau que vous souhaitez utiliser pour le téléchargement.
6. Entrez y pour redémarrer maintenant.
7. 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>>
```

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

Ce serveur Web doit être accessible.

```
<<var_url_boot_software>>
```

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

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

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 9.6 n'est pas la version du logiciel en cours de démarrage, procédez comme suit pour installer le nouveau logiciel. Si ONTAP 9.6 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.A.
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. Saisissez 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 des disques.

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

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

À partir d'un programme de port de console connecté au port de console Du contrôleur de stockage A (nœud A), exécutez le script de configuration du nœud. Ce script apparaît lors du premier démarrage de ONTAP 9.6 sur le nœud.

La procédure de configuration du nœud et du cluster a été légèrement modifiée dans ONTAP 9.6. L'assistant d'installation du cluster est maintenant utilisé pour configurer le premier nœud d'un cluster. NetApp ONTAP System Manager (anciennement OnCommand® System Manager) est utilisé pour 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 d'une configuration assistée de 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 `10.63.172.162` Dans le champ serveur NTP principal.

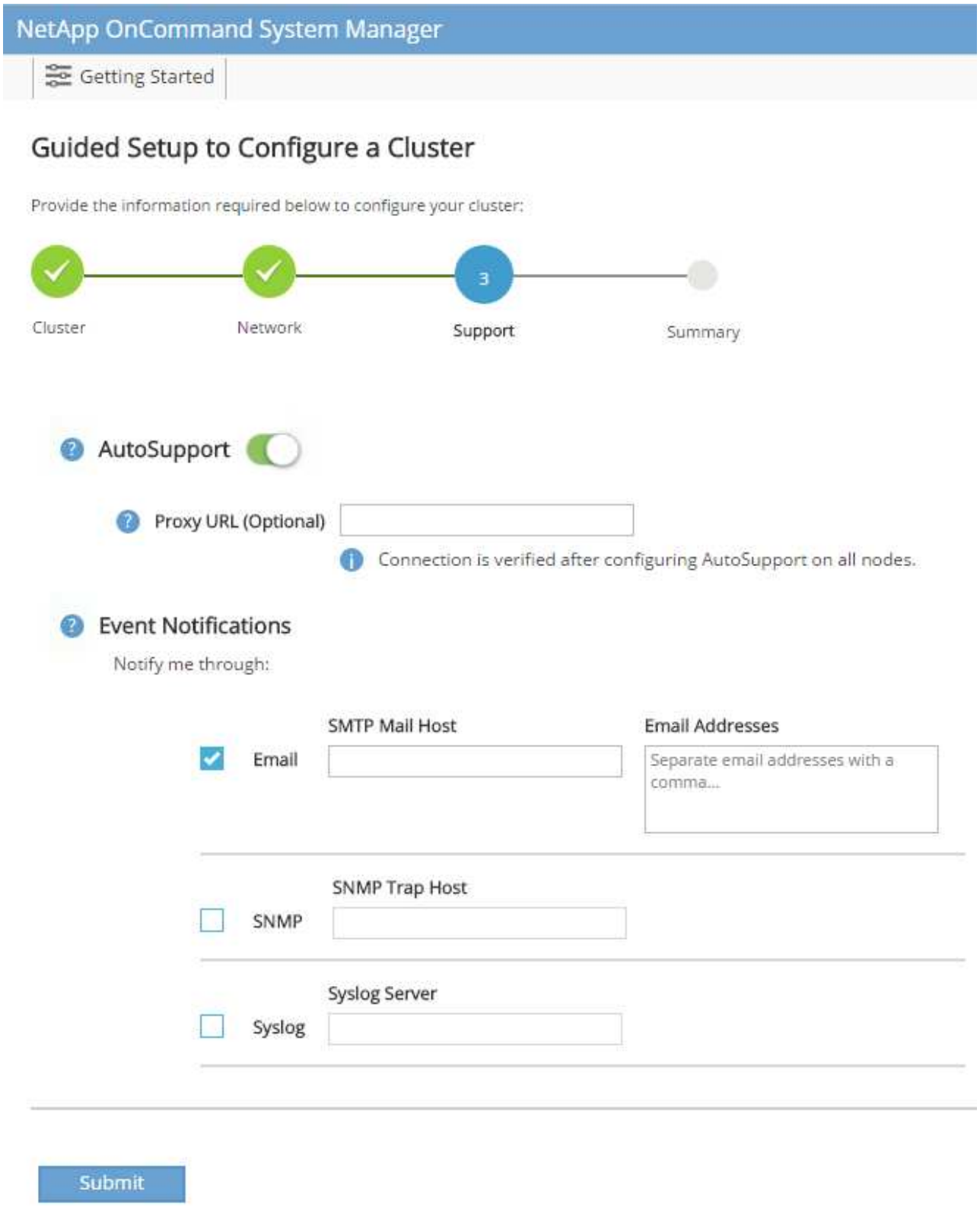
> Vous pouvez également entrer un autre serveur NTP. L'adresse IP `10.63.172.162` de `<<var_ntp_server_ip>>` Est l'IP de gestion Nexus.

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.



Lorsque le système indique que 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 la personnalité des ports UTA2 intégrés

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

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

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

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

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

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

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

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 C190_B_1 -newname AFF C190-02_mgmt1
```

Définissez le rétablissement automatique sur la gestion du cluster

Définissez le paramètre de restauration automatique sur l'interface de gestion du cluster.

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

Configurez l'interface réseau du processeur de service

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

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

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

Activez le basculement du stockage dans ONTAP

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

1. Vérification de l'état du basculement du stockage

```
storage failover show
```

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

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

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

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

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

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

```
cluster ha show
```

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

```
High Availability Configured: true
```

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

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

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

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

```
storage failover hwassist show
```

> Le message `Keep Alive Status: Error:` indique que l'un des contrôleurs n'a pas reçu d'alertes de maintien en service hwassist de la part de son partenaire, ce qui 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
```

Ne supprime pas le port de données du broadcast domain par défaut

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

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

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Désactiver le contrôle de flux sur les ports UTA2

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

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

Configurer le groupe d’interface LACP dans ONTAP

Ce type de groupe d’interface nécessite au moins deux interfaces Ethernet et un switch qui prend en charge LACP. assurez-vous qu’il est configuré en fonction des étapes décrites dans ce guide à la section 5.1.

Dans l’invite de cluster, effectuez la procédure suivante :

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Configurer les trames Jumbo dans ONTAP

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

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Créez des VLAN dans ONTAP

Pour créer des VLAN dans ONTAP, procédez comme suit :

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

   ```
   network port vlan create –node <<var_nodeA>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   network port vlan create –node <<var_nodeB>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
   <<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
   <<var_nfs_vlan_id>>
   ```

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

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. Créez des ports MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Créez des agrégats de données 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 tant que aggr1_NODEA n'est pas 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 du moteur de l'entité faisant autorité et sélectionnez md5 comme 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 vServers.

Configurez NFSv3 dans ONTAP

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

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

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

1. Créez une règle pour chaque hôte ESXi dans la stratégie d'exportation par défaut.
2. Pour chaque hôte ESXi créé, attribuez une règle. Chaque hôte a son propre index de règles. Votre premier hôte ESXi dispose de l'index de règles 1, votre second hôte ESXi dispose de l'index de règles 2, etc.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Assigner la export policy au volume root du SVM d'infrastructure.

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

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

Créez le service iSCSI dans ONTAP

Pour créer le service iSCSI sur le SVM, exécutez la commande suivante. Cette commande démarre également le service iSCSI et définit l'IQN iSCSI pour la SVM. Vérifiez que le protocole iSCSI a été configuré.

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

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

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 DP
   volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
   aggr1_nodeB –size 1GB –type DP
   ```

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

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

3. Créer les relations de mise en miroir.

   ```
   snapmirror create -source-path Infra-SVM:rootvol -destination-path
   Infra-SVM:rootvol_m01 -type LS -schedule 15min
   snapmirror create -source-path Infra-SVM:rootvol -destination-path
   Infra-SVM:rootvol_m02 -type LS -schedule 15min
   ```

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

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

Configurez l'accès HTTPS dans ONTAP

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

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

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

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

```
security certificate show
```

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

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

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

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

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Pour obtenir les valeurs des paramètres requis à l'étape suivante, exécutez la commande Security Certificate show.

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 à la SVM d'être disponible par le web.

```
set –privilege admin
vserver services web modify –name spi –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 -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Créer des LUN dans ONTAP

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

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

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

Création des LIFs iSCSI dans ONTAP

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

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

Création de quatre LIF iSCSI, deux sur chaque nœud

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface show
```

Création des LIFs NFS dans ONTAP

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

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

Créer une LIF NFS.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Ajoutez un administrateur SVM d'infrastructure

Le tableau suivant répertorie les informations nécessaires pour ajouter un administrateur SVM.

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

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

1. Exécutez la commande suivante :

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

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

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

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

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

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"Ensuite, déployez le serveur rack Cisco UCS C-Series."

Déployez un serveur en rack Cisco UCS C-Series

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

Procédez à la configuration initiale du serveur autonome Cisco UCS C-Series pour CIMC

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

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

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

La version CIMC utilisée dans cette validation est CIMC 4.0.(4).

Tous les serveurs

1. Reliez le dongle (KVM) du clavier, de la vidéo et de la souris Cisco (fourni avec le serveur) au port KVM situé à l'avant du serveur. Branchez un moniteur VGA et un clavier USB sur les ports de dongle KVM appropriés.

   Mettez le serveur sous tension et appuyez sur F8 lorsque vous êtes invité à entrer dans la configuration CIMC.

2. Dans l'utilitaire de configuration de CIMC, définissez les options suivantes :
   a. Mode carte d'interface réseau (NIC) :

      Ressource dédiée `[X]`

   b. IP (de base) :

      IPV4 : `[X]`

      DHCP activé : `[ ]`

      CIMC IP : `<<cimc_ip>>`

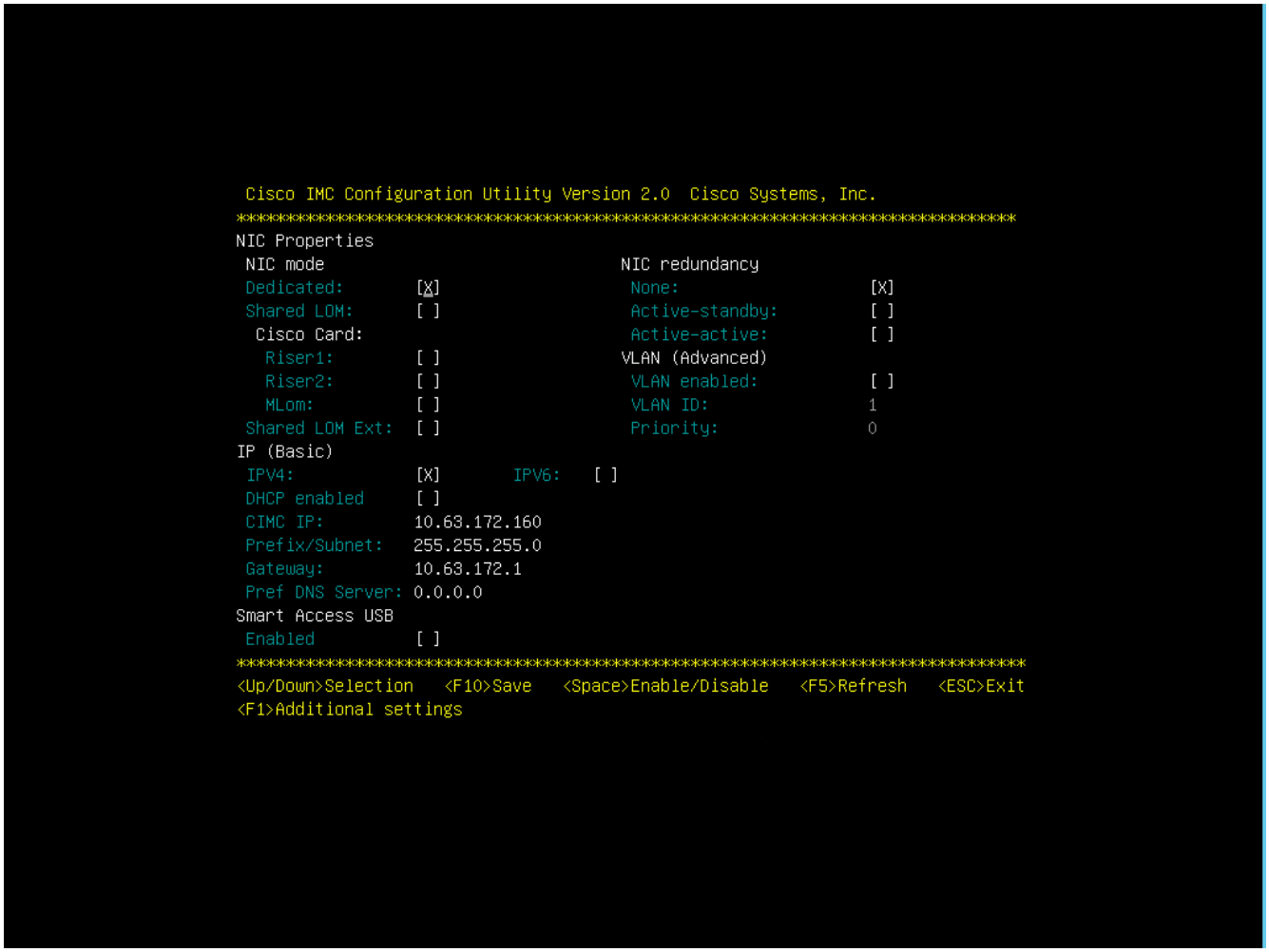
      Préfixe/sous-réseau : `<<cimc_netmask>>`

      Passerelle : `<<cimc_gateway>>`

   c. VLAN (avancé) : laissez désactivé pour désactiver le marquage VLAN.

      Redondance des cartes réseau

      Aucune : `[X]`



3. Appuyez sur F1 pour afficher les réglages supplémentaires :
   a. Propriétés communes :

      Nom d'hôte : `<<esxi_host_name>>`

      DNS dynamique : `[ ]`

      Paramètres par défaut : laisser effacé.

   b. Utilisateur par défaut (de base) :

      Mot de passe par défaut : `<<admin_password>>`

      Saisissez à nouveau le mot de passe : `<<admin_password>>`

      Propriétés du port : utilisez les valeurs par défaut.

   Profils de port : laisser désactivé.
4. Appuyez sur F10 pour enregistrer la configuration de l'interface CIMC.
5. Une fois la configuration enregistrée, appuyez sur Echap pour quitter.

Configuration du démarrage iSCSI des serveurs Cisco UCS C-Series

Dans cette configuration FlexPod Express, le VIC11457 est utilisé pour le démarrage iSCSI.

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

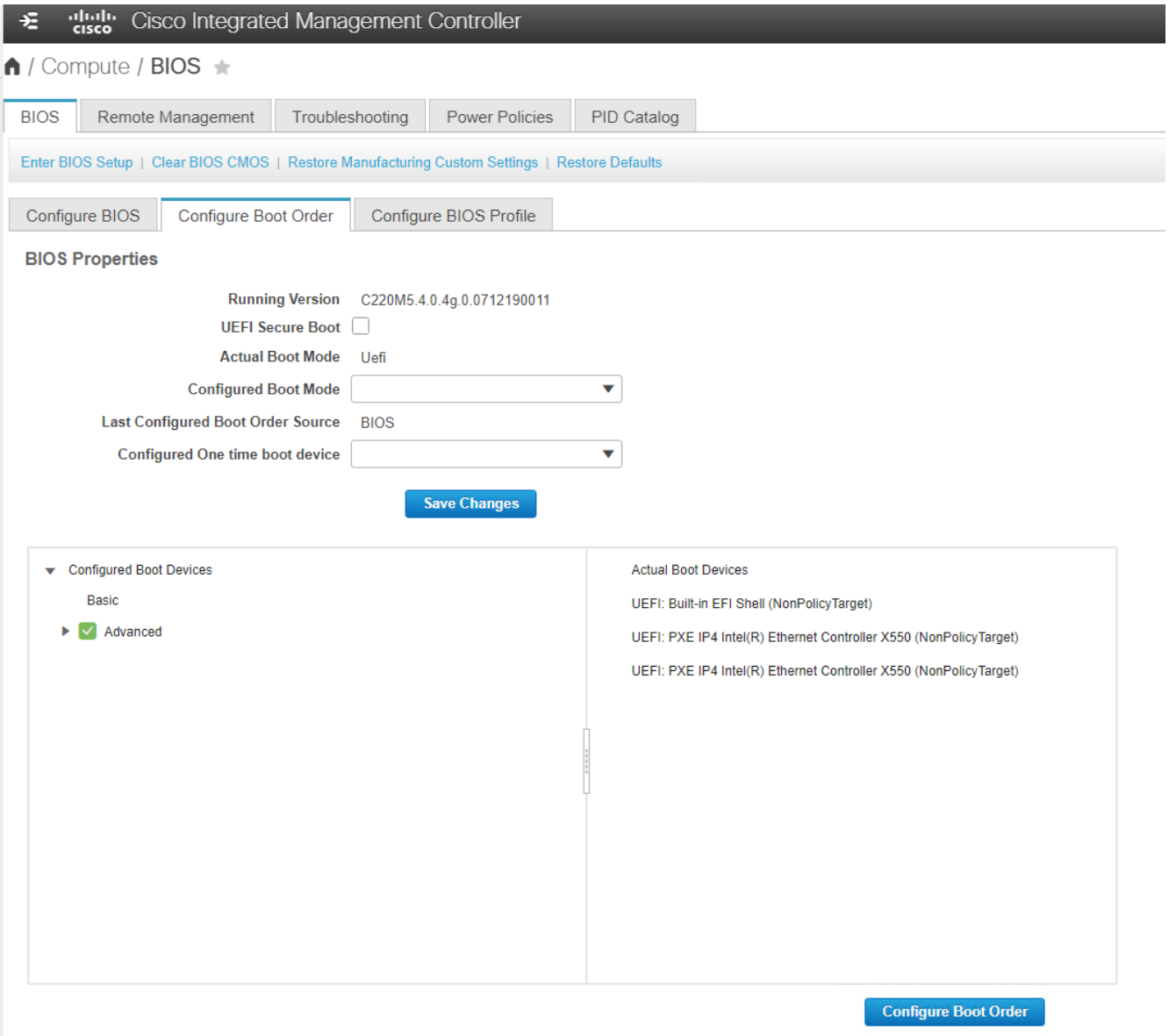
Une police en italique indique les variables uniques pour chaque hôte ESXi.

Détails	Valeur de détail
Initiateur hôte VMware ESXi a name	<<var_ucs_initiator_name_A>>
Hôte ESXi iSCSI-A IP	<<var_esxi_Host_iscsiA_ip>>
Masque de réseau iSCSI-A de l'hôte ESXi	<<var_esxi_host_iscsiA_mask>>
Hôte ESXi iSCSI : passerelle par défaut	<<var_esxi_Host_iscsiA_Gateway>>
Nom de l'initiateur B de l'hôte ESXi	<<var_ucs_initiator_name_B>>
Adresse IP iSCSI-B de l'hôte ESXi	<<var_esxi_Host_iscsiB_ip>>
Masque de réseau iSCSI-B de l'hôte ESXi	<<var_esxi_host_iscsiB_mask>>
Passerelle iSCSI-B de l'hôte ESXi	<<var_esxi_Host_iscsiB_Gateway>>
Adresse IP iscsi_lif01a	<<var_iscsi_lif01a>>
Adresse IP iscsi_lif02a	<<var_iscsi_lif02a>>
Adresse IP iscsi_lif01b	<<var_iscsi_lif01b>>
Adresse IP iscsi_lif02b	<<var_iscsi_lif02b>>
IQN de l'infra_SVM	<<var_SVM_IQN>>

Configuration de l'ordre de démarrage

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

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



3. Configurez les périphériques suivants en cliquant sur le périphérique sous Ajouter un périphérique de démarrage et en accédant à l'onglet Avancé :

   a. Ajouter des supports virtuels :

      NOM : KVM-CD-DVD

      SOUS-TYPE : DVD MAPPÉ KVM

      État : activé

      Ordre : 1

   b. Ajouter démarrage iSCSI :

      Nom : iSCSI-A

      État : activé

      Ordre : 2

Slot: MLOM

Port : 1

c. Cliquez sur Ajouter un démarrage iSCSI :

Nom : iSCSI-B

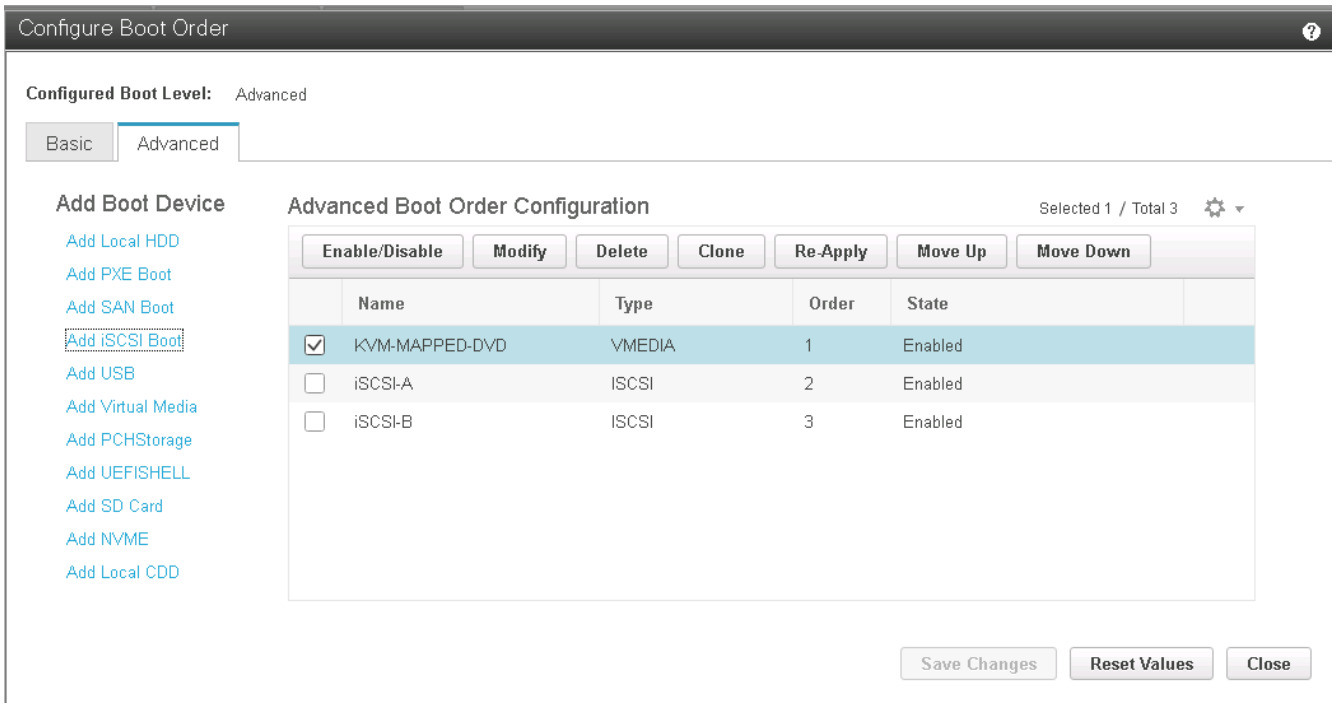
État : activé

Ordre: 3

Slot: MLOM

Port : 3

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

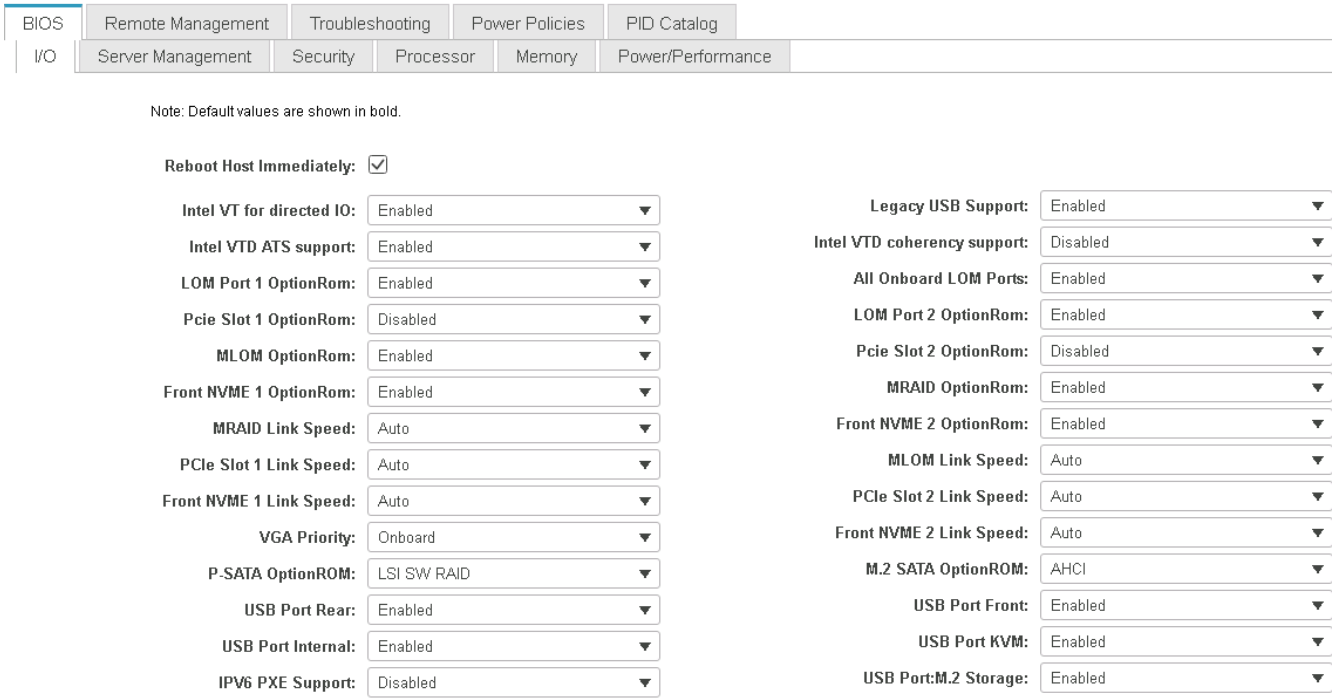


6. Redémarrez le serveur pour démarrer avec votre nouvel ordre de démarrage.

Désactiver le contrôleur RAID (le cas échéant)

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

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

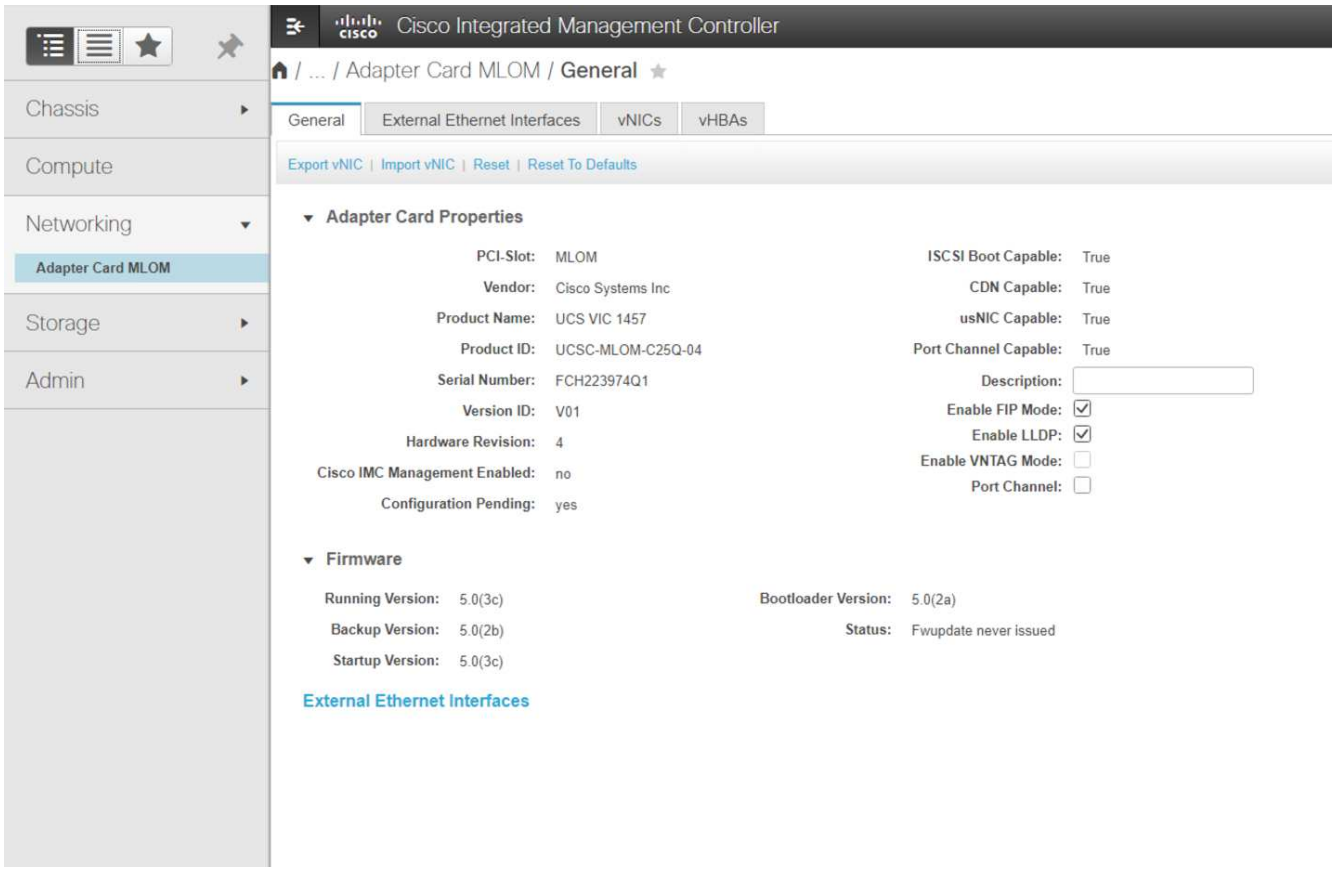


Configurer Cisco VIC11457 pour le démarrage iSCSI

Les étapes de configuration suivantes concernent le Cisco VIC 1457 pour l'amorçage iSCSI.

> Le port par défaut entre les ports 0, 1, 2 et 3 doit être désactivé avant que les quatre ports individuels puissent être configurés. Si le canal de port n'est pas désactivé, seuls deux ports apparaissent pour le VIC 1457. Pour activer le canal de port sur le CIMC, procédez comme suit :

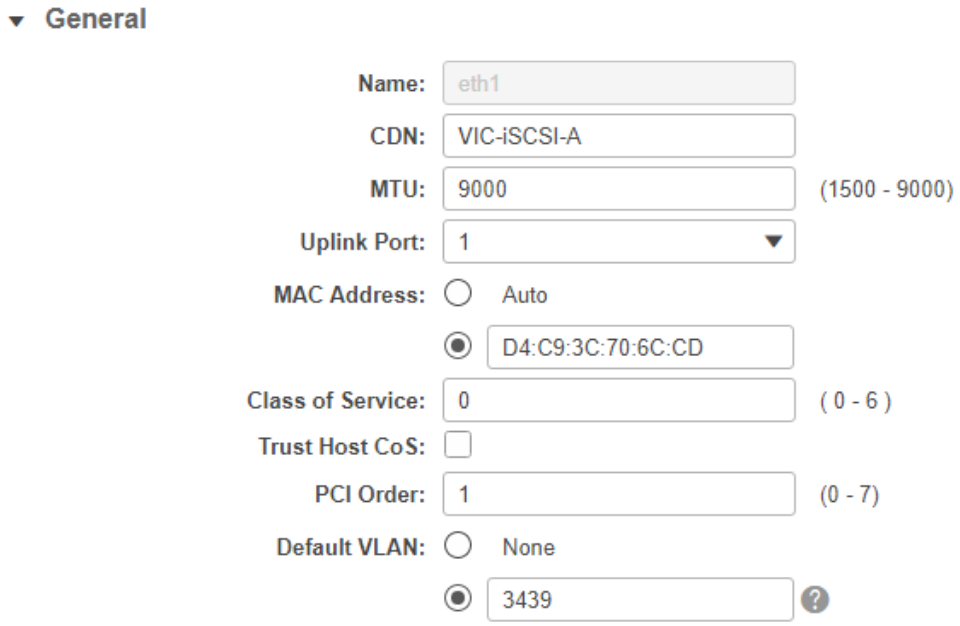
1. Sous l'onglet réseau, cliquez sur la carte d'adaptateur MLOM.
2. Sous l'onglet général, décochez le canal de port.
3. Enregistrez les modifications et redémarrez le CIMC.



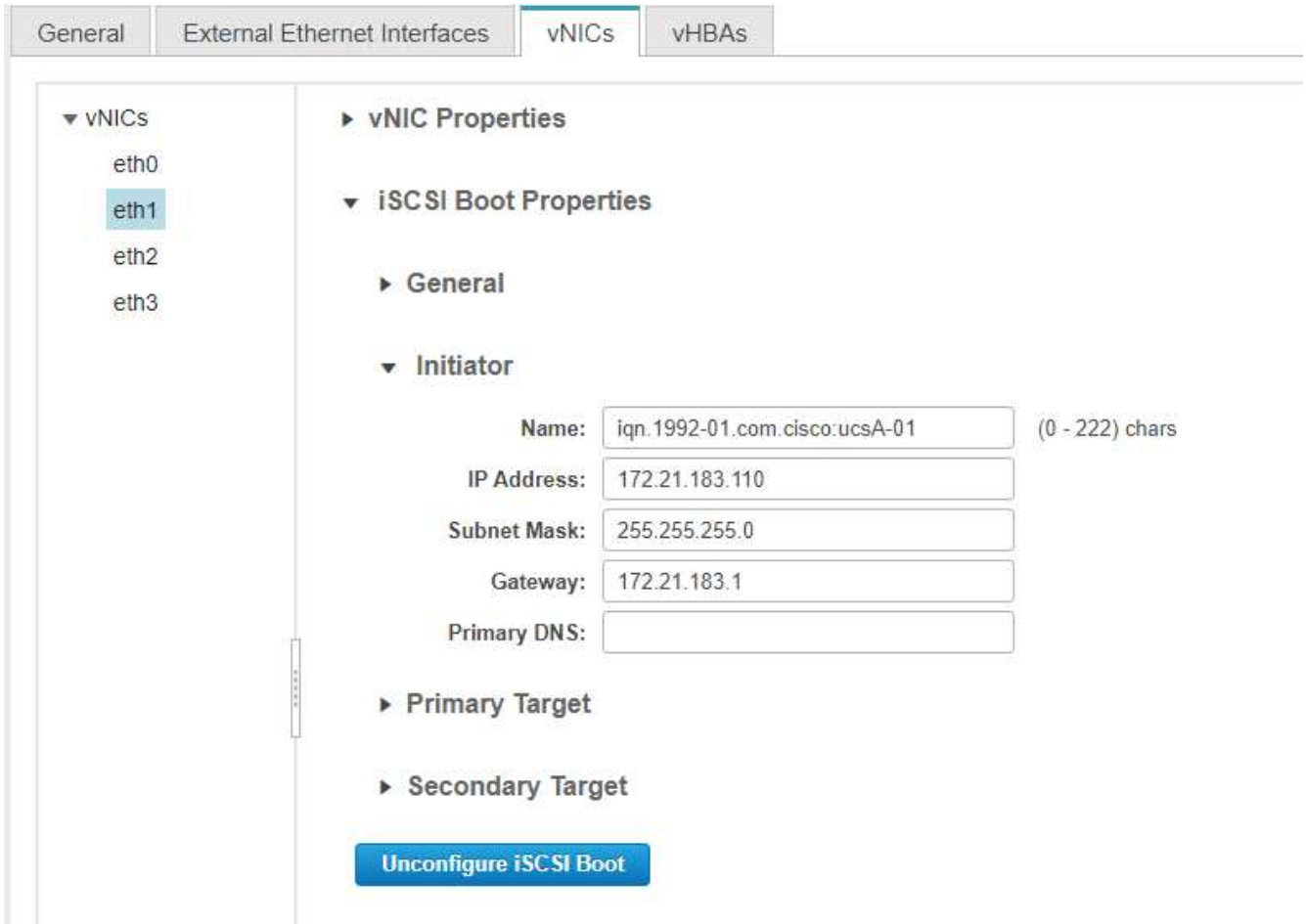
Créez des vNIC iSCSI

Pour créer des vNIC iSCSI, procédez comme suit :

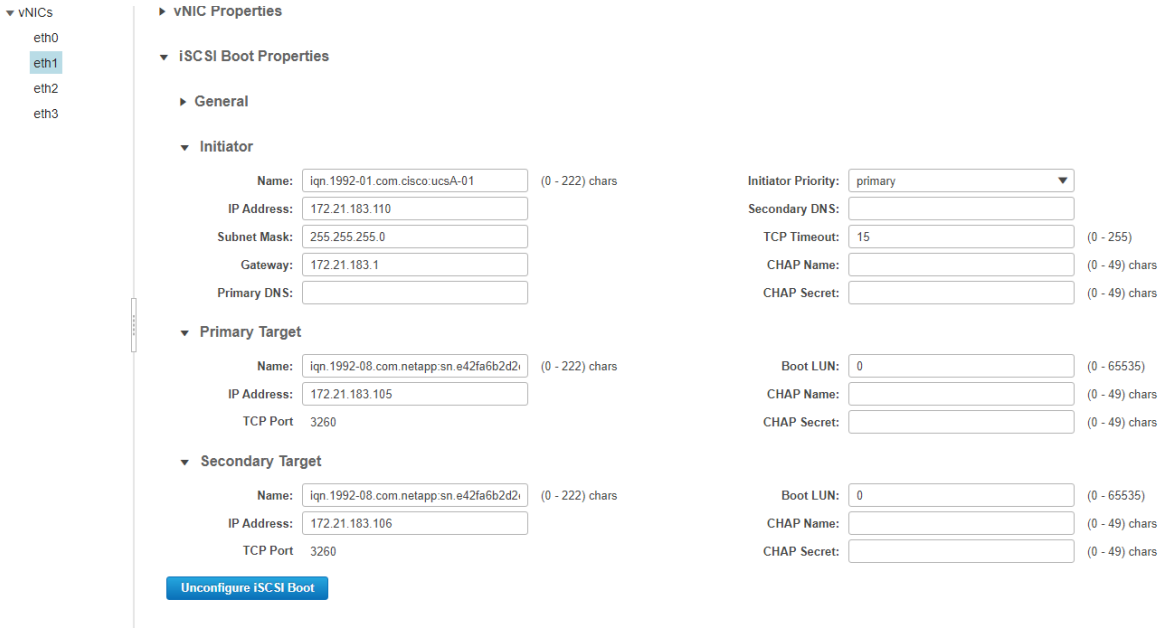
1. Sous l'onglet réseau, cliquez sur carte d'adaptateur MLOM.
2. Cliquez sur Ajouter vNIC pour créer une vNIC.
3. Dans la section Ajouter vNIC, entrez les paramètres suivants :
   - Nom : eth1
   - Nom CDN : iSCSI-vNIC-A
   - MTU : 9000
   - VLAN par défaut : `<<var_iscsi_vlan_a>>`
   - Mode VLAN : TRUNK
   - Activer le démarrage PXE : vérifier
4. Cliquez sur Ajouter vNIC, puis sur OK.
5. Répétez le processus pour ajouter un second vNIC :
   - Nommez le vNIC eth3.
   - Nom CDN : iSCSI-vNIC-B
   - Entrez `<<var_iscsi_vlan_b>>` Comme le VLAN.
   - Définissez le port de liaison montante sur 3.



6. Sélectionnez vNIC eth1 sur la gauche.



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



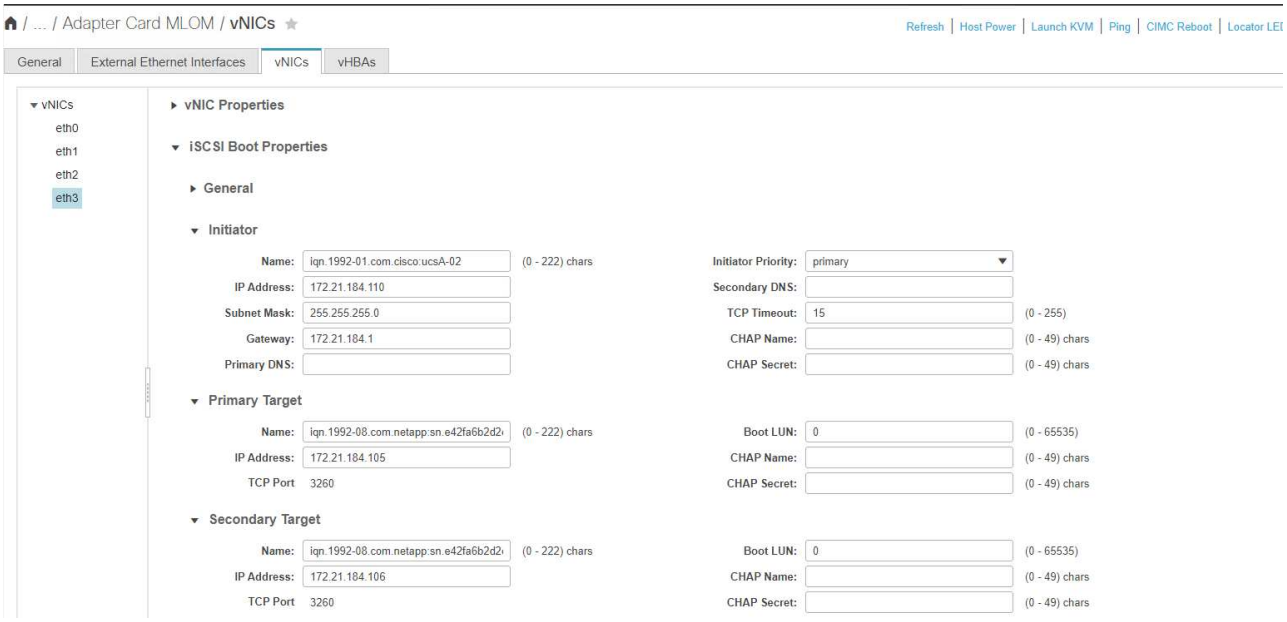
8. Saisissez les détails de la cible principale :
   - Nom : numéro IQN de l'infra-SVM
   - Adresse IP : adresse IP de iscsi_lif01a
   - LUN de démarrage : 0
9. Saisissez les détails de la cible secondaire :
   - Nom : numéro IQN de l'infra-SVM
   - Adresse IP : adresse IP de iscsi_lif02a
   - LUN de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

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

> Assurez-vous d'enregistrer les noms IQN pour chaque vNIC. Vous en avez besoin pour une étape ultérieure. De plus, les noms IQN des initiateurs doivent être uniques pour chaque serveur et pour le vNIC iSCSI.

10. Cliquez sur Save Changes.
11. Sélectionnez le vNIC eth3 et cliquez sur le bouton iSCSI Boot situé en haut de la section Host Ethernet interfaces.
12. Répétez le processus pour configurer eth3.

13. Entrer les détails de l'initiateur :
    - Nom : `<<var_ucsa_initiator_name_b>>`
    - Adresse IP : `<<var_esxi_hostb_iscsib_ip>>`
    - Masque de sous-réseau : `<<var_esxi_hostb_iscsib_mask>>`
    - Passerelle : `<<var_esxi_hostb_iscsib_gateway>>`



14. Saisissez les détails de la cible principale :
    - Nom : numéro IQN de l'infra-SVM
    - Adresse IP : adresse IP de iscsi_lif01b
    - LUN de démarrage : 0
15. Saisissez les détails de la cible secondaire :
    - Nom : numéro IQN de l'infra-SVM
    - Adresse IP : adresse IP de iscsi_lif02b
    - LUN de démarrage : 0

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

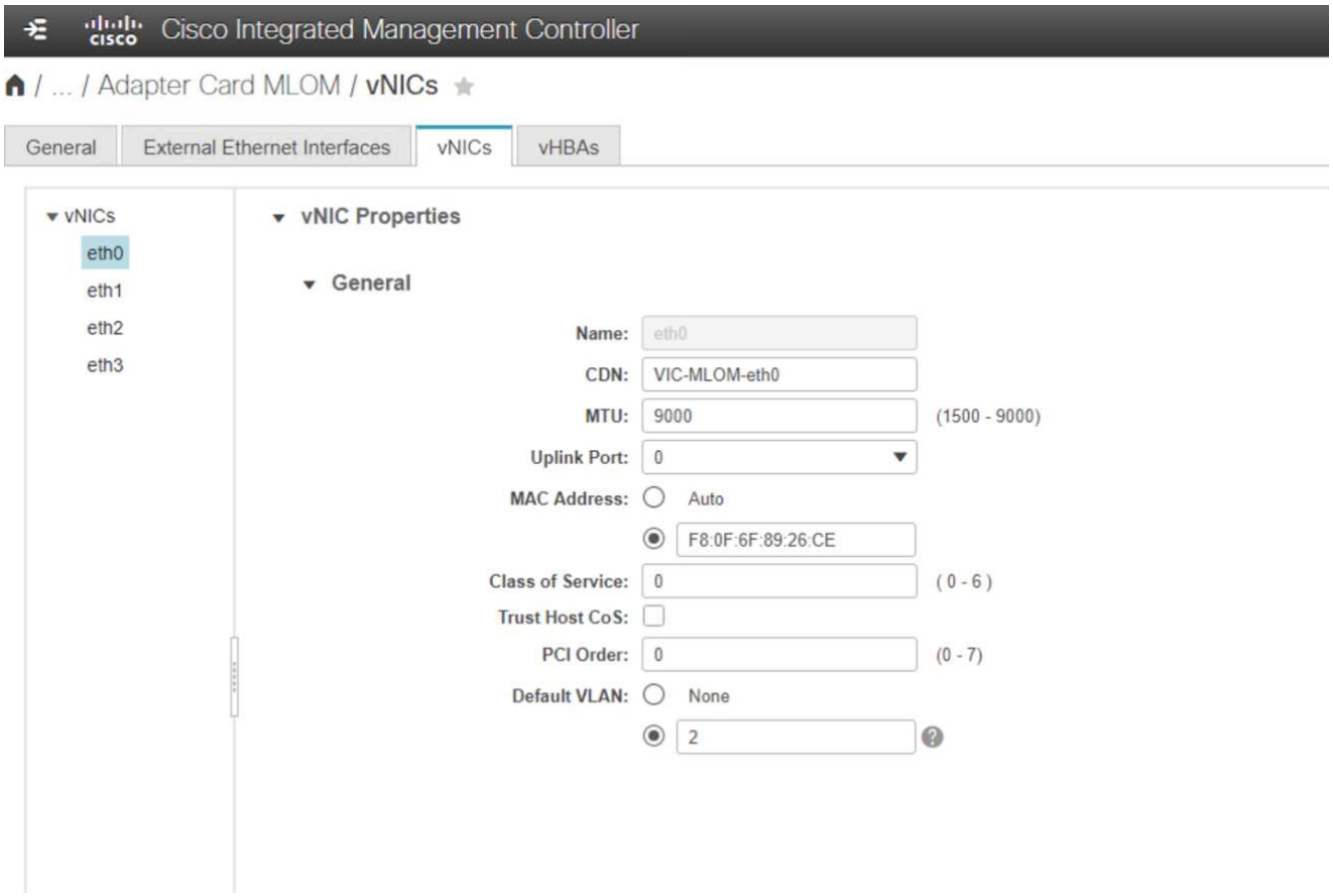
> Assurez-vous d'enregistrer les noms IQN pour chaque vNIC. Vous en avez besoin pour une étape ultérieure.

16. Cliquez sur Save Changes.
17. Répétez ce processus pour configurer l'initialisation iSCSI pour le serveur Cisco UCS B.

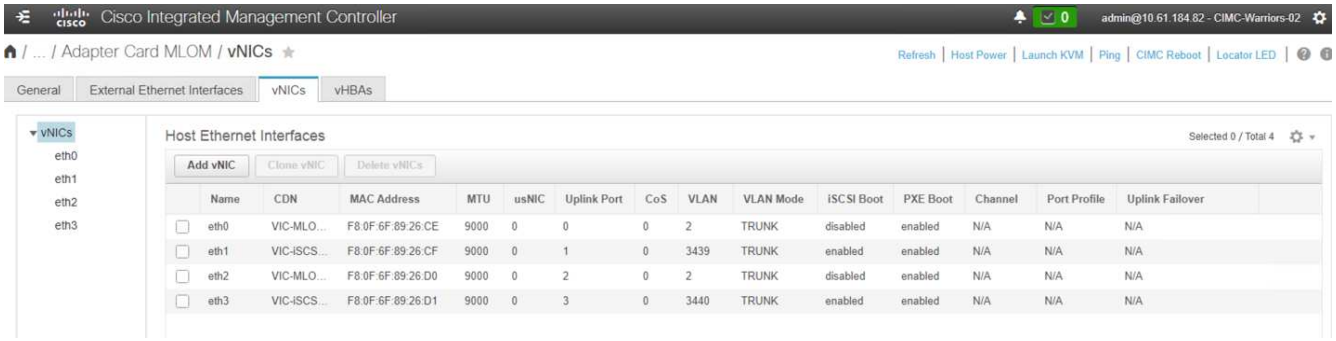
Configurer vNIC pour ESXi

Pour configurer vNIC pour ESXi, procédez comme suit :

1. Dans la fenêtre du navigateur de l'interface CIMC, cliquez sur Inventaire, puis sur cartes Cisco VIC dans le volet droit.
2. Sous mise en réseau > carte d'adaptateur MLOM, sélectionnez l'onglet vNIC, puis les vNIC en dessous.
3. Sélectionnez eth0, puis cliquez sur Propriétés.
4. Définissez la MTU sur 9000. Cliquez sur Save Changes.
5. Définissez le VLAN sur le VLAN natif 2.



6. Répétez les étapes 3 et 4 pour eth1, en vérifiant que le port uplink est défini sur 1 pour eth1.



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

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

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

Configuration du stockage de démarrage SAN ONTAP

Création des igroups iSCSI

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

Pour créer des igroups, exécutez les commandes suivantes depuis la connexion SSH du nœud de gestion du cluster. Pour afficher les trois groupes initiateurs créés au cours de cette étape, exécutez la `igroup show` commande.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

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

Mappez les LUN de démarrage sur les igroups

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-A –igroup
VM-Host-Infra-A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-B –igroup
VM-Host-Infra-B –lun-id 0
```

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

"Suivant : procédure de déploiement de VMware vSphere 6.7U2."

Procédure de déploiement de VMware vSphere 6.7U2

Cette section décrit les procédures détaillées d'installation de VMware ESXi 6.7U2 dans une configuration FlexPod Express. Les procédures de déploiement suivantes sont personnalisées pour inclure les variables d'environnement décrites dans les sections précédentes.

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

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

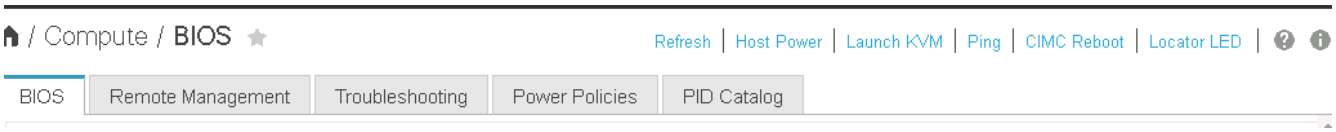
Cette procédure doit être effectuée pour tout nœud ajouté au cluster.

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

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

Tous les hôtes

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



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

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

7. Accédez au fichier image ISO du programme d'installation de VMware ESXi 6.7U2 et cliquez sur Ouvrir. Cliquez sur mapper le périphérique.
8. Sélectionnez le menu Marche/Arrêt et choisissez système de cycle d'alimentation (démarrage à froid). Cliquez sur Oui.

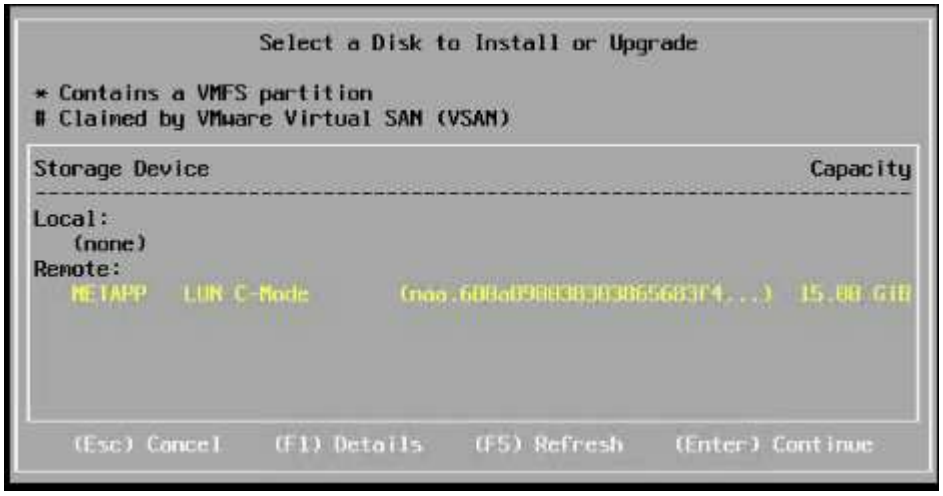
Installez VMware ESXi

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

Téléchargez l'image personnalisée CISCO ESXI 6.7U2

1. Accédez au "Page de téléchargement de VMware vSphere" Pour les ISO personnalisées.
2. Cliquez sur Go to Downloads en regard de l'image personnalisée Cisco pour le CD d'installation de VMware ESXi 6.7U2.
3. Téléchargez l'image personnalisée Cisco pour le CD d'installation de VMware ESXi 6.7U2 (ISO).
4. Lors du démarrage du système, la machine détecte la présence du support d'installation VMware ESXi.
5. Sélectionnez le programme d'installation de VMware ESXi dans le menu qui s'affiche. Le programme d'installation se charge, ce qui peut prendre plusieurs minutes.
6. Une fois le chargement terminé par le programme d'installation, appuyez sur entrée pour poursuivre l'installation.

7. Après avoir lu le contrat de licence de l'utilisateur final, acceptez-le et poursuivez l'installation en appuyant sur F11.
8. Sélectionnez le LUN NetApp précédemment configuré comme disque d'installation pour ESXi, et appuyez sur entrée pour poursuivre l'installation.



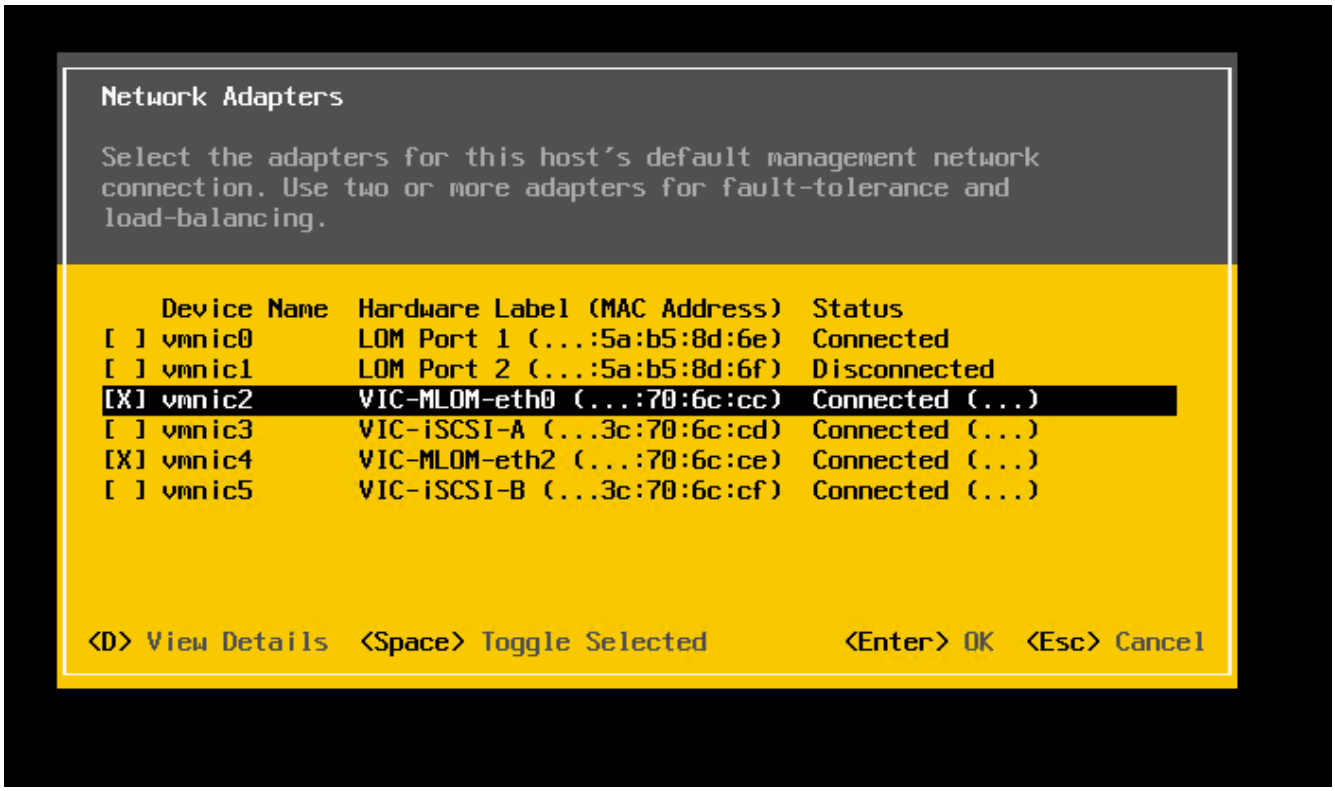
9. Sélectionnez la disposition de clavier appropriée et appuyez sur entrée.
10. Saisissez et confirmez le mot de passe racine, puis appuyez sur entrée.
11. Le programme d'installation vous avertit que les partitions existantes sont supprimées du volume. Poursuivre l'installation en appuyant sur F11.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

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

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

Tous les hôtes

1. Une fois le redémarrage du serveur terminé, entrez l'option permettant de personnaliser le système en appuyant sur F2.
2. Connectez-vous avec root en tant que nom de connexion et mot de passe racine entrés précédemment au cours du processus d'installation.
3. Sélectionnez l'option configurer le réseau de gestion.
4. Sélectionnez cartes réseau et appuyez sur entrée.
5. Sélectionnez les ports souhaités pour vSwitch0. Appuyez sur entrée.
6. Sélectionnez les ports qui correspondent à eth0 et eth1 dans CIMC.



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

25. Sélectionnez Options de dépannage, puis Activer ESXi Shell et SSH.

> Ces options de dépannage peuvent être désactivées après la validation conformément à la stratégie de sécurité du client.

26. Appuyez deux fois sur Echap pour revenir à l'écran principal de la console.
27. Cliquez sur Alt-F1 dans le menu déroulant macros statiques > macros statiques > Alt-F en haut de l'écran.
28. Connectez-vous à l'aide des informations d'identification appropriées pour l'hôte ESXi.
29. À l'invite, entrez la liste suivante des commandes esxcli séquentiellement pour activer la connectivité réseau.

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

Configurer l'hôte ESXi

Utilisez les informations du tableau suivant pour configurer chaque hôte ESXi.

Détails	Valeur de détail
Nom d'hôte ESXi	<<esxi_host_fqdn>>
IP de gestion d'hôte ESXi	<<esxi_host_mgmt_ip>>
Masque de gestion d'hôte ESXi	<<masque de réseau esxi_host_mgmt_mgmt>>
Passerelle de gestion de l'hôte ESXi	<<esxi_host_mgmt_gateway>>
IP NFS de l'hôte ESXi	<<esxi_host_NFS_ip>>
Masque NFS hôte ESXi	<<masque de réseau esxi_Host_NFS>>
Passerelle NFS de l'hôte ESXi	<<esxi_host_NFS_Gateway>>
IP vMotion hôte ESXi	<<esxi_host_vMotion_ip>>
Masque vMotion hôte ESXi	<<esxi_Host_vMotion_masque de réseau>>
Passerelle vMotion de l'hôte ESXi	<<esxi_host_vMotion_Gateway>>
Hôte ESXi iSCSI-A IP	<<esxi_host_iSCSI-A_ip>>
Masque iSCSI-A de l'hôte ESXi	\<<esxi_host_iSCSI-A_netmask>
Passerelle iSCSI-A de l'hôte ESXi	<<esxi_host_iSCSI-A_Gateway>>
Adresse IP iSCSI-B de l'hôte ESXi	<<esxi_host_iSCSI-B_ip>>
Masque iSCSI-B de l'hôte ESXi	\<<esxi_host_iSCSI-B_netmask>
Passerelle iSCSI-B de l'hôte ESXi	<<esxi_host_SCSI-B_Gateway>>

Connectez-vous à l'hôte ESXi

Pour vous connecter à l'hôte ESXi, procédez comme suit :

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

Configurez le démarrage iSCSI

Pour configurer le démarrage iSCSI, procédez comme suit :

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

3. Cliquez sur iSciBootvSwitch.
4. Sélectionnez Modifier les paramètres.
5. Définissez la MTU sur 9000 et cliquez sur Enregistrer.
6. Renommez le port iSCSIBootPG en iSCSIBootPG-A.

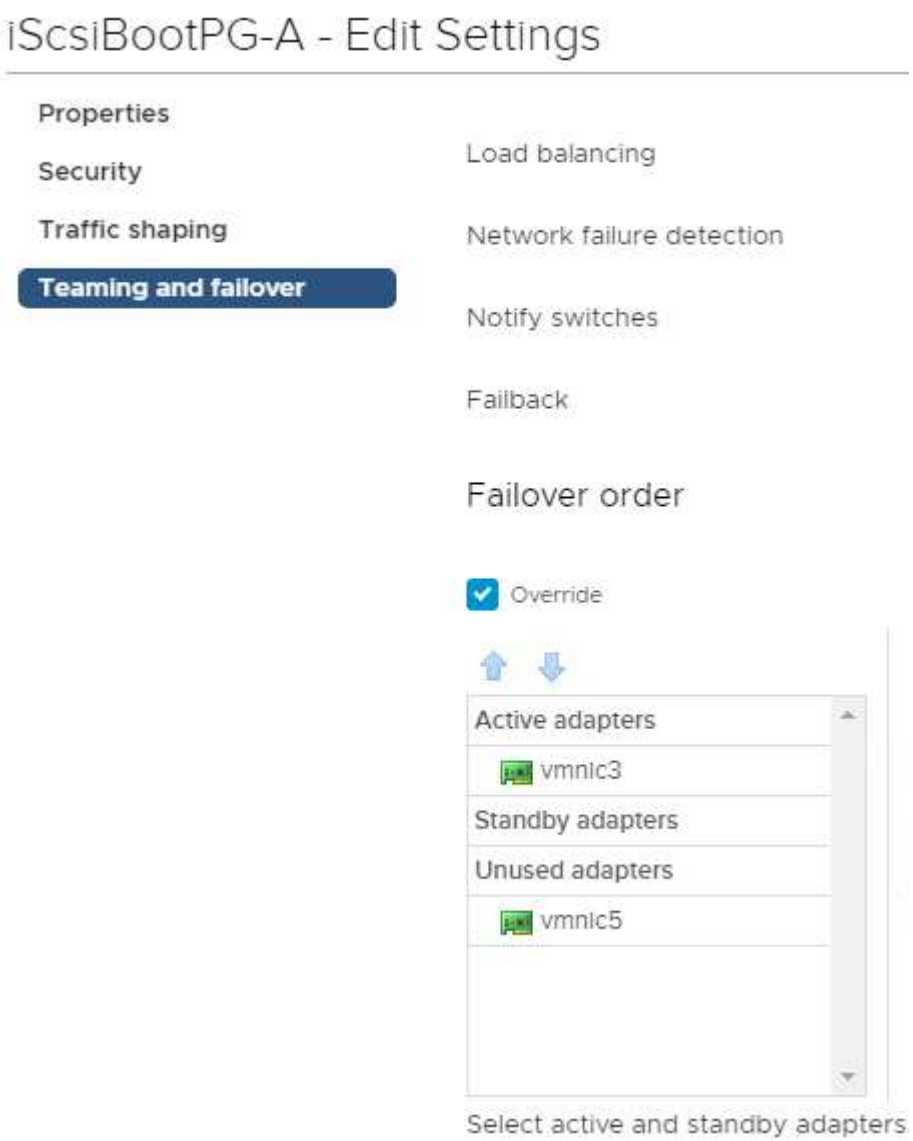
> Vmnic3 et vmnic5 sont utilisés pour le démarrage iSCSI dans cette configuration. Si vous disposez de cartes réseau supplémentaires dans votre hôte ESXi, vous pourriez avoir différents numéros vmnic. Pour vérifier quelles cartes réseau sont utilisées pour le démarrage iSCSI, faites correspondre les adresses MAC des cartes vNIC iSCSI dans CIMC aux adresses vmnics dans ESXi.

7. Dans le volet central, sélectionnez l'onglet VMkernel NIC.
8. Sélectionnez Ajouter une carte réseau VMkernel.
   a. Spécifiez un nouveau nom de groupe de ports de iScsiBootPG-B.
   b. Sélectionnez iSciBootvSwitch pour le commutateur virtuel.
   c. Entrez `<<iscsib_vlan_id>>` Pour l'ID VLAN.

d. Remplacez la MTU par 9000.
e. Développez Paramètres IPv4.
f. Sélectionnez Configuration statique.
g. Entrez `<<var_hosta_iscsib_ip>>` Pour adresse.
h. Entrez `<<var_hosta_iscsib_mask>>` Pour masque de sous-réseau.
i. Cliquez sur Créer .

Définissez la MTU sur 9000 sur iScsiBootPG-A.

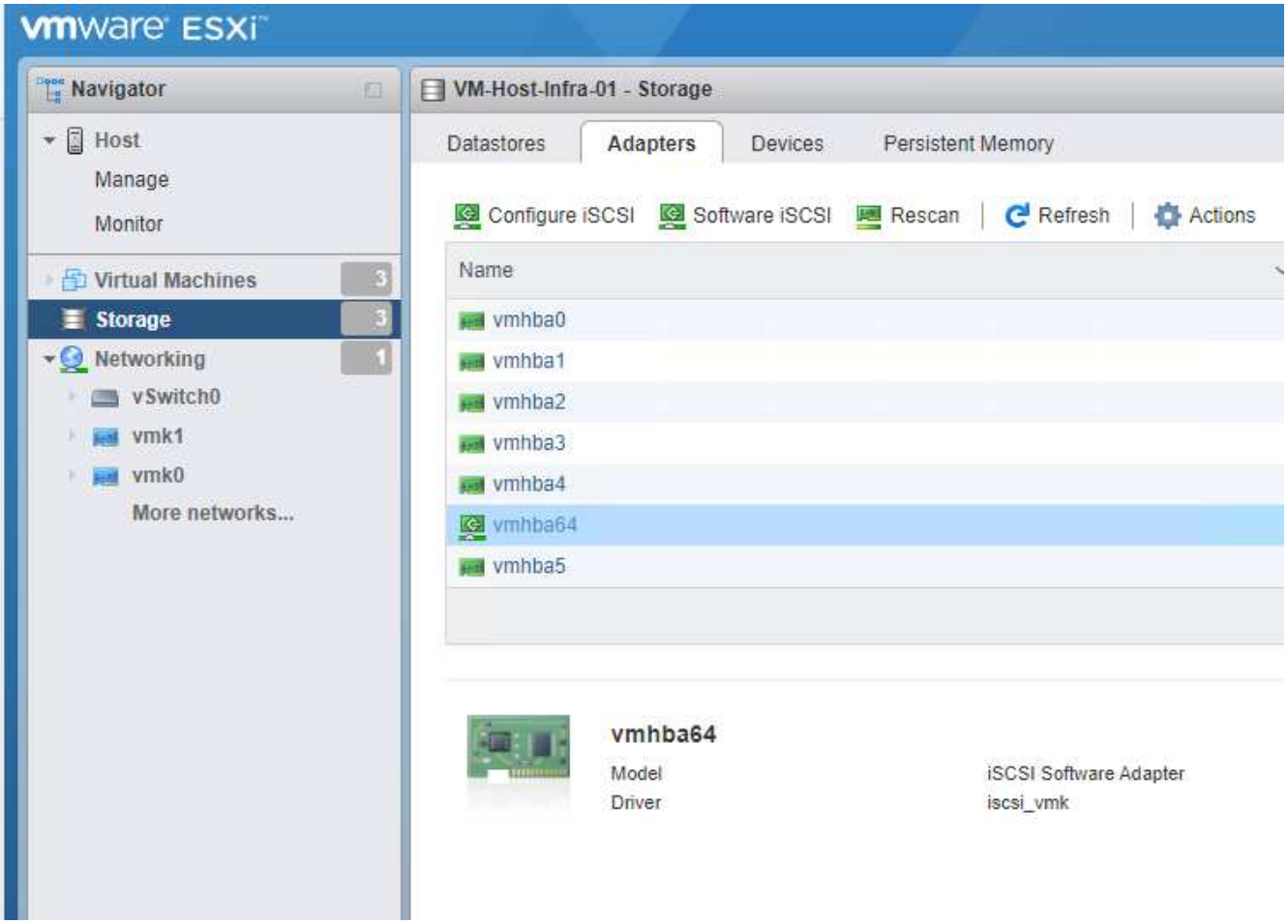
9. Pour configurer le basculement, procédez comme suit :
   a. Cliquez sur Modifier les paramètres sur iSCSIBootPG-A > Tiering et basculement > ordre de basculement > vmnic3. Vmnic3 doit être actif et vmnic5 ne doit pas être utilisé.
   b. Cliquez sur Modifier les paramètres dans iSCSIBootPG-B > agrégation et basculement > ordre de basculement > vmnic5. Vmnic5 doit être actif et vmnic3 ne doit pas être utilisé.



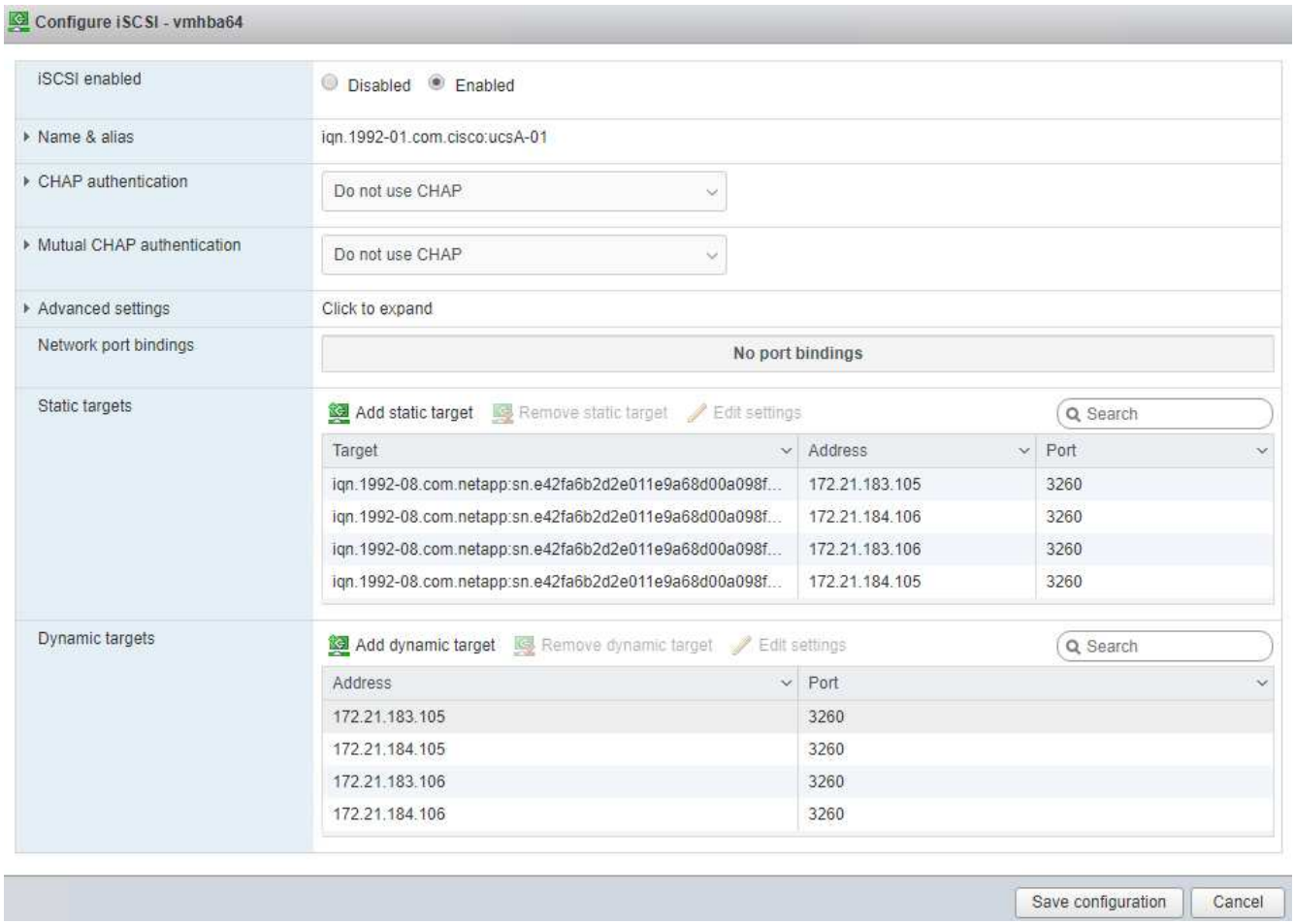
Configurez les chemins d’accès multiples iSCSI

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

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



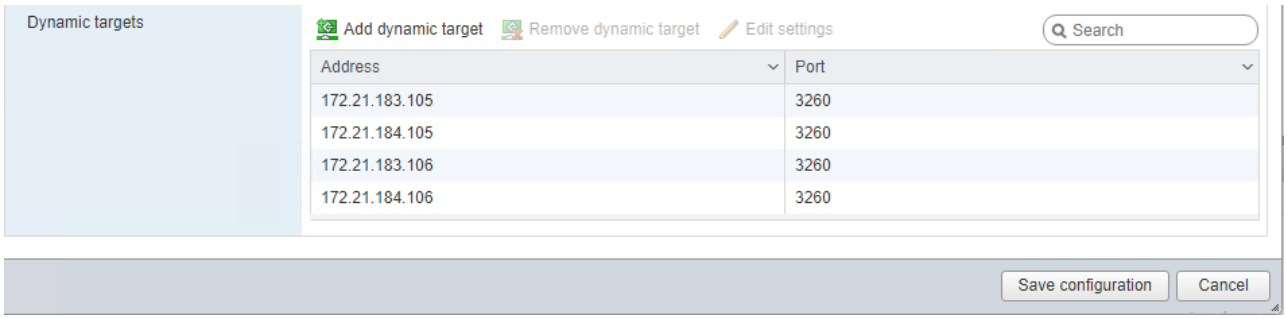
3. Sous cibles dynamiques, cliquez sur Ajouter une cible dynamique.



4. Saisissez l'adresse IP `iscsi_lif01a`.

   a. Répétez l'opération avec les adresses IP `iscsi_lif01b`, `iscsi_lif02a`, et `iscsi_lif02b`.

   b. Cliquez sur Enregistrer la configuration.



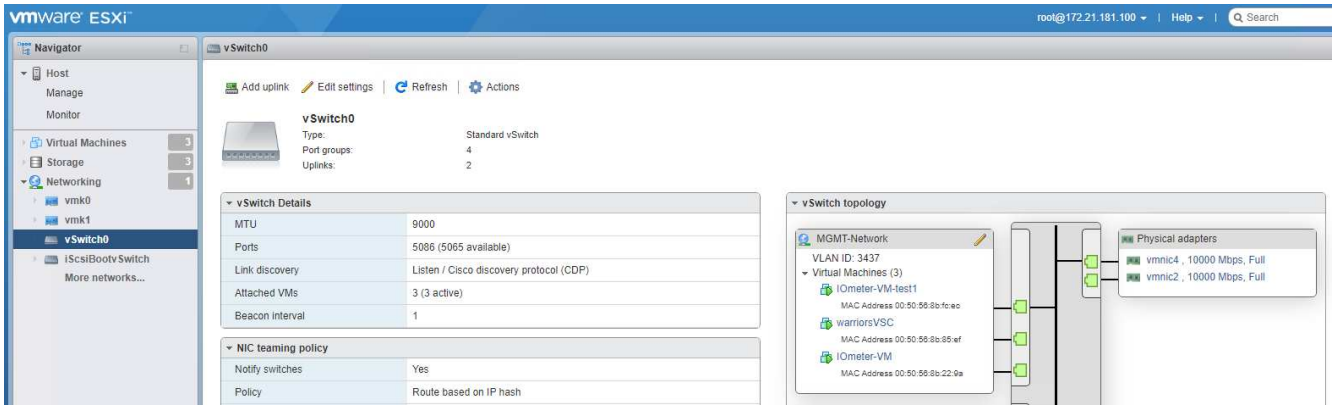
Vous pouvez trouver les adresses IP de LIF iSCSI en exécutant la commande network interface show sur le cluster NetApp ou en consultant l'onglet Network interfaces dans System Manager.

Configurez l'hôte ESXi

Pour configurer le démarrage ESXi, procédez comme suit :

1. Dans le volet de navigation de gauche, sélectionnez réseau.

2. Sélectionnez vSwitch0.



3. Sélectionnez Modifier les paramètres.
4. Remplacez la MTU par 9000.
5. Développez agrégation de cartes réseau et vérifiez que vmnic2 et vmnic4 sont tous deux définis sur actif et que NIC Teaming and Failover est défini sur routage basé sur le hachage IP.

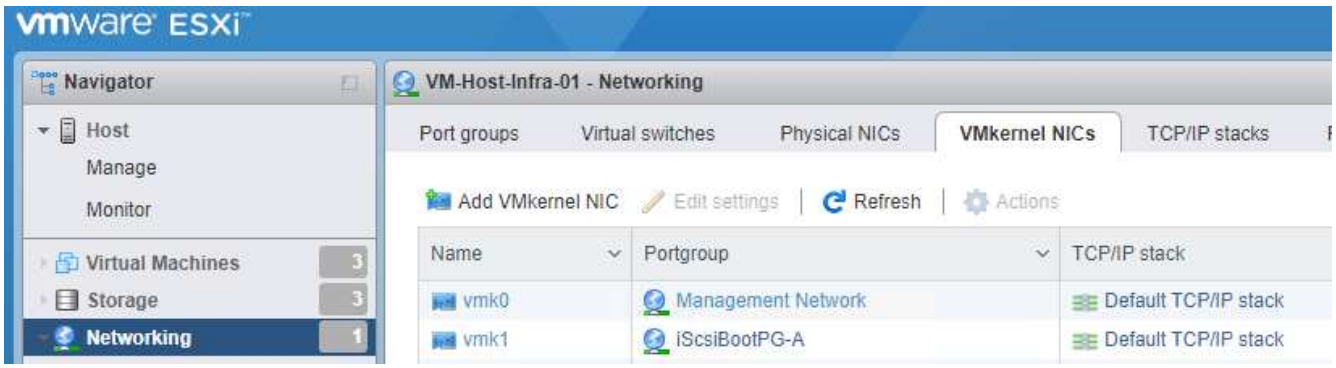
> La méthode de hachage IP d'équilibrage de charge nécessite la configuration correcte du commutateur physique sous-jacent à l'aide de SRC-DST-IP EtherChannel avec un canal de port statique (mode- on). Il est possible que la connectivité soit intermittente en raison d'éventuelles erreurs de configuration du commutateur. Si c'est le cas, arrêtez temporairement l'un des deux ports de liaison montante associés sur le commutateur Cisco pour restaurer la communication vers le port VMware de gestion VMware ESXi lors du dépannage des paramètres du canal de port.

Configurez les groupes de ports et les NIC VMkernel

Pour configurer les groupes de ports et les NIC VMKernel, procédez comme suit :

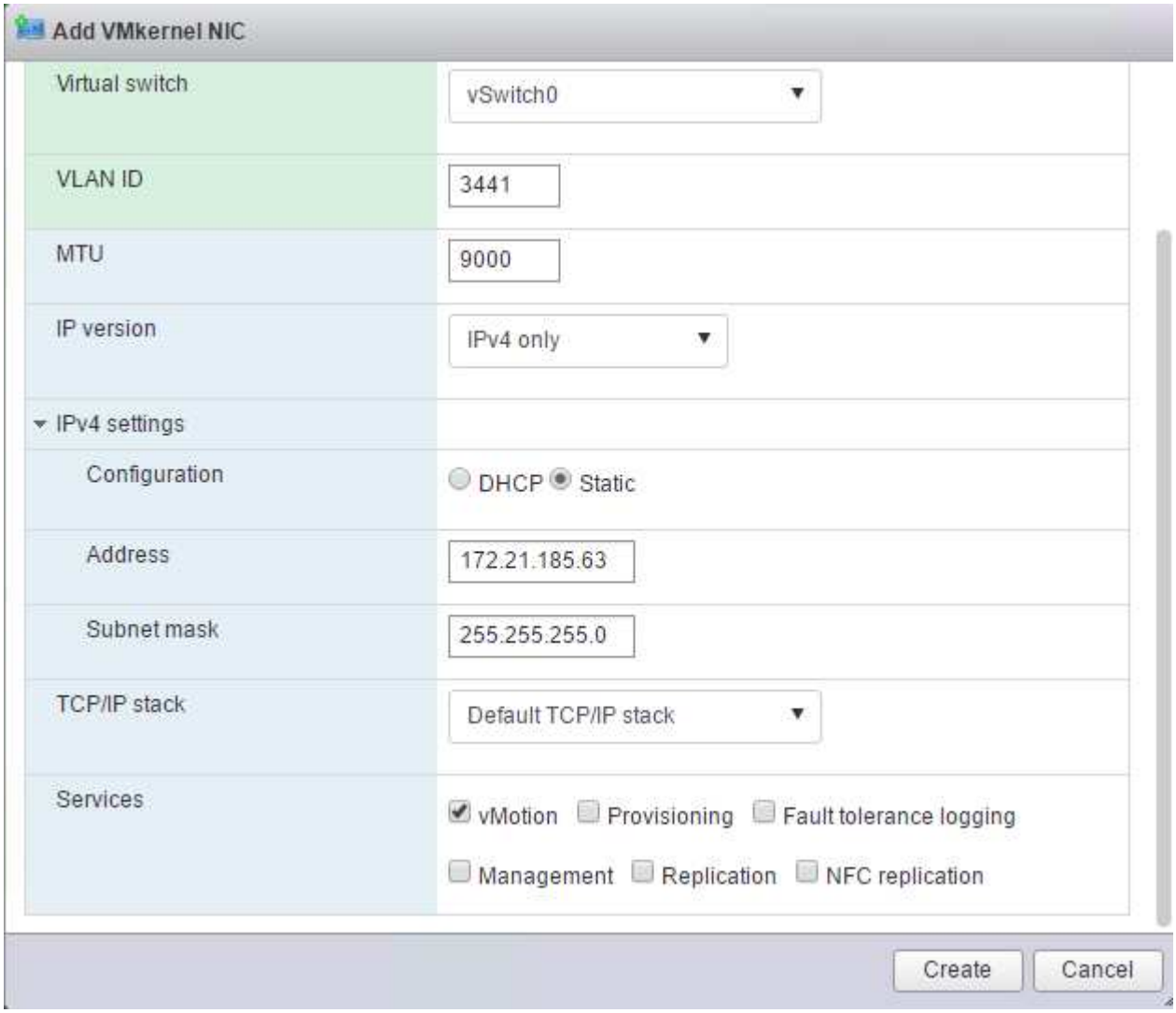
1. Dans le volet de navigation de gauche, sélectionnez réseau.
2. Cliquez avec le bouton droit de la souris sur l'onglet groupes de ports.

3. Cliquez avec le bouton droit de la souris sur réseau VM et sélectionnez Modifier. Définissez l'ID du VLAN sur `<<var_vm_traffic_vlan>>`.
4. Cliquez sur Ajouter un groupe de ports.
   a. Nommez le groupe de ports MGMT-Network.
   b. Entrez `<<mgmt_vlan>>` Pour l'ID VLAN.
   c. Vérifiez que vSwitch0 est sélectionné.
   d. Cliquez sur enregistrer.
5. Cliquez sur l'onglet VMkernel NIC.



6. Sélectionnez Ajouter une carte réseau VMkernel.
   a. Sélectionnez Nouveau groupe de ports.
   b. Attribuez un nom au groupe de ports NFS-Network.
   c. Entrez `<<nfs_vlan_id>>` Pour l'ID VLAN.
   d. Remplacez la MTU par 9000.
   e. Développez Paramètres IPv4.
   f. Sélectionnez Configuration statique.
   g. Entrez `<<var_hosta_nfs_ip>>` Pour adresse.
   h. Entrez `<<var_hosta_nfs_mask>>` Pour masque de sous-réseau.
   i. Cliquez sur Créer .
7. Répétez ce processus pour créer le port VMkernel vMotion.
8. Sélectionnez Ajouter une carte réseau VMkernel.
   a. Sélectionnez Nouveau groupe de ports.
   b. Nommez le port group vMotion.
   c. Entrez `<<vmotion_vlan_id>>` Pour l'ID VLAN.
   d. Remplacez la MTU par 9000.
   e. Développez Paramètres IPv4.
   f. Sélectionnez Configuration statique.
   g. Entrez `<<var_hosta_vmotion_ip>>` Pour adresse.
   h. Entrez `<<var_hosta_vmotion_mask>>` Pour masque de sous-réseau.

i. Assurez-vous que la case vMotion est cochée après les paramètres IPv4.

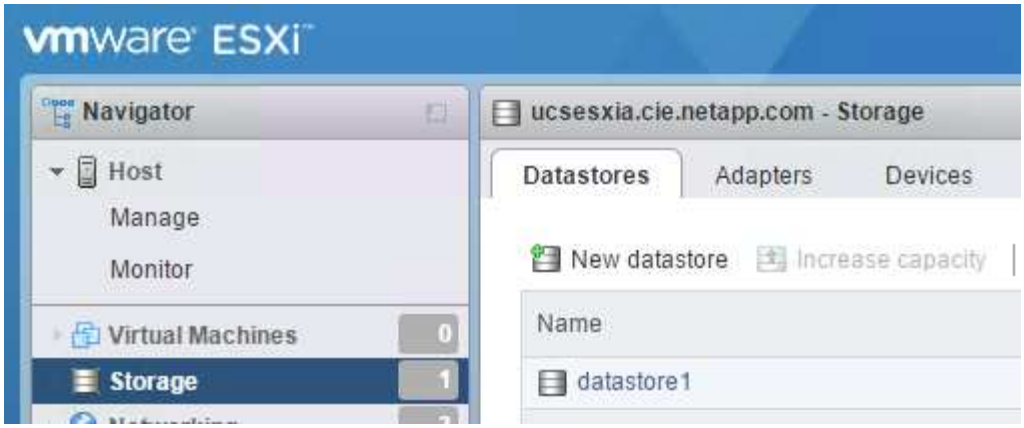


Il existe de nombreuses façons de configurer la mise en réseau VMware ESXi, y compris en utilisant le commutateur distribué VMware vSphere si votre licence le permet. Les autres configurations réseau sont prises en charge par FlexPod Express si elles sont requises pour répondre aux exigences de l'entreprise.

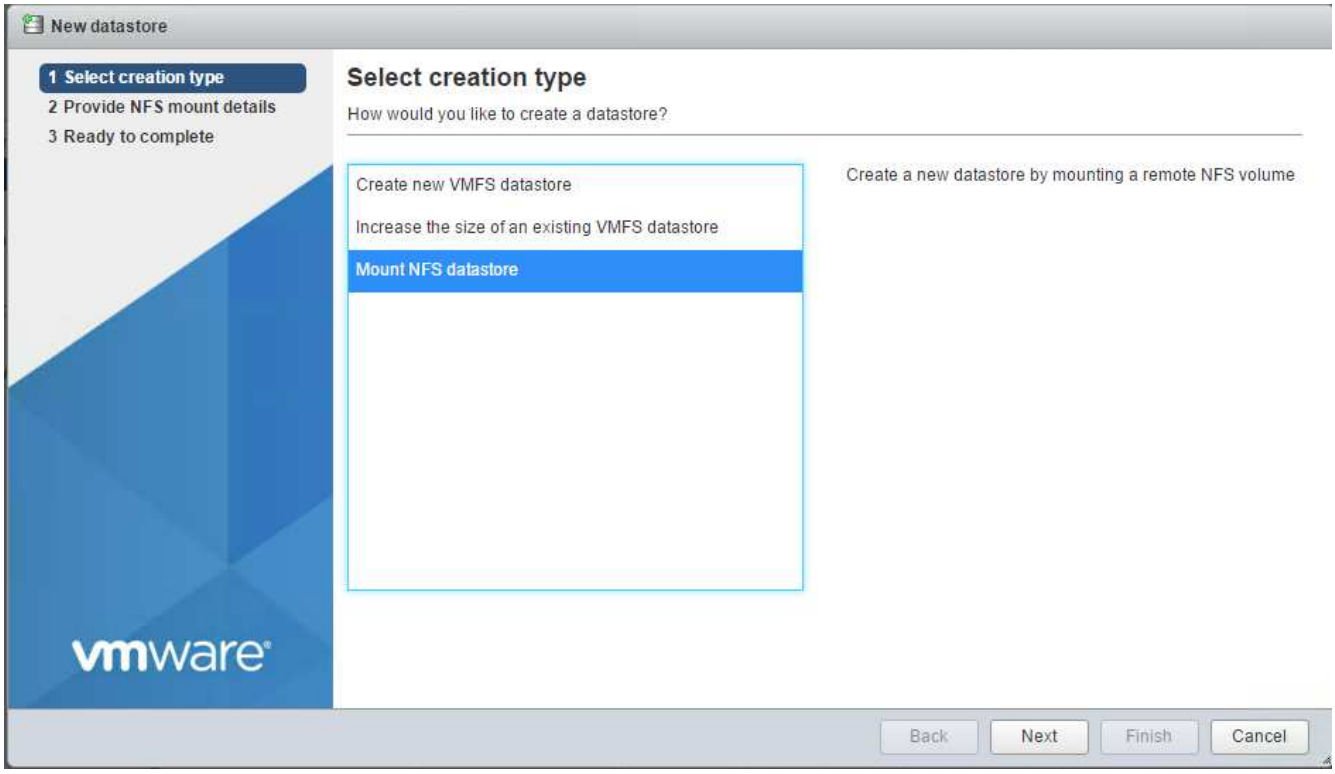
Montez les premiers datastores

Les premiers datastores à être montés sont les `infra_datastore` Datastore pour les VM et `infra_swap` Datastore pour les fichiers swap de VM.

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



2. Sélectionnez Mount NFS datastore.



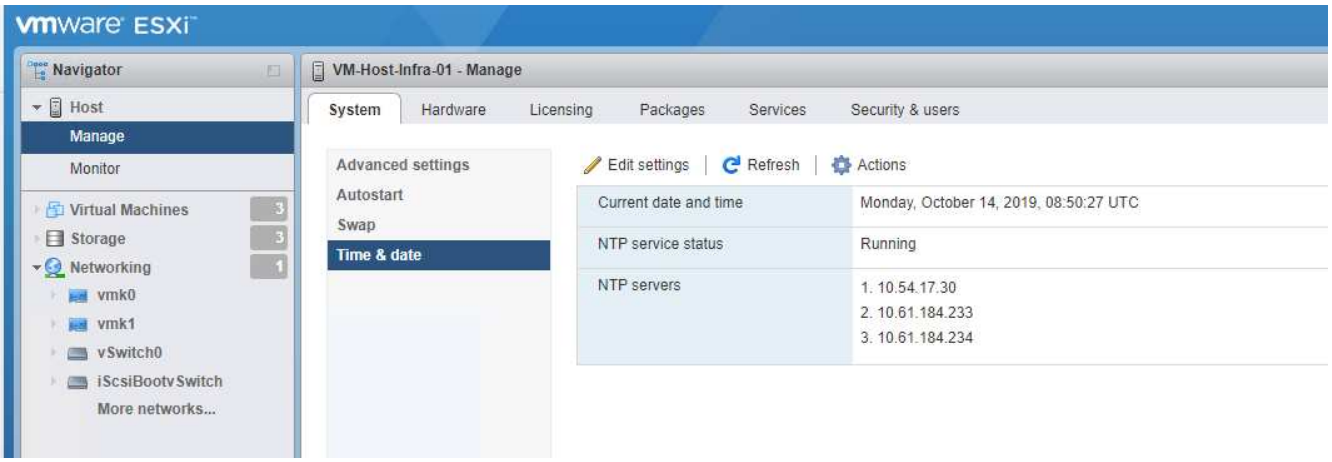
3. Entrez les informations suivantes dans la page Détails du montage NFS :
   - Nom : `infra_datastore`
   - Serveur NFS : `<<var_nodea_nfs_lif>>`
   - Partager : `/infra_datastore`
   - Assurez-vous que NFS 3 est sélectionné.
4. Cliquez sur Terminer. La tâche terminée s'affiche dans le volet tâches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

- Assurez-vous que NFS 3 est sélectionné.

Configurez NTP

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

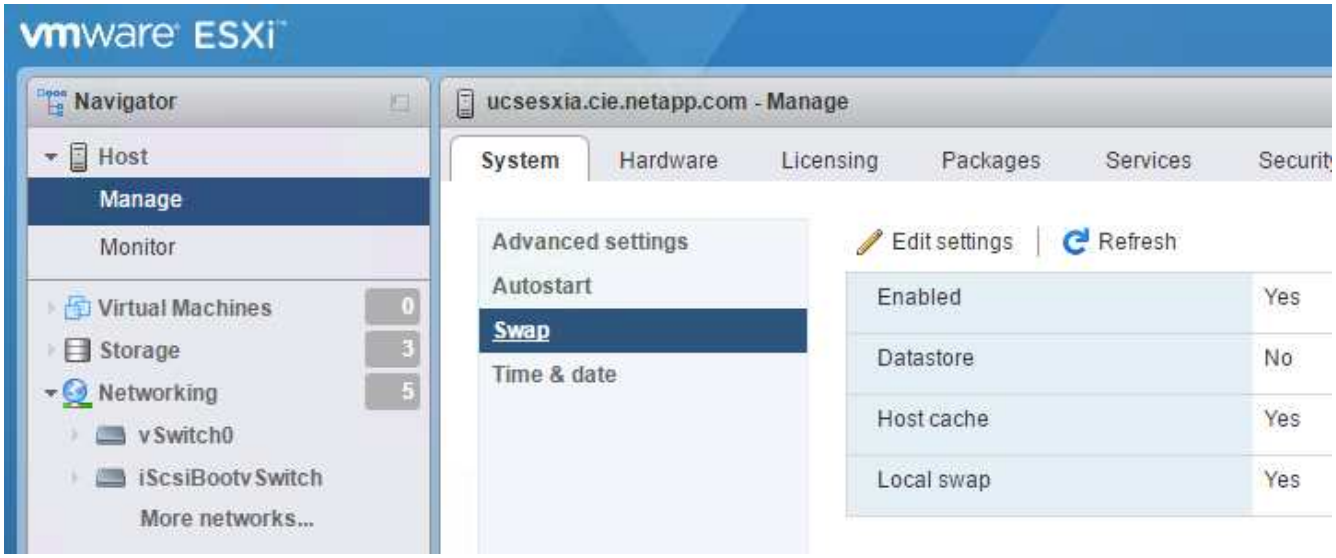
1. Cliquez sur gérer dans le volet de navigation de gauche. Sélectionnez système dans le volet de droite, puis cliquez sur heure et date.
2. Sélectionnez utiliser le protocole d'heure du réseau (Activer le client NTP).
3. Sélectionnez Démarrer et Arrêter avec l'hôte comme stratégie de démarrage du service NTP.
4. Entrez `<<var_ntp>>` En tant que serveur NTP. Vous pouvez définir plusieurs serveurs NTP.
5. Cliquez sur Enregistrer.



Déplacez l'emplacement du fichier d'échange VM

Cette procédure fournit des détails sur le déplacement de l'emplacement du fichier d'échange VM.

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



2. Cliquez sur Modifier les paramètres. Sélectionnez `infra_swap` Dans les options datastore.

3. Cliquez sur Enregistrer.

"Suivant : procédure d'installation de VMware vCenter Server 6.7U2."

Procédure d'installation de VMware vCenter Server 6.7U2

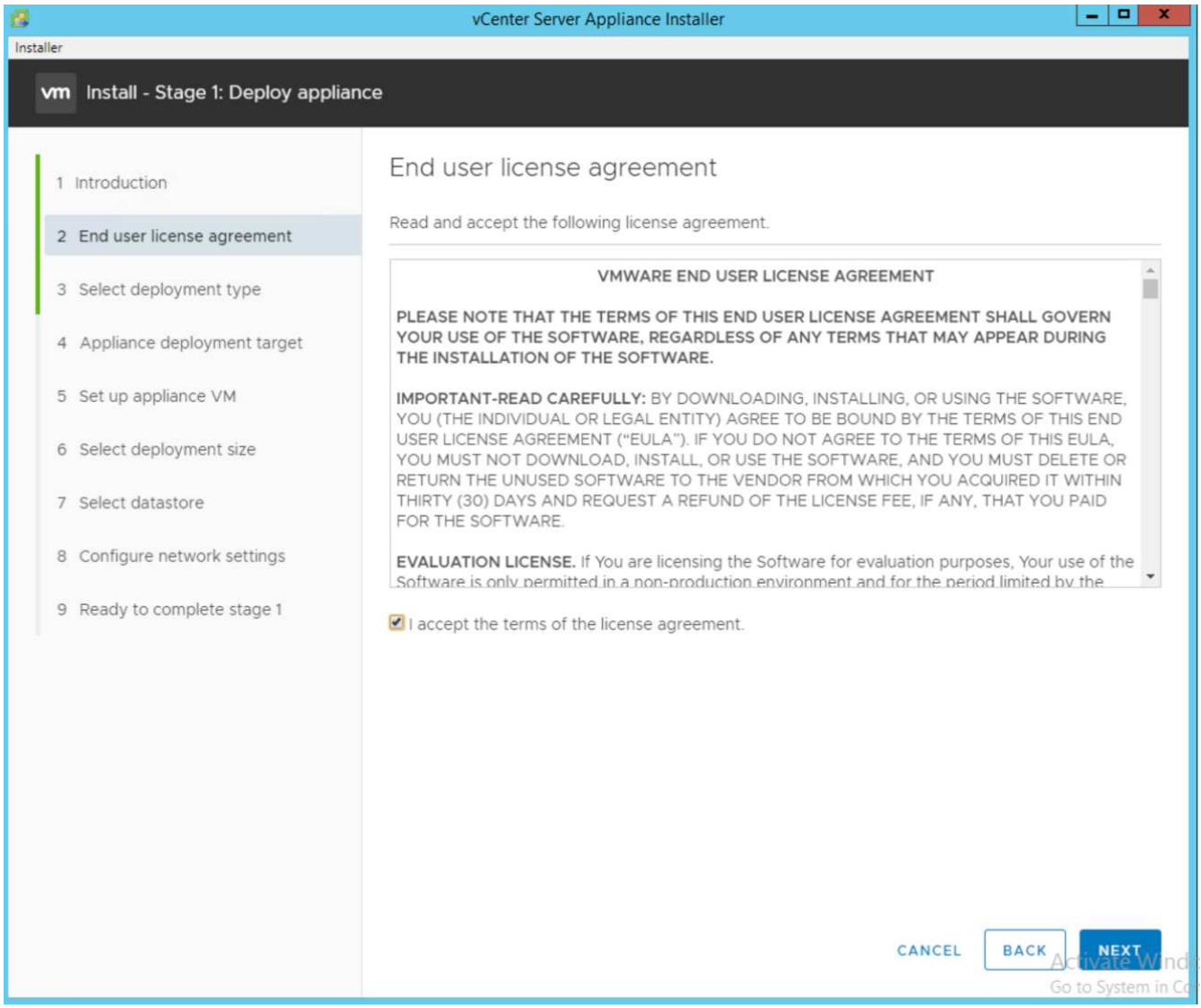
Cette section décrit les procédures détaillées d'installation de VMware vCenter Server 6.7 dans une configuration FlexPod Express.

FlexPod Express utilise VMware vCenter Server Appliance (VCSA).

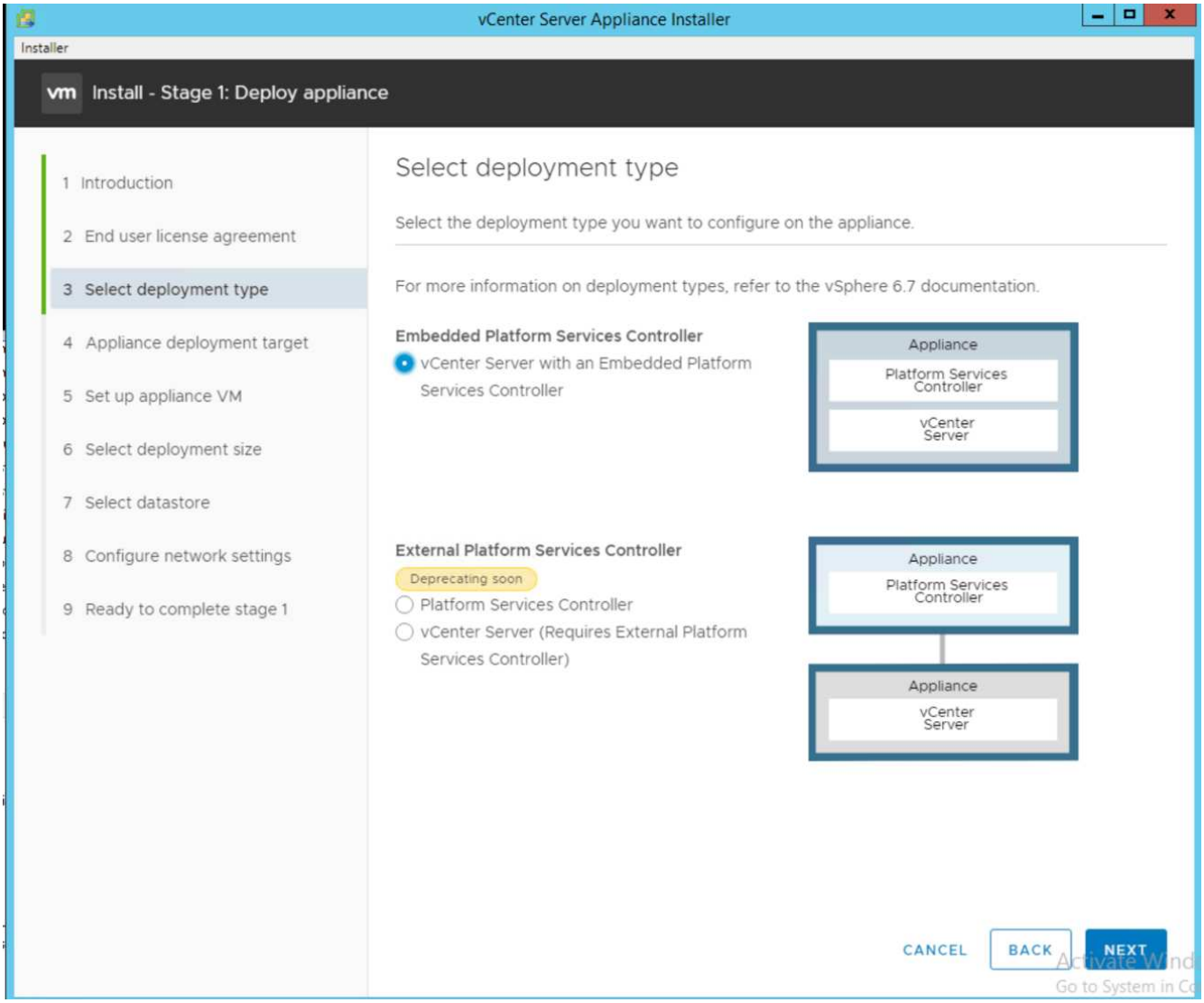
Téléchargez l'appliance VMware vCenter Server

Pour télécharger VMware vCenter Server Appliance (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.
3. Bien que l'installation de Microsoft Windows vCenter Server soit prise en charge, VMware recommande le VCSA pour les nouveaux déploiements.
4. Montez l'image ISO.
5. Accédez au répertoire vcsa- ui-installer > win32. Double-cliquez sur `installer.exe`.
6. Cliquez sur installation.
7. Cliquez sur Suivant sur la page Introduction.

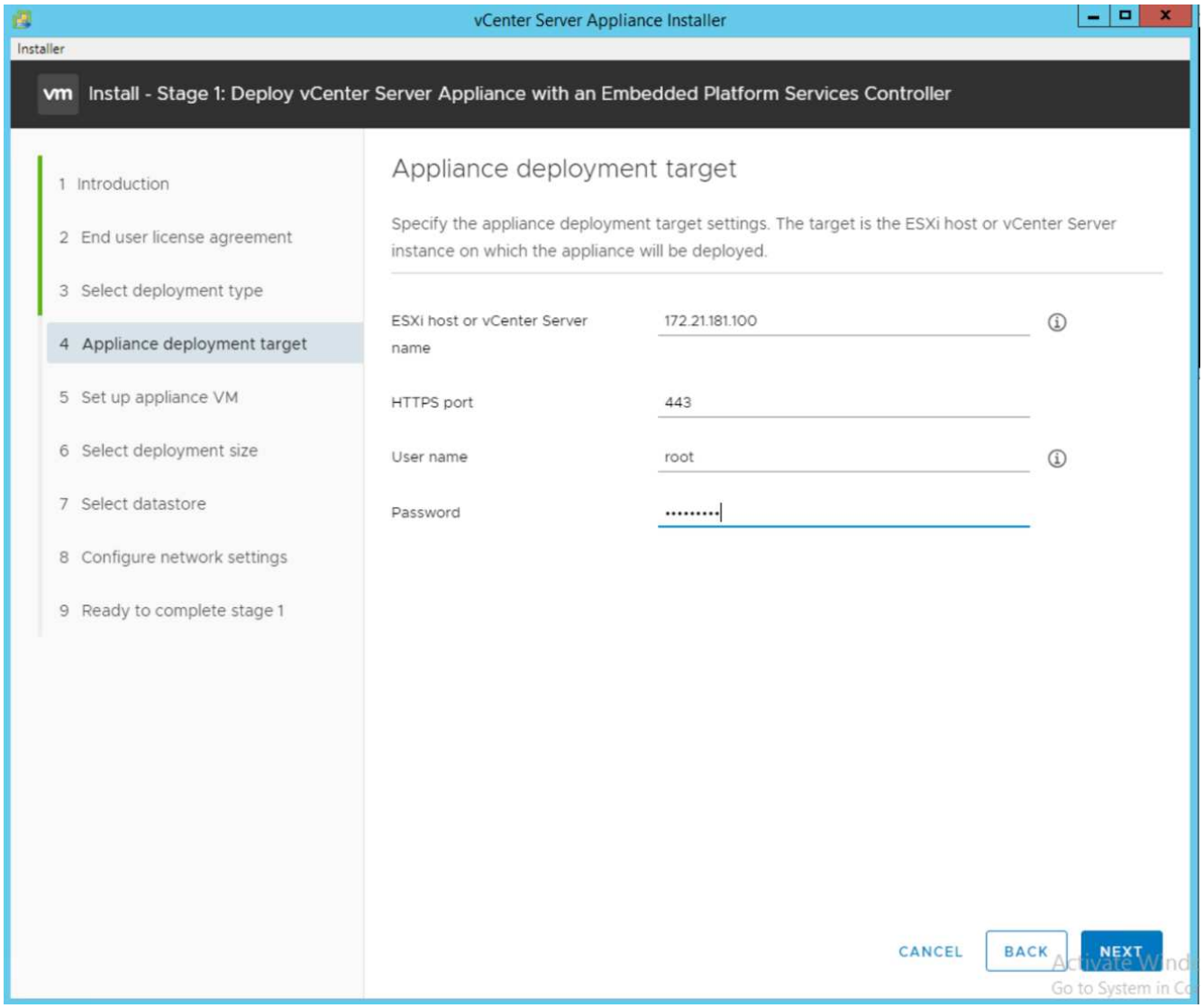


8. Sélectionnez Embedded Platform Services Controller comme type de déploiement.

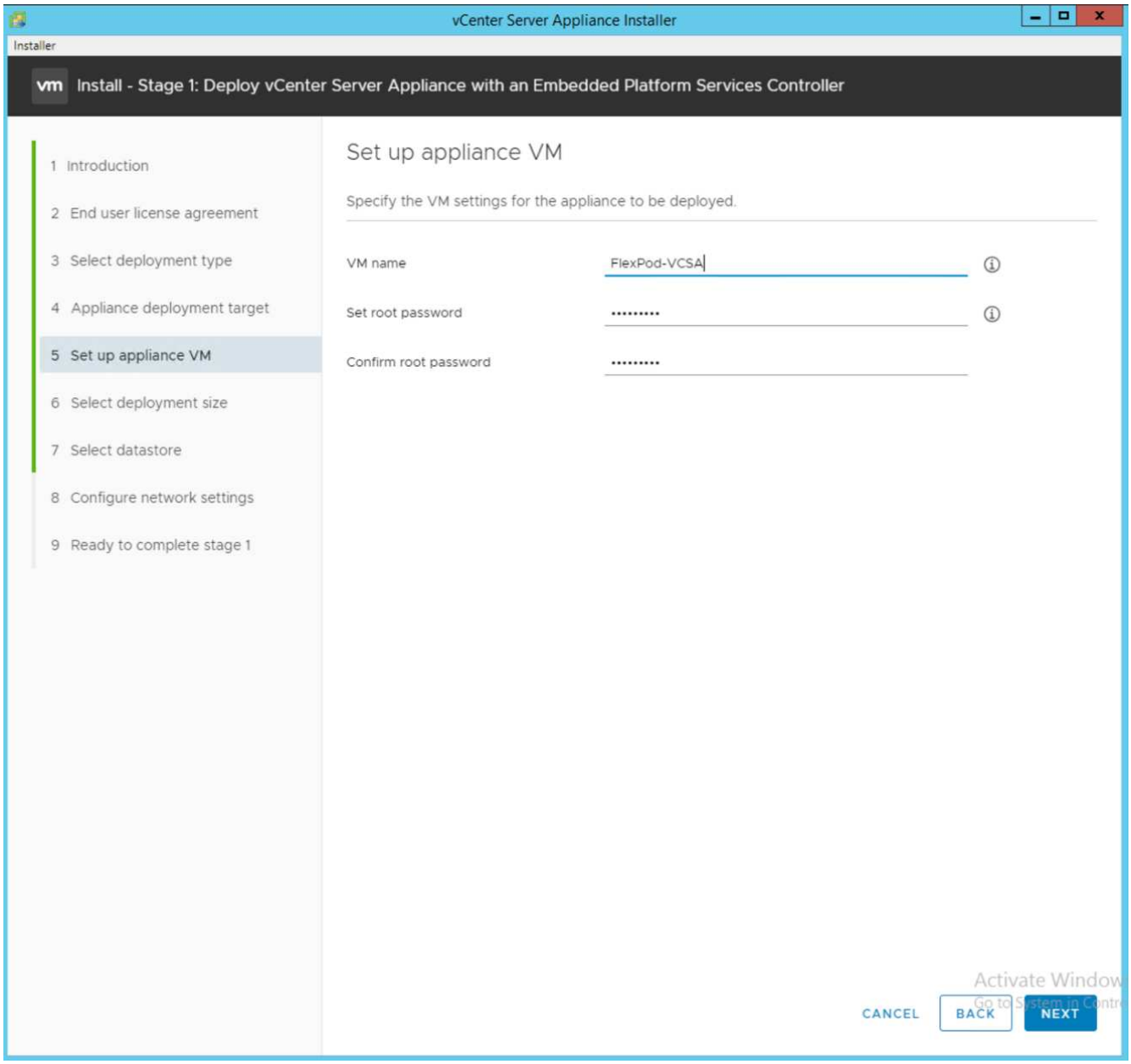


Si nécessaire, le déploiement de contrôleur de services de plateforme externe est également pris en charge dans le cadre de la solution FlexPod Express.

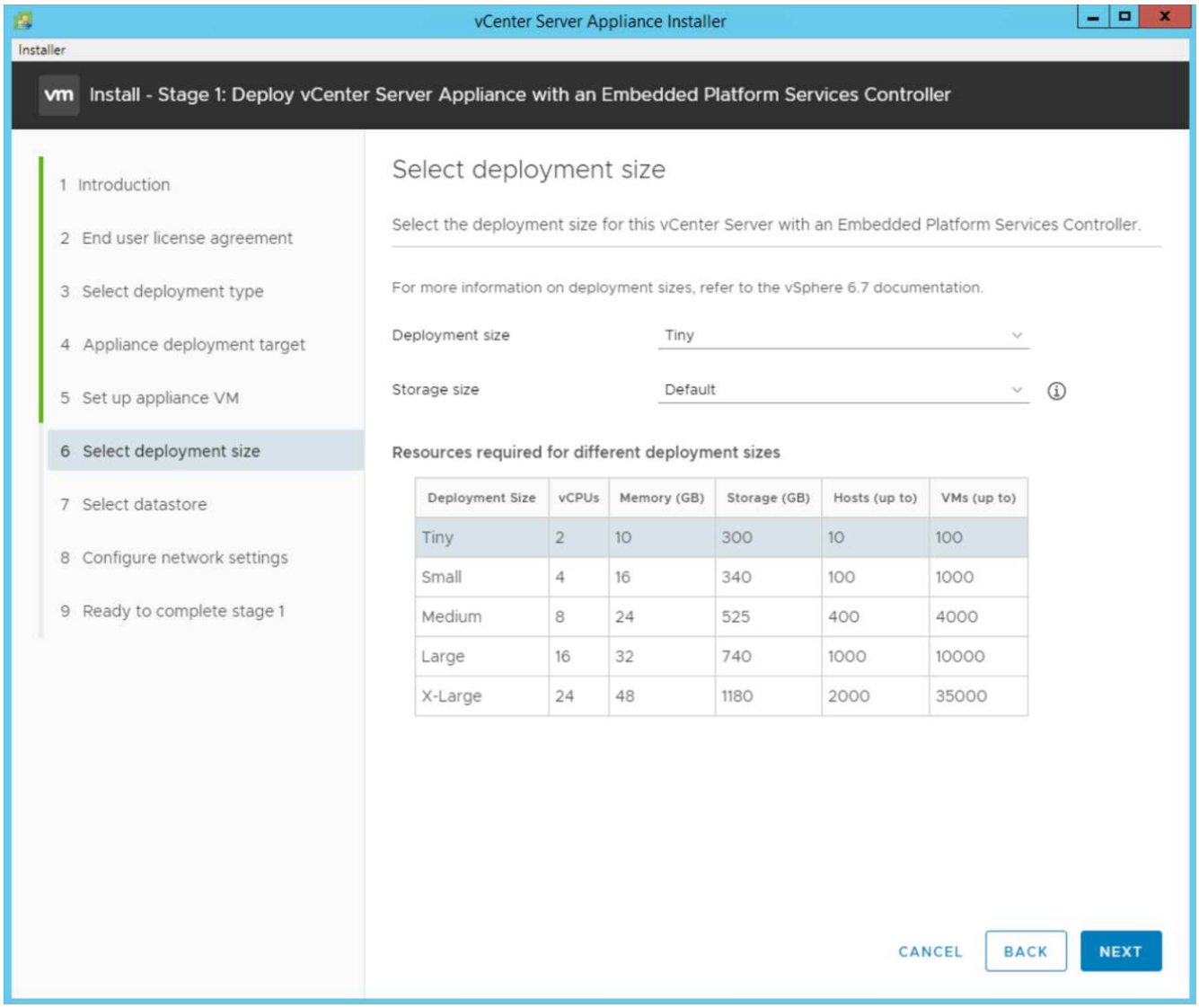
9. Dans la cible de déploiement de l'appliance, entrez l'adresse IP d'un hôte ESXi que vous avez déployé, le nom d'utilisateur root et le mot de passe root.



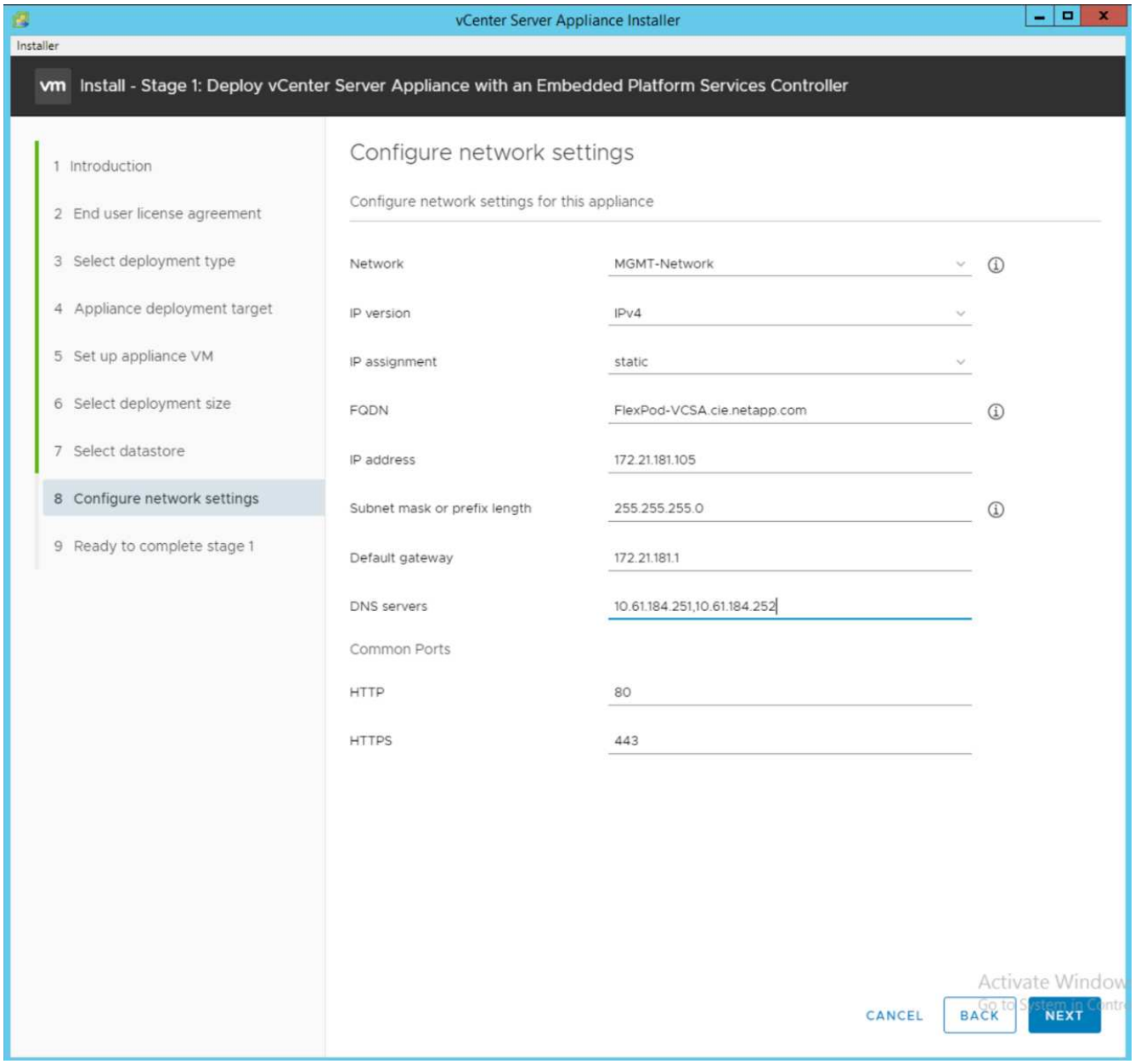
10. Définissez la machine virtuelle de l'appliance en saisissant VCSA comme nom de machine virtuelle et mot de passe root que vous souhaitez utiliser pour le VCSA.



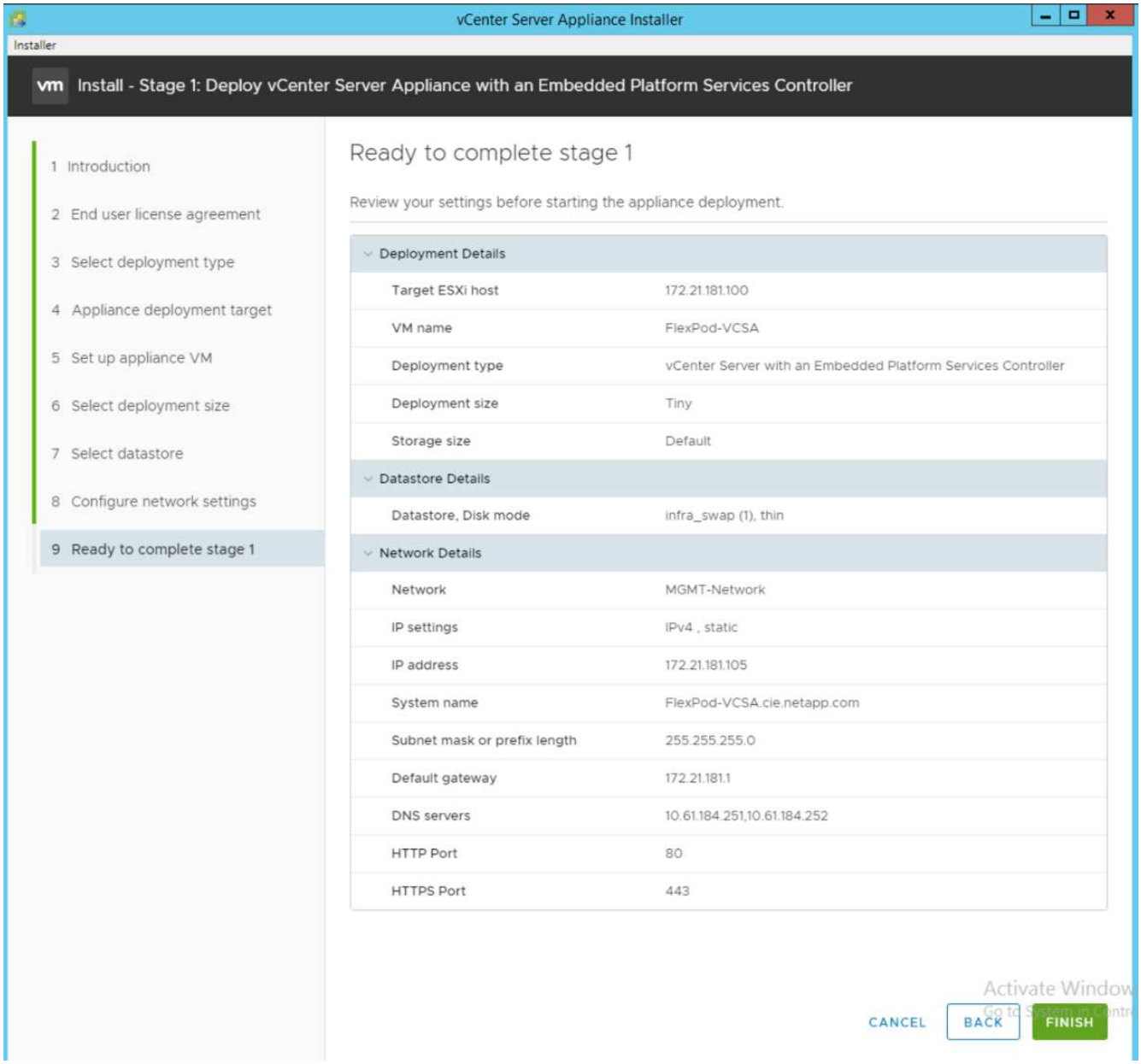
11. Choisissez la taille de déploiement qui correspond le mieux à votre environnement. Cliquez sur Suivant.



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

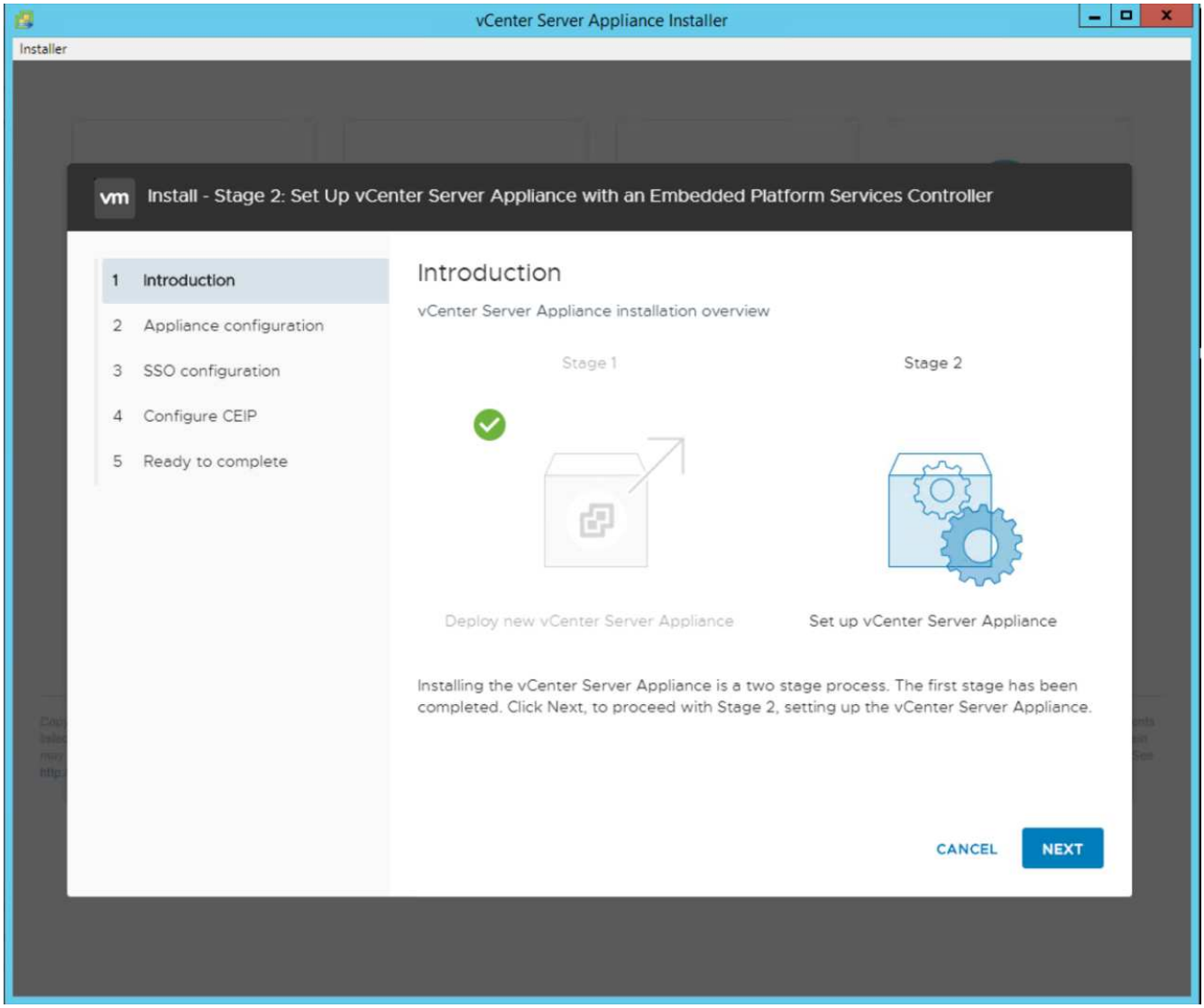


15. Passez en revue les paramètres de l'étape 1 avant de commencer le déploiement de l'appliance.

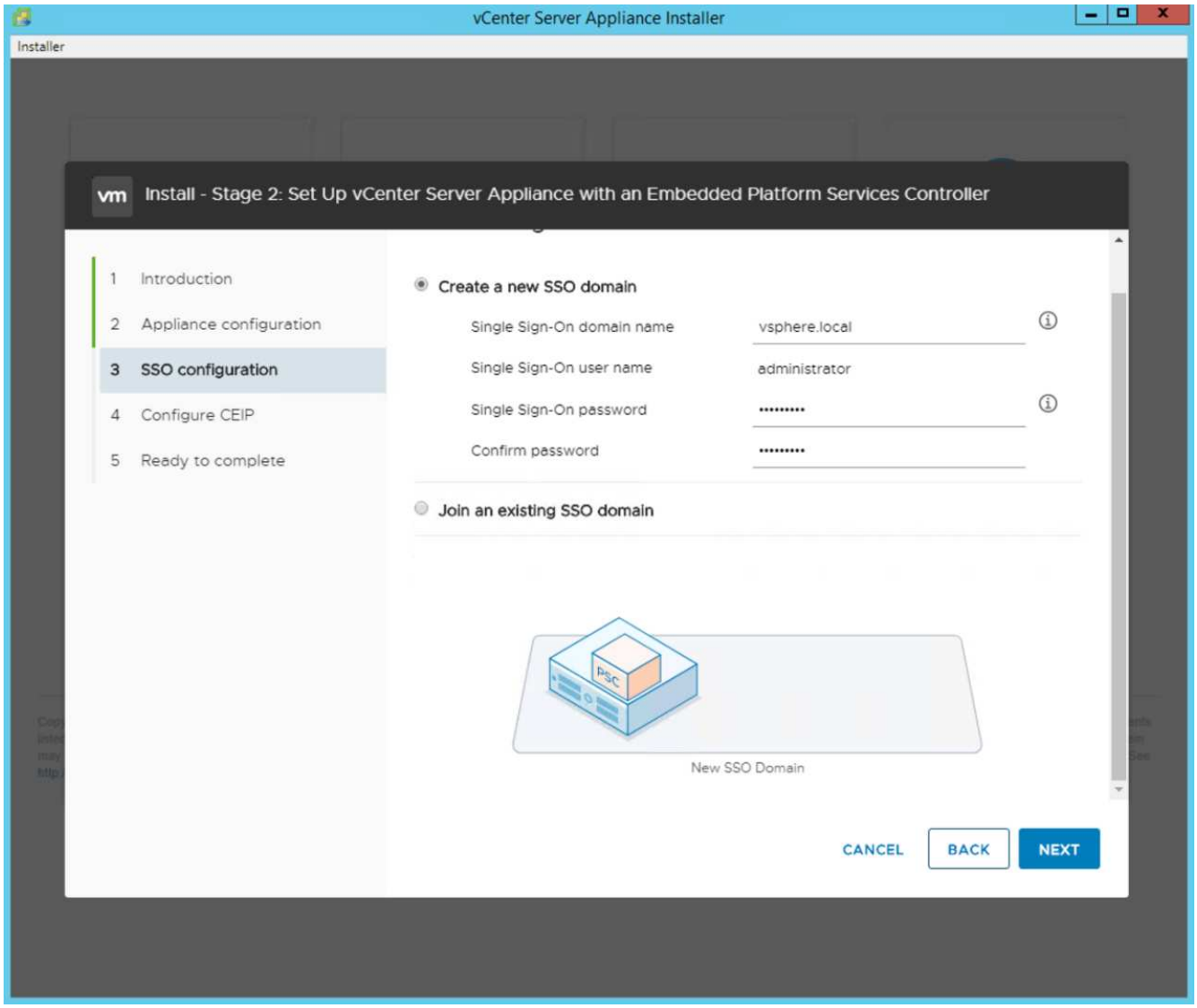


Le VCSA s'installe maintenant. Ce processus prend plusieurs minutes.

16. 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.
17. Sur la page Introduction de l'étape 2, cliquez sur Suivant.

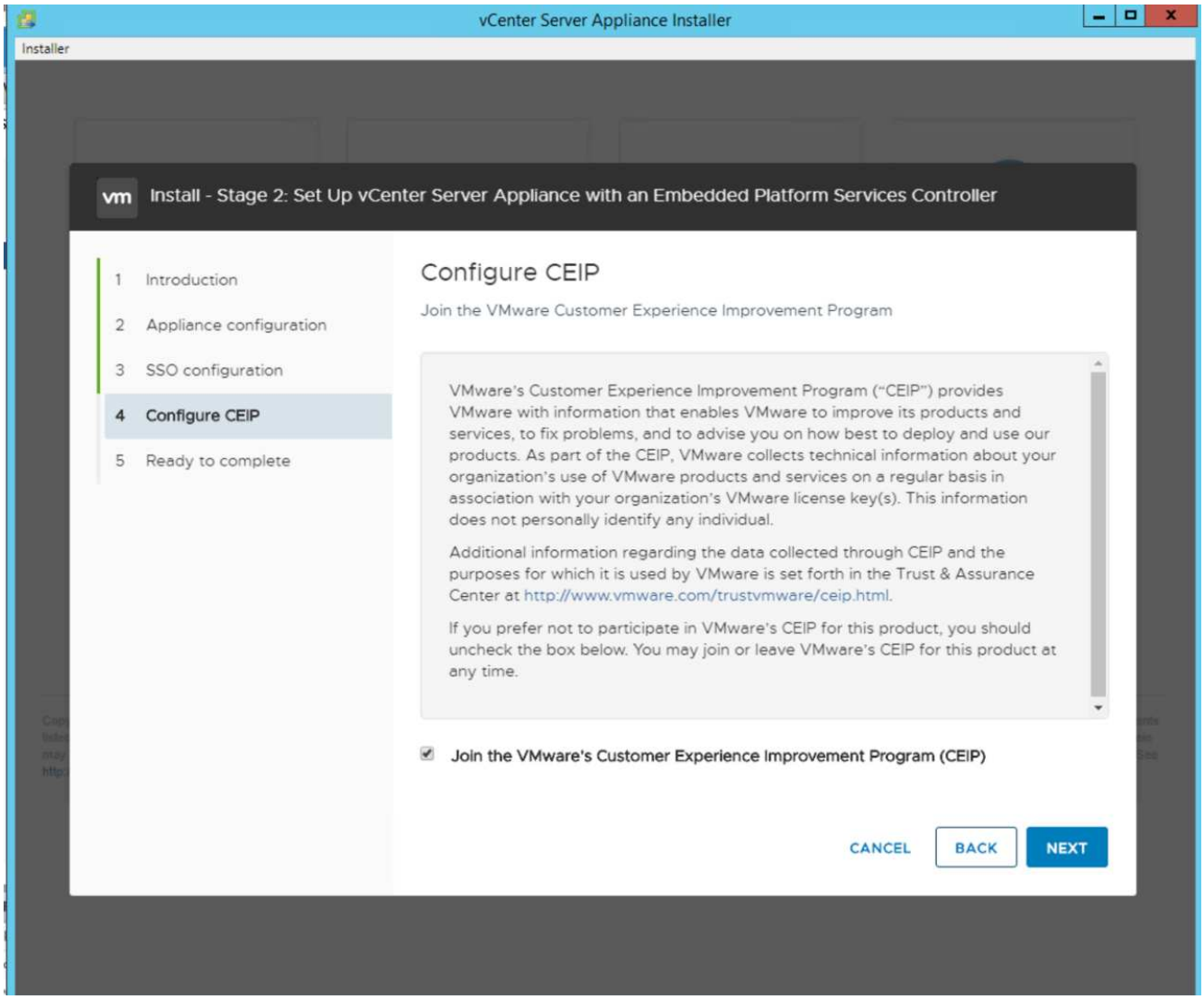


18. Entrez `<<var_ntp_id>>` Pour l'adresse du serveur NTP. Vous pouvez entrer plusieurs adresses IP NTP.
19. Si vous prévoyez d'utiliser la haute disponibilité (HA) de vCenter Server, assurez-vous que l'accès SSH est activé.
20. Configurez le nom de domaine SSO, le mot de passe et le nom du site. Cliquez sur Suivant.

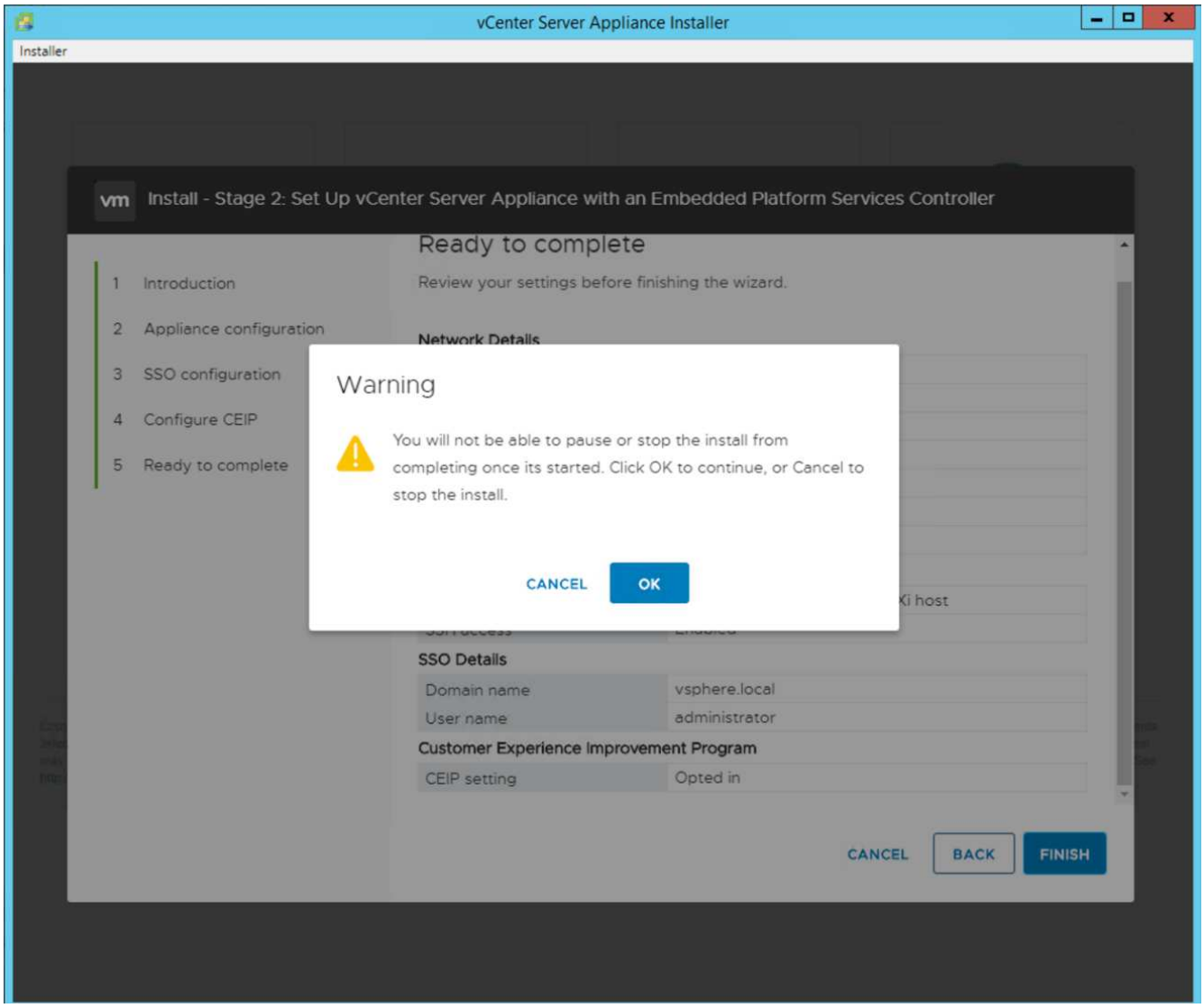


Notez ces valeurs pour votre référence, en particulier si vous vous écartez du `vsphere.local` nom de domaine.

21. Rejoignez le programme VMware Customer Experience si nécessaire. Cliquez sur Suivant.



22. Affichez le récapitulatif de vos paramètres. Cliquez sur Terminer ou utilisez le bouton Retour pour modifier les paramètres.
23. Un message s'affiche indiquant que vous ne pourrez pas interrompre ou arrêter l'installation une fois qu'elle a démarré. Cliquez sur OK pour continuer.



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

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

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

"Suivant : configuration de la mise en cluster VMware vCenter Server 6.7U2 et vSphere."

Configuration de la mise en cluster VMware vCenter Server 6.7U2 et vSphere

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

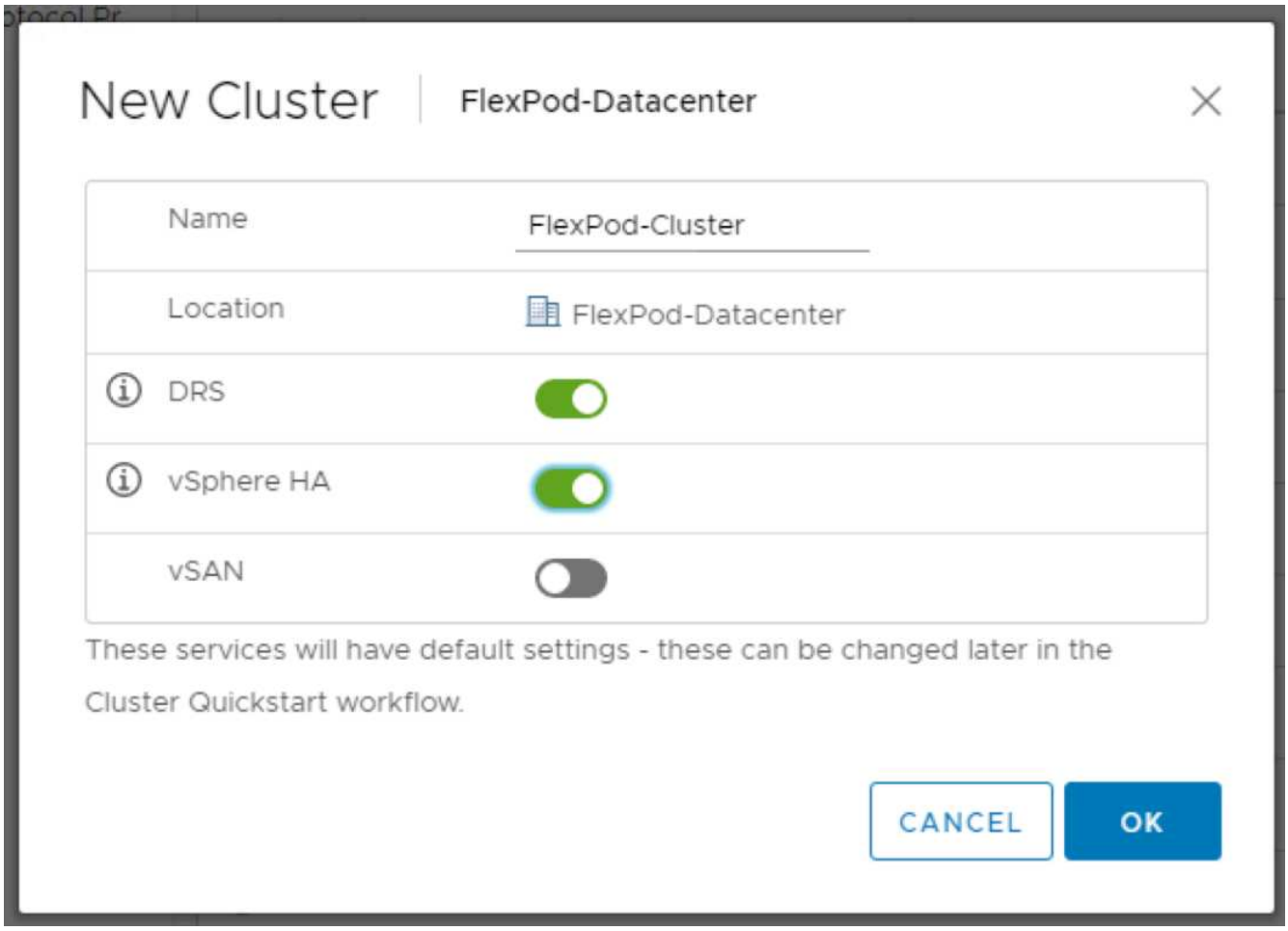
1. Accédez à `https://<<FQDN or IP of vCenter>>/vsphere-client/`.
2. Cliquez sur lancer vSphere client.
3. Connectez-vous à l'aide du nom d'utilisateur Administrator@vsphere.local et du mot de passe SSO que vous avez saisi lors du processus d'installation de VCSA.
4. Cliquez avec le bouton droit de la 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.

Créez un cluster vSphere

Pour créer un cluster vSphere, procédez comme suit :

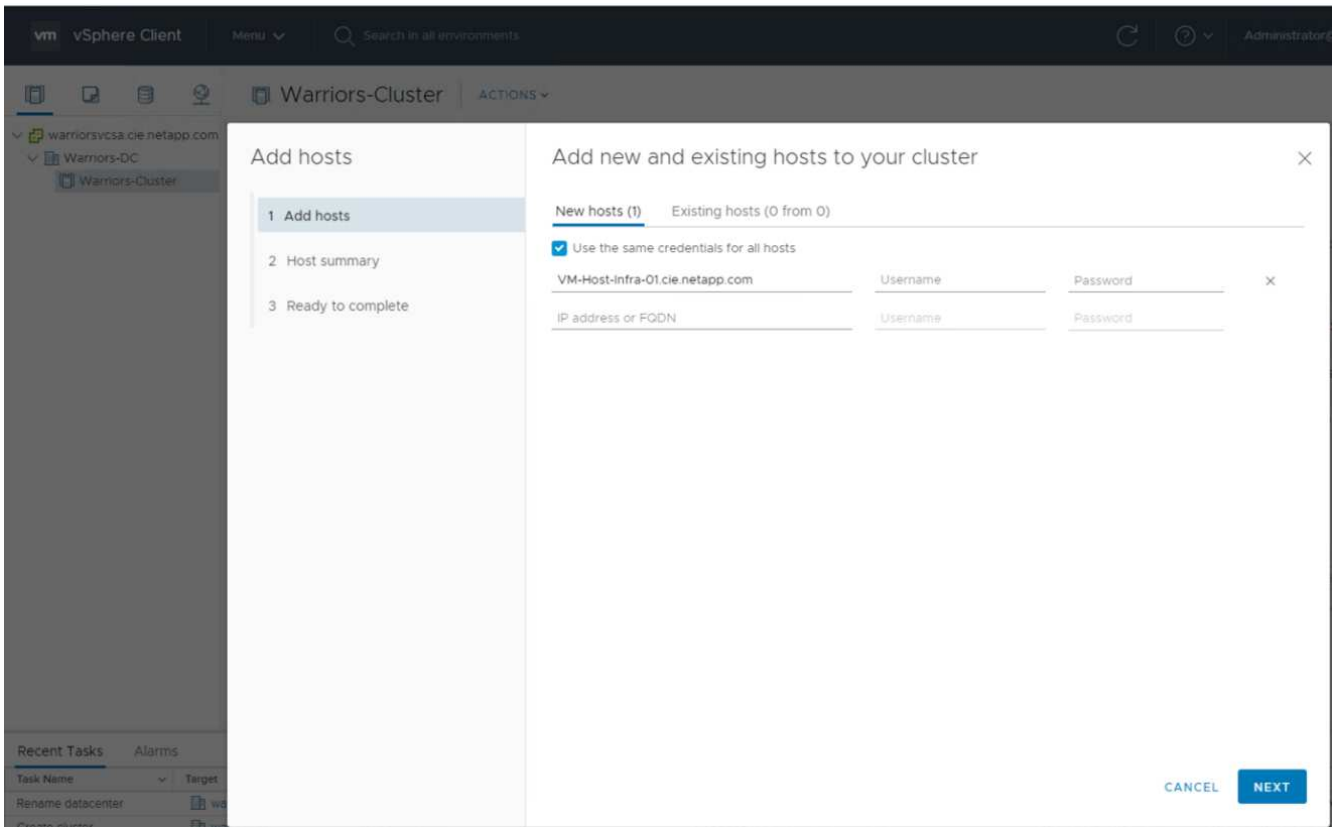
1. Cliquez avec le bouton droit de la souris sur le nouveau centre de données et sélectionnez Nouveau cluster.
2. Indiquez un nom pour le cluster.
3. Activez la reprise sur incident et vSphere HA en cochant les cases.
4. Cliquez sur OK.



Ajoutez les hôtes ESXi au cluster

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

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



2. Pour ajouter un hôte ESXi au cluster, procédez comme suit :
   a. Entrez l'IP ou le FQDN de l'hôte. Cliquez sur Suivant.
   b. Entrez le nom d'utilisateur root et le mot de passe. Cliquez sur Suivant.
   c. Cliquez sur Oui pour remplacer le certificat de l'hôte par un certificat signé par le serveur de certificats VMware.
   d. Cliquez sur Suivant sur la page Récapitulatif de l'hôte.
   e. Cliquez sur l'icône verte + pour ajouter une licence à l'hôte vSphere.
3. Si vous le souhaitez, cette étape peut être effectuée ultérieurement.
   a. Cliquez sur Suivant pour laisser le mode de verrouillage désactivé.
   b. Cliquez sur Next (Suivant) sur la page VM location.
   c. Consultez la page prêt à terminer. Utilisez le bouton Retour pour effectuer des modifications ou sélectionnez Terminer.
4. Répétez les étapes 1 et 2 pour l'hôte Cisco UCS B.

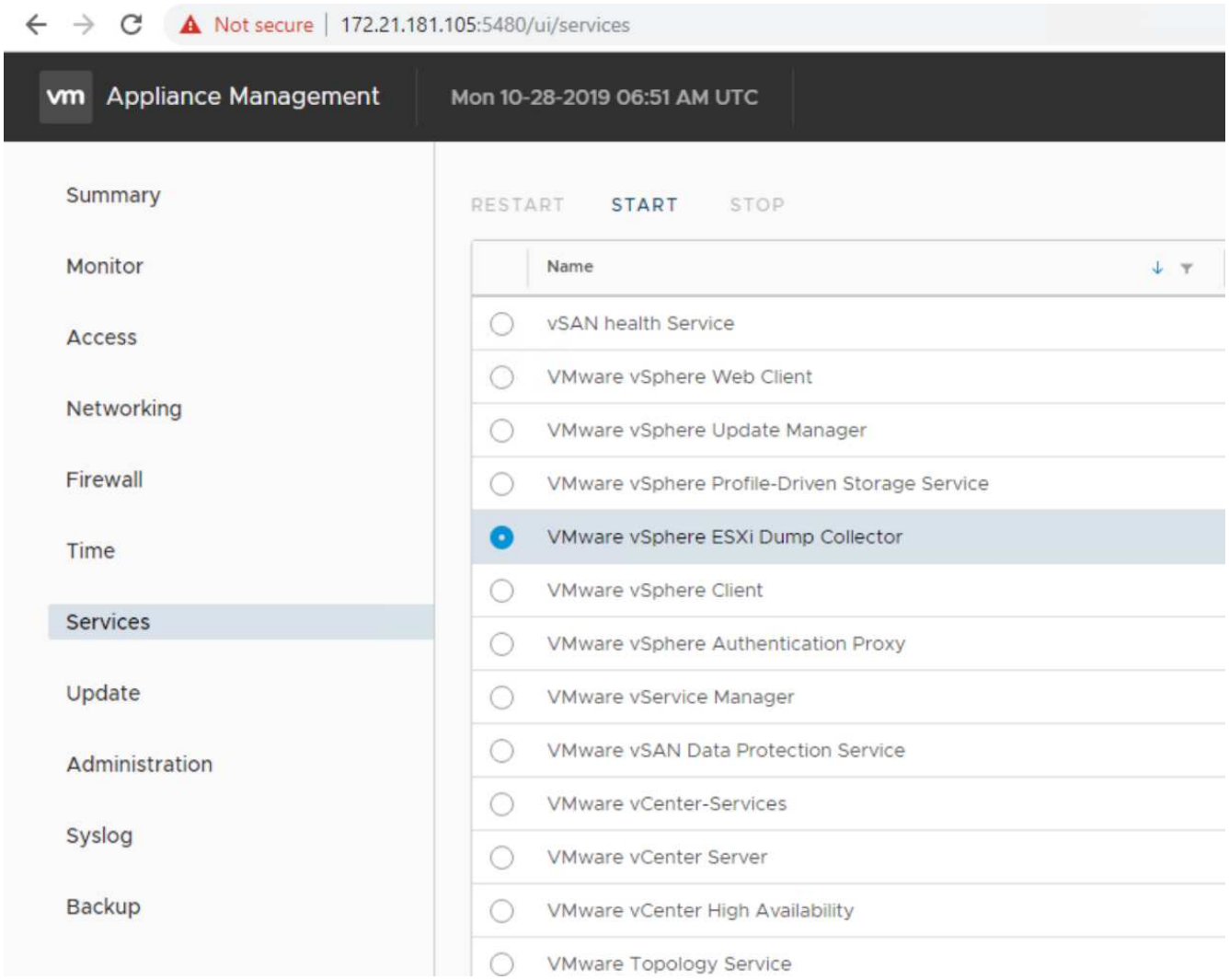
> Ce processus doit être effectué pour tout hôte supplémentaire ajouté à la configuration FlexPod Express.

Configurer coredump sur les hôtes ESXi

Pour configurer coredump sur les hôtes ESXi, procédez comme suit :

1. Connectez-vous à https:// "VCenter" IP:5480/, entrez root pour le nom d'utilisateur et entrez le mot de passe root.

2. Cliquez sur services et sélectionnez VMware vSphere ESXI Dump Collector.
3. Démarrez le service VMware vSphere ESXI Dump Collector.



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

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

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

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

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

`ip_address_of_core_dump_collector` Cette validation correspond à l'adresse IP de vCenter.

"Ensuite, les procédures de déploiement de NetApp Virtual Storage Console 9.6."

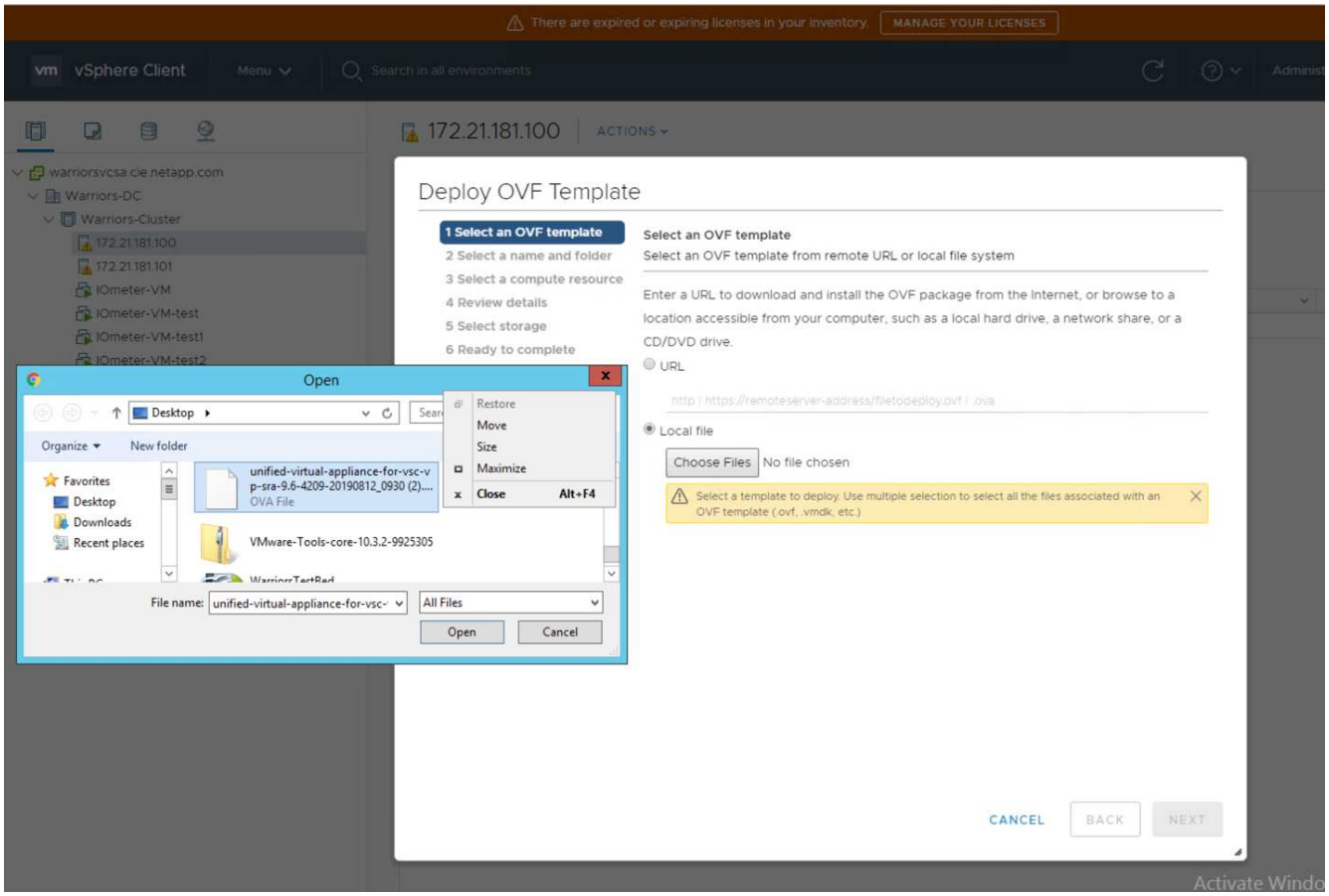
Procédures de déploiement de NetApp Virtual Storage Console 9.6

Cette section décrit les procédures de déploiement de NetApp Virtual Storage Console (VSC).

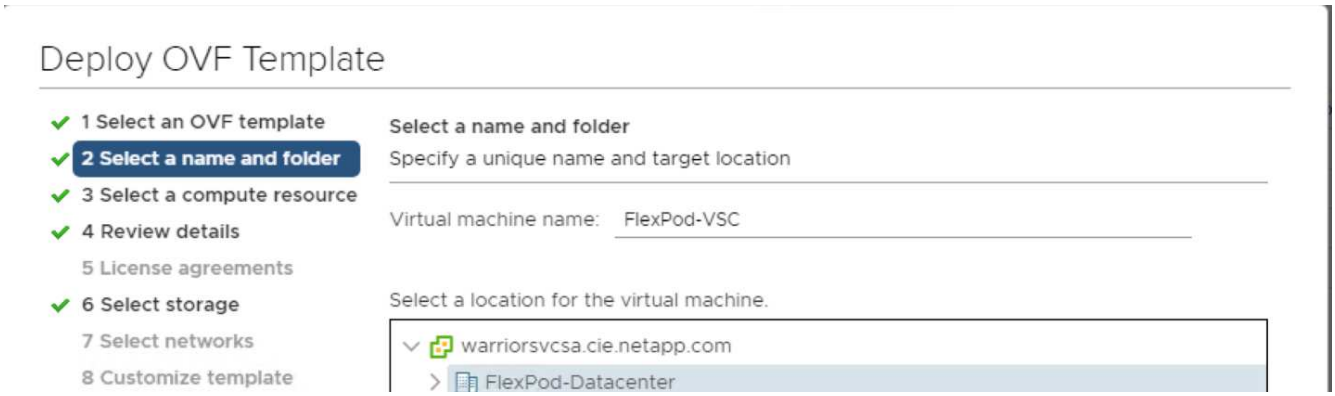
Installez Virtual Storage Console 9.6

Pour installer le logiciel VSC 9.6 à l'aide d'un déploiement OVF (Open Virtualization format), procédez comme suit :

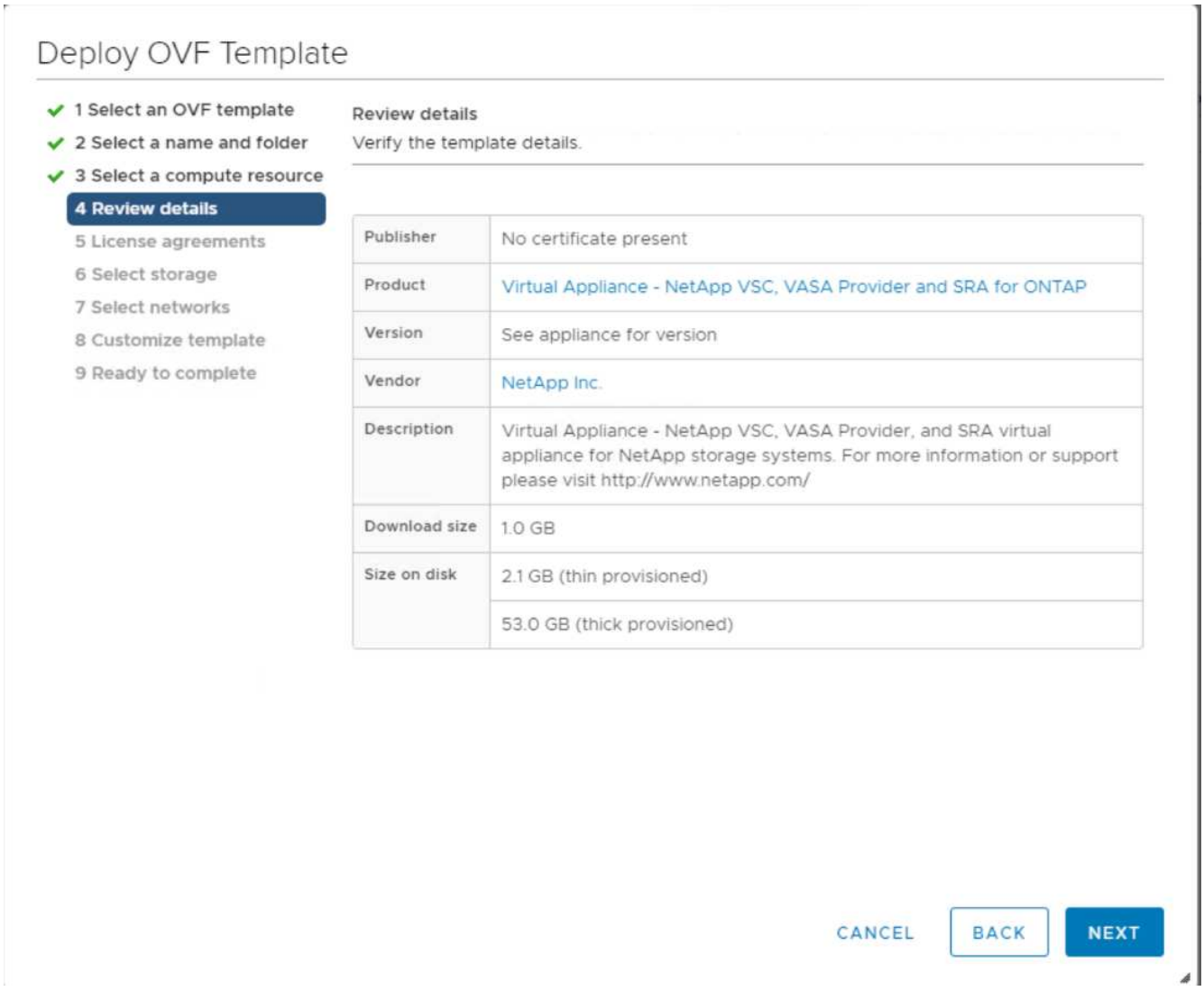
1. Accédez à vSphere Web client > Cluster hôte > déployer le modèle OVF.
2. Accédez au fichier OVF VSC téléchargé depuis le site de support NetApp.



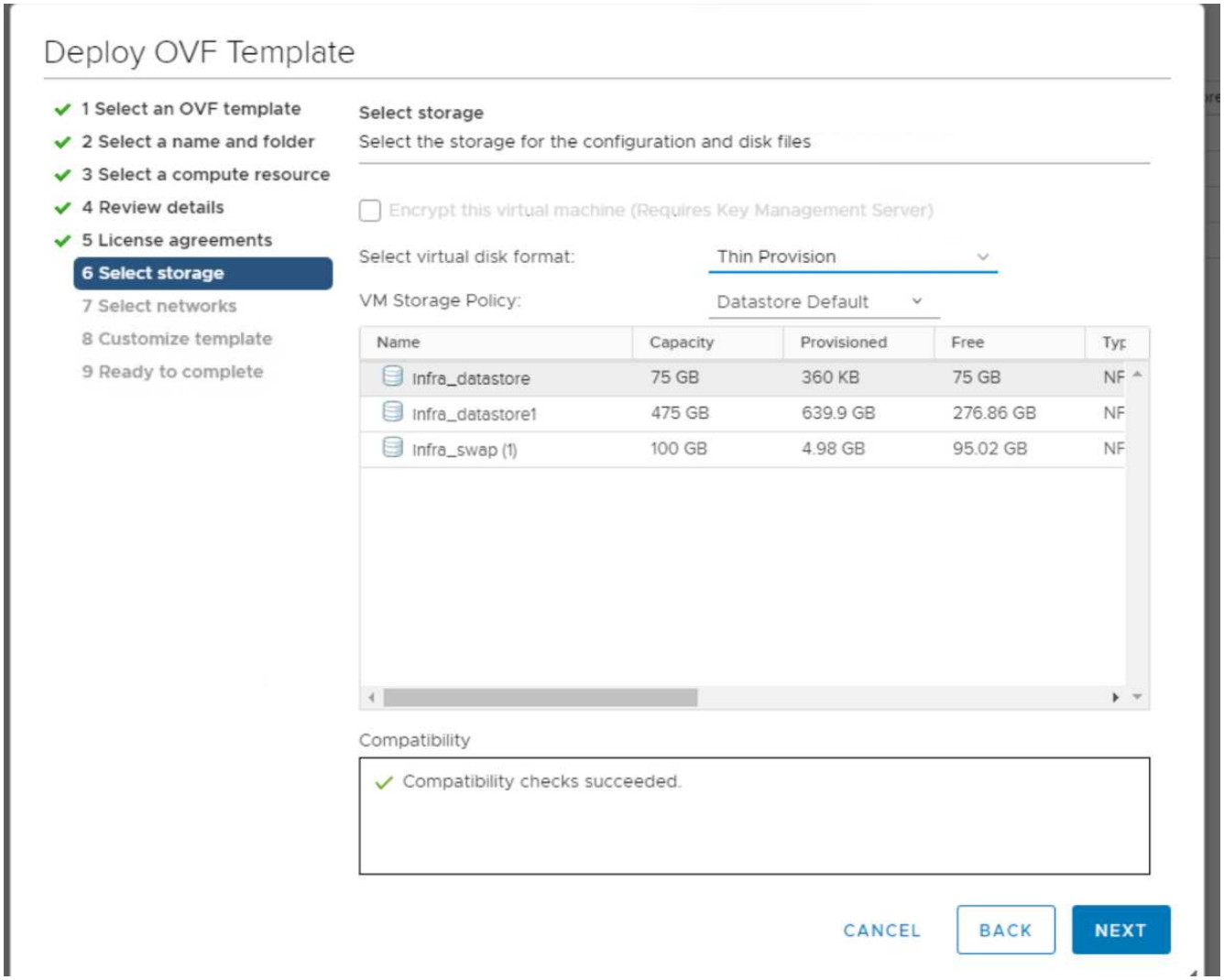
3. Entrez le nom de la machine virtuelle et sélectionnez un centre de données ou un dossier dans lequel déployer. Cliquez sur Suivant.



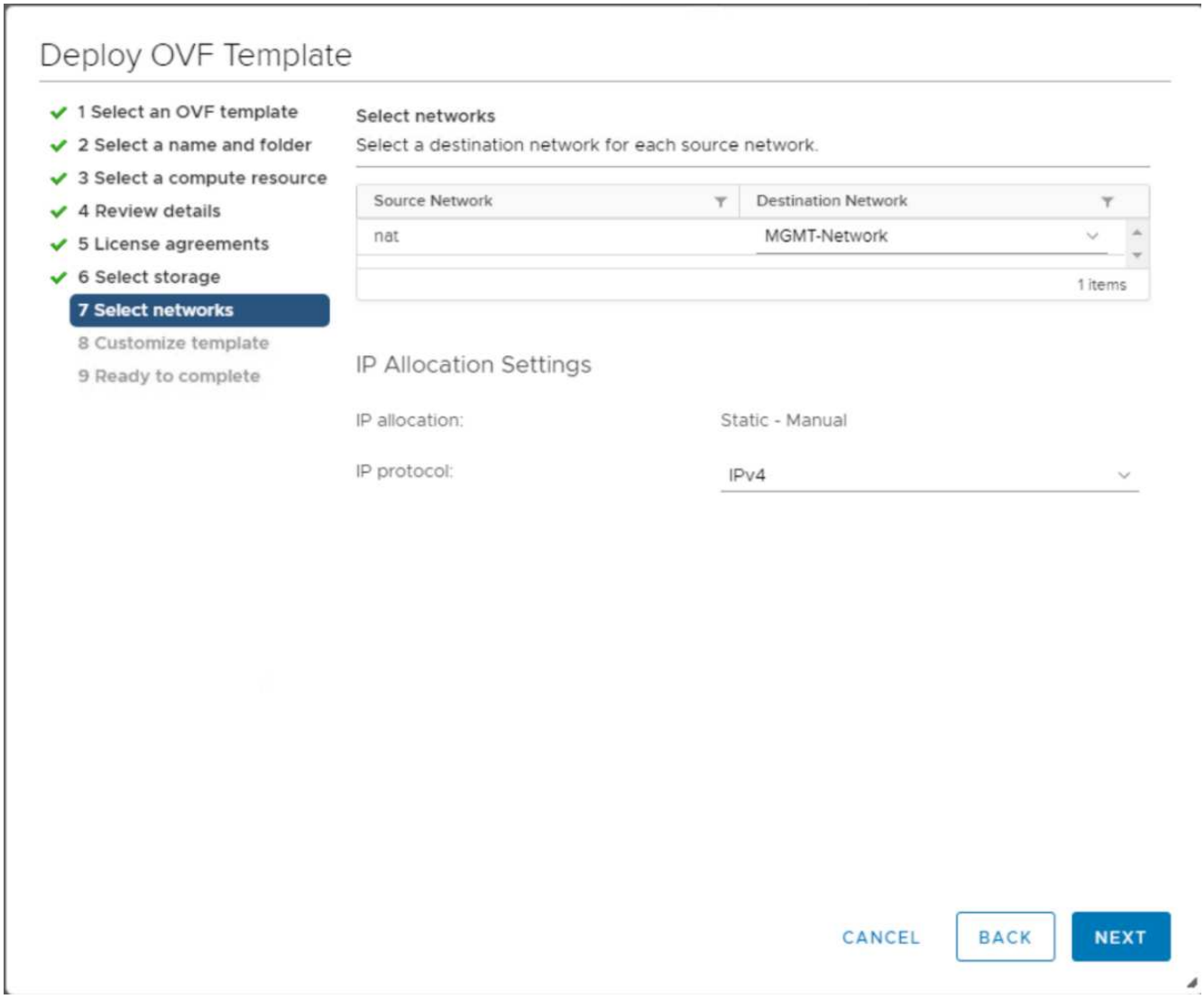
4. Sélectionnez le cluster FlexPod-Cluster ESXi et cliquez sur Next (Suivant).
5. Vérifiez les détails et cliquez sur Next (Suivant).



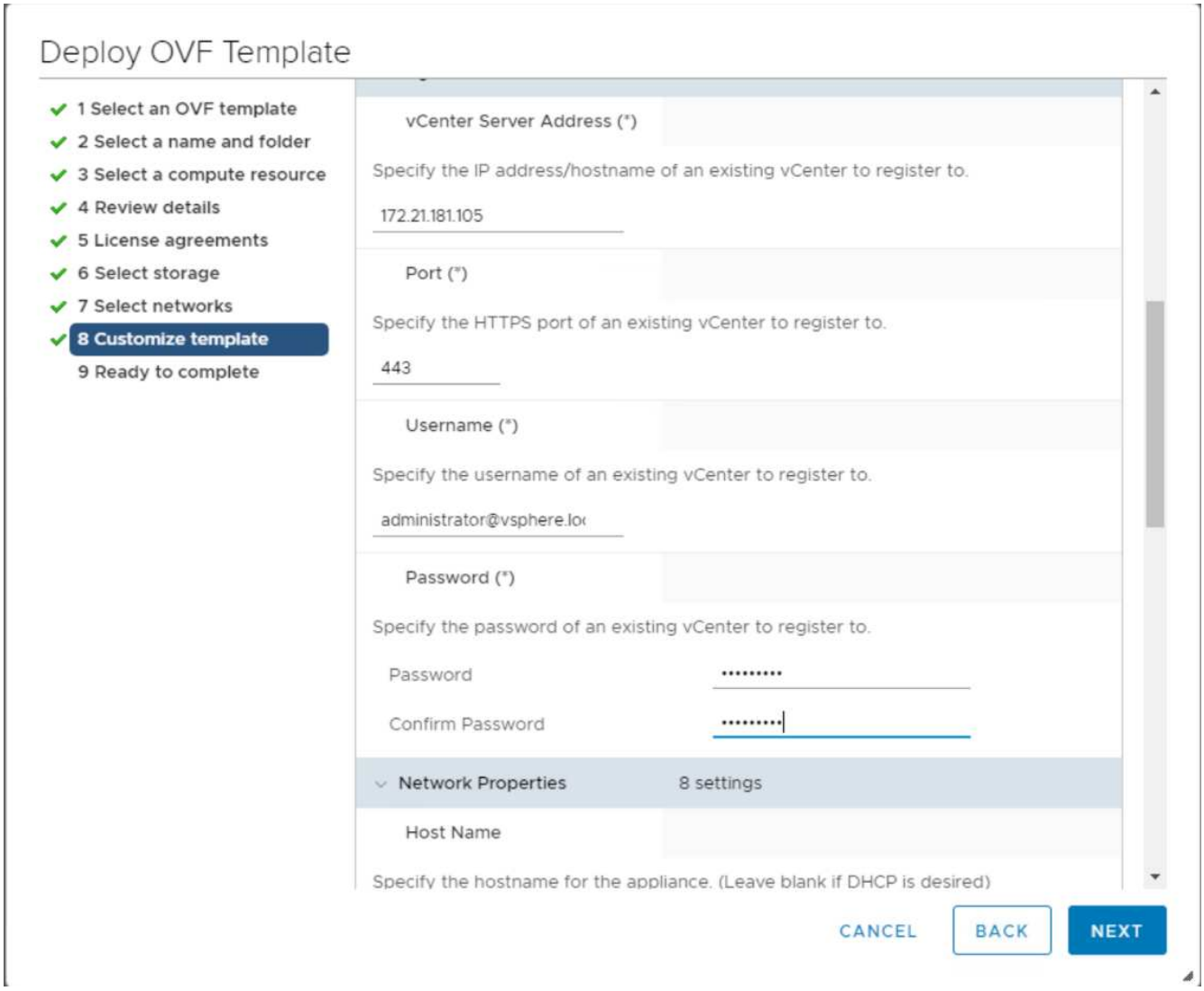
6. Cliquez sur accepter pour accepter la licence et cliquez sur Suivant.
7. Sélectionnez le format de disque virtuel Thin Provision et l'un des datastores NFS. Cliquez sur Suivant.



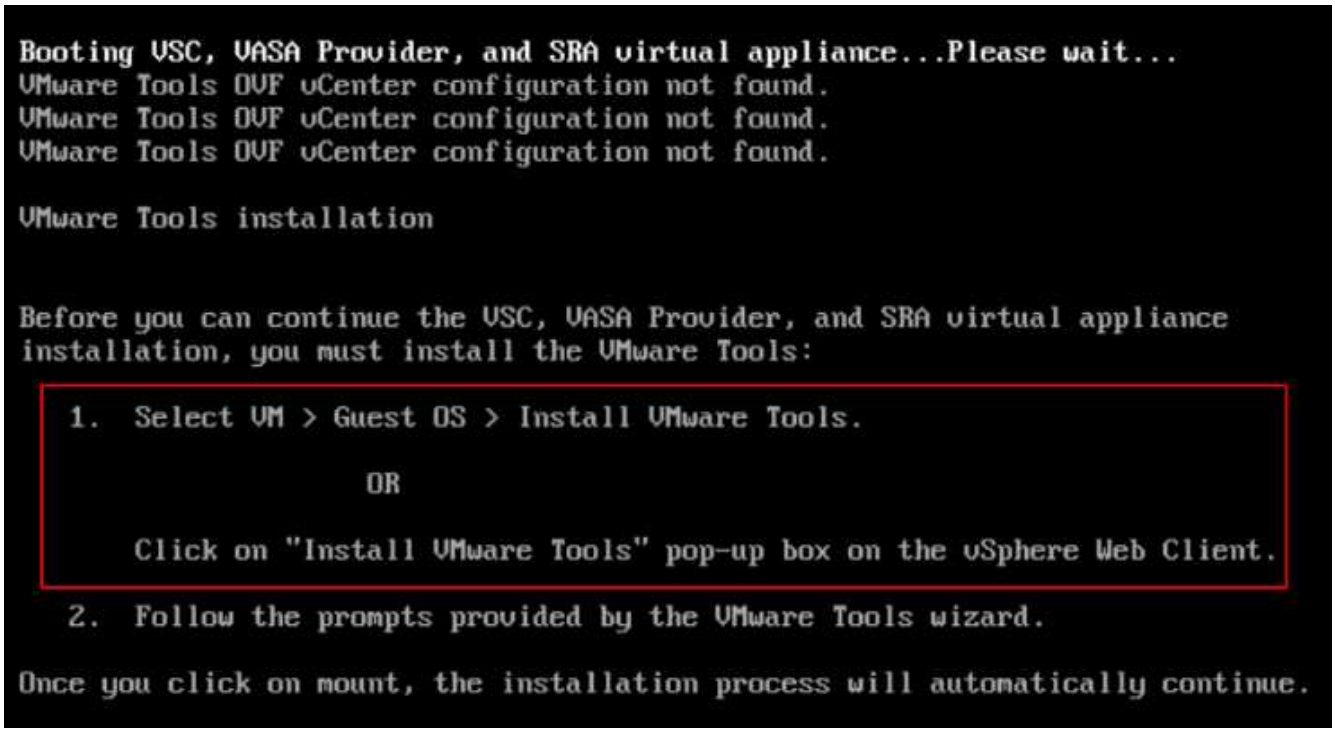
8. Dans Sélectionner les réseaux, choisissez un réseau de destination et cliquez sur Suivant.



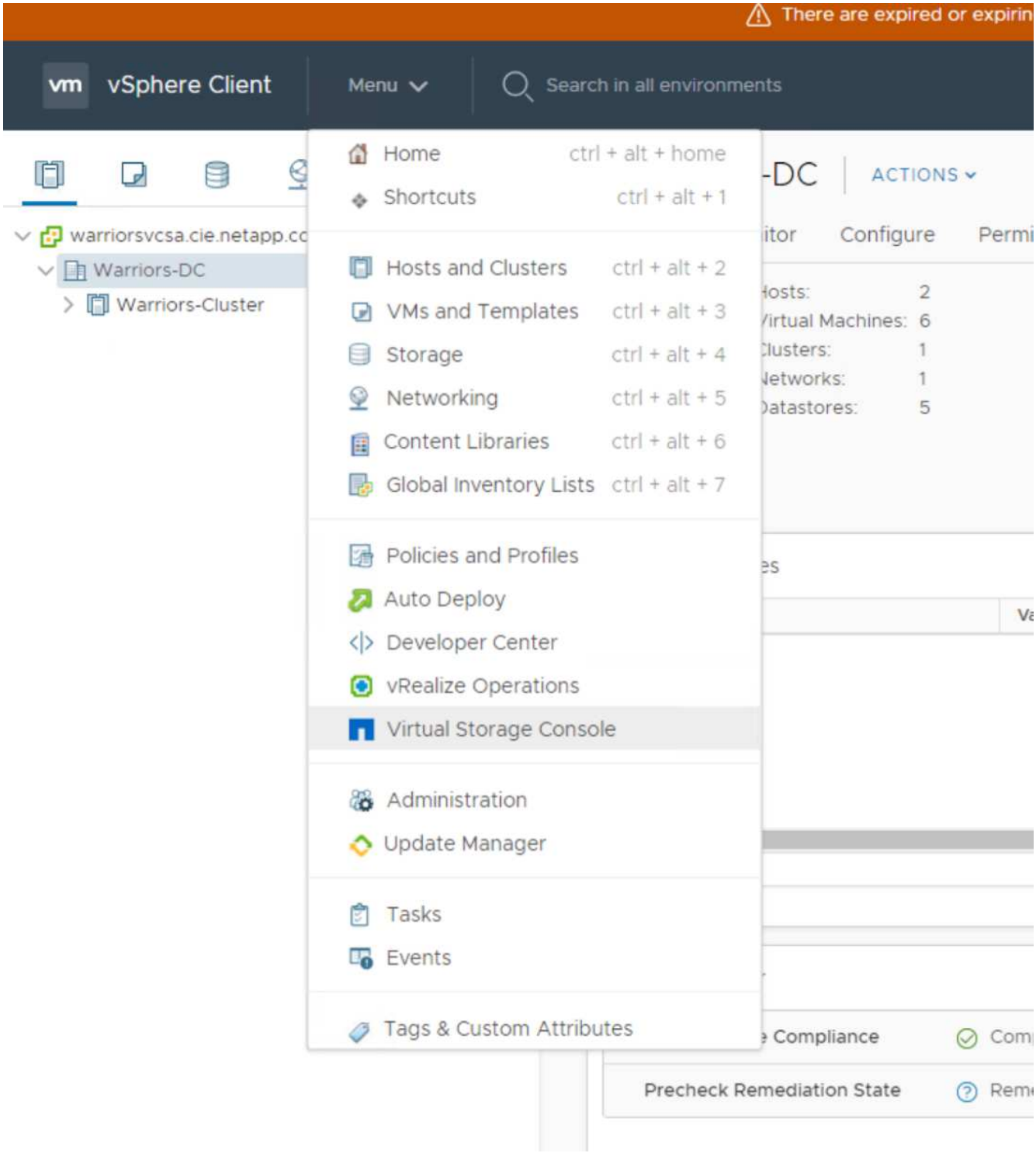
9. Dans Customize Template, entrez le mot de passe de l'administrateur VSC, le nom vCenter ou l'adresse IP, ainsi que d'autres détails de configuration, puis cliquez sur Next.



10. Vérifiez les détails de configuration saisis et cliquez sur Finish pour terminer le déploiement de la machine virtuelle NetApp-VSC.
11. Mettez sous tension la machine virtuelle NetApp-VSC et ouvrez la console de VM.
12. Au cours du processus de démarrage des machines virtuelles NetApp-VSC, une invite s'affiche pour vous inviter à installer VMware Tools. Depuis vCenter, sélectionnez NetApp-VSC VM > Guest OS > Install VMware Tools.



13. Des informations sur la configuration réseau et l'enregistrement vCenter ont été fournies lors de la personnalisation du modèle OVF. Par conséquent, une fois que la machine virtuelle NetApp-VSC est exécutée, VSC, vSphere API for Storage Awareness (VASA) et VMware Storage Replication adapter (SRA) sont enregistrés auprès de vCenter.
14. Déconnectez-vous du client vCenter et reconnectez-vous. Vérifiez que NetApp VSC est installé depuis le menu Accueil.



Téléchargez et installez le plug-in NetApp NFS VAAI

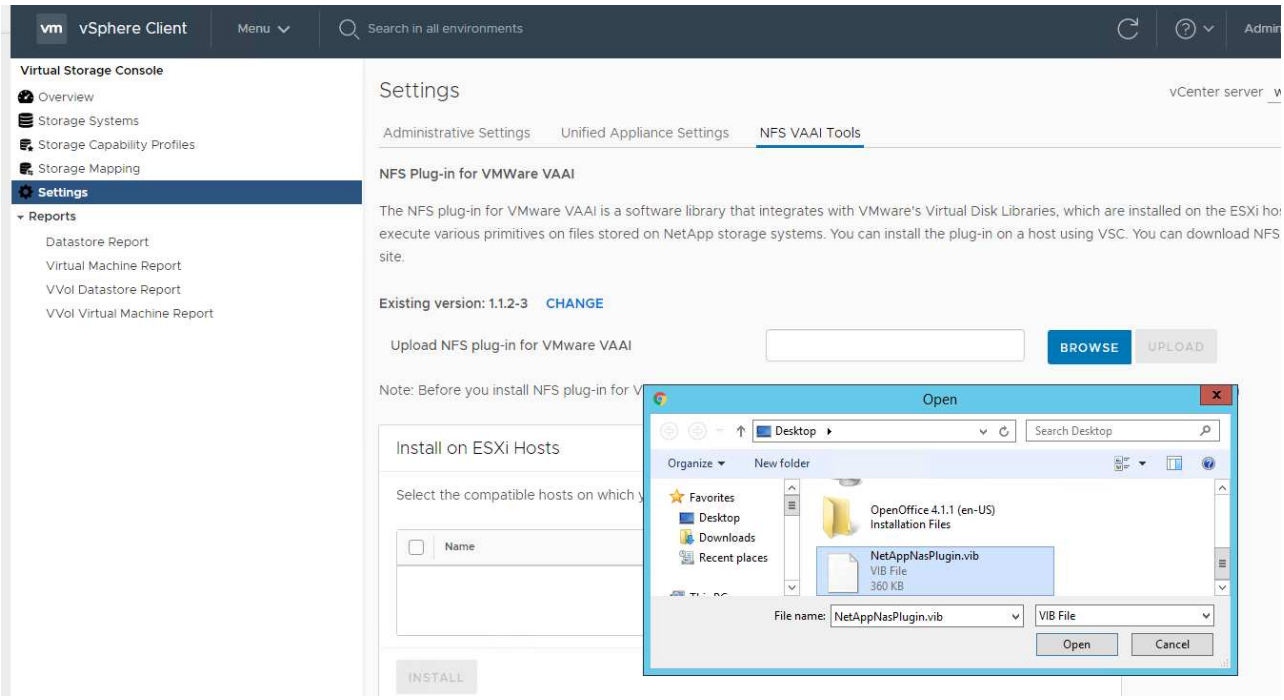
Pour télécharger et installer le plug-in NetApp NFS VAAI, effectuez les opérations suivantes :

1. Téléchargez le plug-in NetApp NFS 1.1.2 pour VMware `.vib` Fichier de la page de téléchargement du plug-in NFS et enregistrez-le sur votre ordinateur local ou hôte d'administration.
2. Téléchargez le plug-in NetApp NFS pour VMware VAAI :
   a. Accédez au "page de téléchargement de logiciels".

b. Faites défiler l'écran et cliquez sur Plug-in NetApp NFS pour VMware VAAI.

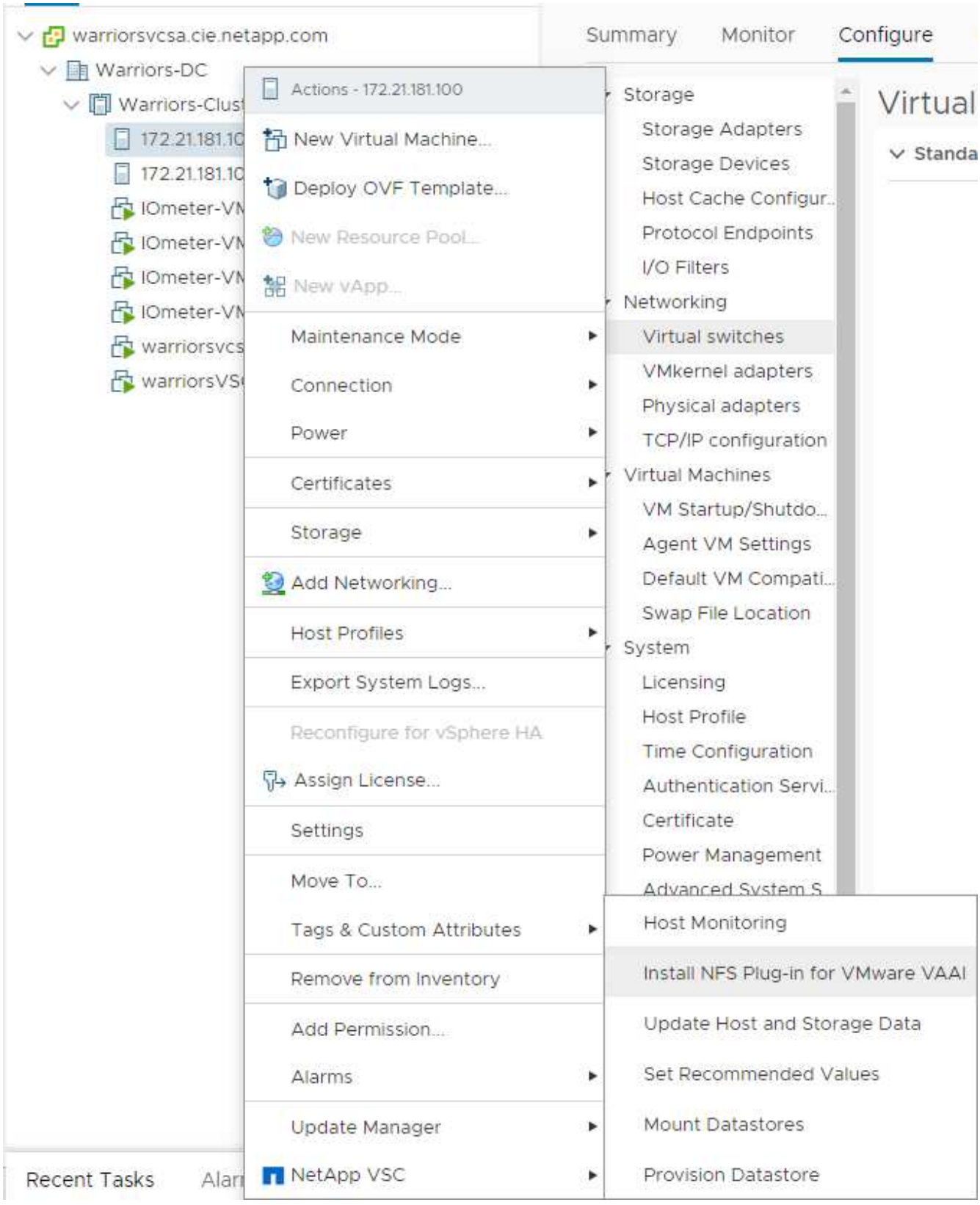
c. Dans l'écran d'accueil du client Web vSphere, sélectionnez Virtual Storage Console.

d. Sous Virtual Storage Console > Paramètres > NFS VAAI Tools, téléchargez le plug-in NFS en choisissant Sélectionner un fichier et en naviguant jusqu'à l'emplacement où le plug-in téléchargé est stocké.



3. Cliquez sur Télécharger pour transférer le plug-in vers vCenter.

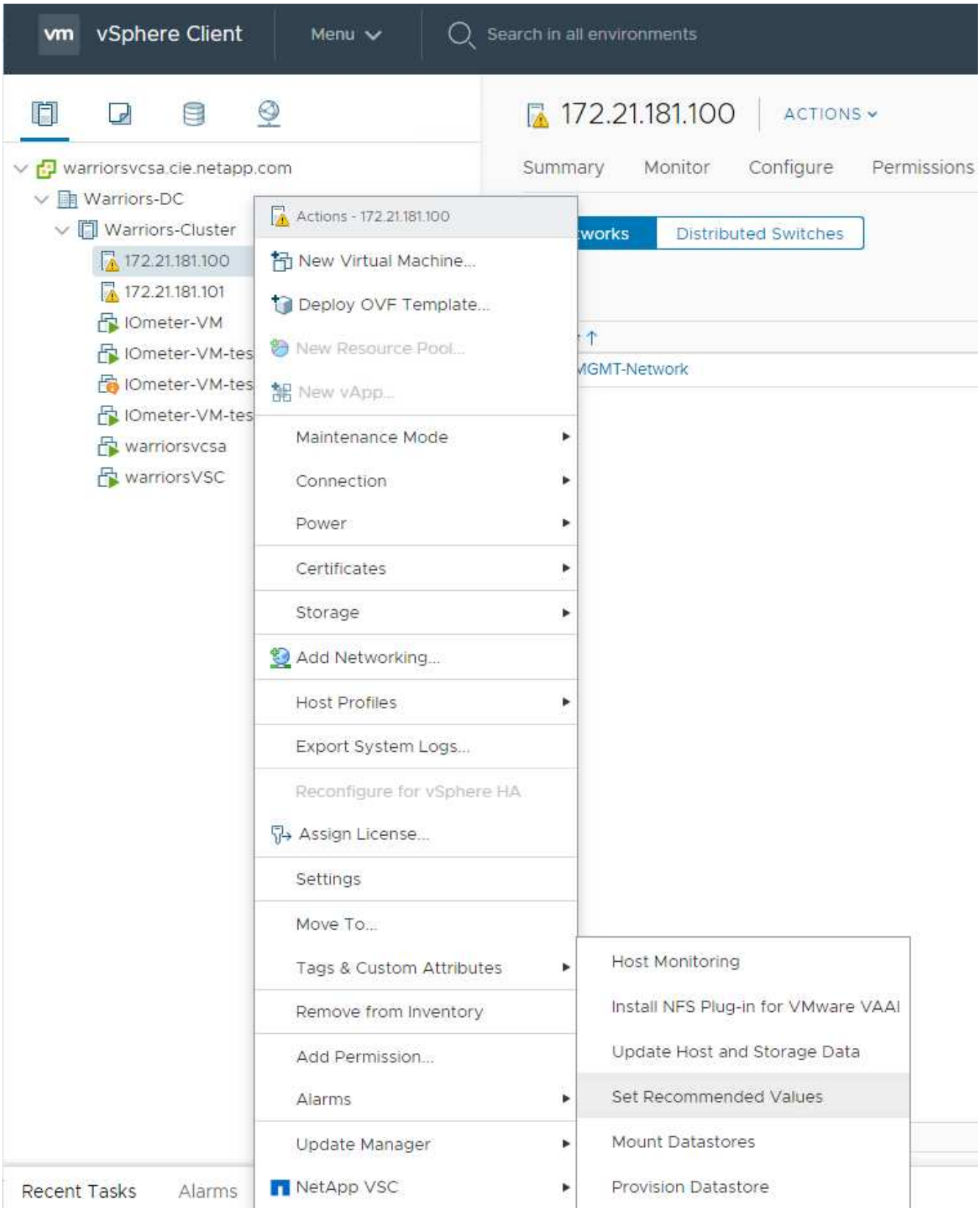
4. Sélectionnez l'hôte, puis NetApp VSC > Install NFS Plug-in for VMware VAAI.



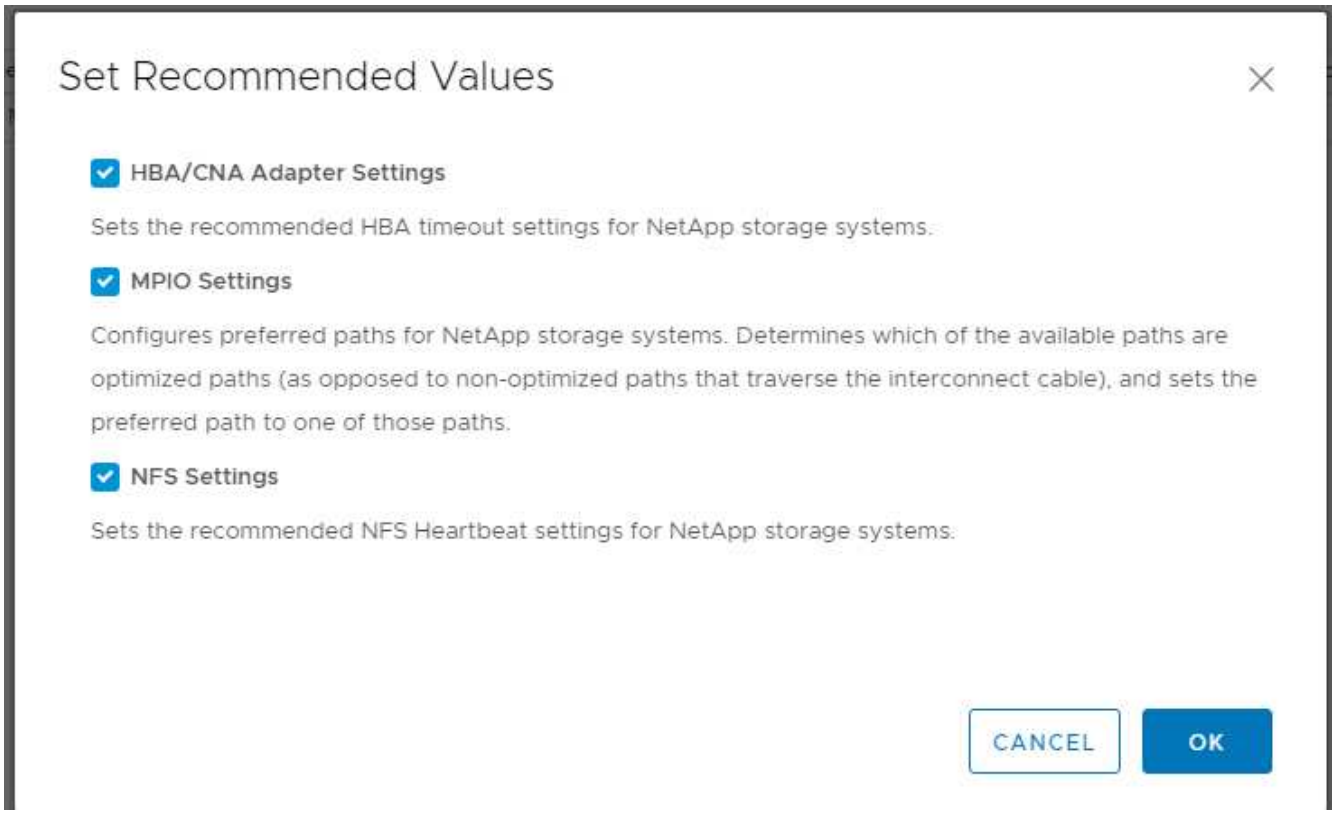
Utilisez les paramètres de stockage optimaux pour les hôtes ESXi

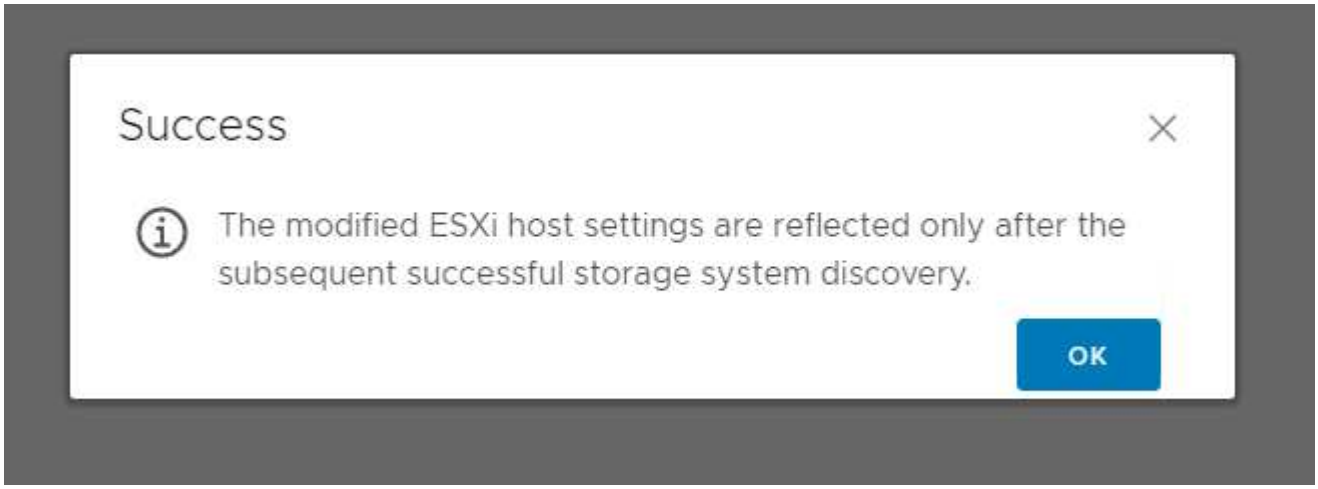
VSC permet de configurer automatiquement les paramètres de stockage pour tous les hôtes ESXi connectés aux contrôleurs de stockage NetApp. Pour utiliser ces paramètres, procédez comme suit :

1. Depuis l'écran d'accueil, sélectionnez vCenter > hôtes et clusters. Pour chaque hôte ESXi, cliquez avec le bouton droit de la souris et sélectionnez NetApp VSC > définir les valeurs recommandées.



2. Vérifiez les paramètres que vous souhaitez appliquer aux hôtes vSphere sélectionnés. Cliquez sur OK pour appliquer les paramètres.





3. Redémarrez l'hôte ESXI une fois ces paramètres appliqués.

Conclusion

FlexPod Express propose une solution simple et efficace qui repose sur des composants leaders. Les systèmes FlexPod Express peuvent être personnalisés pour répondre à des besoins spécifiques. Le FlexPod Express est destiné aux moyennes entreprises, aux bureaux distants et aux autres entreprises qui ont besoin de solutions dédiées.

Remerciements

Les auteurs souhaitent reconnaître John George pour son soutien et sa contribution à cette conception.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations fournies dans ce document, consultez ces documents et/ou sites web :

Documentation produit NetApp

http://docs. "netapp".com

FlexPod Express avec guide

NVA-1139-DESIGN : FlexPod Express avec Cisco UCS C-Series et NetApp AFF C190 Series

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

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Novembre 2019	Version initiale.

Guide de design de FlexPod Express avec Cisco UCS C-Series et AFF A220

NVA-1125-DESIGN : FlexPod Express avec Cisco UCS C-Series et AFF A220

Savita Kumari, NetApp en partenariat avec : 

Les tendances du secteur témoignent d'une vaste transformation des data centers en infrastructure partagée et cloud computing. Les entreprises ont également besoin d'une solution simple et efficace pour leurs succursales et bureaux distants, qui leur apporte la technologie qu'elles connaissent bien dans leur data Center.

FlexPod Express est une architecture de data Center préconçue et conforme aux bonnes pratiques. Elle repose sur la plateforme Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus et sur NetApp AFF. Les composants de FlexPod Express sont similaires à ceux de leurs homologues FlexPod Datacenter, ce qui favorise une gestion plus efficace de l'environnement de l'infrastructure INFORMATIQUE complète à petite échelle. Les plateformes FlexPod Datacenter et FlexPod Express sont optimales pour la virtualisation, et pour les systèmes d'exploitation sans système d'exploitation et les charges de travail d'entreprise.

"Suivant : résumé du programme."

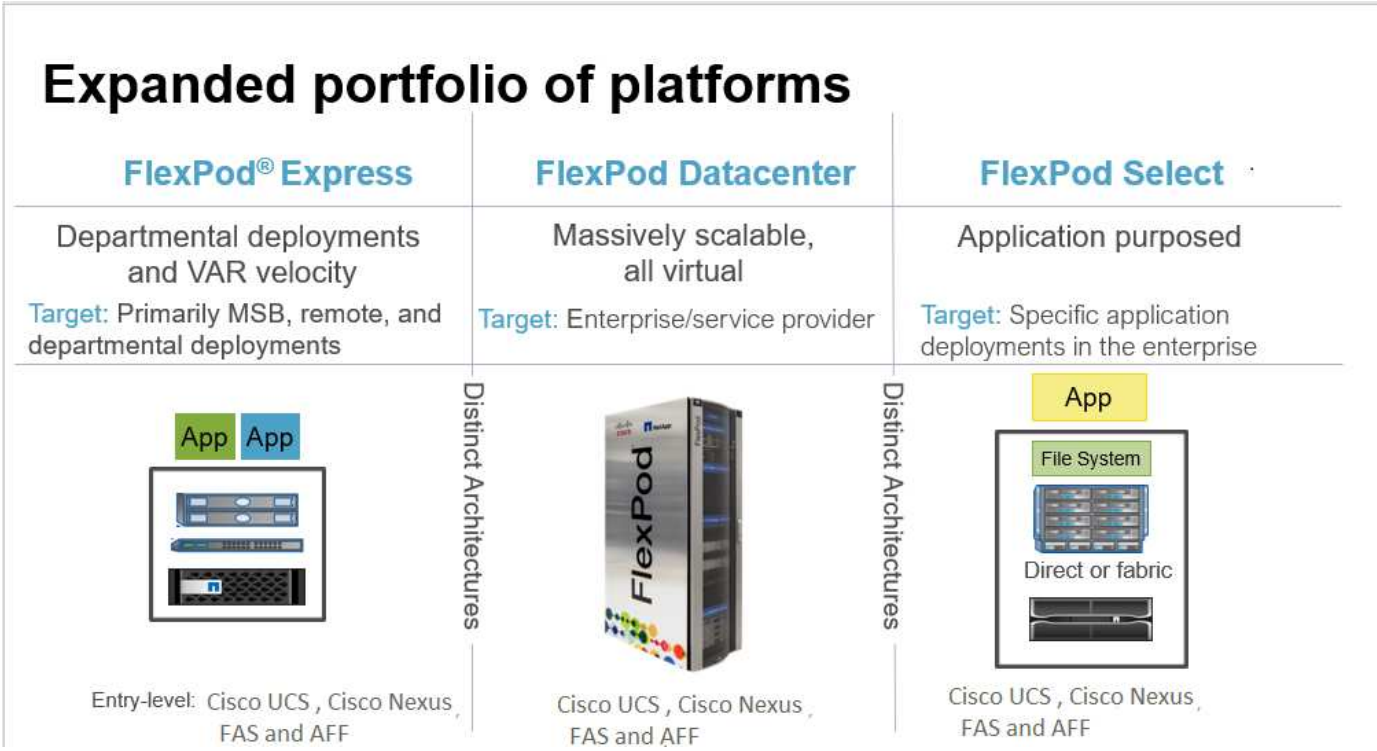
Récapitulatif du programme

Le portefeuille de solutions d'infrastructure convergée FlexPod

Les architectures de référence FlexPod sont fournies sous la forme de designs validés par Cisco (CVD) ou d'architectures vérifiées par NetApp (NVA). Les écarts basés sur les exigences des clients pour une CVD ou une NVA donnée sont autorisés si des variations n'entraînent pas le déploiement de configurations non prises en charge.

Comme illustré dans la figure ci-dessous, la gamme FlexPod comprend trois solutions : les serveurs FlexPod Express, FlexPod Datacenter et FlexPod Select :

- **FlexPod Express.** offre une solution d'entrée de gamme composée 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.



Programme d'architecture vérifiée NetApp

Le programme NVA propose une architecture vérifiée pour les solutions NetApp. Une architecture NVA assure les qualités suivantes avec la solution NetApp :

- 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 VMware vSphere. Cette conception tire également parti du tout nouveau système AFF A220, qui exécute le logiciel NetApp ONTAP 9.4, des commutateurs Cisco Nexus 3172P et des serveurs Cisco UCS C220 M5 comme nœuds d'hyperviseur.

Bien que ce document soit validé pour AFF A220, cette solution prend également en charge les baies

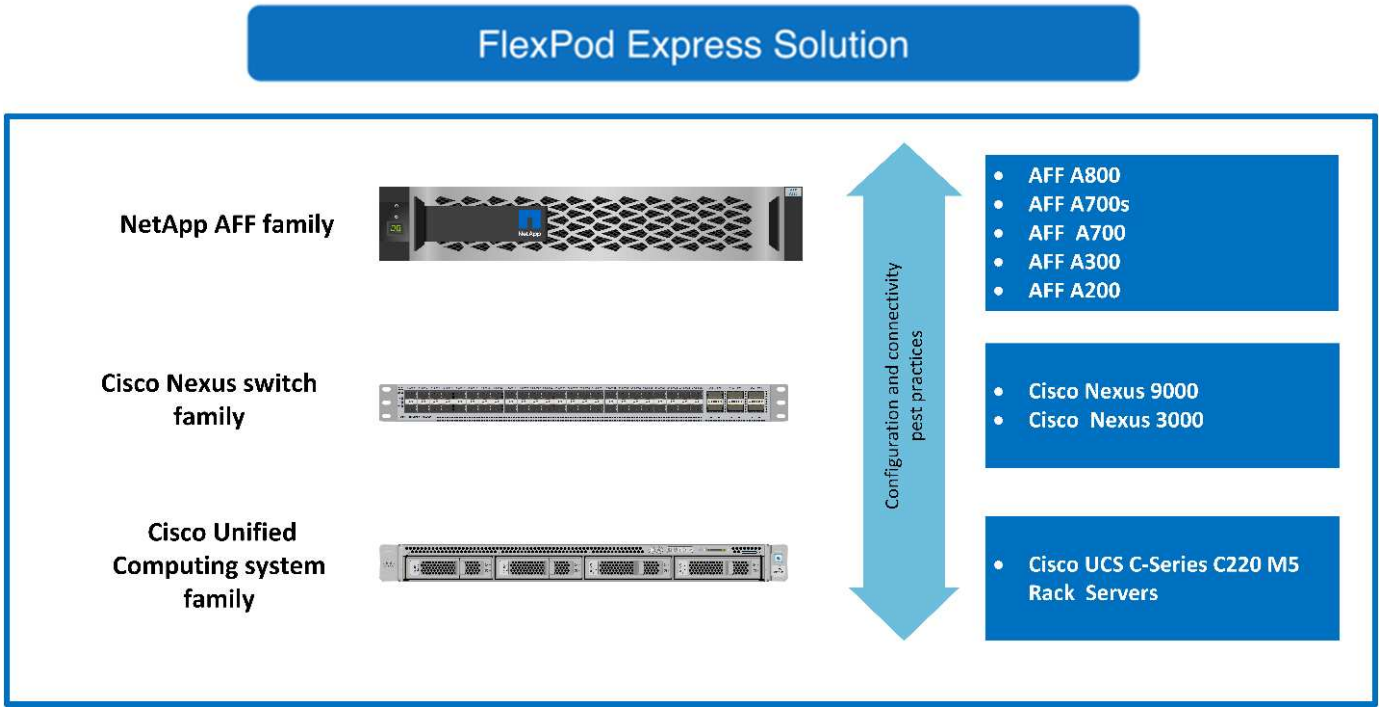
FAS2700.

"Ensuite : présentation de la solution."

Présentation de la solution

FlexPod Express est conçu pour exécuter des charges de travail de virtualisation mixtes. Elle est destinée aux bureaux distants, aux succursales et aux moyennes entreprises. Il convient également aux grandes entreprises qui souhaitent mettre en œuvre une solution dédiée. Cette nouvelle solution pour FlexPod Express inclut de nouvelles technologies telles que NetApp ONTAP 9.4, NetApp AFF A220 et VMware vSphere 6.7.

La figure suivante présente les composants matériels inclus dans la solution FlexPod Express.

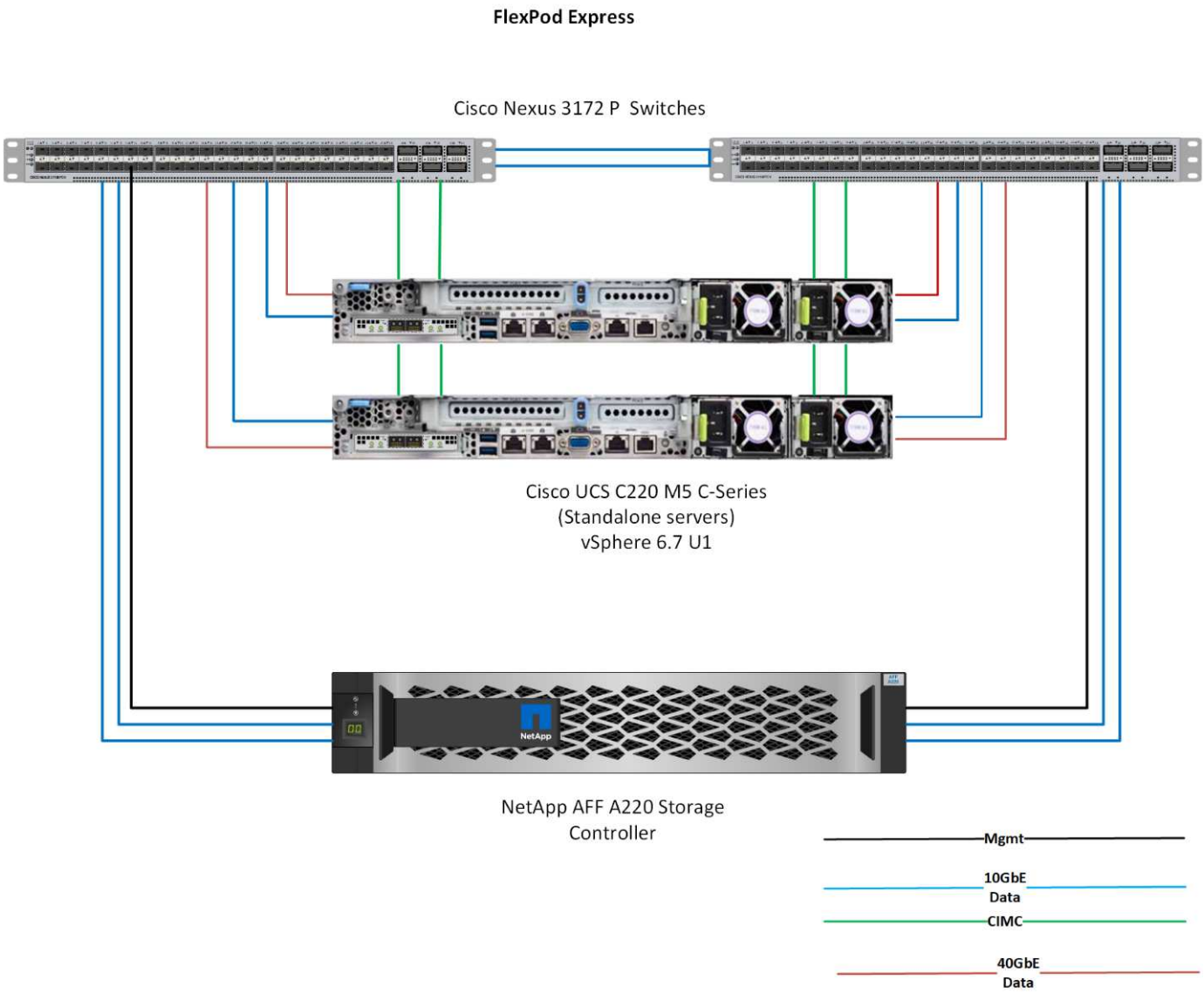


Public visé

Ce document est destiné à ceux qui souhaitent tirer parti d'une infrastructure conçue pour optimiser l'efficacité IT et favoriser l'innovation IT. Le public cible de ce document inclut, sans s'y limiter, les ingénieurs commerciaux, les consultants sur le terrain, le personnel des services professionnels, les responsables INFORMATIQUES, les ingénieurs partenaires et les clients.

Technologie de la solution

Cette solution tire parti des dernières technologies de NetApp, Cisco et VMware. Cette solution présente le nouveau système NetApp AFF A220, qui exécute le logiciel ONTAP 9.4, deux commutateurs Cisco Nexus 3172P et des serveurs en rack Cisco UCS C220 M5 exécutant VMware vSphere 6.7. Cette solution validée utilise une technologie 10 Gigabit Ethernet (10GbE). La figure suivante présente une vue d'ensemble. Des conseils sont également fournis sur la manière d'évoluer en ajoutant deux nœuds d'hyperviseur à la fois afin que l'architecture FlexPod Express puisse s'adapter aux besoins commerciaux en constante évolution de l'entreprise.



L'Ethernet 40 GbE n'est pas validé, mais il s'agit d'une infrastructure prise en charge.

"Ensuite, les exigences technologiques."

Exigences technologiques

FlexPod Express requiert une combinaison de composants matériels et logiciels qui dépend de l'hyperviseur et de la vitesse réseau sélectionnés. En outre, FlexPod Express dispose des composants matériels requis pour ajouter des nœuds d'hyperviseur au système par unités 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.

Le tableau suivant répertorie les composants matériels requis pour toutes les configurations FlexPod Express

et pour implémenter la solution. Ils peuvent varier selon la mise en œuvre de la solution et les besoins du client.

Sous-jacent	Quantité
Cluster à deux nœuds AFF A220	1
Serveur Cisco UCS C220 M5	2
Commutateur Cisco Nexus 3172P	2
Carte Cisco UCS Virtual interface Card (VIC) 1387 pour serveur en rack Cisco UCS C220 M5	2
Adaptateur Cisco CVR-QSFP-SFP10G	4

Configuration logicielle requise

Les tableaux suivants répertorient les composants logiciels requis pour l'implémentation des architectures de la solution FlexPod Express.

Le tableau suivant répertorie la configuration logicielle requise pour l'implémentation FlexPod Express de base.

Logiciel	Version	Détails
Contrôleur de gestion intégrée Cisco (CIMC)	3.1.3	Pour serveurs en rack C220 M5
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Pour commutateurs Cisco Nexus 3172P
NetApp ONTAP	9.4	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	6.7
VMware vSphere ESXi	6.7
Plug-in NetApp VAAI pour ESXi	1.1.2

"Suivant : choix de conception."

Choix de conception

Les technologies suivantes ont été choisies lors du processus de conception de l'architecture. Chaque technologie répond à un usage spécifique de la solution d'infrastructure FlexPod Express.

AFF A220 Series NetApp avec ONTAP 9.4

Cette solution tire parti de deux des derniers produits NetApp : les logiciels NetApp AFF A220 et ONTAP 9.4.

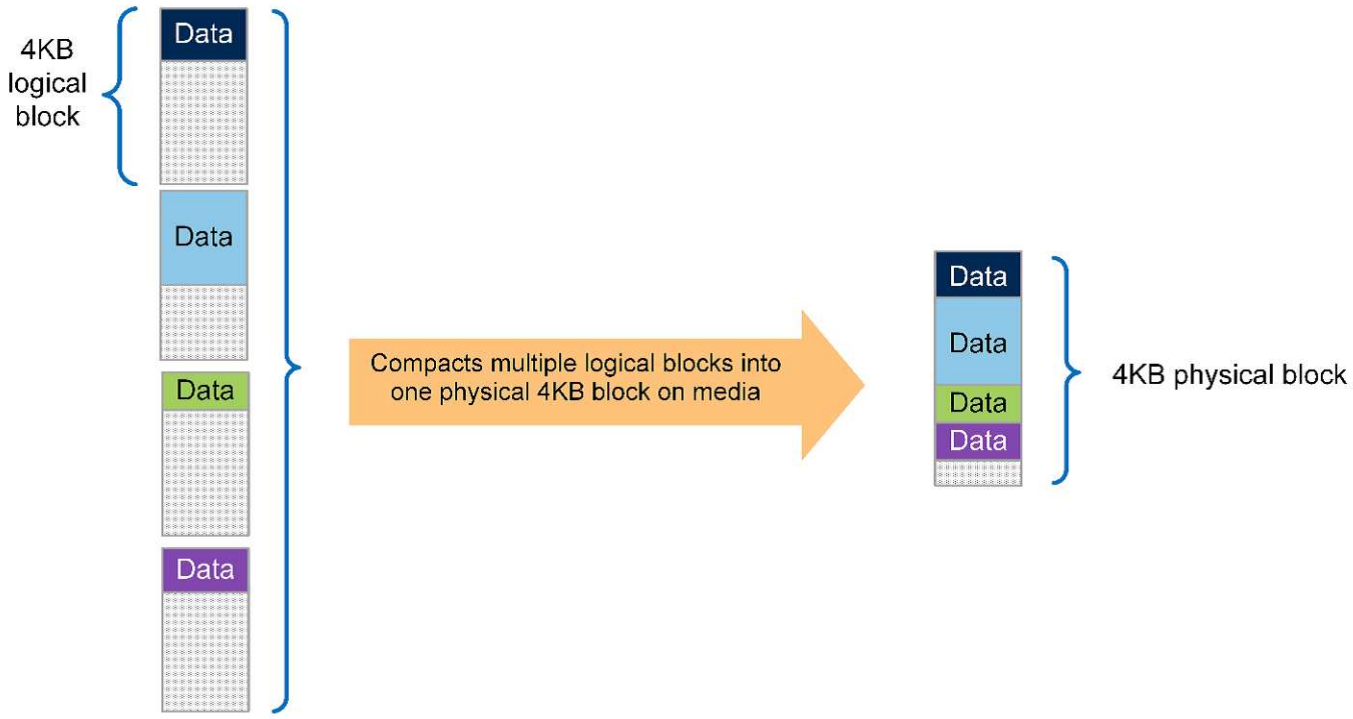
Système AFF A220

Pour plus d'informations sur le système matériel AFF A220, consultez le "Page d'accueil de AFF A-Series".

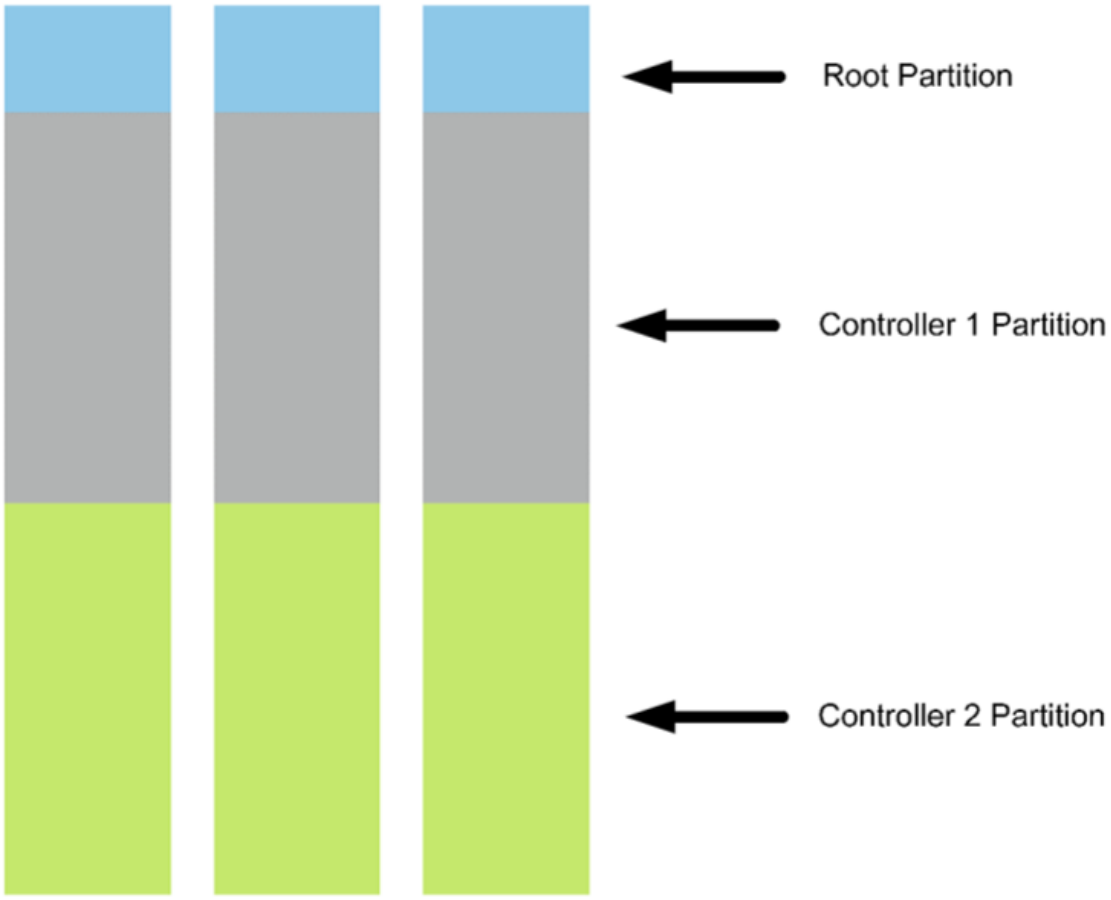
Le logiciel ONTAP 9.4

Les systèmes AFF A220 de NetApp utilisent le nouveau logiciel ONTAP 9.4. ONTAP 9.4 est le logiciel de gestion des données d'entreprise leader du secteur. Il allie une simplicité et une flexibilité inédites à de puissantes fonctionnalités de gestion des données, d'efficacité du stockage et d'intégration cloud.

ONTAP 9.4 propose plusieurs fonctionnalités particulièrement adaptées à la solution FlexPod Express. L'engagement de NetApp en faveur de l'efficacité du stockage est avant tout primordial, ce qui peut constituer l'une des fonctionnalités les plus importantes pour les déploiements de petite taille. ONTAP 9.4 propose aujourd'hui les fonctionnalités d'efficacité du stockage, telles que la déduplication, la compression et le provisionnement fin, avec un nouvel ajout de compaction. Étant donné que le système WAFL de NetApp écrit toujours des blocs de 4 Ko, la compaction combine plusieurs blocs dans un bloc de 4 Ko lorsque l'espace alloué des blocs de 4 Ko n'est pas utilisé. La figure suivante illustre ce processus.



De plus, le partitionnement données-racines peut être utilisé sur le système AFF A220. Ce partitionnement permet de répartit l'agrégat racine et deux agrégats de données sur les disques du système. Par conséquent, les deux contrôleurs d'un cluster AFF A220 à deux nœuds peuvent tirer parti des performances de tous les disques de l'agrégat. Voir la figure suivante.



Il s'agit de quelques fonctionnalités clés qui complètent la solution FlexPod Express. Pour plus de détails sur les fonctions et fonctionnalités supplémentaires de ONTAP 9.4, consultez le "Fiche technique sur le logiciel de gestion des données ONTAP 9". Voir aussi NetApp "Centre de documentation ONTAP 9" , qui a été mis à jour pour inclure ONTAP 9.4.

Cisco Nexus 3000 Series

Le Cisco Nexus 3172P est un commutateur robuste et économique qui offre une commutation 1/10/40/100 Gbit/s. Le commutateur Cisco Nexus 3172PQ, appartenant à la gamme Unified Fabric, est un commutateur compact à 1 rack (1RU) pour des déploiements en Top des data centers. (Voir la figure suivante.) Il offre jusqu'à soixante-douze ports 1/10GbE par incrément de 1RU ou quarante-huit ports 1/10GbE plus six ports 40 GbE par incrément de 1RU. Et pour une flexibilité maximale de couche physique, il prend également en charge 1/10/40 Gbit/s.

Comme tous les différents modèles de la gamme Cisco Nexus exécutent le même système d'exploitation sous-jacent, NX-OS prend en charge plusieurs modèles Cisco Nexus dans les solutions FlexPod Express et FlexPod Datacenter.

Les spécifications de performances comprennent :

- Débit de trafic à débit de ligne (couches 2 et 3) sur tous les ports
- Unités de transmission maximales configurables (MTU) jusqu'à 9216 octets (trames jumbo)

Pour en savoir plus sur les commutateurs Cisco Nexus 3172, consultez le "Fiche technique des commutateurs Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL et 3172TQ-XL".

Cisco UCS C-Series

Le serveur en rack Cisco UCS C-Series a été choisi pour FlexPod Express, car ses nombreuses options de configuration le permettent d'être personnalisé pour des exigences spécifiques dans un déploiement FlexPod Express.

Les serveurs en rack Cisco UCS C-Series offrent une solution informatique unifiée dans un format standard afin de réduire le coût total de possession et d'accroître l'agilité.

Les serveurs en rack Cisco UCS C-Series offrent les avantages suivants :

- Un point d'entrée indépendant des formats dans Cisco UCS
- Un déploiement simplifié et rapide des applications
- Extension des innovations et avantages de l'informatique unifiée aux serveurs rack
- Un plus grand choix pour les clients avec des avantages uniques dans un pack rack familier

Le serveur en rack Cisco UCS C220 M5 (figure précédente) est l'une des infrastructures d'entreprise et des serveurs applicatifs polyvalents les plus polyvalents du marché. Il s'agit d'un serveur en rack à deux sockets haute densité qui offre des performances et une efficacité de pointe pour une large gamme de charges de travail, notamment pour la virtualisation, la collaboration et les applications sans système d'exploitation. Les serveurs rack Cisco UCS C-Series peuvent être déployés en tant que serveurs autonomes ou en tant que partie intégrante de Cisco UCS pour tirer parti des innovations de Cisco en matière d'informatique unifiée, qui permettent de réduire le coût total de possession des clients et d'augmenter leur souplesse commerciale.

Pour plus d'informations sur les serveurs C220 M5, reportez-vous au "Fiche technique du serveur rack Cisco UCS C220 M5".

Options de connectivité pour les serveurs en rack C220 M5

Les options de connectivité des serveurs en rack C220 M5 sont les suivantes :

- **Cisco UCS VIC 1387**

  Le système Cisco UCS VIC 1387 (dans la figure suivante) offre des ports QSFP+ 40 GbE et FC over Ethernet (FCoE) améliorés à deux ports dans un format modulaire mLOM (LAN-on-board). Le slot mLOM

peut être utilisé pour installer un VIC Cisco sans utiliser de logement PCIe (Peripheral Component Interconnect Express), ce qui permet une meilleure extensibilité des E/S.

Pour plus d'informations sur l'adaptateur Cisco UCS VIC 1387, consultez la "Carte d'interface virtuelle Cisco UCS 1387" feuille de données.

- **ADAPTATEUR CVR-QSFP-SFP10G**

  Le module Cisco QSA convertit un port QSFP en port SFP ou SFP+. Grâce à cet adaptateur, les clients peuvent utiliser n'importe quel module SFP+ ou SFP ou câble pour se connecter à un port à faible vitesse à l'autre extrémité du réseau. Cette flexibilité permet une transition économique vers 40 GbE en maximisant l'utilisation des plateformes QSFP haute densité 40 GbE. Cet adaptateur prend en charge toutes les câbles et tous les câbles SFP+ et prend en charge plusieurs modules SFP 1 GbE. Comme ce projet a été validé par une connectivité 10GbE et que le VIC 1387 utilisé est 40 GbE, l'adaptateur CVR-QSFP-SFP10G (dans la figure suivante) est utilisé pour la conversion.

VMware vSphere 6.7

VMware vSphere 6.7 est une option d'hyperviseur unique à utiliser avec FlexPod Express. VMware vSphere permet aux entreprises de réduire leur empreinte électrique et de climatisation tout en bénéficiant de la pleine capacité de calcul achetée. De plus, VMware vSphere permet une protection contre les défaillances matérielles (VMware High Availability ou VMware HA), ainsi qu'un équilibrage de la charge des ressources de

calcul sur un cluster d'hôtes vSphere (VMware Distributed Resource Scheduler ou VMware DRS).

Comme il ne redémarre que le noyau, VMware vSphere 6.7 permet aux clients de « démarrer rapidement » où il charge vSphere ESXi sans redémarrer le matériel. Cette fonctionnalité est disponible uniquement avec les plates-formes et les pilotes qui sont sur la liste blanche de démarrage rapide. VSphere 6.7 étend les fonctionnalités du client vSphere, soit environ 90 % de la capacité du client Web vSphere.

Dans vSphere 6.7, VMware a étendu cette fonctionnalité pour permettre aux clients de définir la compatibilité EVC (Enhanced vMotion Compatibility) par machine virtuelle (VM) plutôt que par hôte. Dans vSphere 6.7, VMware a également révélé les API pouvant être utilisées pour créer des clones instantanés.

Voici quelques-unes des fonctionnalités de vSphere 6.7 U1 :

- Client vSphere basé sur le Web HTML5 et doté d'une fonction très complète
- VMotion pour les machines virtuelles NVIDIA GRID vGPU. Prise en charge du FPGA Intel.
- VCenter Server converge Tool pour passer d'un PSC externe à un PCS interne.
- Améliorations pour VSAN (mises à jour HCI).
- Bibliothèque de contenu améliorée.

Pour plus d'informations sur vSphere 6.7 U1, consultez "Nouveautés de vCenter Server 6.7 mise à jour 1". Bien que cette solution ait été validée avec vSphere 6.7, elle prend en charge toutes les versions de vSphere compatibles avec les autres composants par l'outil de matrice d'interopérabilité NetApp. NetApp recommande de déployer vSphere 6.7U1 pour obtenir ses correctifs et ses fonctionnalités améliorées.

Architecture de démarrage

Les options prises en charge pour l'architecture de démarrage FlexPod Express sont les suivantes :

- LUN SAN iSCSI
- Carte SD Cisco FlexFlash
- Disque local

Comme FlexPod Datacenter démarre à partir de LUN iSCSI, la gestion de la solution est améliorée grâce au démarrage iSCSI pour FlexPod Express.

"Ensuite, vérification de la solution."

Vérification de la solution

Cisco et NetApp ont conçu et développé FlexPod Express comme une plateforme d'infrastructure de premier plan pour leurs clients. Son design avec des composants de pointe leur permet aux clients de faire confiance à FlexPod Express pour leur infrastructure. Conformément aux principes fondamentaux du portefeuille FlexPod, l'architecture FlexPod Express a été testée en profondeur par les ingénieurs et architectes de data centers Cisco et NetApp. De la redondance et la disponibilité à chaque fonctionnalité individuelle, l'architecture FlexPod Express est validée pour inculquer une confiance à nos clients et établir une confiance dans le processus de conception.

VMware vSphere 6.7 a été vérifié sur les composants de l'infrastructure FlexPod Express. Cette validation

incluait des options de connectivité uplink 10 GbE pour l'hyperviseur.

"Suivant: Conclusion."

Conclusion

FlexPod Express propose une solution simple et efficace qui repose sur des composants de pointe. FlexPod Express peut être adapté à des besoins spécifiques en faisant évoluer et en proposant des options de plateforme d'hyperviseur. FlexPod Express a été conçu pour répondre aux besoins des moyennes entreprises, des bureaux distants, des succursales et d'autres entreprises qui ont besoin de solutions dédiées.

"Suivant : où trouver des informations supplémentaires ?"

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce document, consultez ces documents et sites web :

- Documentation NetApp

  "https://docs.netapp.com"

- Guide de déploiement de FlexPod Express avec VMware vSphere 6.7 et NetApp AFF A220

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

Guide de déploiement de FlexPod Express avec Cisco UCS C-Series et AFF A220

NVA-1123-DEPLOY : guide de déploiement de FlexPod Express avec VMware vSphere 6.7 et NetApp AFF A220

Savita Kumari, NetApp

En partenariat avec : 

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 de data Center préconçue et conforme aux bonnes pratiques. Elle repose sur la plateforme 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, et pour 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 peuvent être dimensionnées et optimisées pour prendre en charge de nombreux cas d’utilisation et besoins. 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 constitue 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

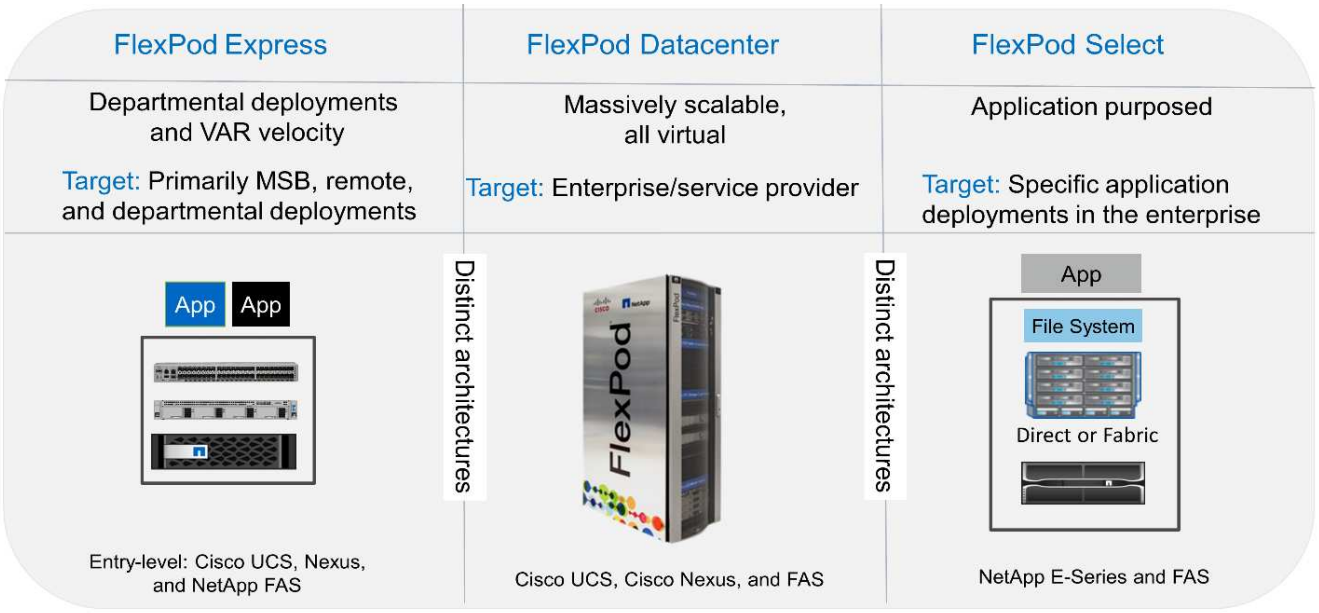
Cette solution FlexPod Express fait partie du programme d’infrastructure convergée FlexPod.

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.



Programme d'architecture vérifiée NetApp

Le programme d'architecture vérifiée NetApp propose une architecture validée pour les solutions NetApp Une architecture vérifiée NetApp fournit une architecture de solution NetApp qui apporte les qualités suivantes :

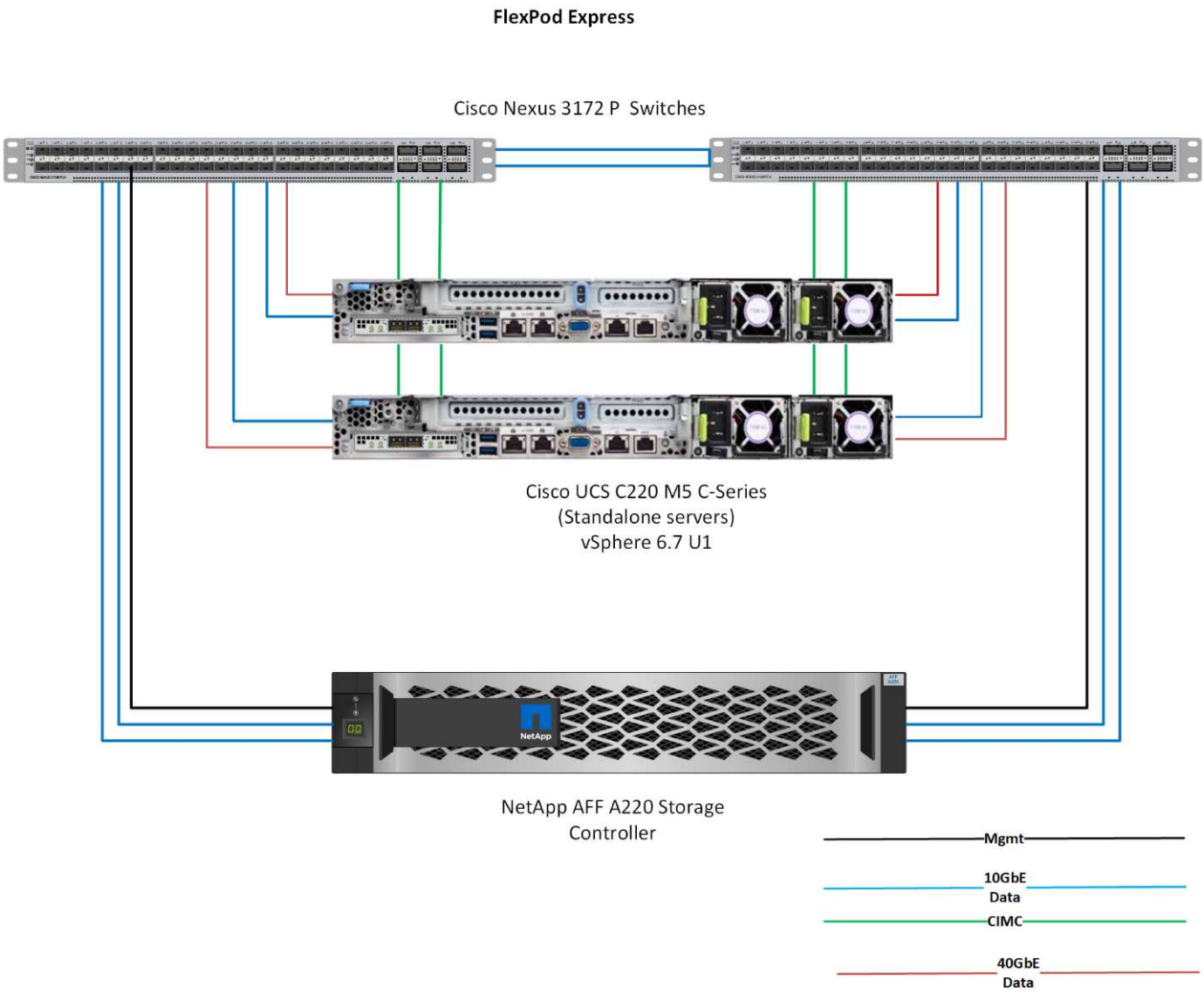
- Testée en profondeur
- Normative par nature
- Réduction des risques de déploiement
- Optimisée pour accélérer la mise en service

Ce guide détaille la conception de FlexPod Express avec VMware vSphere. Cette conception utilise également le tout nouveau système AFF A220, qui exécute NetApp ONTAP 9.4, Cisco Nexus 3172P et des serveurs Cisco UCS C-Series C220 M5 comme nœuds d'hyperviseur.

Technologie de la solution

Cette solution tire parti des dernières technologies de NetApp, Cisco et VMware. Cette solution comprend le nouveau NetApp AFF A220 exécutant ONTAP 9.4, deux commutateurs Cisco Nexus 3172P et des serveurs en rack Cisco UCS C220 M5 exécutant VMware vSphere 6.7. Cette solution validée utilise une technologie 10GbE. Des recommandations sont également fournies quant à la manière de faire évoluer les capacités de calcul en ajoutant deux nœuds d'hyperviseur à la fois afin que l'architecture FlexPod Express puisse s'adapter aux besoins métier en constante évolution de l'entreprise.

La figure suivante montre FlexPod Express avec VMware vSphere 10GbE.



Cette validation utilise une connectivité 10GbE et un Cisco UCS VIC 1387, soit 40 GbE. Pour obtenir une connectivité 10GbE, l'adaptateur CVR-QSFP-SFP10G est utilisé.

Récapitulatif du cas d'utilisation

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

- Bureaux distants ou succursales
- Moyennes entreprises
- Les environnements qui nécessitent une solution dédiée et économique

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

Bien que cette solution ait été validée avec vSphere 6.7, elle prend en charge toutes les versions de vSphere compatibles avec les autres composants par l'outil de matrice d'interopérabilité NetApp. NetApp recommande de déployer vSphere 6.7U1 pour obtenir ses correctifs et ses fonctionnalités améliorées.

Voici quelques-unes des fonctionnalités de vSphere 6.7 U1 :

- Client vSphere basé sur le Web HTML5 offrant une fonctionnalité complète
- VMotion pour les machines virtuelles NVIDIA GRID vGPU. Prise en charge du FPGA Intel
- VCenter Server converge Tool pour passer d'un PSC externe à un PCS interne
- Améliorations pour VSAN (mises à jour HCI)
- Bibliothèque de contenu améliorée

Pour plus d'informations sur vSphere 6.7 U1, consultez "Nouveautés de vCenter Server 6.7 mise à jour 1".

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.

Le tableau suivant répertorie les composants matériels requis pour toutes les configurations FlexPod Express.

Sous-jacent	Quantité
PAIRE HAUTE DISPONIBILITÉ AFF A220	1
Serveur Cisco C220 M5	2
Commutateur Cisco Nexus 3172P	2
Carte d'interface virtuelle Cisco UCS (VIC) 1387 pour serveur C220 M5	2
ADAPTATEUR CVR-QSFP-SFP10G	4

Le tableau suivant répertorie le matériel requis en plus de la configuration de base pour l'implémentation de la solution 10GbE.

Sous-jacent	Quantité
Serveur Cisco UCS C220 M5	2
Cisco VIC 1387	2
ADAPTATEUR CVR-QSFP-SFP10G	4

Configuration logicielle requise

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

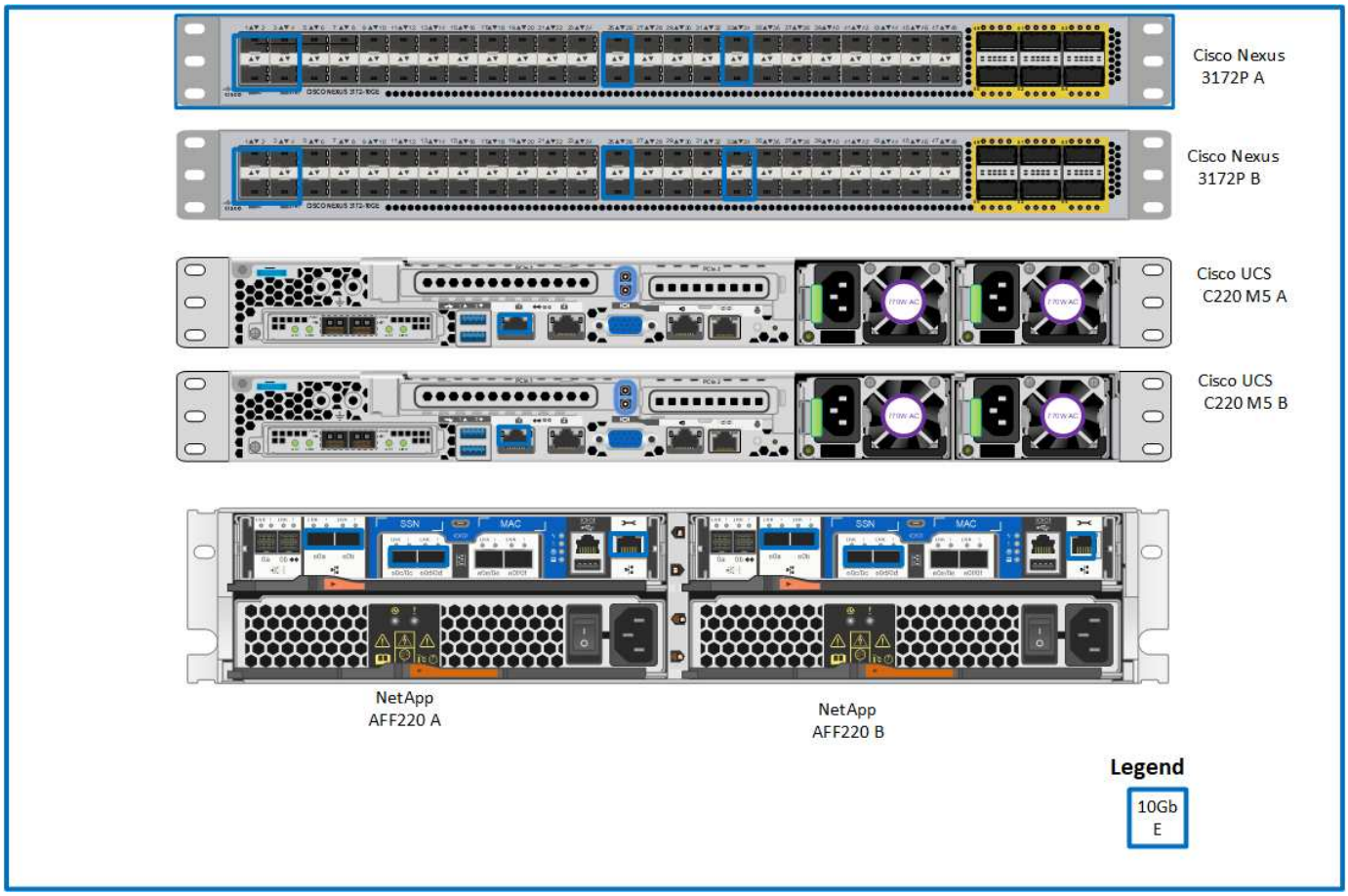
Logiciel	Version	Détails
Contrôleur de gestion intégrée Cisco (CIMC)	3.1(3g)	Pour les serveurs en rack Cisco UCS C220 M5
Pilote nenic Cisco	1.0.25.0	Pour les cartes d'interface VIC 1387
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Pour commutateurs Cisco Nexus 3172P
NetApp ONTAP	9.4	Pour les contrôleurs AFF A220

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

Logiciel	Version
Appliance de serveur VMware vCenter	6.7
Hyperviseur VMware vSphere ESXi	6.7
Plug-in NetApp VAAI pour ESXi	1.1.2

Informations sur le câblage FlexPod Express

La figure suivante montre le câblage de validation de référence.



Le tableau suivant présente les informations de câblage du commutateur Cisco Nexus 3172P A.

Périphérique local	Port local	Périphérique distant	Port distant
Commutateur Cisco Nexus 3172P A	Eth1/1	Contrôleur de stockage A AFF A220 NetApp	e0c
	Eth1/2	Contrôleur de stockage B AFF A220 NetApp	e0c
	Eth1/3	Serveur autonome Cisco UCS C220 C-Series A	MLOM1 avec adaptateur CVR-QSFP-SFP10G
	Eth1/4	Serveur autonome Cisco UCS C220 C-Series B	MLOM1 avec adaptateur CVR-QSFP-SFP10G
	Eth1/25	Commutateur Cisco Nexus 3172P B	Eth1/25
	Eth1/26	Commutateur Cisco Nexus 3172P B	Eth1/26
	Eth1/33	Contrôleur de stockage A AFF A220 NetApp	E0M
	Eth1/34	Serveur autonome Cisco UCS C220 C-Series A	CIMC

Le tableau suivant présente les informations de câblage du commutateur Cisco Nexus 3172P B.

Périphérique local	Port local	Périphérique distant	Port distant
Commutateur Cisco Nexus 3172P B	Eth1/1	Contrôleur de stockage A AFF A220 NetApp	e0d
	Eth1/2	Contrôleur de stockage B AFF A220 NetApp	e0d
	Eth1/3	Serveur autonome Cisco UCS C220 C-Series A	MLOM2 avec adaptateur CVR-QSFP-SFP10G
	Eth1/4	Serveur autonome Cisco UCS C220 C-Series B	MLOM2 avec adaptateur CVR-QSFP-SFP10G
	Eth1/25	Commutateur Cisco Nexus 3172P A	Eth1/25
	Eth1/26	Commutateur Cisco Nexus 3172P A	Eth1/26
	Eth1/33	Contrôleur de stockage B AFF A220 NetApp	E0M
	Eth1/34	Serveur autonome Cisco UCS C220 C-Series B	CIMC

Le tableau suivant présente les informations de câblage pour le contrôleur de stockage NetApp AFF A220 A.

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
	e0c	Commutateur Cisco Nexus 3172P A	Eth1/1
	e0d	Commutateur Cisco Nexus 3172P B	Eth1/1
	E0M	Commutateur Cisco Nexus 3172P A	Eth1/33

Le tableau suivant présente les informations de câblage pour le contrôleur de stockage AFF A220 B.

Périphérique local	Port local	Périphérique distant	Port distant
Contrôleur de stockage B AFF A220 NetApp	e0a	Contrôleur de stockage A AFF A220 NetApp	e0a
	e0b	Contrôleur de stockage A AFF A220 NetApp	e0b
	e0c	Commutateur Cisco Nexus 3172P A	Eth1/2
	e0d	Commutateur Cisco Nexus 3172P B	Eth1/2
	E0M	Commutateur Cisco Nexus 3172P B	Eth1/33

Procédures de déploiement

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

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

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

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

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

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

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

Les numéros de VLAN sont nécessaires dans toute la configuration de FlexPod Express. Les VLAN sont appelés `<<var_xxxx_vlan>>`, où `xxxx` Utilise le VLAN (par exemple iSCSI-A).

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

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

Procédure de déploiement Cisco Nexus 3172P

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

Configuration initiale du commutateur Cisco Nexus 3172P

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

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

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

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

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

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

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

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

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

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

Activer les fonctionnalités avancées

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

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

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

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

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

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

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

Effectuer une configuration globale Spanning Tree

La plateforme Cisco Nexus utilise une nouvelle fonctionnalité de protection appelée Bridge assurance. La fonctionnalité Bridge assurance protège les données contre une liaison unidirectionnelle ou toute autre défaillance logicielle avec un périphérique qui continue à transférer le trafic de données lorsqu'il n'exécute plus

l'algorithme Spanning Tree. Les ports peuvent être placés dans l'un des différents États, y compris le réseau ou la périphérie, selon la plate-forme.

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

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

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

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

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

Définir les VLAN

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

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

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

Configurez les descriptions des ports d'accès et de gestion

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

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

Commutateur Cisco Nexus A

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Commutateur Cisco Nexus B

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Configuration des interfaces de gestion des serveurs et du stockage

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

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

Commutateur Cisco Nexus A

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

Commutateur Cisco Nexus B

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

Effectuez la configuration globale du canal de port virtuel

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

Un VPC offre les avantages suivants :

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

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

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

Commutateur Cisco Nexus A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Commutateur Cisco Nexus B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configurer les canaux du port de stockage

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

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

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

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

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

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

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

Configurez les connexions du serveur

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

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

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

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

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

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

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

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

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

Uplink dans l'infrastructure réseau existante

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

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

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

Procédure de déploiement du stockage NetApp (partie 1)

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

Installation des contrôleurs de stockage NetApp AFF2xx

NetApp Hardware Universe

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

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

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

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

Contrôleurs de stockage

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

NetApp ONTAP 9.4

Fiche de configuration

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

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

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

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

Configurez le nœud A

Pour configurer le nœud A, procédez comme suit :

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

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

2. Laissez le système démarrer.

   ```
   autoboot
   ```

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

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

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

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

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

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

   Ce serveur Web doit être accessible.

```
<<var_url_boot_software>>
```

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

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

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

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

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

Configurer le nœud B

Pour configurer le nœud B, procédez comme suit :

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

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

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

```
autoboot
```

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

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

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

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

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

   Ce serveur Web doit être accessible.

```
<<var_url_boot_software>>
```

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

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

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

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

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

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

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

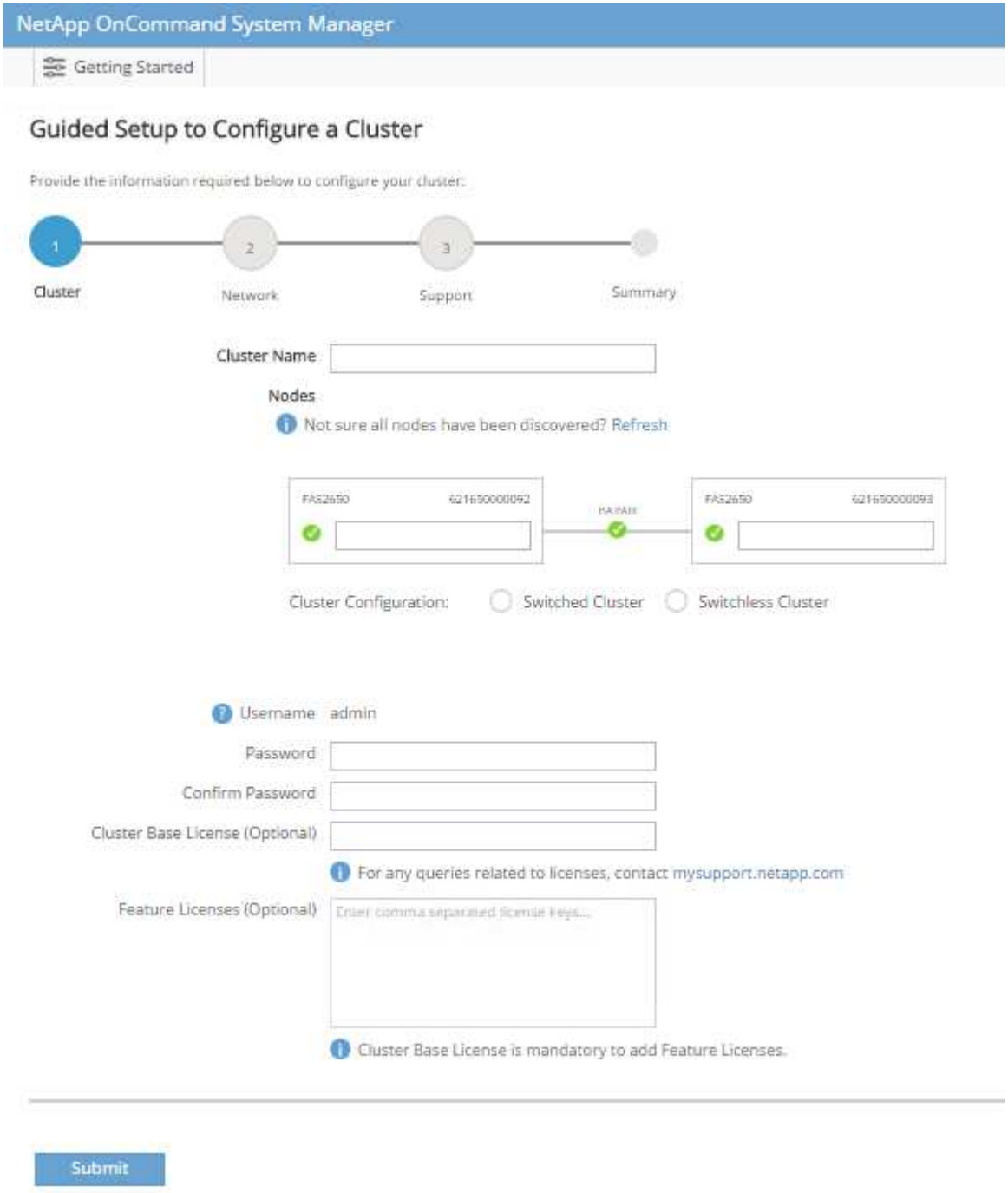
1. Suivez les invites pour configurer le nœud A.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

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

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

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



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

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

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

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

   Vous pouvez entrer plusieurs adresses IP de serveur DNS.

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

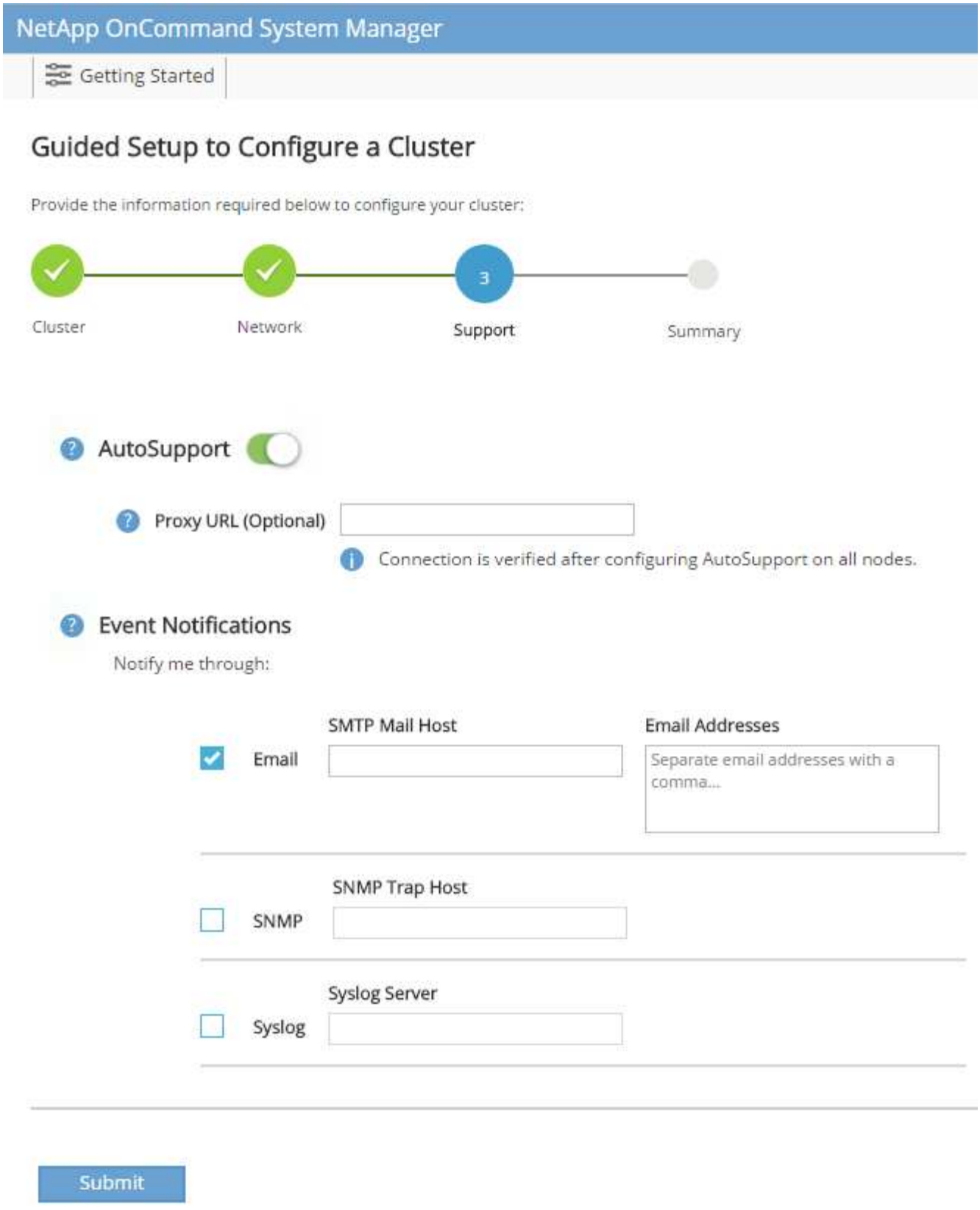
   Vous pouvez également entrer un autre serveur NTP.

8. Configuration des informations de support.

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

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

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



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

Suite de la configuration du cluster de stockage

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

Zéro de tous les disques de spare

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

```
disk zerospares
```

Définissez l'option de personnalisation des ports UTA2 intégrés

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

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

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

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

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

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

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

Renommage des interfaces logiques de gestion

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

1. Affiche les noms des LIF de gestion actuelles.

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

2. Renommer la LIF de gestion de cluster.

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

3. Renommez la LIF de gestion du nœud B.

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

Définissez le rétablissement automatique sur la gestion du cluster

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

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

Configurez l'interface réseau du processeur de service

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

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

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

Activez le basculement du stockage dans ONTAP

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

de basculement :

1. Vérification de l'état du basculement du stockage

   ```
   storage failover show
   ```

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

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

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

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

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

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

   ```
   cluster ha show
   ```

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

   ```
   High Availability Configured: true
   ```

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

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

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

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

   ```
   storage failover hwassist show
   ```

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

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Créez un domaine de diffusion MTU de trames Jumbo dans ONTAP

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

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Supprime les ports de données du broadcast domain par défaut

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

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

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Désactiver le contrôle de flux sur les ports UTA2

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

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

Configurez le protocole LACP IFGRP dans ONTAP

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

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

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Configuration des trames Jumbo dans NetApp ONTAP

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

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Créez des VLAN dans ONTAP

Pour créer des VLAN dans ONTAP, procédez comme suit :

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

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

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

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. Créez des ports MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Créez des agrégats dans ONTAP

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

Pour créer des agrégats, lancer les commandes suivantes :

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

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

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

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

Configurer le fuseau horaire dans ONTAP

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

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

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

Configurez SNMP dans ONTAP

Pour configurer le SNMP, procédez comme suit :

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

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

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

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

Configurez SNMPv1 dans ONTAP

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

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

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

Configurez SNMPv3 dans ONTAP

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

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

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

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

Configurez AutoSupport HTTPS dans ONTAP

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

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

Créez un serveur virtuel de stockage

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

1. Exécutez le `vserver create` commande.

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

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

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

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

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

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

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

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

configuré.

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

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

Configurez NFSv3 dans ONTAP

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

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

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

1. Créez une règle pour chaque hôte ESXi dans la stratégie d'exportation par défaut.
2. Pour chaque hôte ESXi créé, attribuez une règle. Chaque hôte a son propre index de règles. Votre premier hôte ESXi dispose de l'index de règles 1, votre second hôte ESXi dispose de l'index de règles 2, etc.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Assigner la export policy au volume root du SVM d'infrastructure.

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

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

Créez le service iSCSI dans ONTAP

Pour créer le service iSCSI, procédez comme suit :

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

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

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

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

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

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

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

3. Créer les relations de mise en miroir.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

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

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

Configurez l'accès HTTPS dans ONTAP

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

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

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

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

```
security certificate show
```

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

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

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

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

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

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

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configurez et activez l'accès SSL et HTTPS, et désactivez l'accès HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

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

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

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

Créez un volume NetApp FlexVol dans ONTAP

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

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Activez la déduplication dans ONTAP

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

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

Créer des LUN dans ONTAP

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

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

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

Création des LIFs iSCSI dans ONTAP

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

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

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

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Création des LIFs NFS dans ONTAP

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

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

1. Créer une LIF NFS.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Ajoutez un administrateur SVM d'infrastructure

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

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

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

1. Exécutez la commande suivante :

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

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

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

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

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

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

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

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

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

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

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

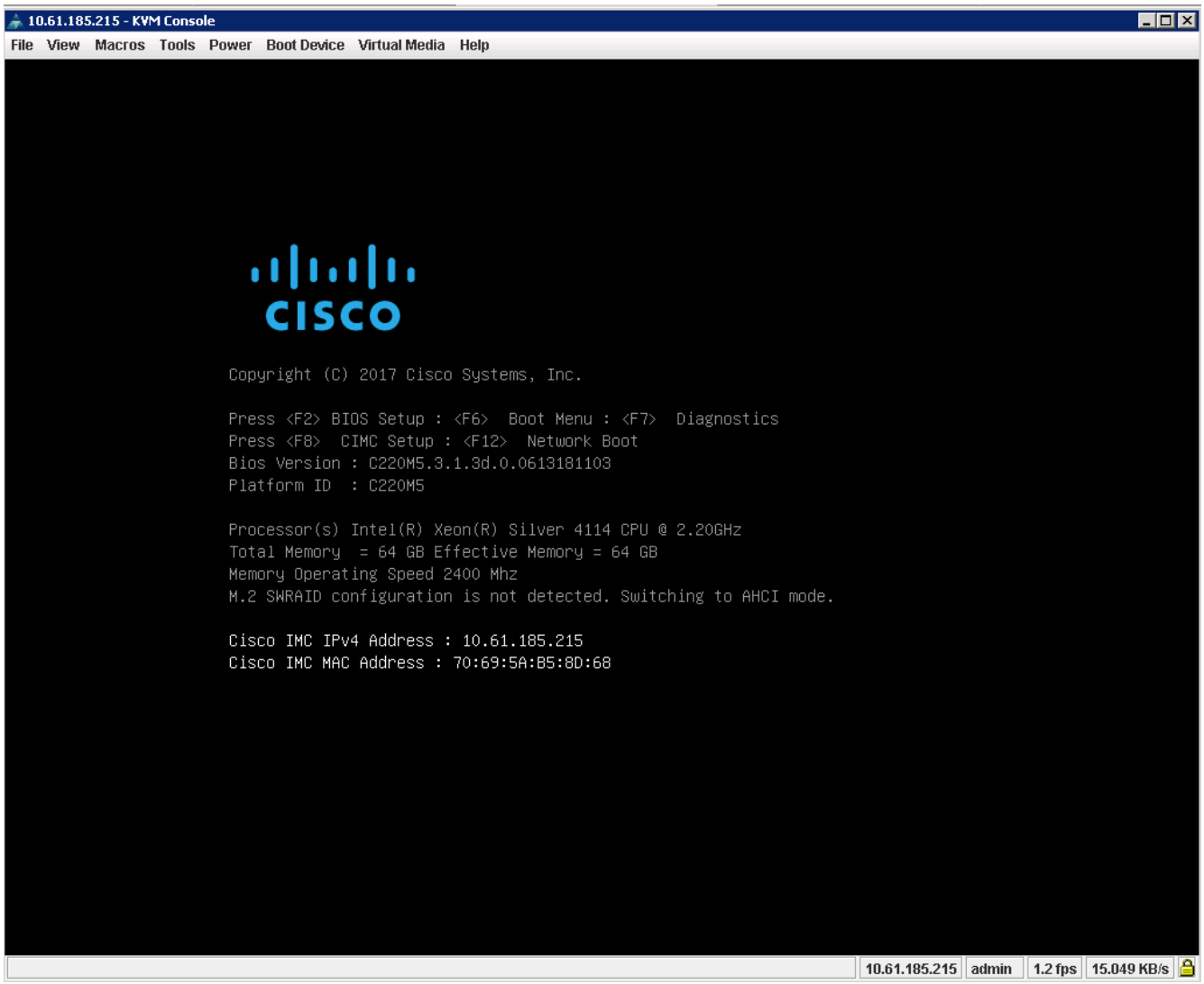
Le tableau suivant répertorie les informations nécessaires à la configuration de CIMC pour chaque serveur autonome Cisco UCS C-Series.

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

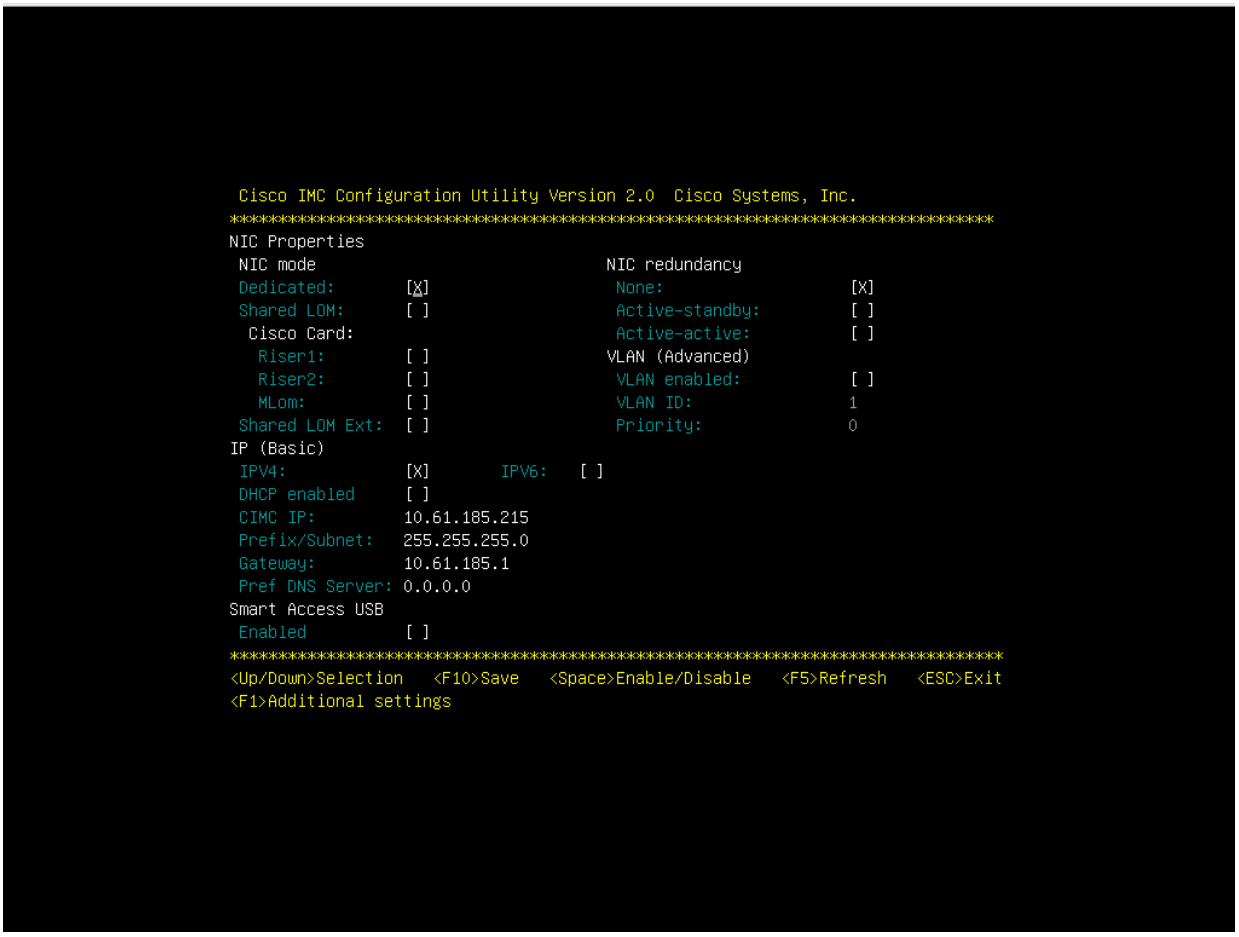
La version CIMC utilisée dans cette validation est CIMC 3.1.3(g).

Tous les serveurs

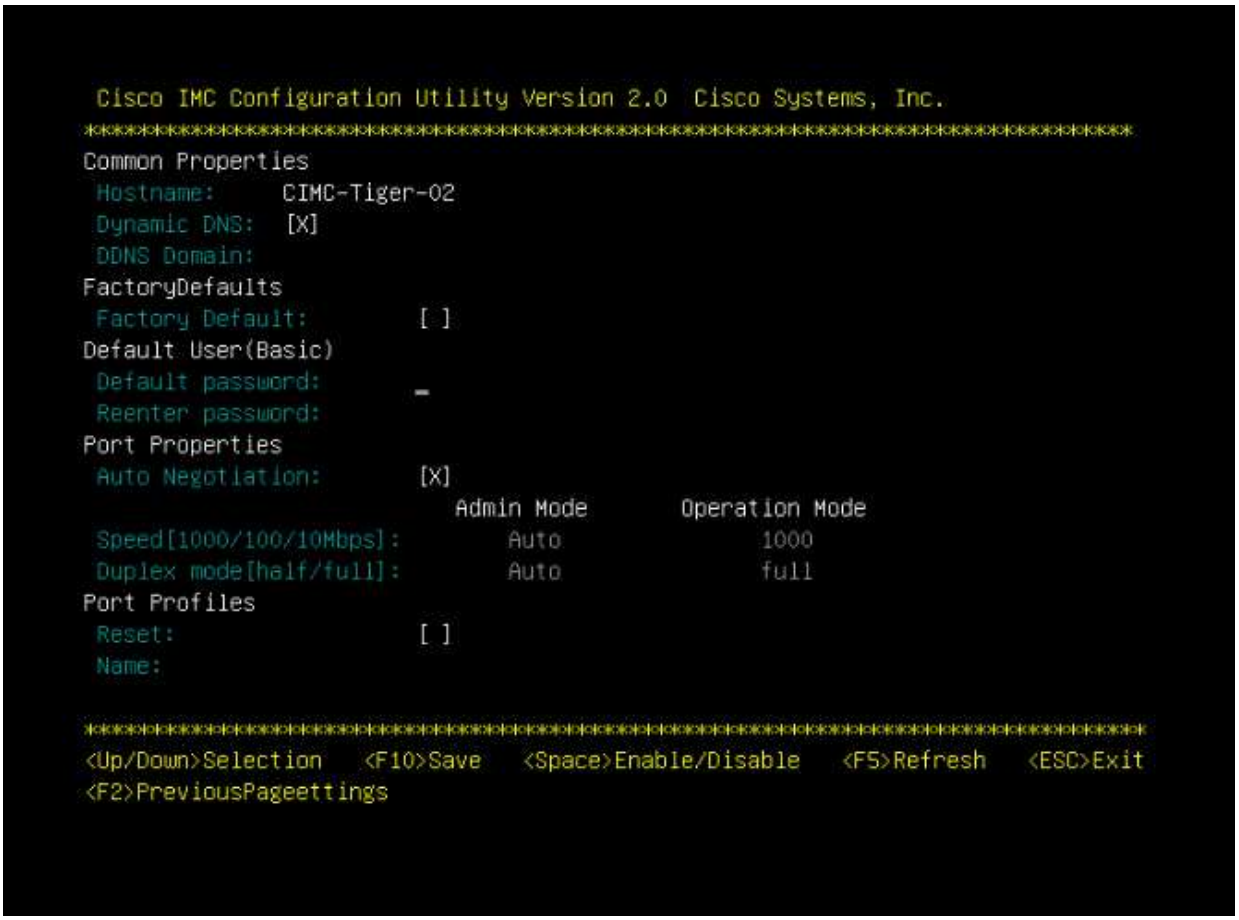
1. Reliez le dongle (KVM) du clavier, de la vidéo et de la souris Cisco (fourni avec le serveur) au port KVM situé à l'avant du serveur. Branchez un moniteur VGA et un clavier USB sur les ports de dongle KVM appropriés.
2. Mettez le serveur sous tension et appuyez sur F8 lorsque vous êtes invité à entrer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



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



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



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

Configuration du démarrage iSCSI des serveurs Cisco UCS C-Series

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

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

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

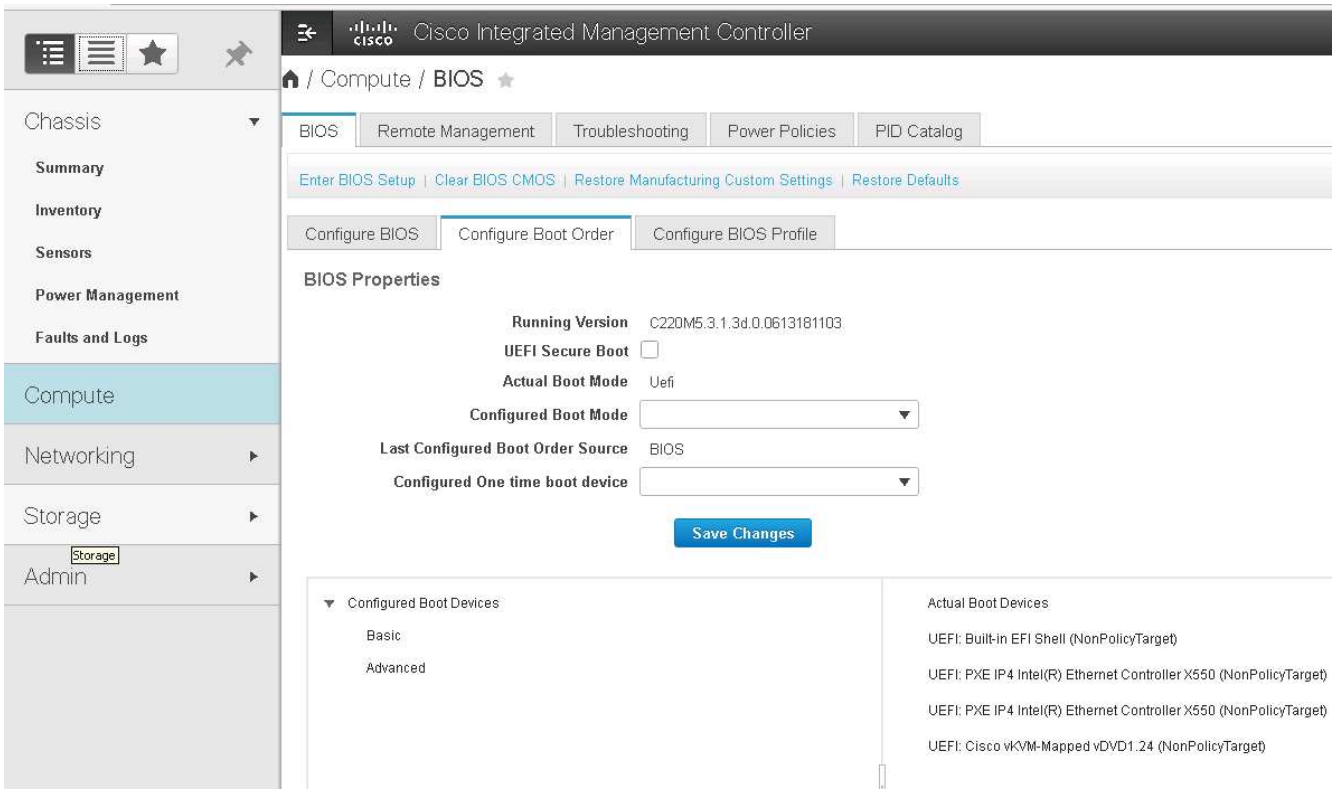
Détails	Valeur de détail
Initiateur hôte VMware ESXi a name	<<var_ucs_initiator_name_A>>
Hôte ESXi iSCSI-A IP	<<var_esxi_Host_iscsiA_ip>>
Masque de réseau iSCSI-A de l'hôte ESXi	<<var_esxi_host_iscsiA_mask>>
Hôte ESXi iSCSI : passerelle par défaut	<<var_esxi_Host_iscsiA_Gateway>>
Nom de l'initiateur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

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

Configuration de l'ordre de démarrage

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

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



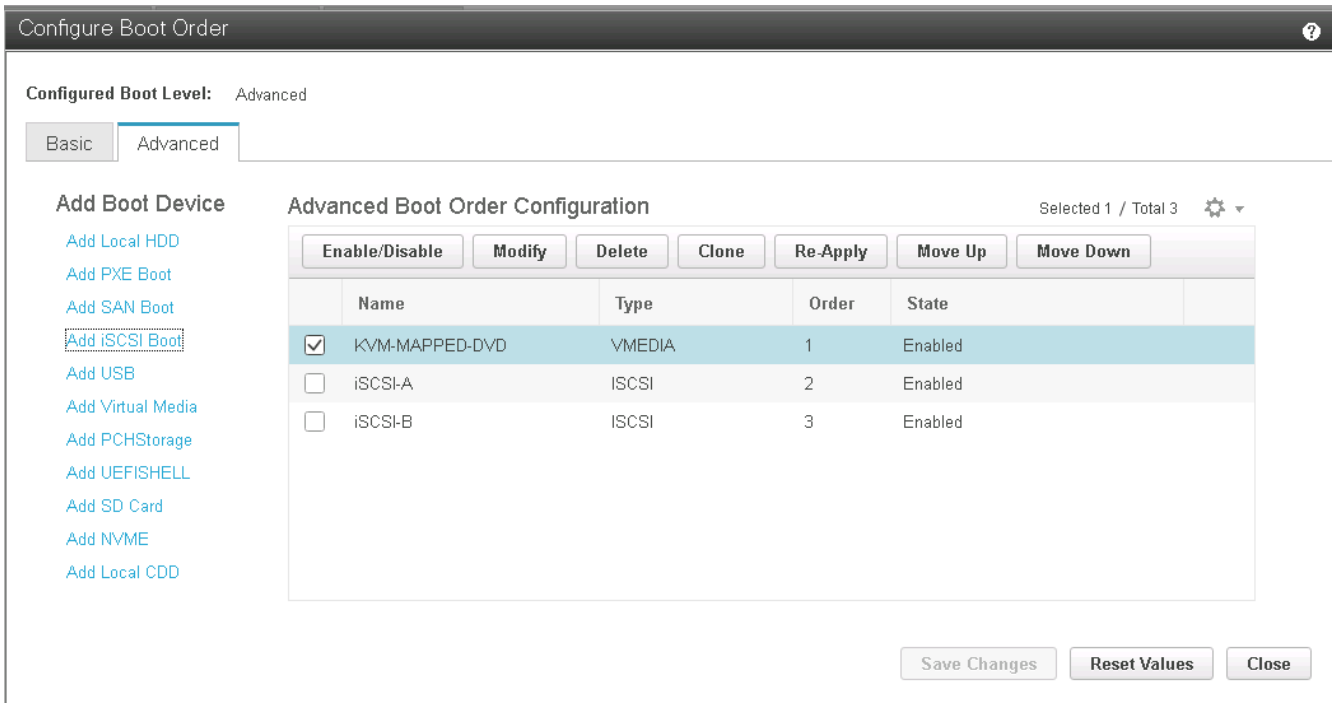
3. Configurez les périphériques suivants en cliquant sur le périphérique sous Ajouter un périphérique de démarrage et en accédant à l'onglet Avancé.
   - Ajouter un média virtuel
     - NOM : KVM-CD-DVD
     - SOUS-TYPE : DVD MAPPÉ KVM
     - État : activé
     - Ordre : 1
   - Ajouter un démarrage iSCSI.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

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

◦ Cliquez sur Ajouter un démarrage iSCSI.

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

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

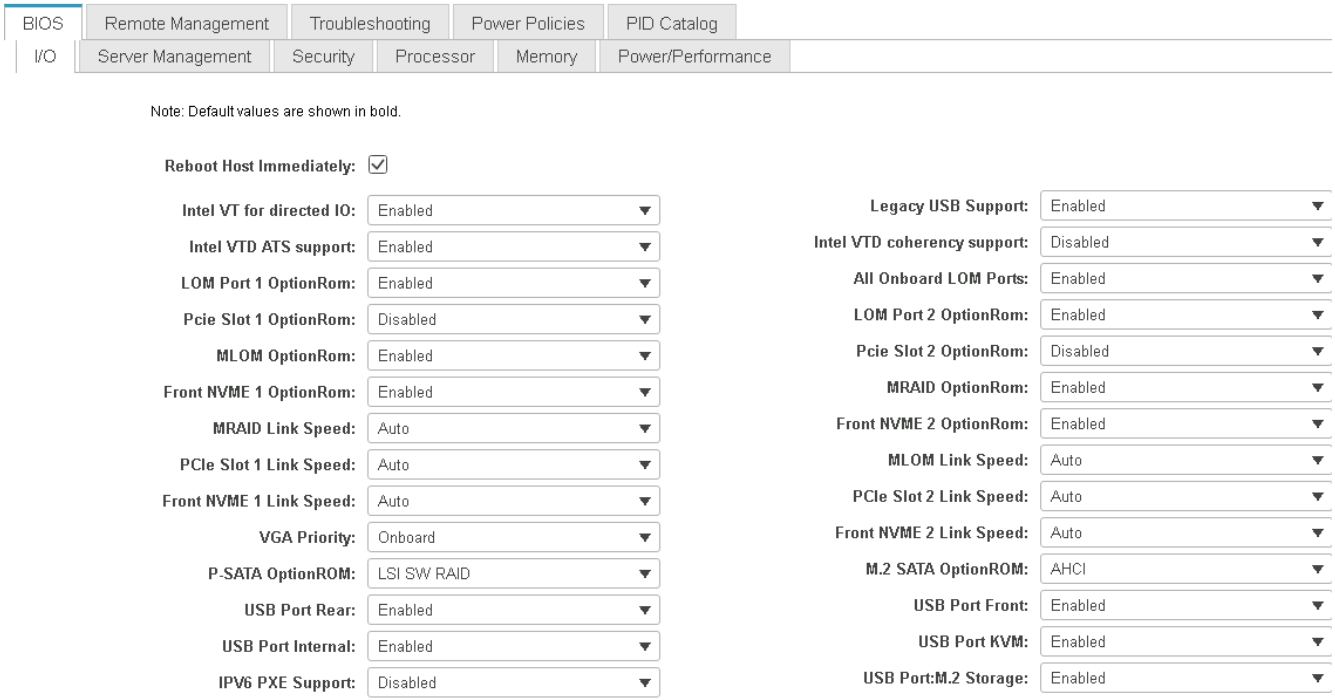


6. Redémarrez le serveur pour démarrer avec votre nouvel ordre de démarrage.

Désactiver le contrôleur RAID (le cas échéant)

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

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



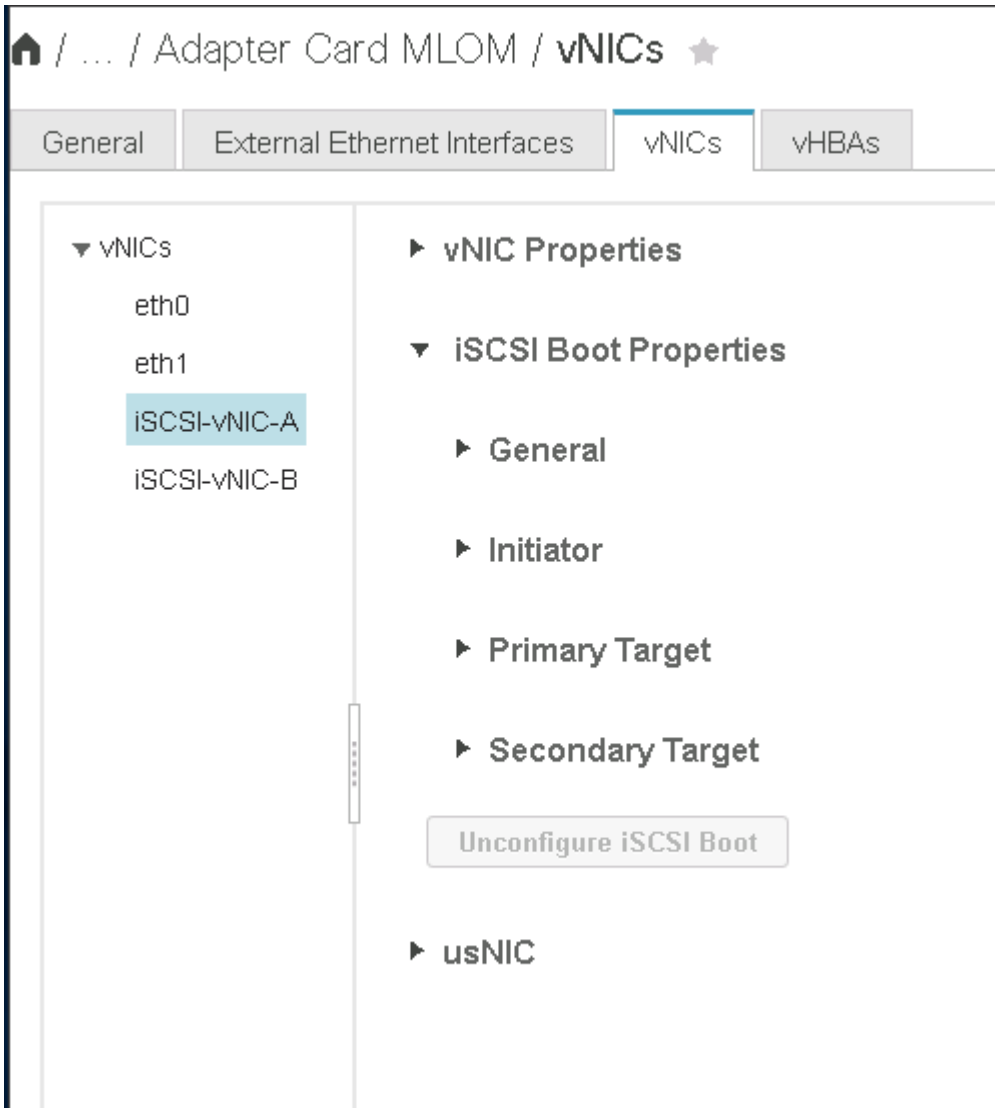
Configurer Cisco VIC11387 pour le démarrage iSCSI

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

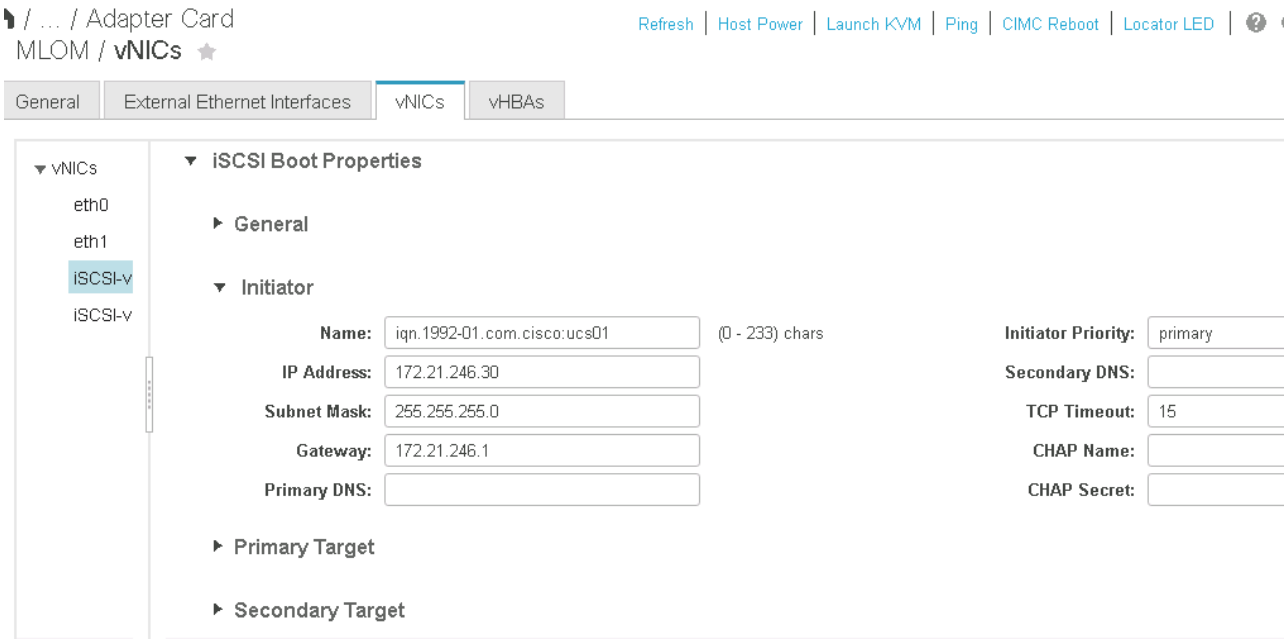
Créez des vNIC iSCSI

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

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



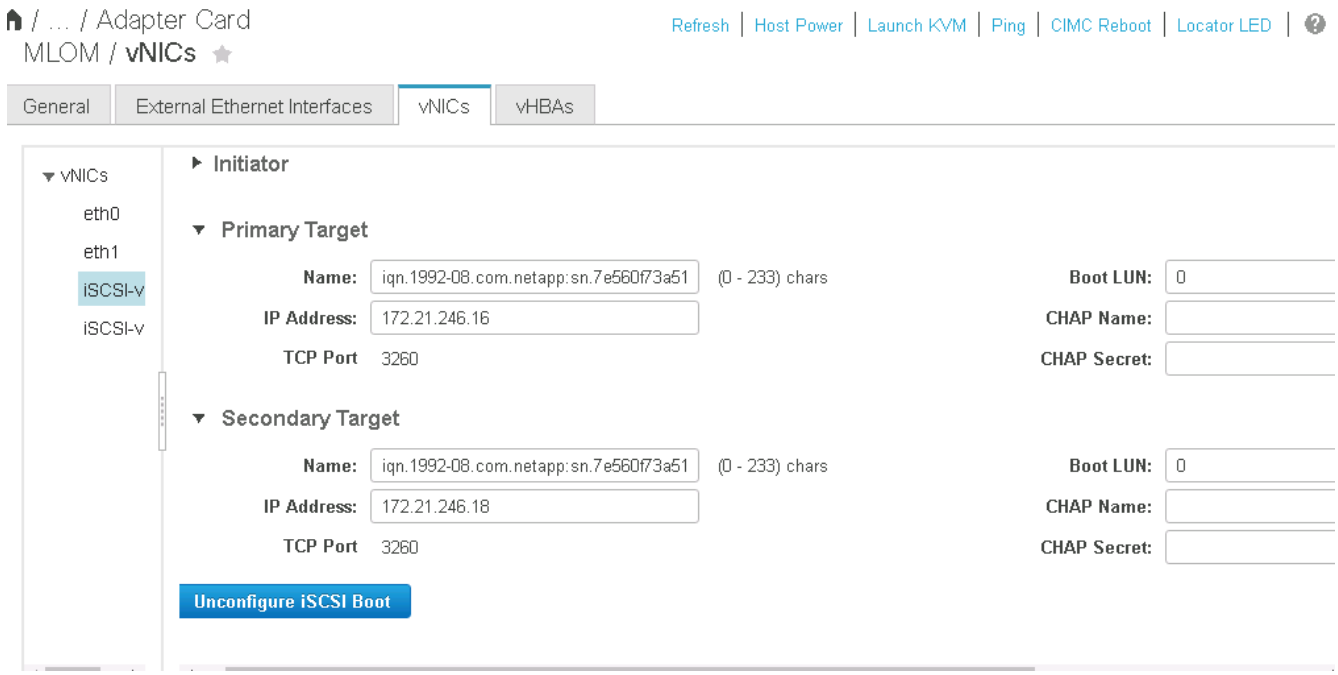
6. Sous Propriétés de démarrage iSCSI, entrez les détails de l'initiateur :
    - Nom : <<var_ucsa_initiator_name_a>>
    - Adresse IP : <<var_esxi_hostA_iscsiA_ip>>
    - Masque de sous-réseau : <<var_esxi_hostA_iscsiA_mask>>
    - Passerelle : <<var_esxi_hostA_iscsiA_Gateway>>



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

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

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



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

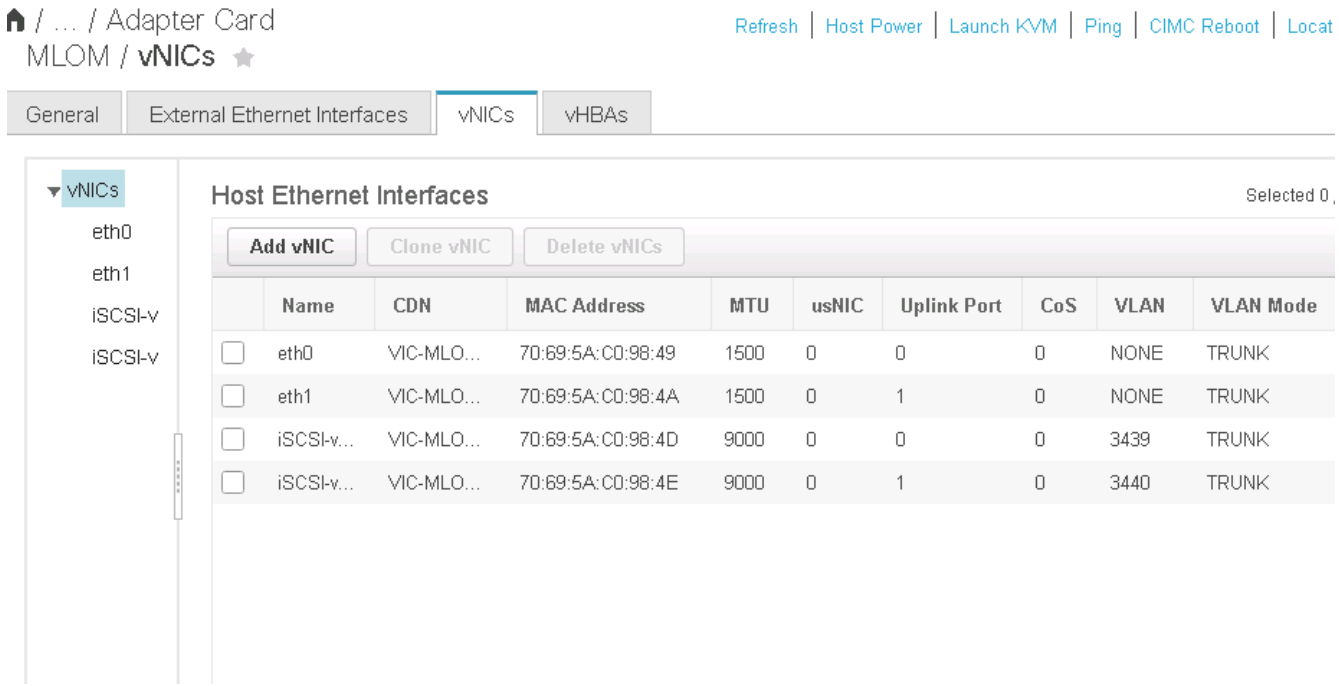
    Vous pouvez obtenir le numéro IQN de stockage en utilisant le `vserver iscsi show` commande.

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

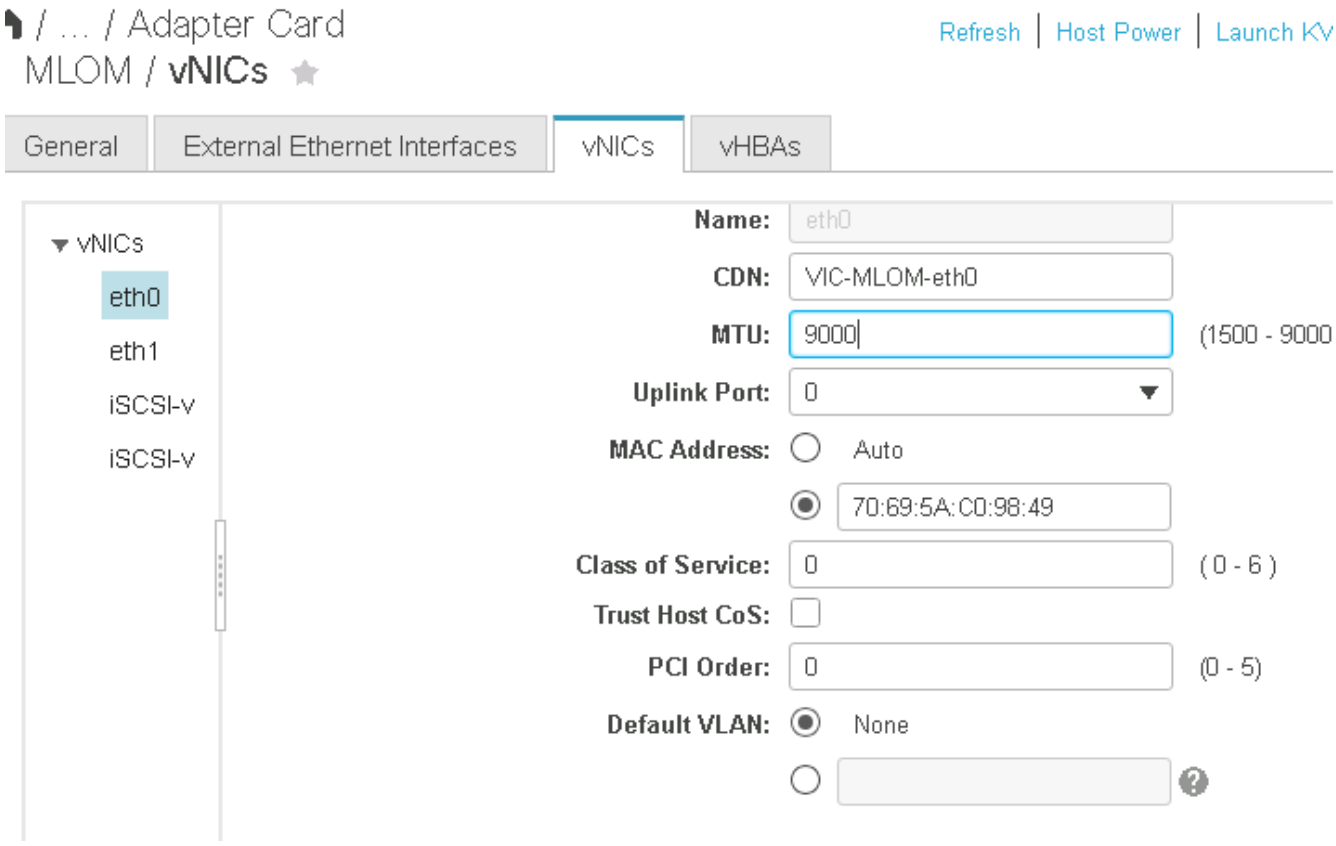
16. Répétez ce processus pour configurer l'initialisation iSCSI pour le serveur Cisco UCS B.

Configurer vNIC pour ESXi

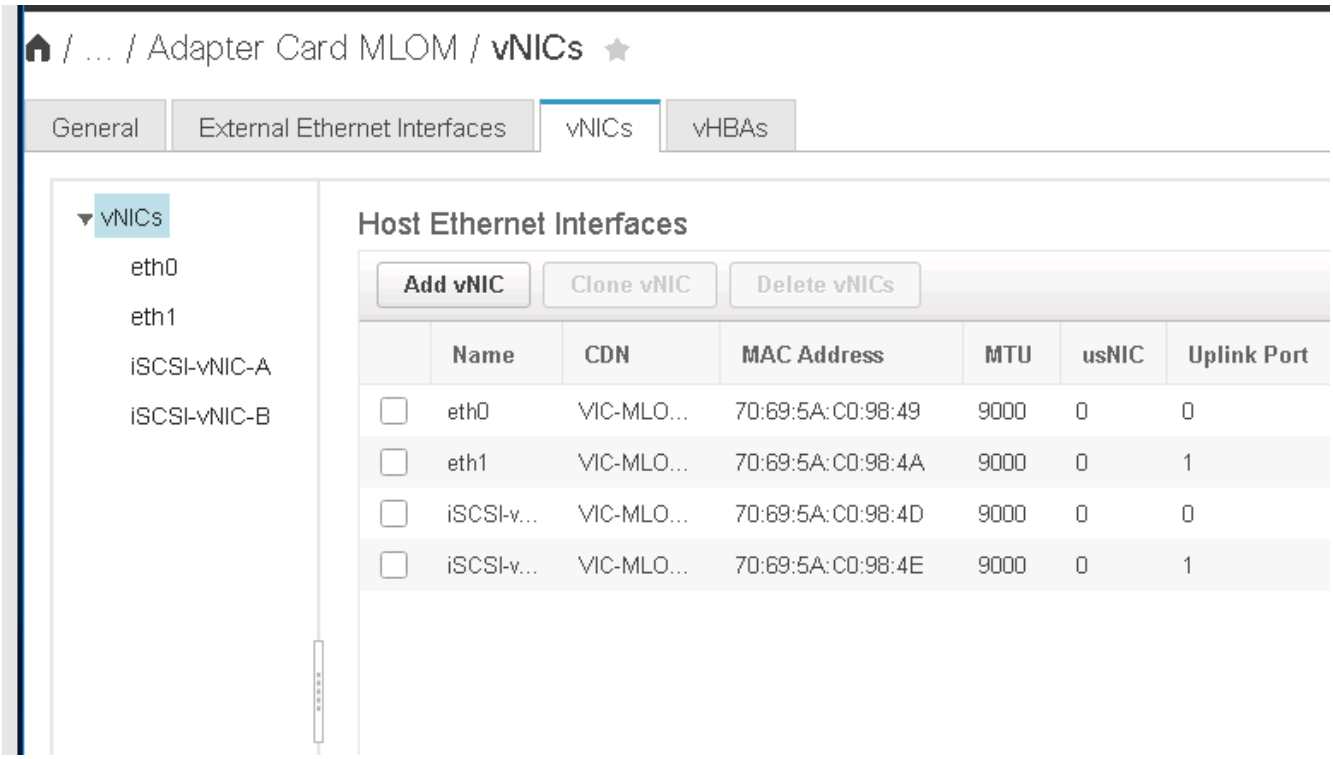
1. Dans la fenêtre du navigateur de l'interface CIMC, cliquez sur Inventaire, puis sur cartes Cisco VIC dans le volet droit.
2. Sous cartes d'adaptateur, sélectionnez Cisco UCS VIC 1387, puis les vNIC en dessous.



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



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



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

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

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

Configuration du stockage de démarrage SAN ONTAP

Création des igroups iSCSI

Pour créer des igroups, effectuez l'étape suivante :

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

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

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

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

Mappez les LUN de démarrage sur les igroups

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

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

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

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

Procédure de déploiement de VMware vSphere 6.7

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

Il existe plusieurs méthodes pour installer VMware ESXi dans un tel environnement. Cette procédure utilise la

console KVM virtuelle et les fonctions de média virtuel de l'interface CIMC pour les serveurs Cisco UCS C-Series pour mapper les supports d'installation à distance à chaque serveur.

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

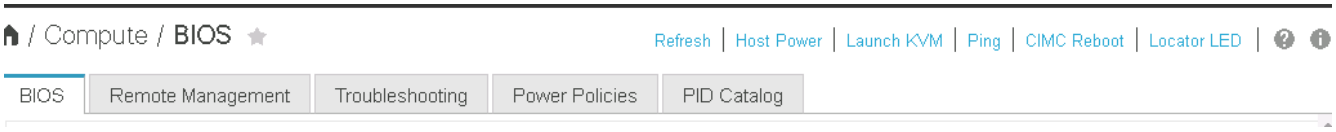
Cette procédure doit être effectuée pour tout nœud ajouté au cluster.

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

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

Tous les hôtes

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



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

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

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

Installez VMware ESXi

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

Téléchargez l'image personnalisée DE VMWARE ESXI 6.7 Cisco

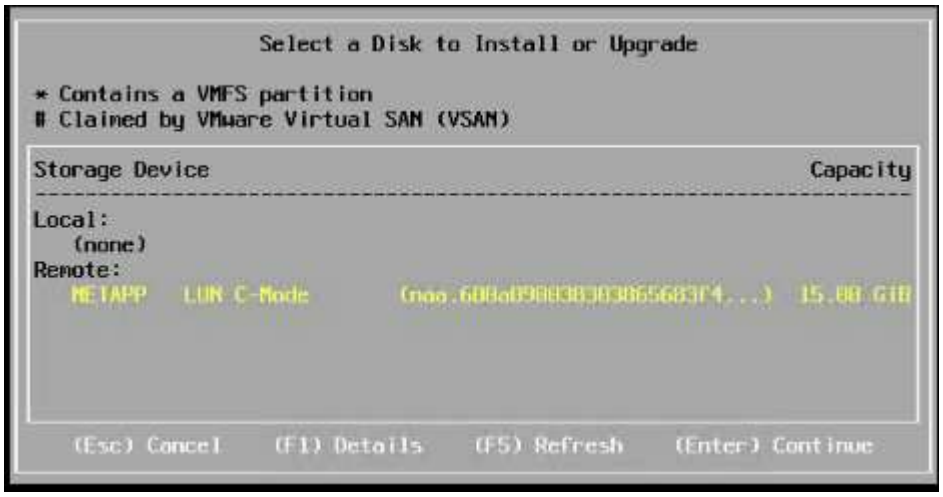
1. Accédez au "Page de téléchargement de VMware vSphere" Pour les ISO personnalisées.
2. Cliquez sur Go to Downloads en regard du CD d'installation de Cisco Custom image for ESXi 6.7 GA.
3. Téléchargez le CD d'installation Cisco Custom image for ESXi 6.7 GA (ISO).

Tous les hôtes

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

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

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



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

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

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

Tous les hôtes

1. Une fois le redémarrage du serveur terminé, entrez l'option permettant de personnaliser le système en appuyant sur F2.
2. Connectez-vous avec root en tant que nom de connexion et mot de passe racine entrés précédemment au cours du processus d'installation.
3. Sélectionnez l'option configurer le réseau de gestion.
4. Sélectionnez cartes réseau et appuyez sur entrée.
5. Sélectionnez les ports souhaités pour vSwitch0. Appuyez sur entrée.

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

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

Configurer l'hôte ESXi

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

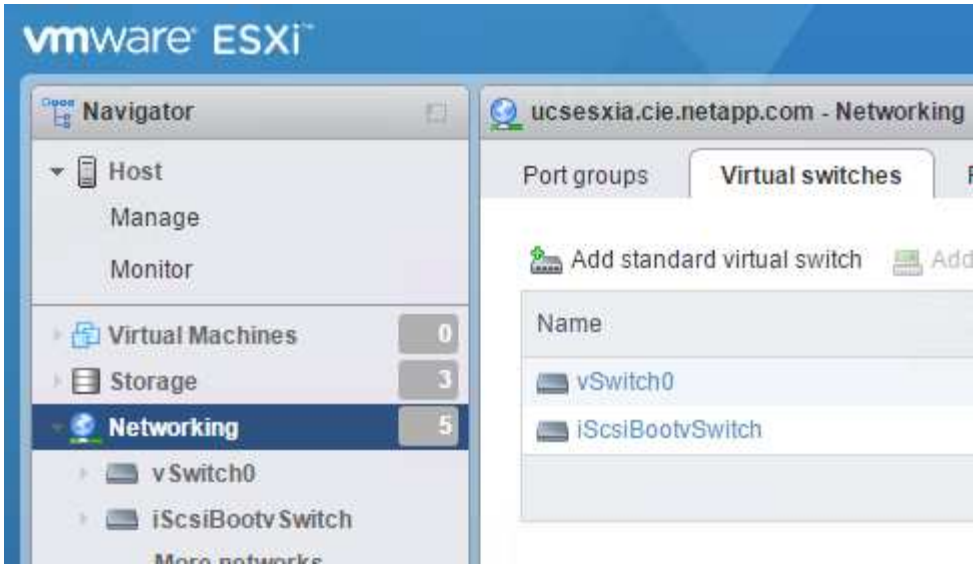
Détails	Valeur
Nom d’hôte ESXi	
IP de gestion d’hôte ESXi	
Masque de gestion d’hôte ESXi	
Passerelle de gestion de l’hôte ESXi	
IP NFS de l’hôte ESXi	
Masque NFS hôte ESXi	
Passerelle NFS de l’hôte ESXi	
IP vMotion hôte ESXi	
Masque vMotion hôte ESXi	
Passerelle vMotion de l’hôte ESXi	
Hôte ESXi iSCSI-A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

Connectez-vous à l’hôte ESXi

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

Configurez le démarrage iSCSI

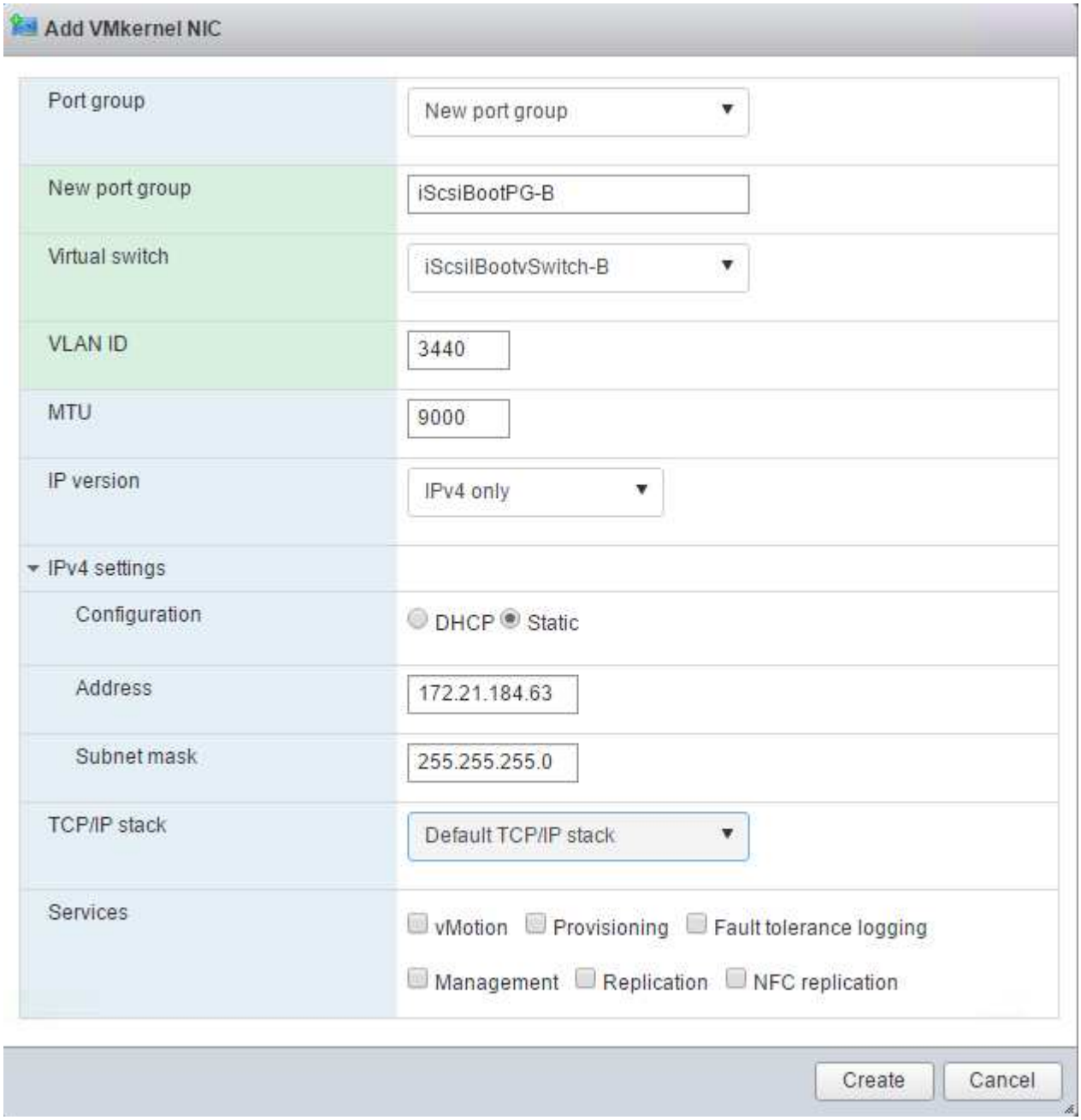
1. Sélectionnez réseau sur la gauche.
2. Sur la droite, sélectionnez l’onglet commutateurs virtuels.



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

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

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

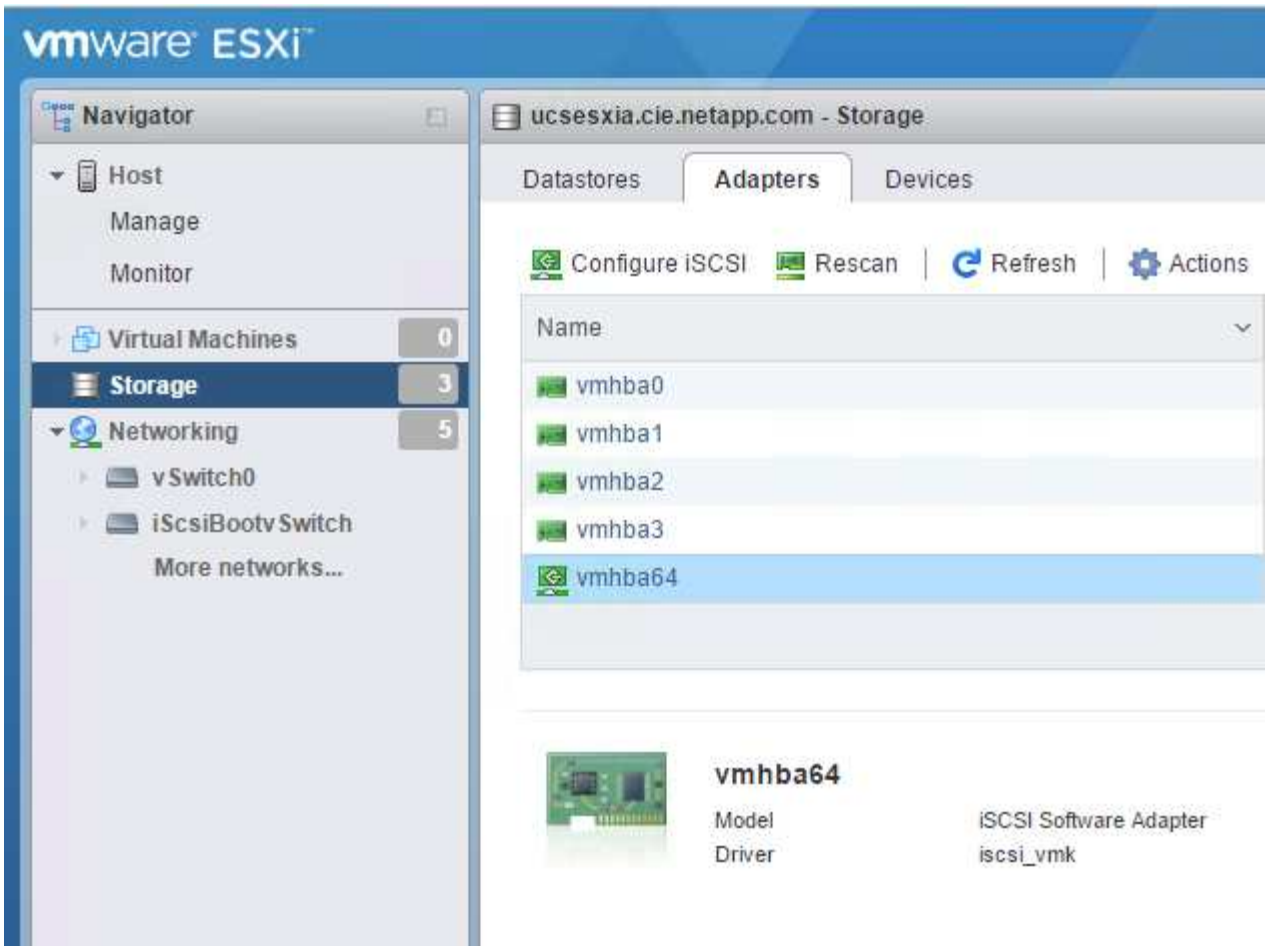


Définissez la MTU sur 9000 activé `iScsiBootPG- A.`

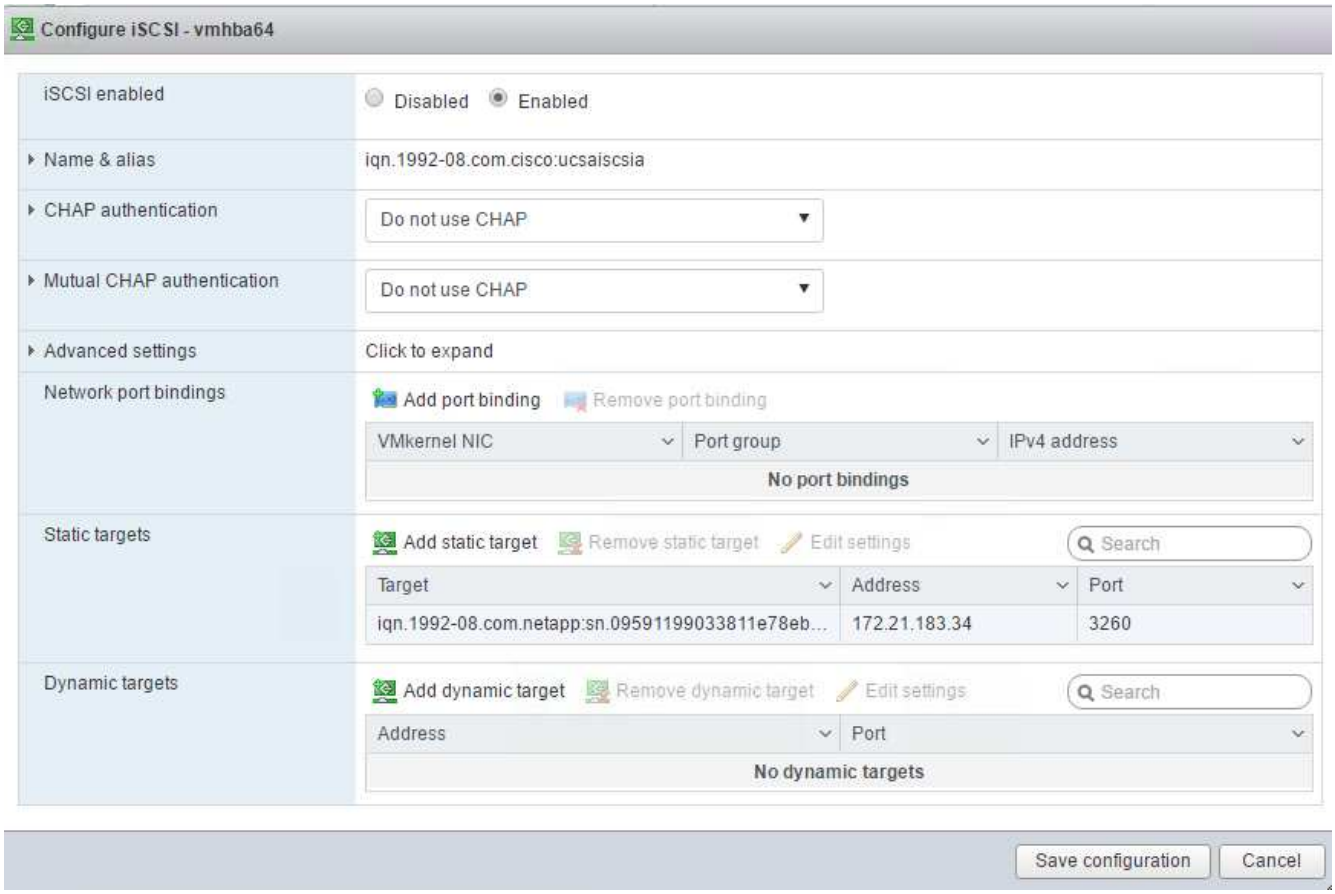
Configurez les chemins d'accès multiples iSCSI

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

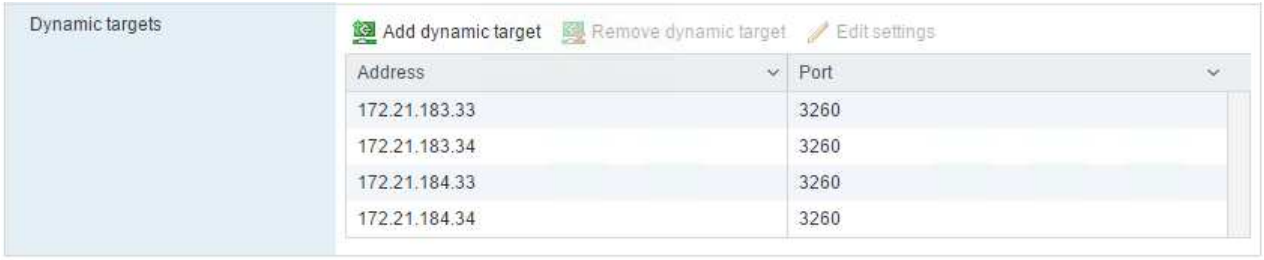
1. Sélectionnez stockage dans le volet de navigation de gauche. Cliquez sur adaptateurs.
2. Sélectionnez la carte logicielle iSCSI et cliquez sur configurer iSCSI.



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



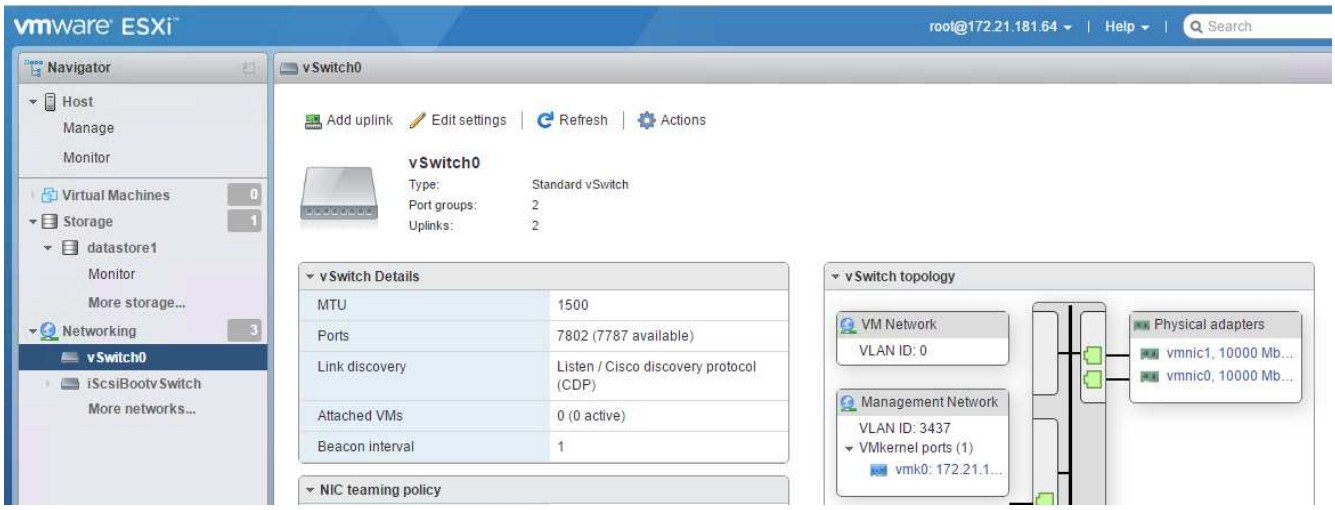
4. Saisissez l'adresse IP `iscsi_lif01a`.
   - Répétez l'opération avec les adresses IP `iscsi_lif01b`, `iscsi_lif02a`, et `iscsi_lif02b`.
   - Cliquez sur Enregistrer la configuration.



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

Configurer l'hôte ESXi

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



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

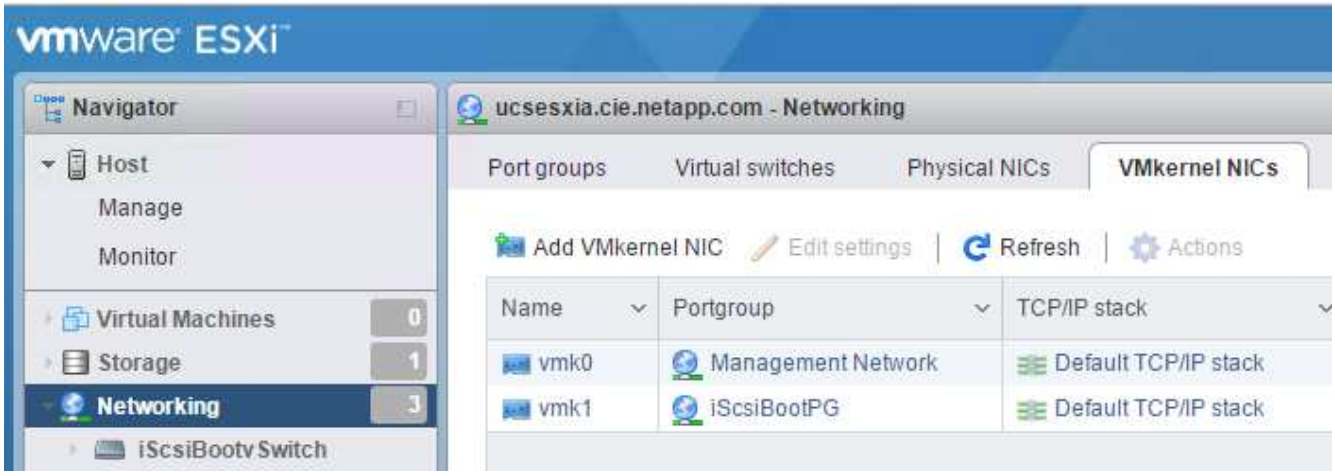
Configuration des groupes de ports et des NIC VMkernel

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

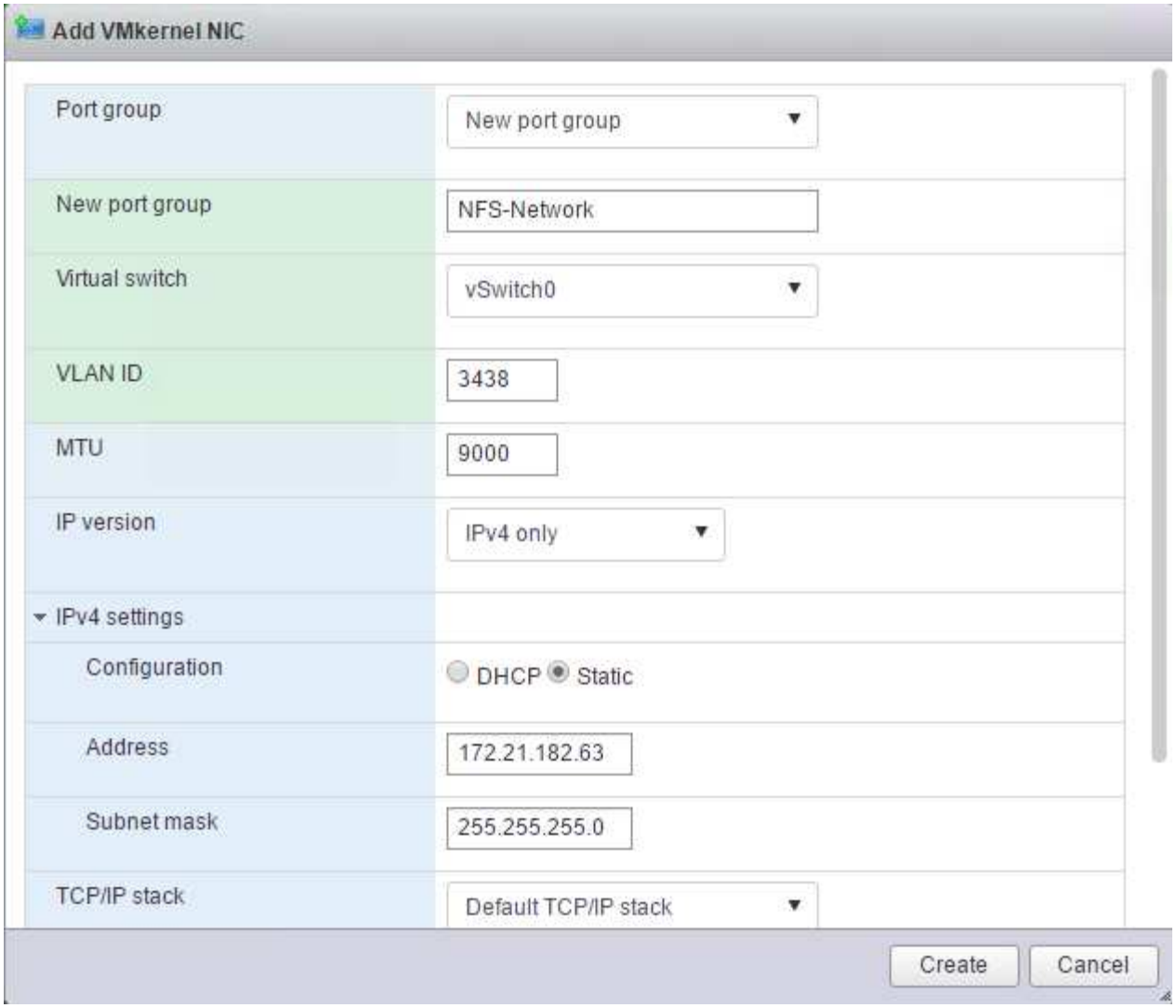
3. Cliquez avec le bouton droit de la souris sur réseau VM et sélectionnez Modifier. Définissez l'ID du VLAN sur `<<var_vm_traffic_vlan>>`.
4. Cliquez sur Ajouter un groupe de ports.
   - Nommer le groupe de ports `MGMT-Network`.
   - Entrez `<<mgmt_vlan>>` Pour l'ID VLAN.
   - Vérifiez que vSwitch0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

- Cliquez sur Ajouter.

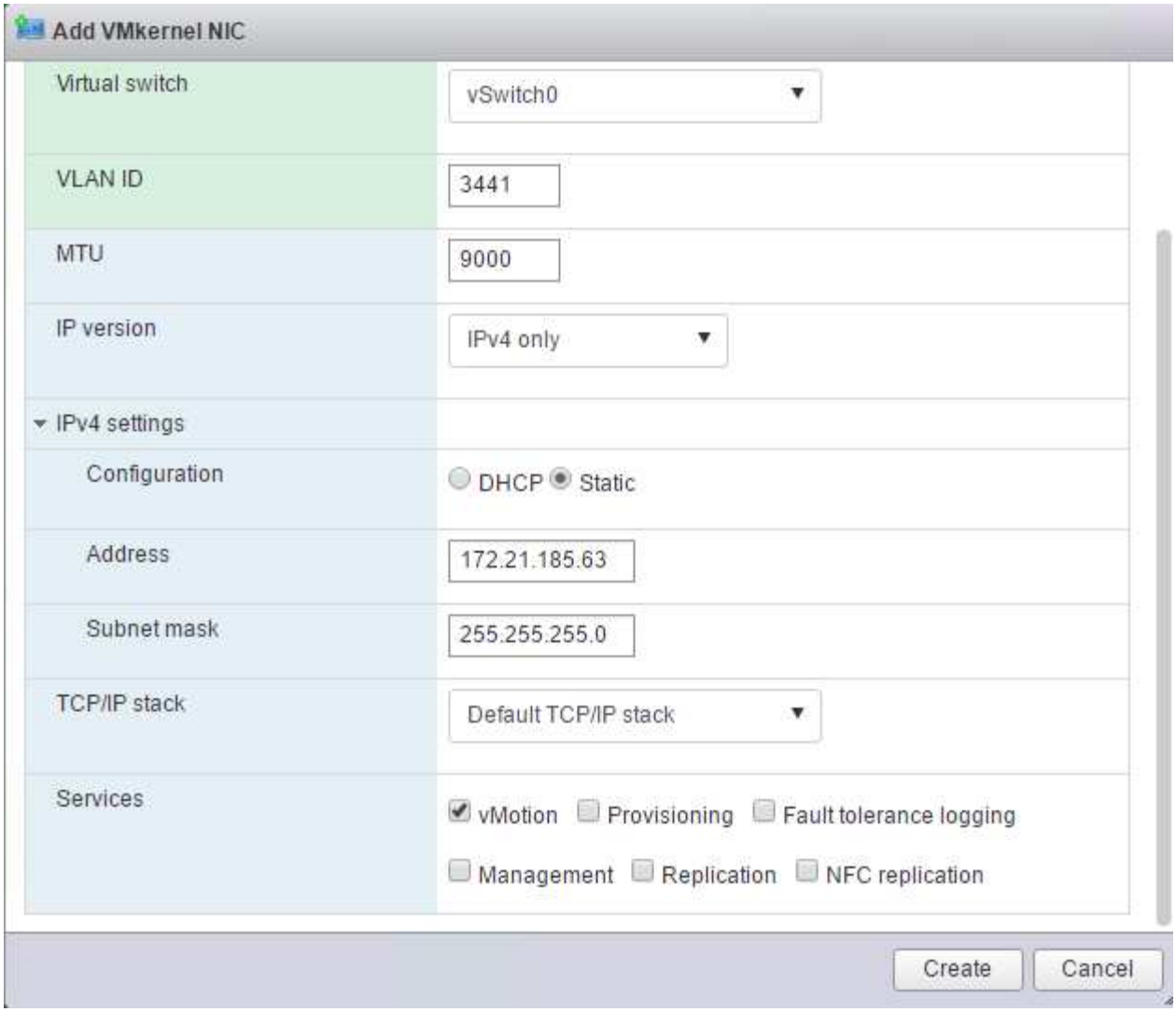
5. Cliquez sur l'onglet VMkernel NIC.



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



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

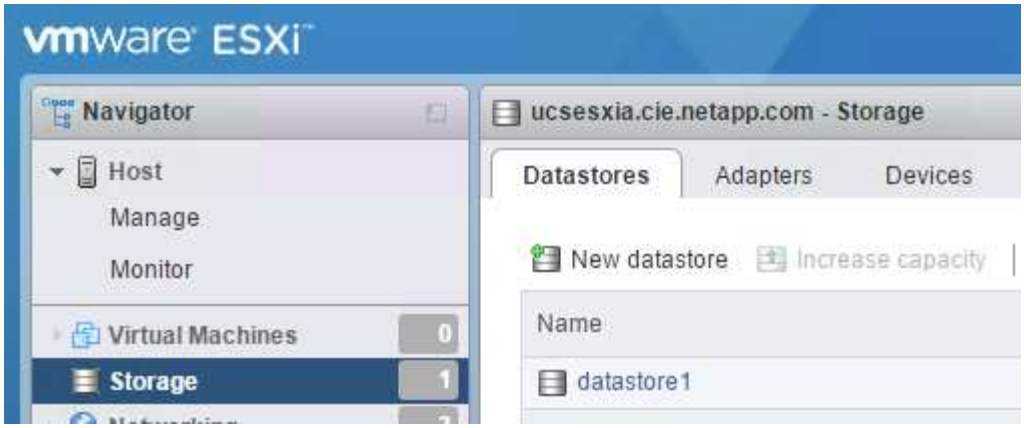


Il existe de nombreuses façons de configurer la mise en réseau VMware ESXi, y compris en utilisant le commutateur distribué VMware vSphere si votre licence le permet. Les autres configurations réseau sont prises en charge par FlexPod Express si elles sont requises pour répondre aux exigences de l'entreprise.

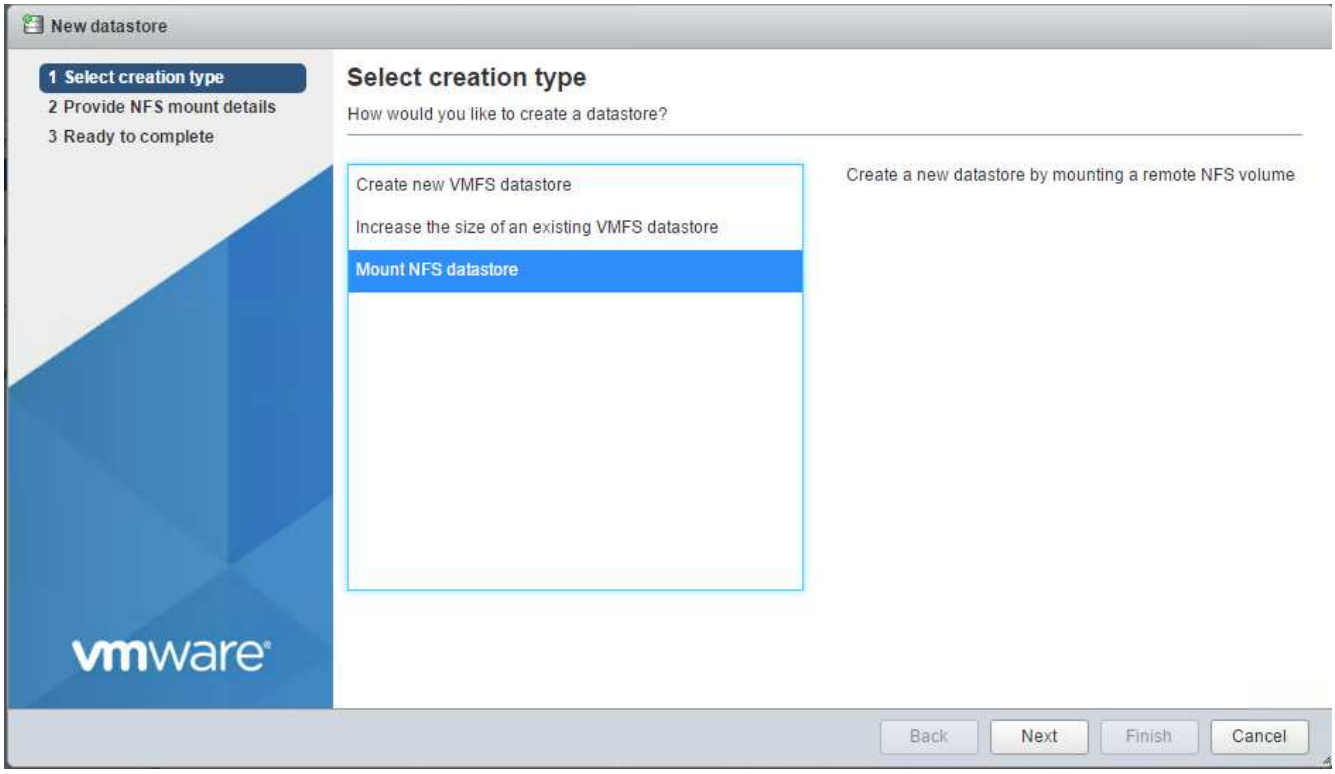
Montez les premiers datastores

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

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



2. Sélectionnez Mount NFS datastore.



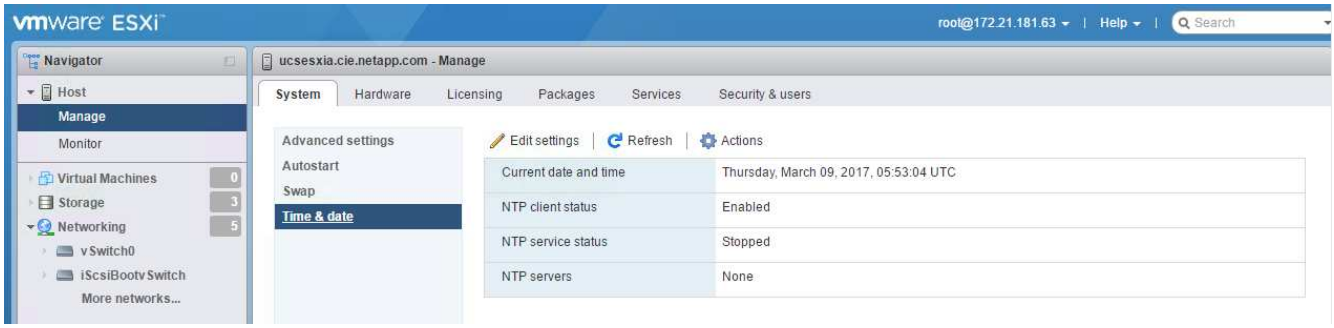
3. Entrez ensuite les informations suivantes dans la page Détails du montage NFS :
   - Nom : `infra_datastore_1`
   - Serveur NFS : `<<var_nodea_nfs_lif>>`
   - Partager : /infra_datastore_1
   - Assurez-vous que NFS 3 est sélectionné.
4. Cliquez sur Terminer. La tâche terminée s'affiche dans le volet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

◦ Assurez-vous que NFS 3 est sélectionné.

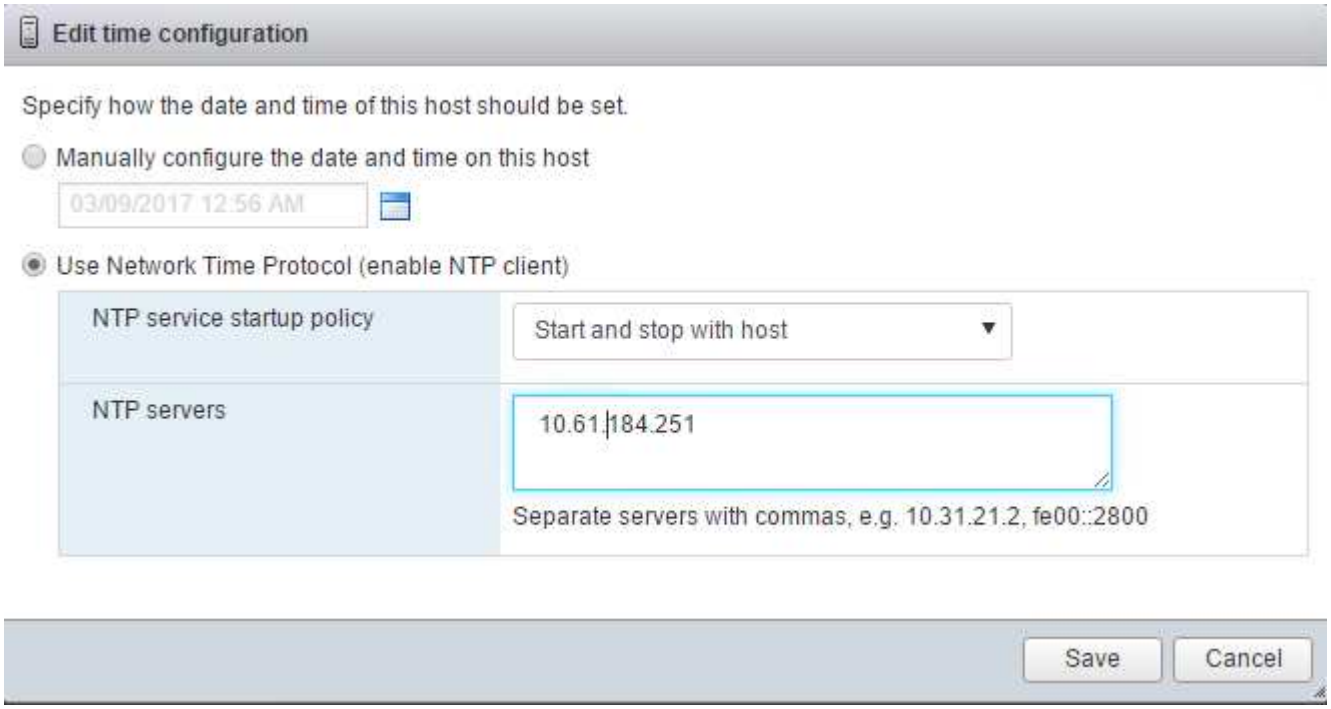
Configurez NTP

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

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



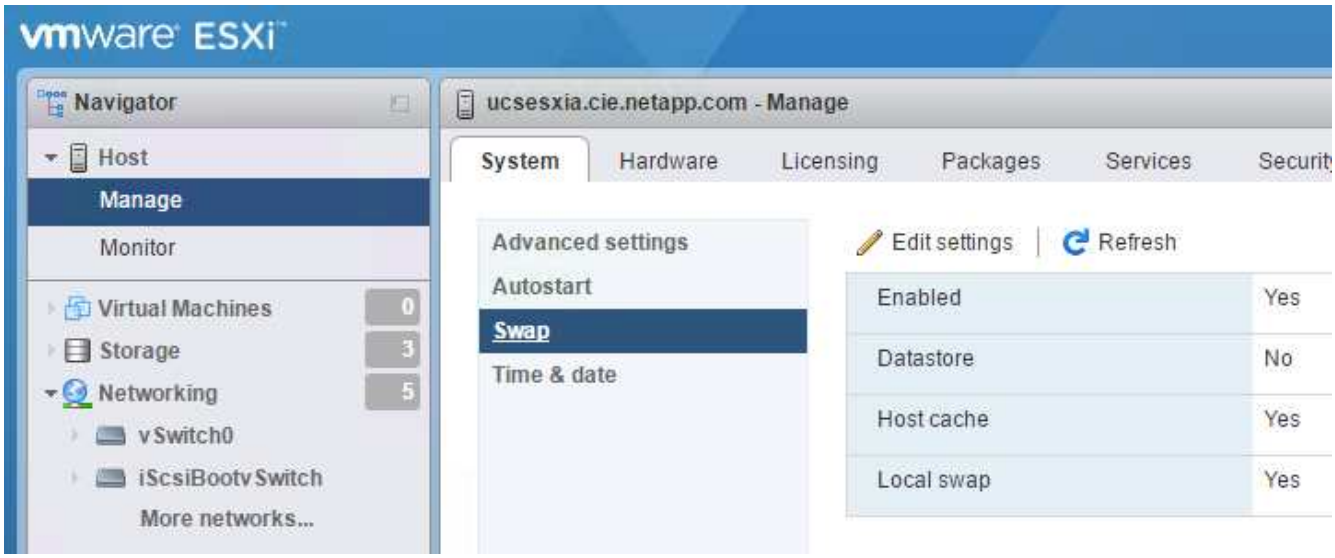
2. Sélectionnez utiliser le protocole d'heure du réseau (Activer le client NTP).
3. Sélectionnez Démarrer et Arrêter avec l'hôte comme stratégie de démarrage du service NTP.
4. Entrez `<<var_ntp>>` En tant que serveur NTP. Vous pouvez définir plusieurs serveurs NTP.
5. Cliquez sur Enregistrer.



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

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

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



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

3. Cliquez sur Enregistrer.

Installer le plug-in NetApp NFS 1.0.20 pour VMware VAAI

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

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

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

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

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

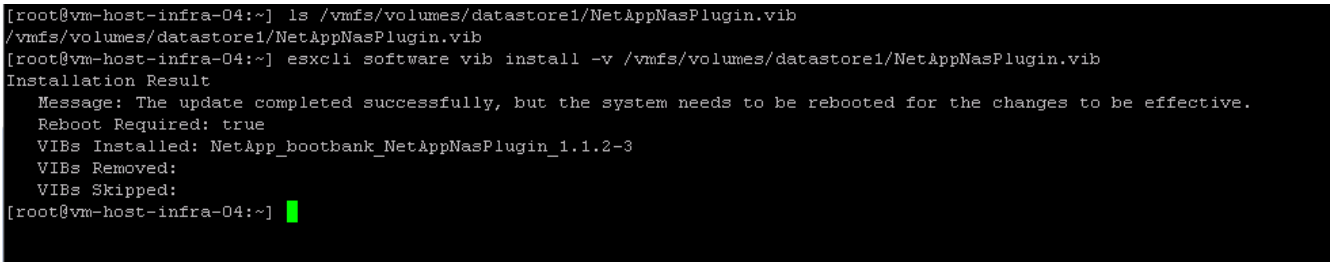
2. Si VAAI n'est pas activé, entrez les commandes suivantes pour activer VAAI :

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

Ces commandes produisent les valeurs de sortie suivantes :

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

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



"Installez VMware vCenter Server 6.7"

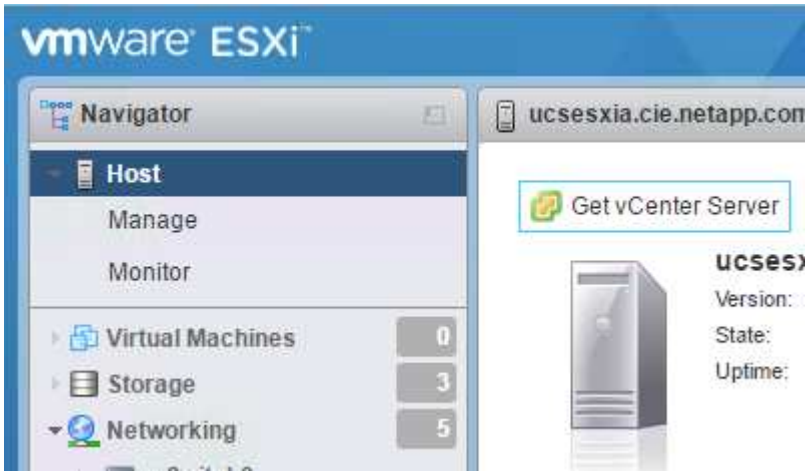
Installez VMware vCenter Server 6.7

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

FlexPod Express utilise VMware vCenter Server Appliance (VCSA).

Téléchargez l'appliance du serveur VMware vCenter

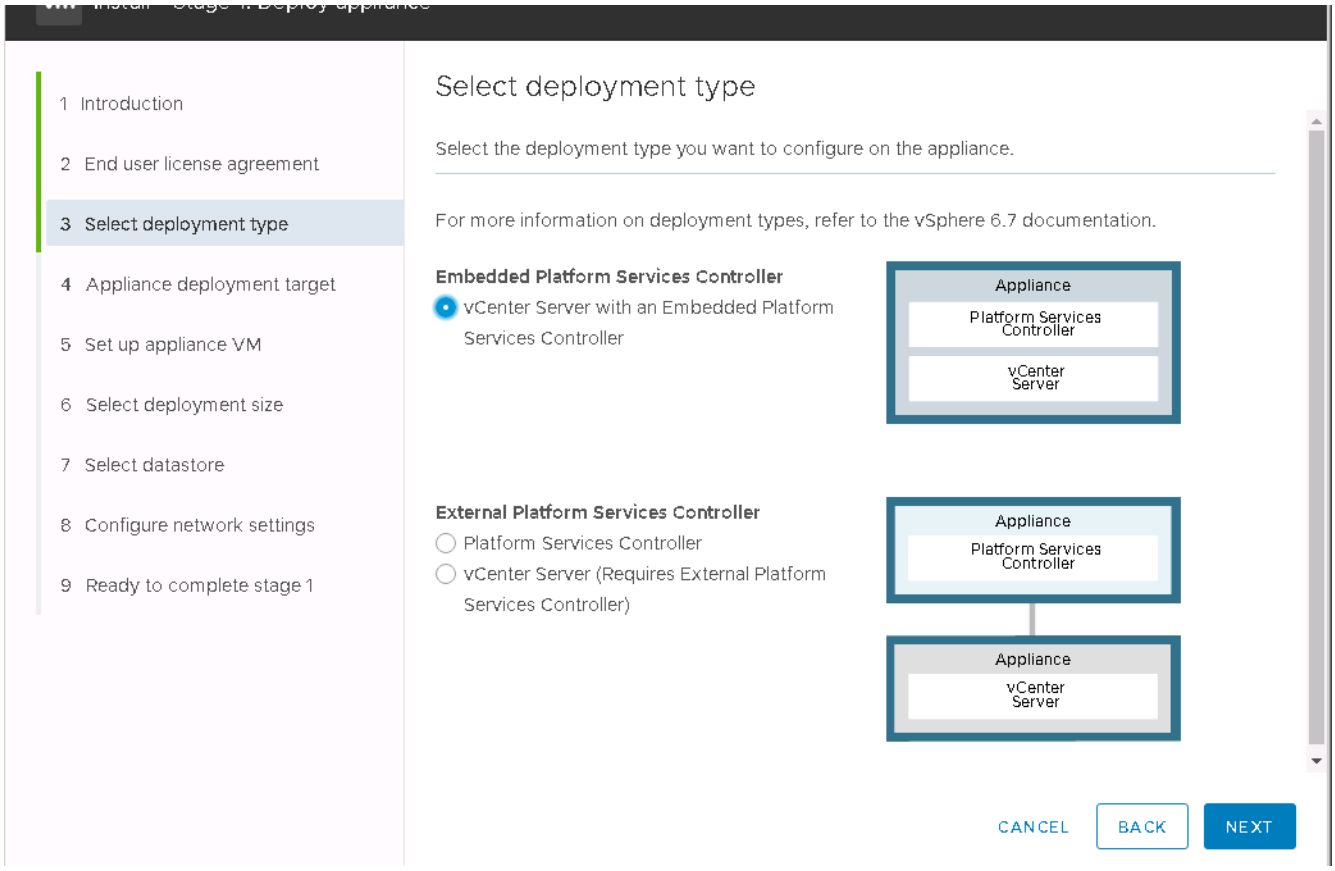
1. Téléchargez le VCSA. Accédez au lien de téléchargement en cliquant sur l'icône obtenir vCenter Server lors de la gestion de l'hôte ESXi.



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

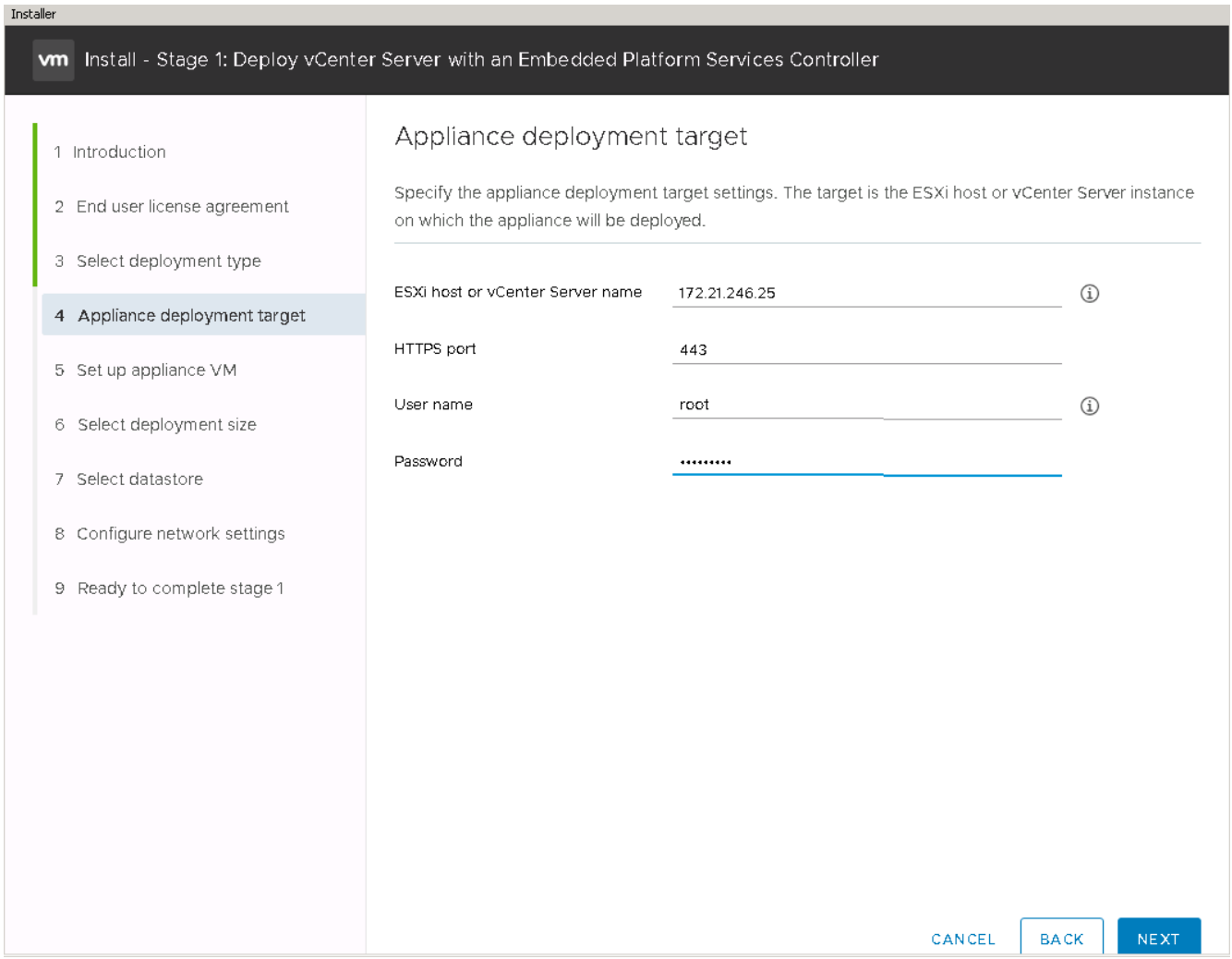
> Bien que l'installation de Microsoft Windows vCenter Server soit prise en charge, VMware recommande le VCSA pour les nouveaux déploiements.

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

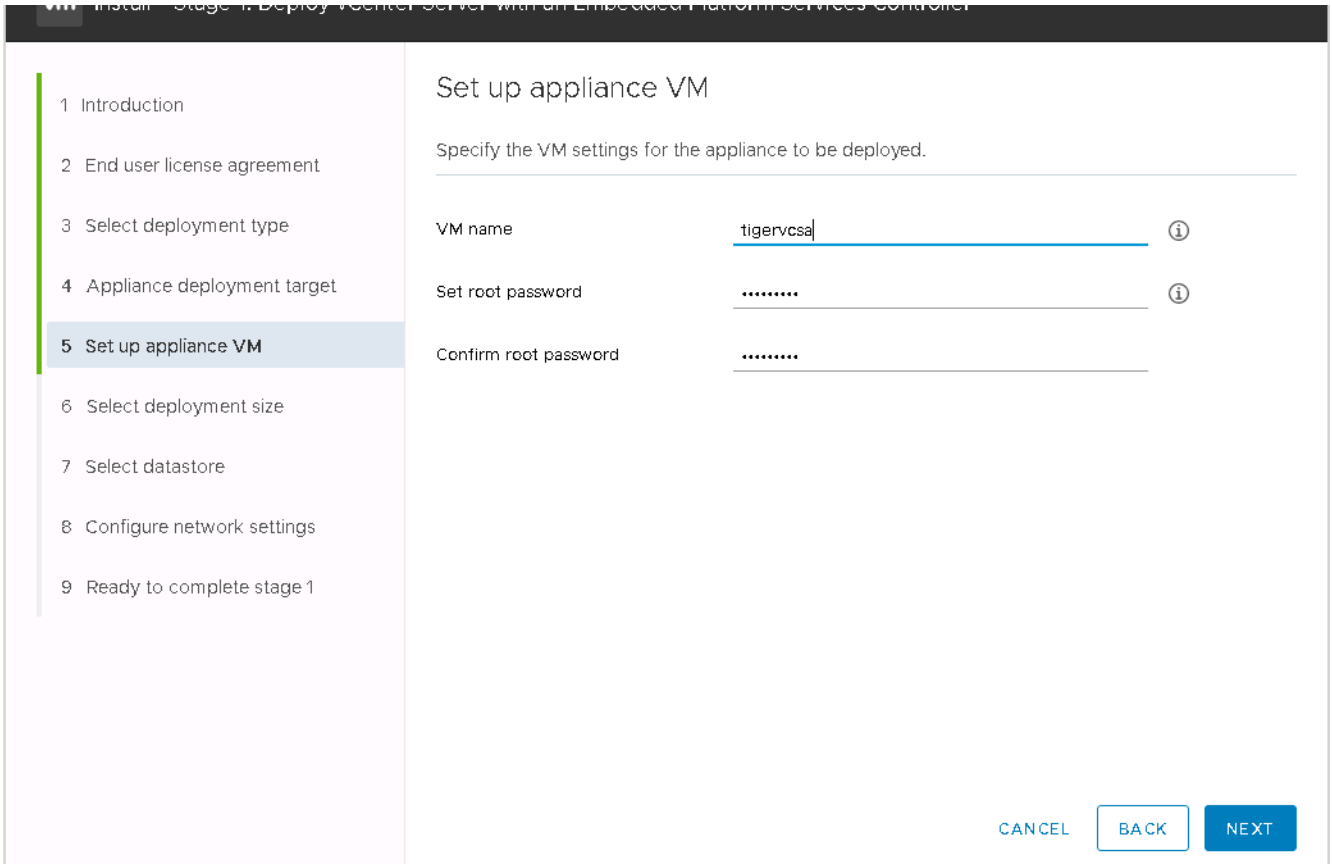


Si nécessaire, le déploiement de contrôleur de services de plateforme externe est également pris en charge dans le cadre de la solution FlexPod Express.

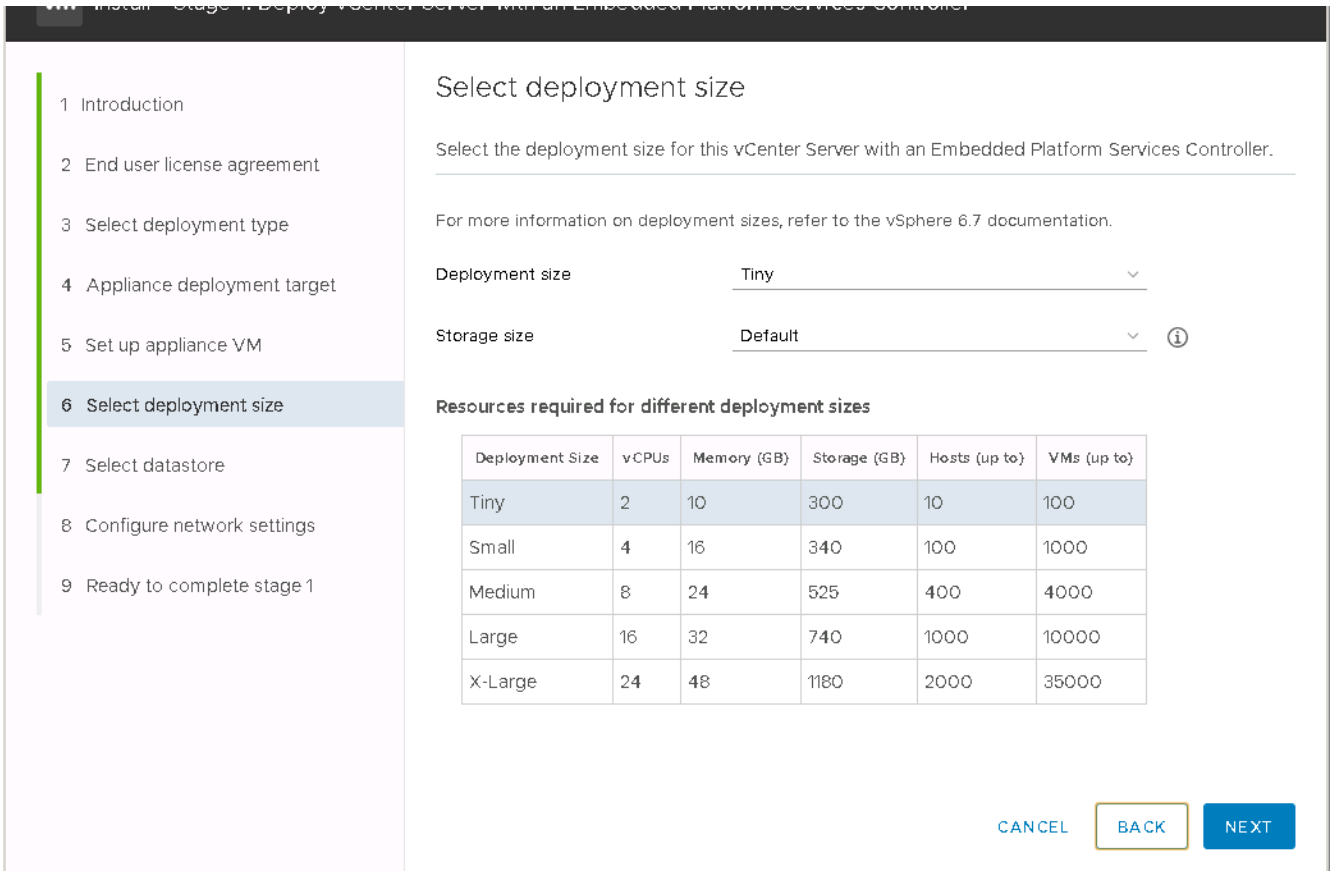
9. Dans la cible de déploiement de l'appliance, entrez l'adresse IP d'un hôte ESXi déployé, ainsi que le nom d'utilisateur root et le mot de passe root.



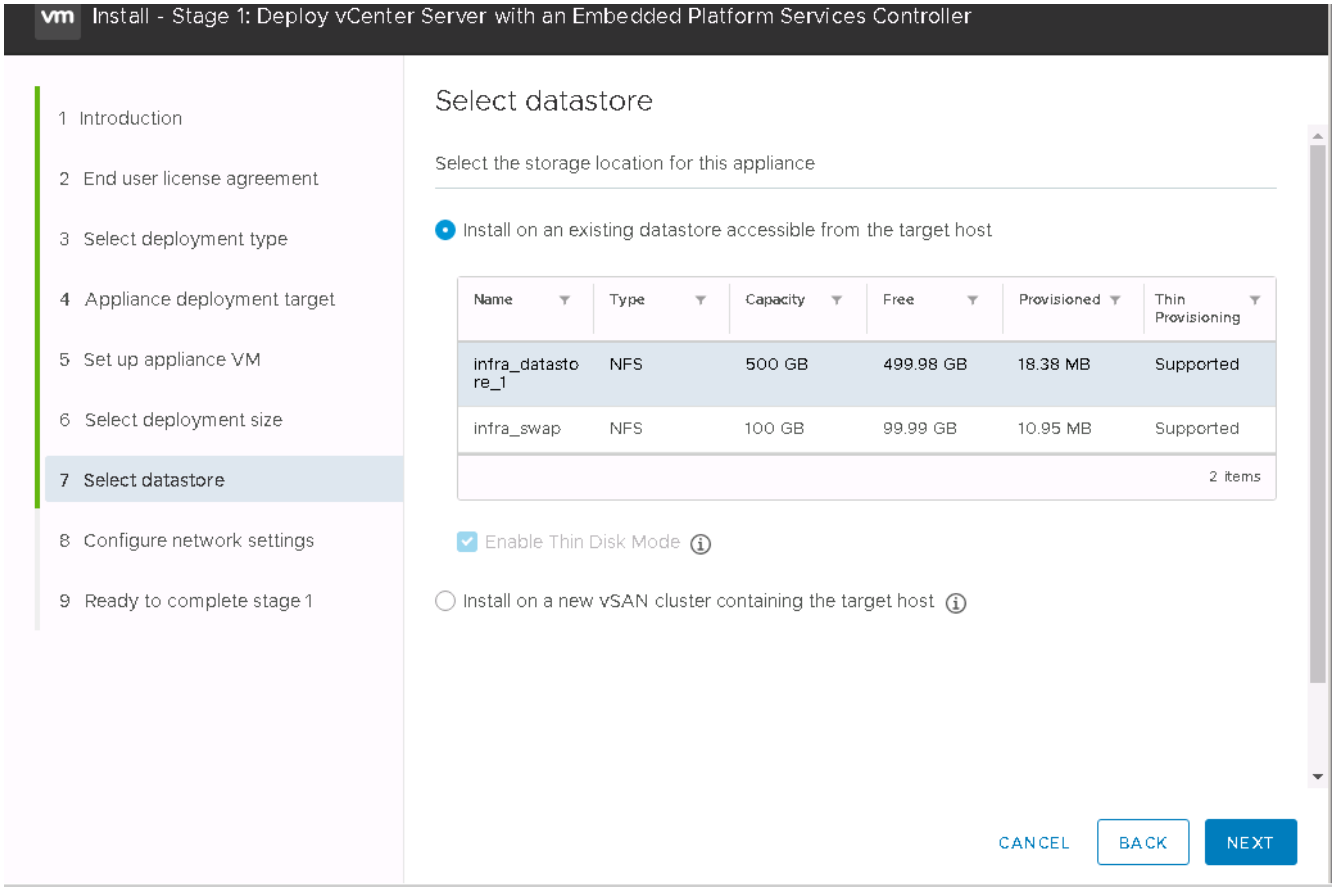
10. Configurez la machine virtuelle de l'appliance en saisissant `VCSA` Comme nom de la VM et mot de passe root, vous souhaitez utiliser pour le VCSA.



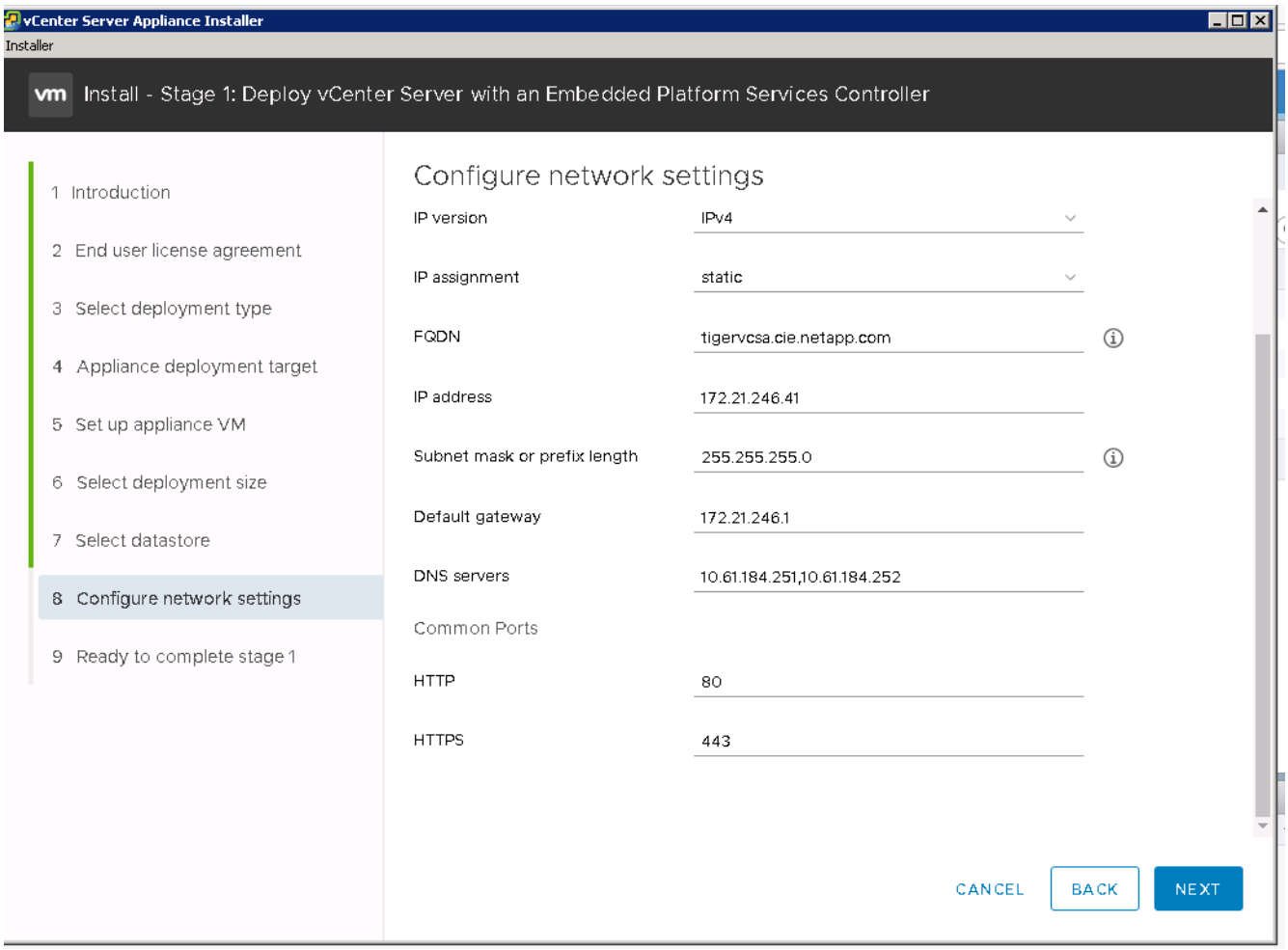
11. Choisissez la taille de déploiement qui correspond le mieux à votre environnement. Cliquez sur Suivant.



12. Sélectionnez le datastore infra_datastore_1. Cliquez sur Suivant.

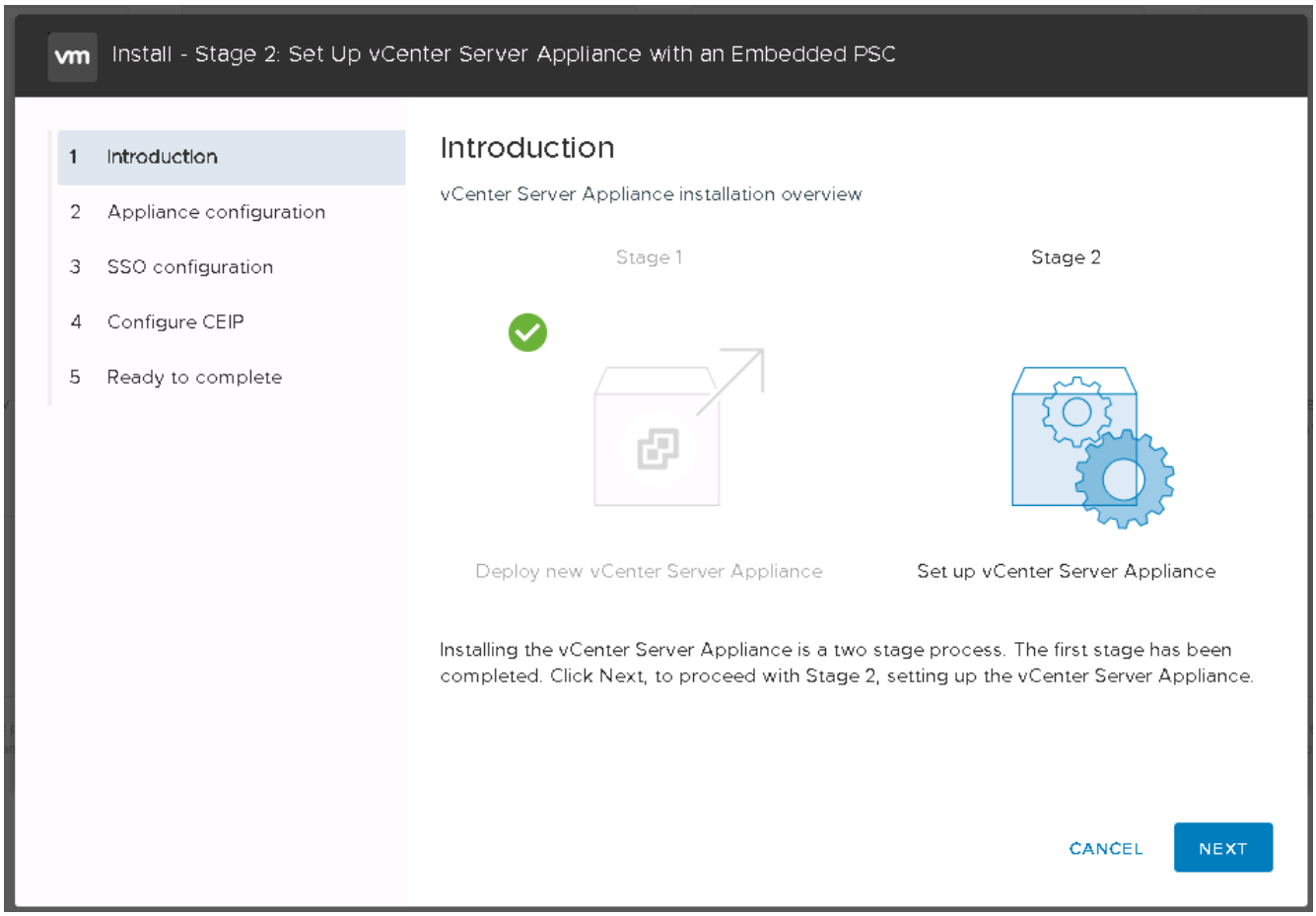


13. Entrez les informations suivantes sur la page configurer les paramètres réseau et cliquez sur Suivant.
    a. Sélectionnez MGMT-réseau pour le réseau.
    b. Saisissez le nom de domaine complet ou l'adresse IP à utiliser pour le VCSA.
    c. Entrez l'adresse IP à utiliser.
    d. Entrez le masque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



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

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



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

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

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

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

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

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

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

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

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

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

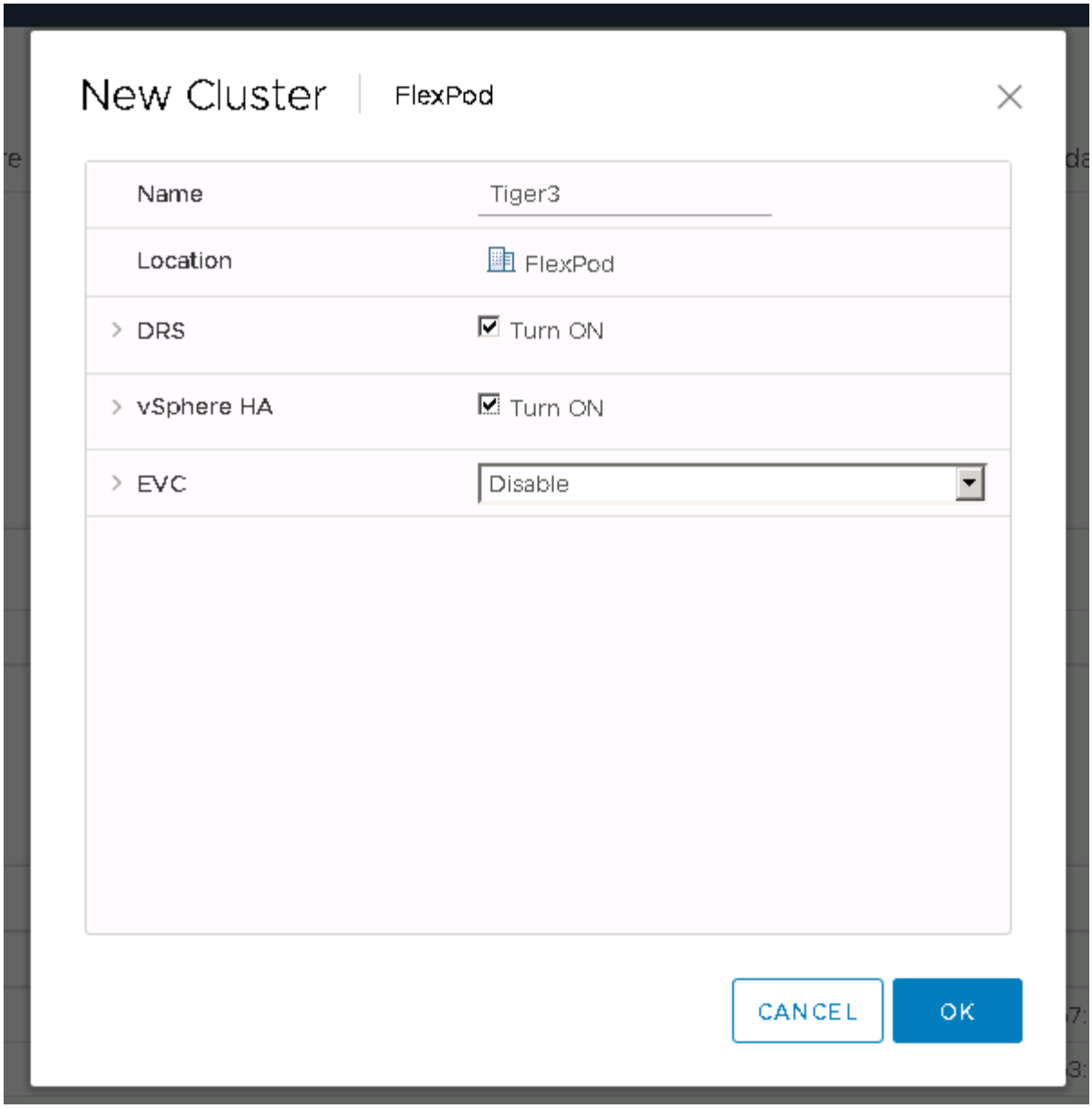
Pour configurer VMware vCenter Server 6.7 et la mise en cluster vSphere, procédez comme suit :

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

Créez le cluster vSphere

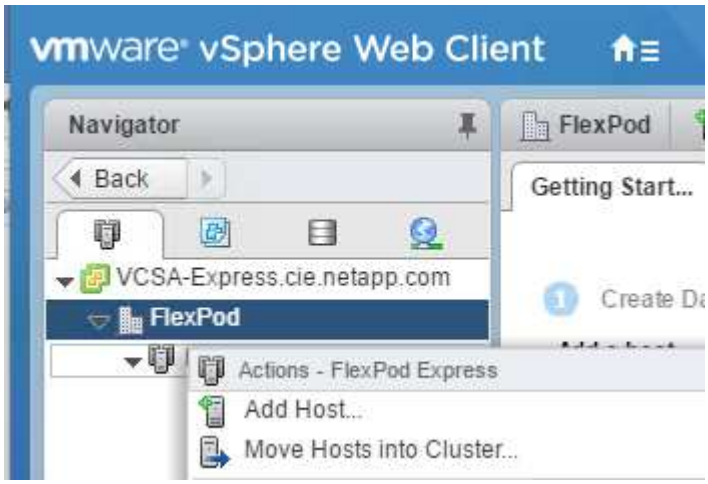
Pour créer un cluster vSphere, procédez comme suit :

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



Ajoutez des hôtes ESXi au cluster

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



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

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

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

Configurer coredump sur les hôtes ESXi

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

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

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

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

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.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations fournies dans ce document, consultez ces documents et/ou sites web :

- Documentation des produits NetApp

  "http://docs.netapp.com"

- Guide de design de FlexPod Express avec VMware vSphere 6.7 et NetApp AFF A220

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

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.

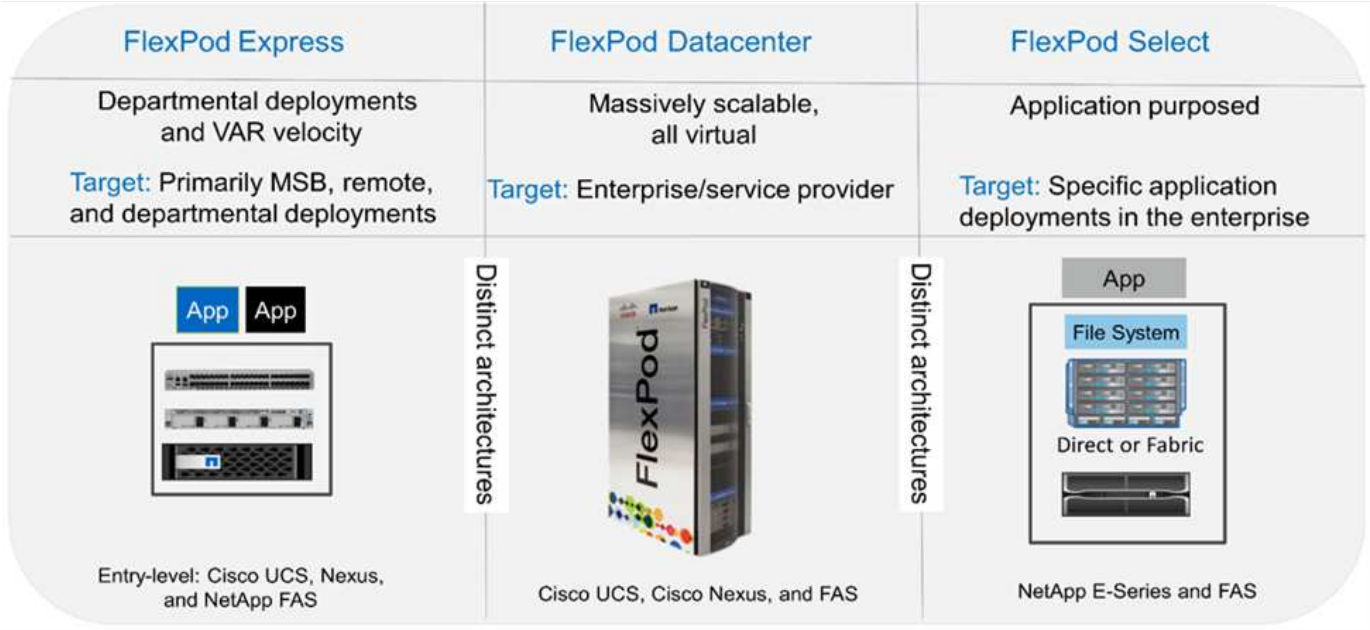
Programme FlexPod d'infrastructure convergée

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

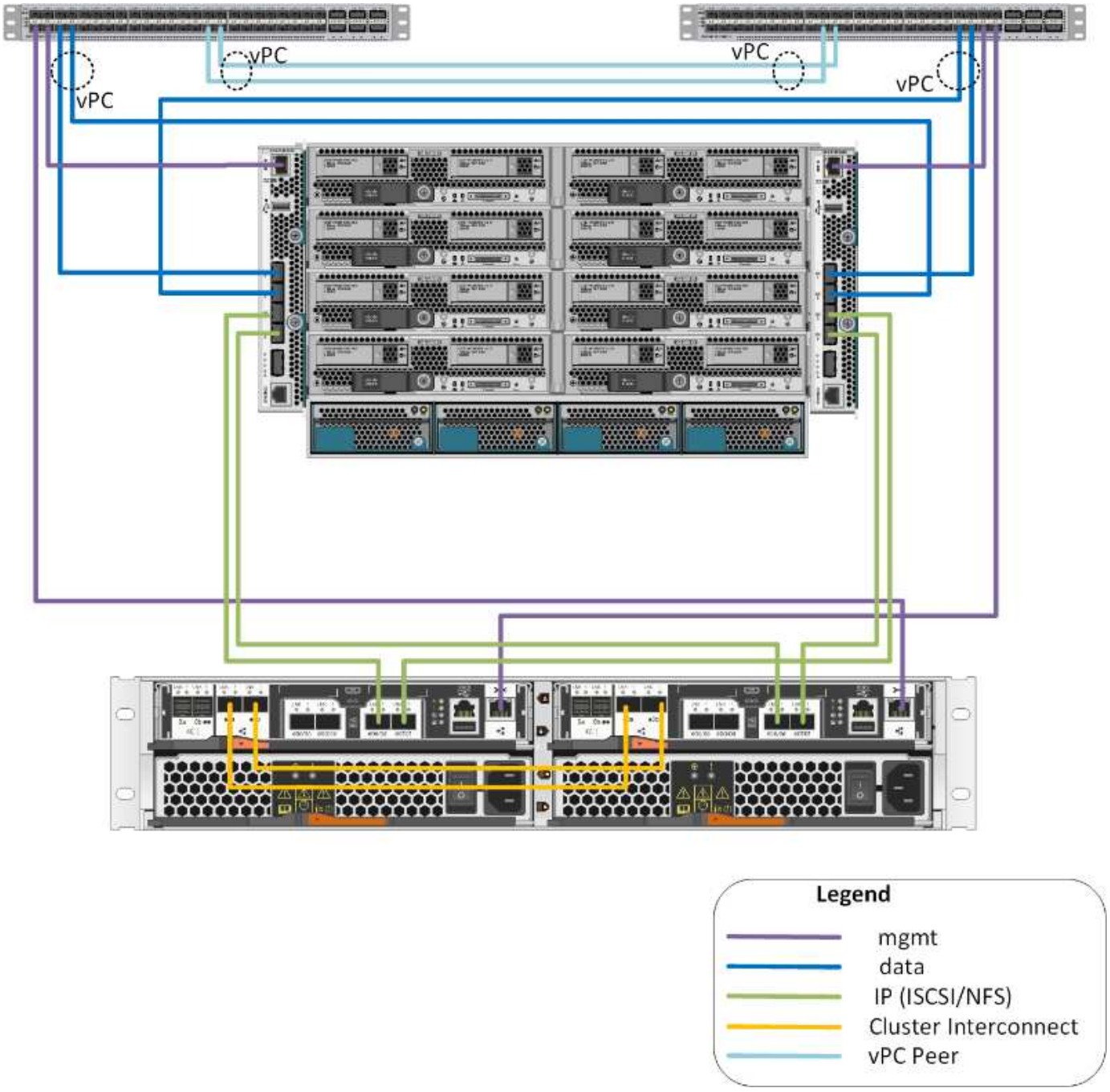
Composants logiciels

- 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
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".

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

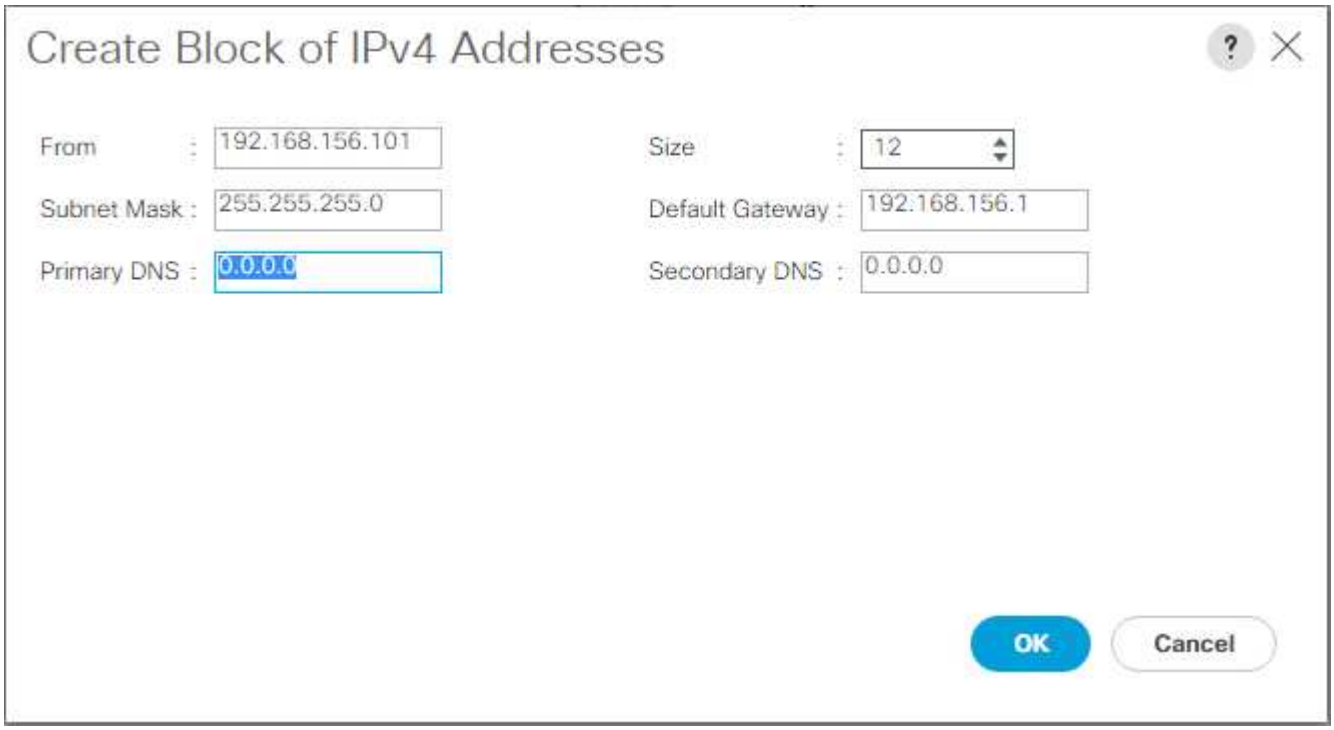
Cisco vous recommande fortement de configurer Call Home dans Cisco UCS Manager. La configuration du service d'appel en cas d'incident accélère la résolution des problèmes. Pour configurer Call Home, procédez comme suit :

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.



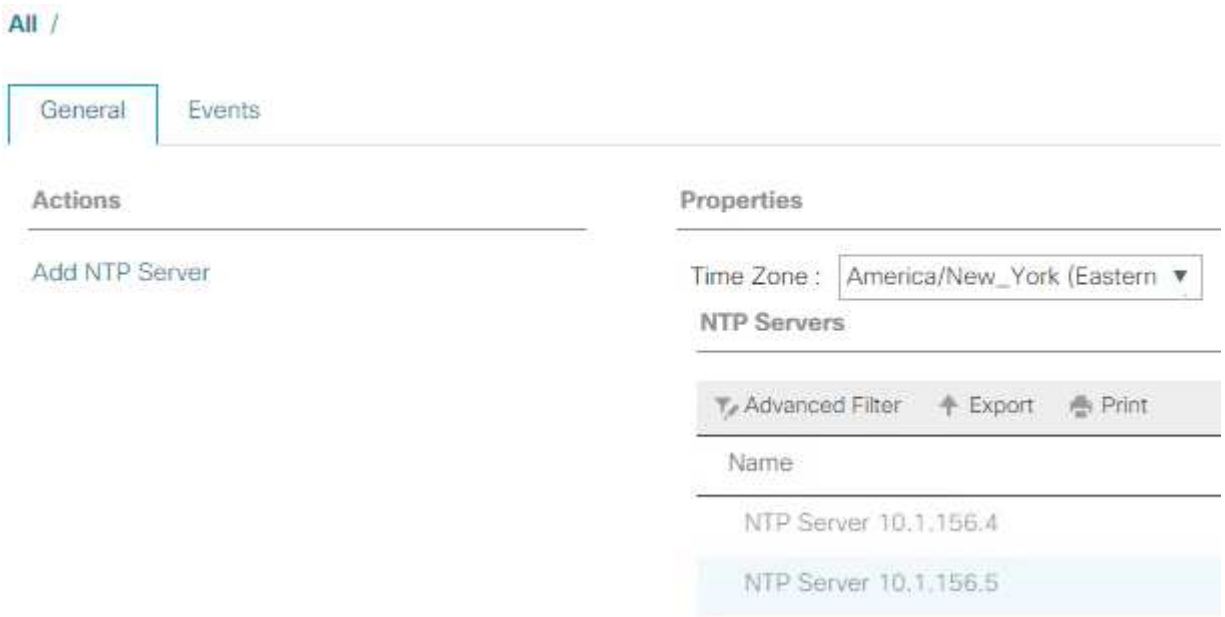
5. Cliquez sur OK pour créer le bloc.
6. Cliquez sur OK dans le message de confirmation.

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

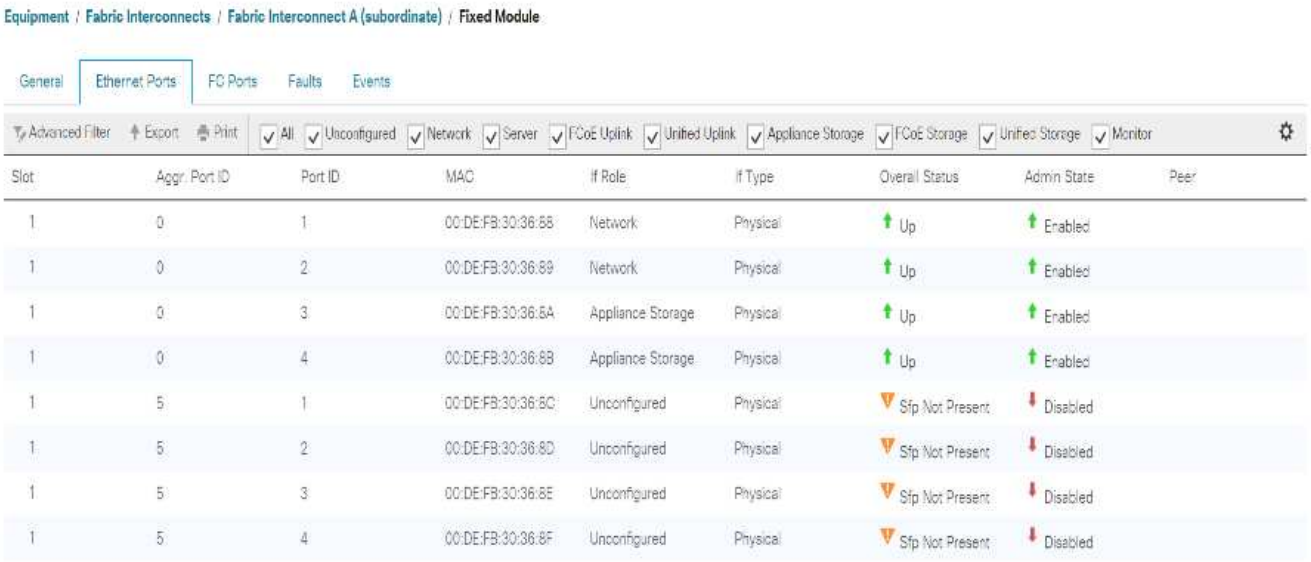
La définition de la politique de découverte facilite l'ajout du châssis Cisco UCS B-Series et d'autres éléments Fabric Extender pour la connectivité Cisco UCS C-Series. Pour modifier la politique de détection du châssis, procédez comme suit :

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.

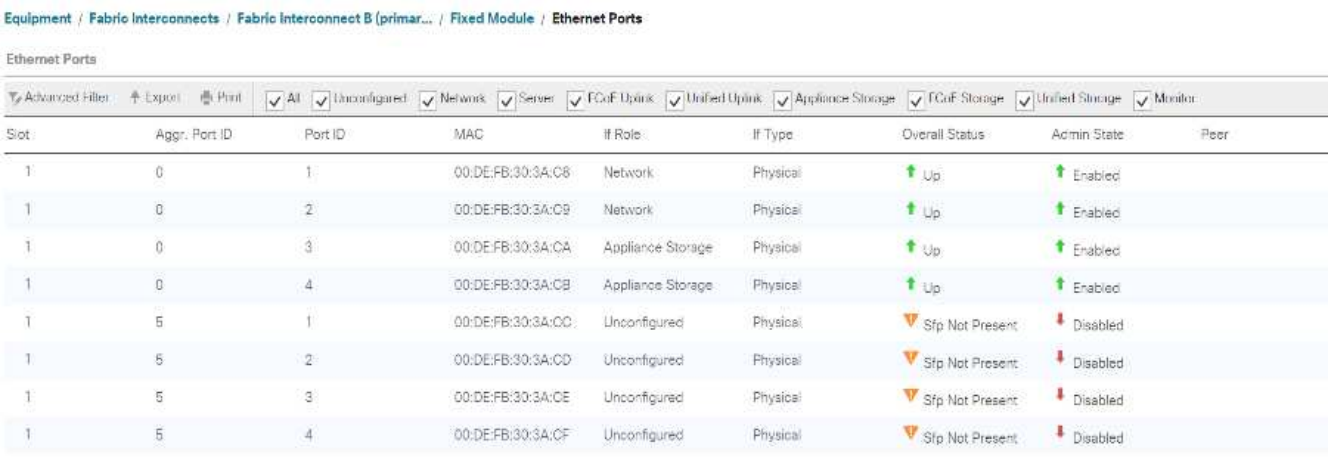
Activez les ports de serveur, de liaison montante et de stockage

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.



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.



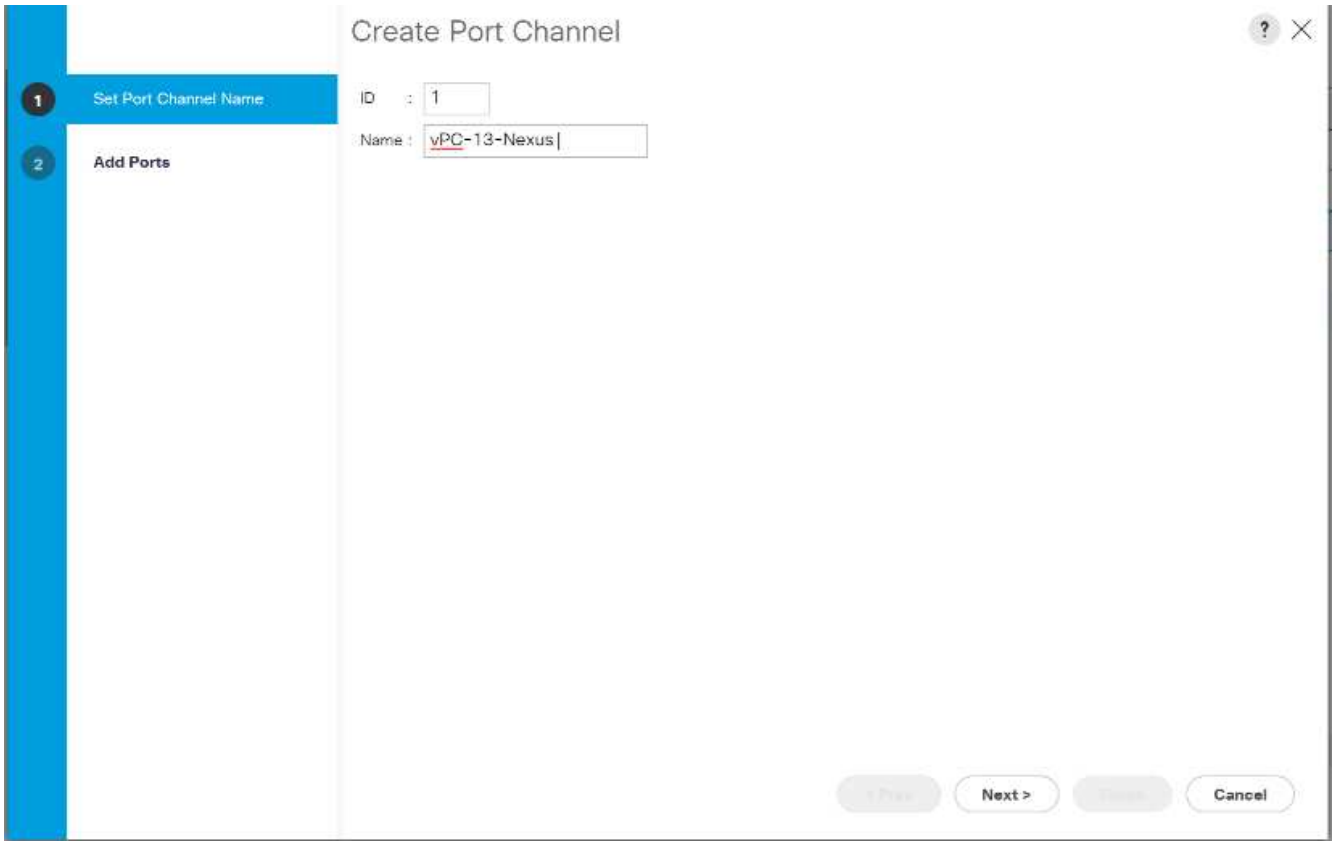
Créez des canaux de port uplink avec les commutateurs Cisco Nexus 31108

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 :

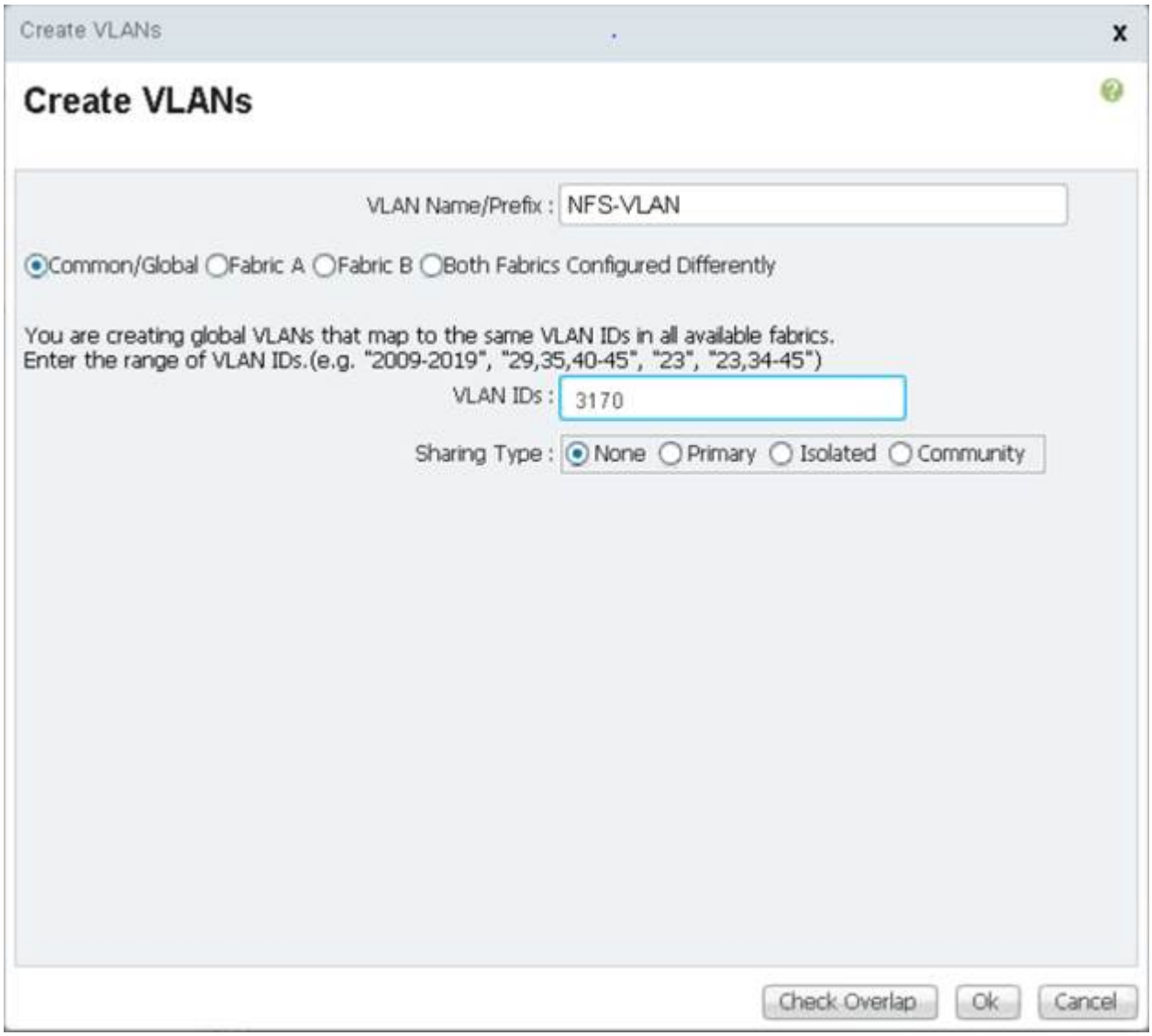
1. Dans Cisco UCS Manager, dans le menu Nouveau de la barre d'outils en haut de la fenêtre, sélectionnez Créer une organisation.
2. Saisissez un nom pour l'organisation.
3. Facultatif : saisissez une description pour l'organisation. Cliquez sur OK.
4. Cliquez sur OK dans le message de confirmation.

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 :

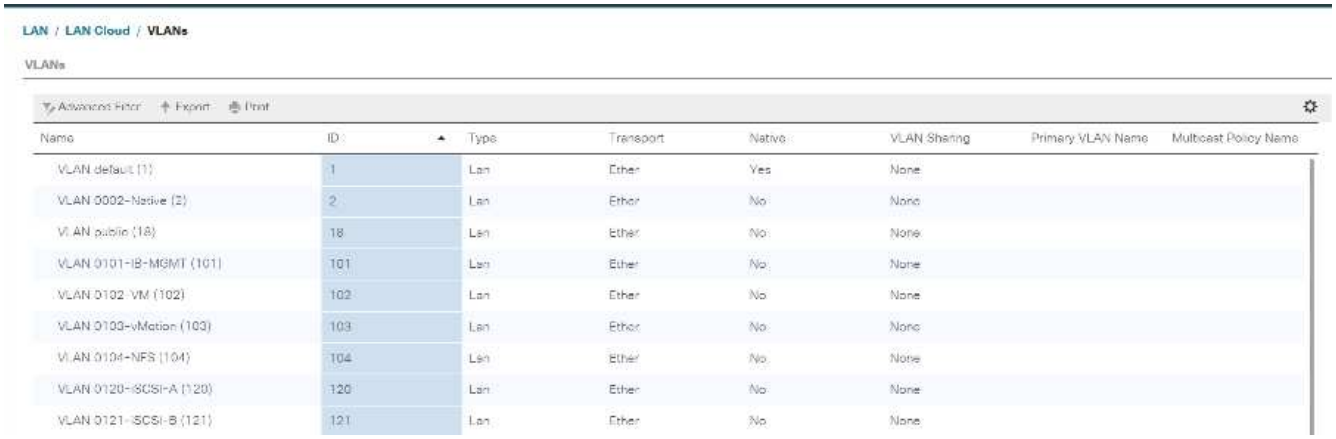
1. Dans Cisco UCS Manager, sélectionnez l'onglet LAN.
2. Étendez le cloud Appliances.
3. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
4. Sélectionnez Créer des VLAN.
5. Indiquez NFS-VLAN comme nom du VLAN NFS de l'infrastructure.
6. Laisser commun/Global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

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

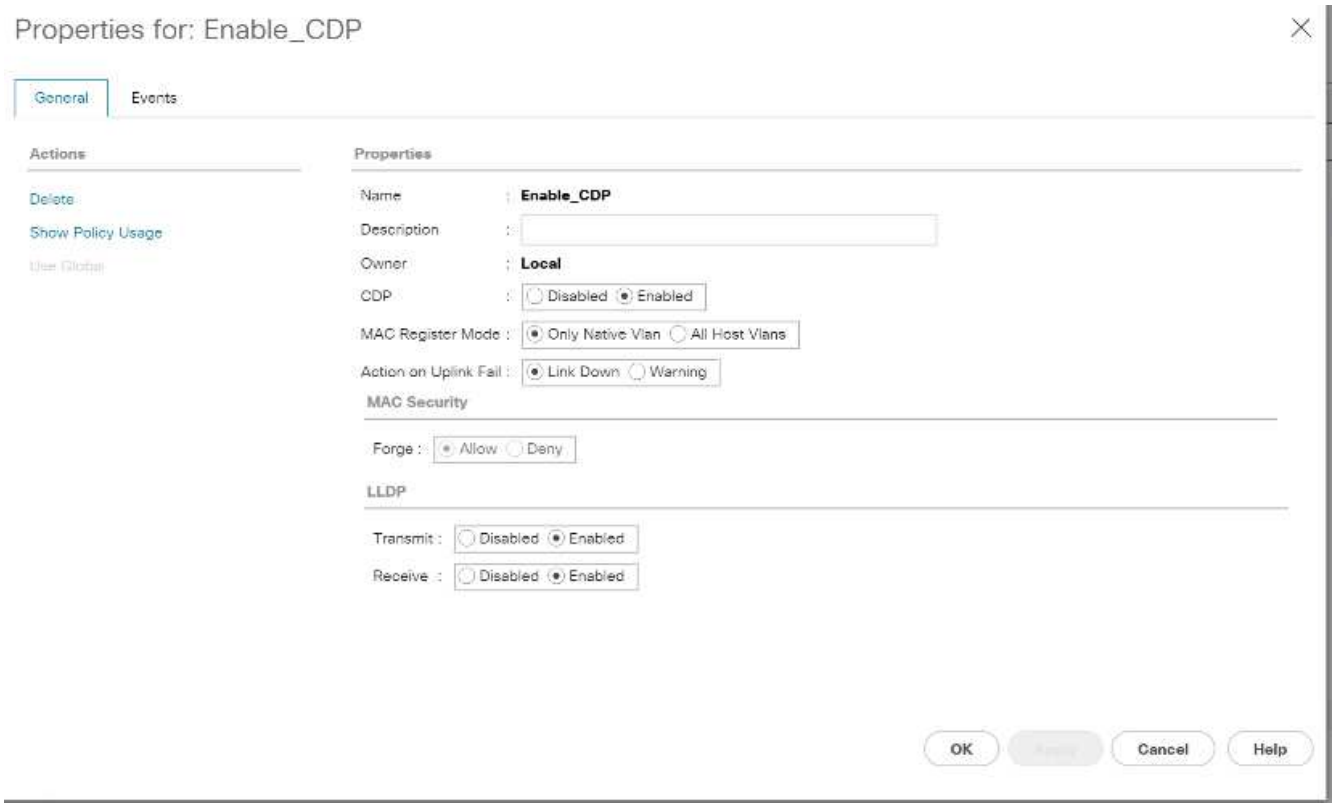


9. Cliquez sur OK, puis à nouveau sur OK pour créer le VLAN.
10. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
11. Sélectionnez Créer des VLAN.
12. Saisissez iSCSI-A-VLAN comme nom pour le VLAN Infrastructure iSCSI Fabric A.
13. Laisser commun/Global sélectionné.
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.

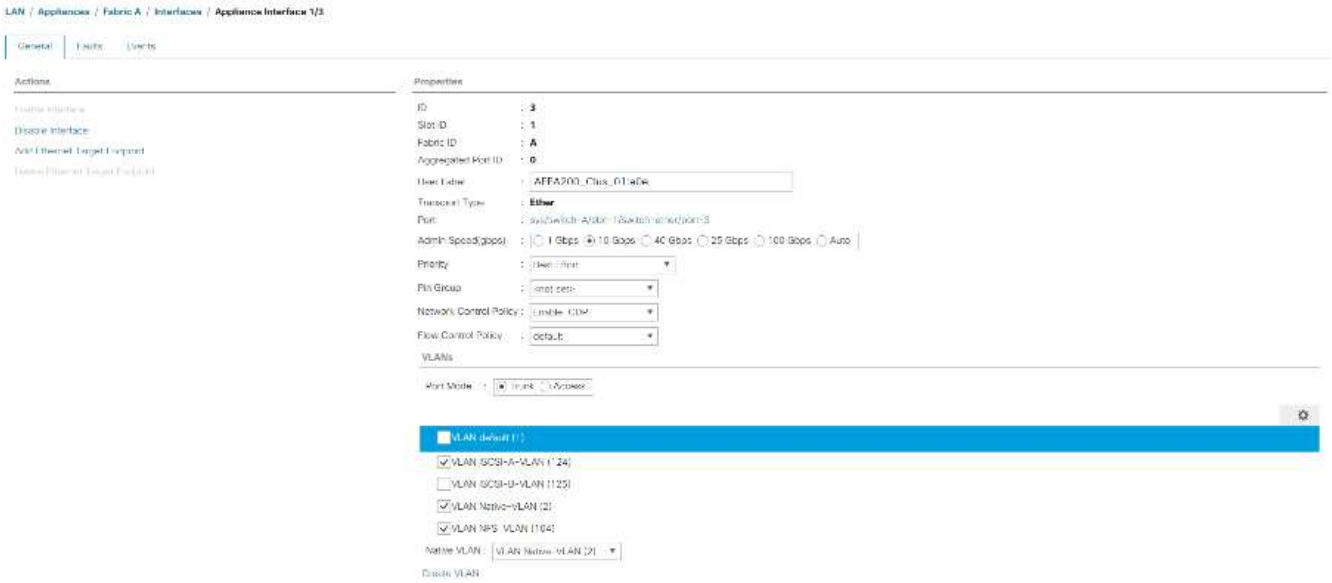
21. Cliquez sur OK, puis à nouveau sur OK pour créer le VLAN.
22. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
23. Sélectionnez Créer des VLAN.
24. Saisissez Native-VLAN comme nom pour le VLAN natif.
25. Laisser commun/Global sélectionné.
26. Entrez `<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



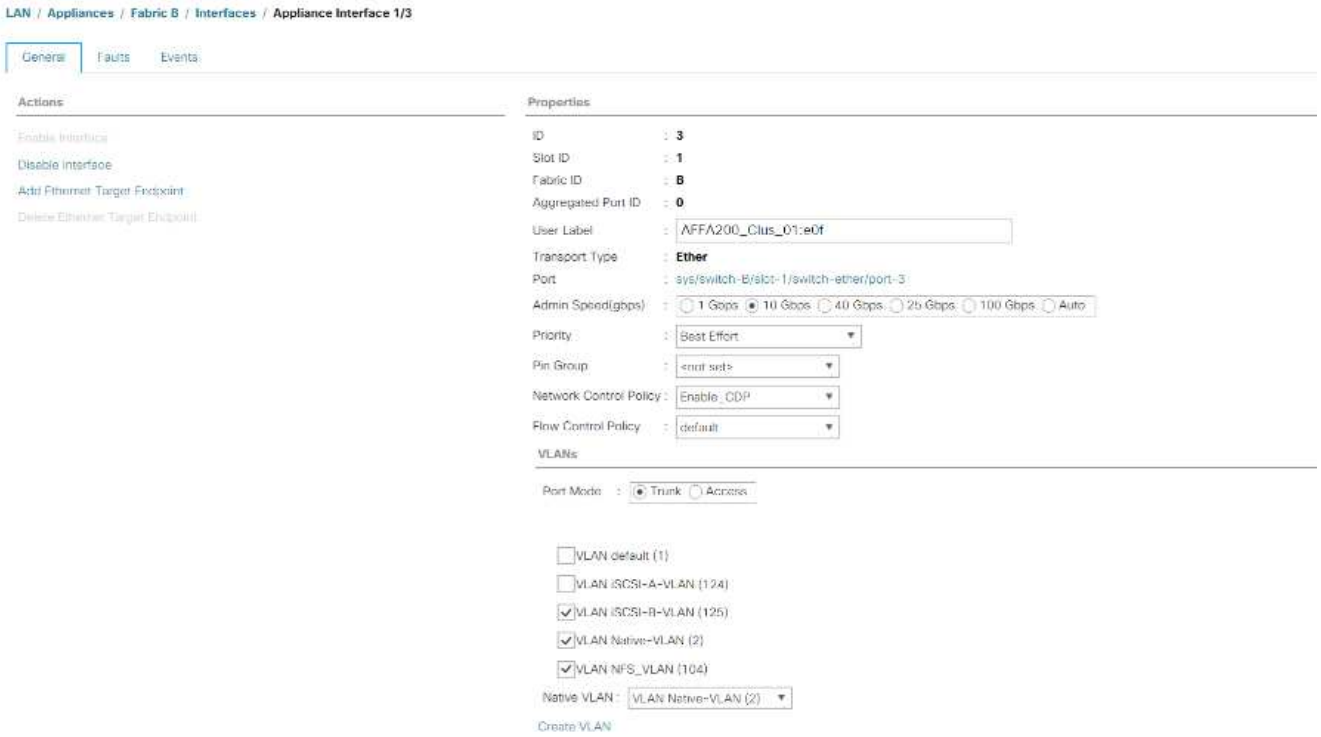
28. Dans le volet de navigation, sous LAN > stratégies, développez appareils et cliquez avec le bouton droit de la souris sur stratégies de contrôle du réseau.
29. Sélectionnez Créer une stratégie de contrôle réseau.
30. Nommez la règle `Enable_CDP_LLPD` Et sélectionnez activé en regard de CDP.
31. Activez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

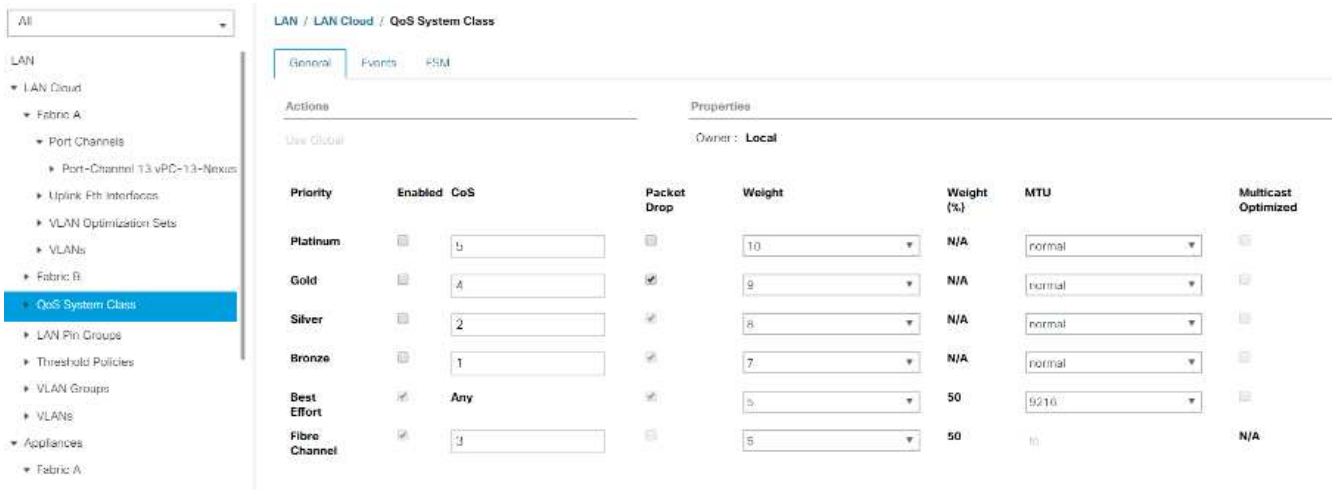


53. Cliquez sur Enregistrer les modifications et sur OK.
54. Sélectionnez Appliance interface 1/4 sous Fabric B.
55. Dans le champ libellé utilisateur, indiquez les informations indiquant le port du contrôleur de stockage, par exemple `<storage_controller_02_name>:e0f`. Cliquez sur Enregistrer les modifications 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)

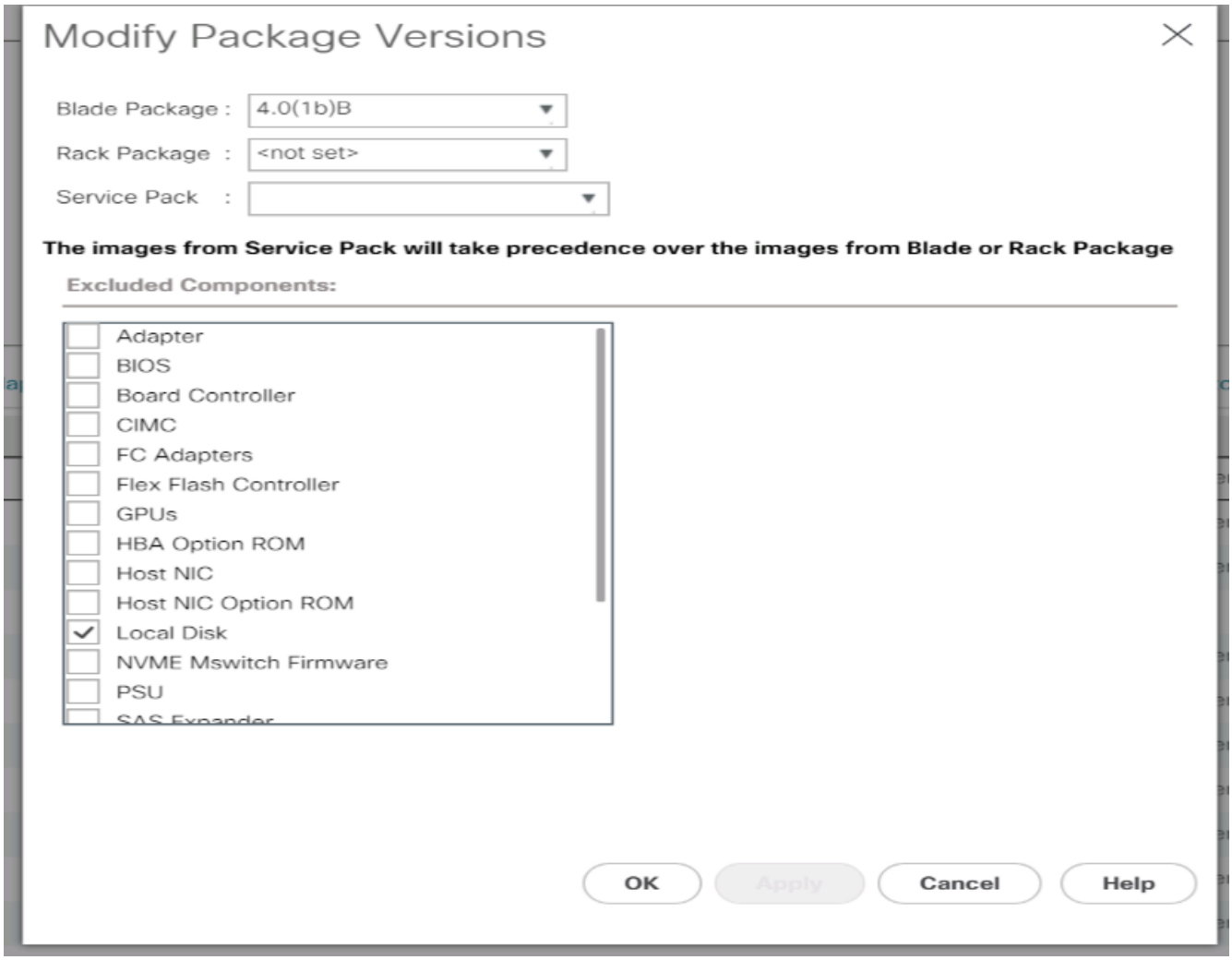
Pour mettre à niveau le logiciel Cisco UCS Manager et le logiciel Cisco UCS Fabric Interconnect vers la version 4.0(1b), reportez-vous à "Guides d'installation et de mise à niveau de Cisco UCS Manager".

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 :

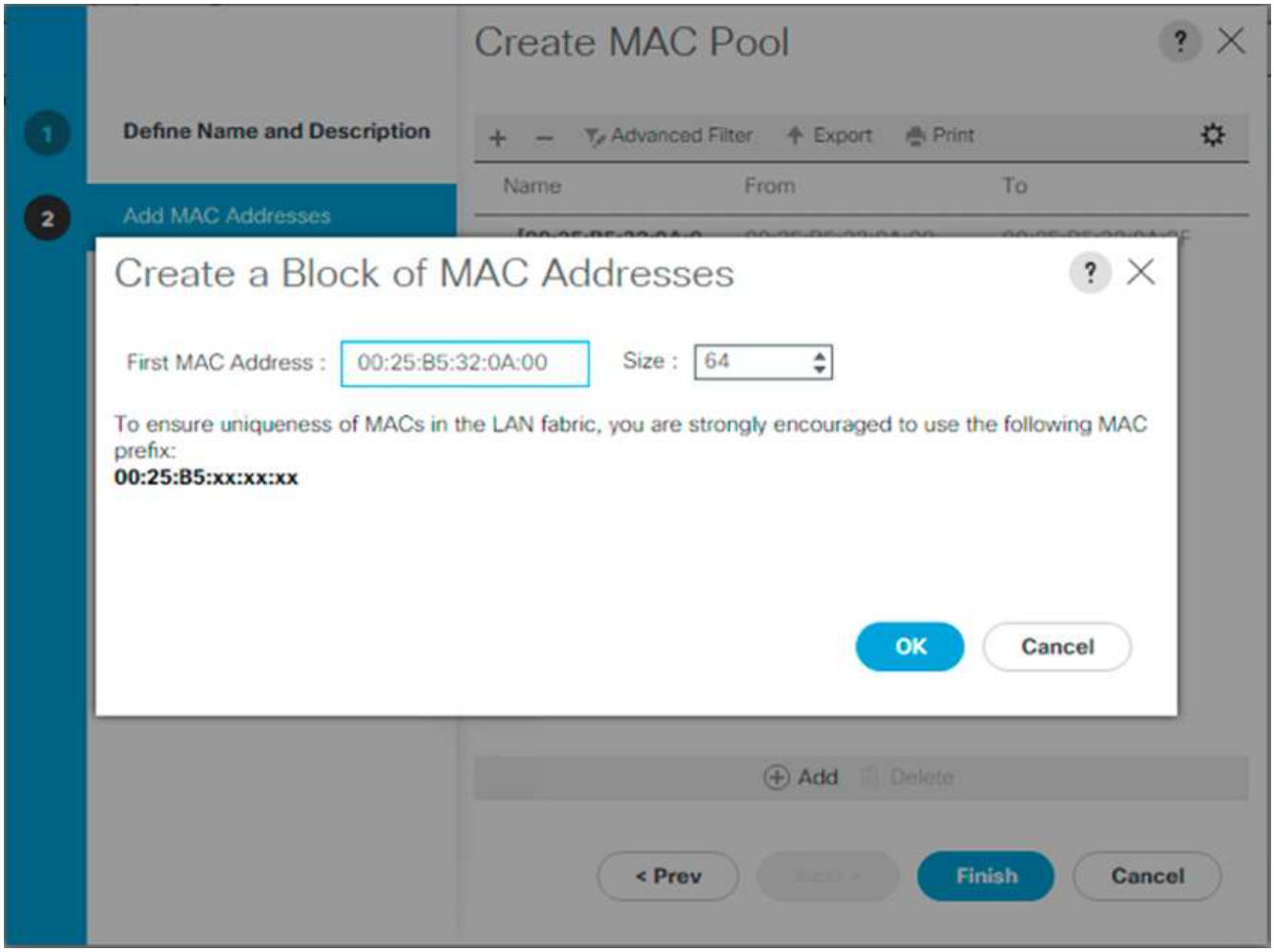
1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez pools > racine.

   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.

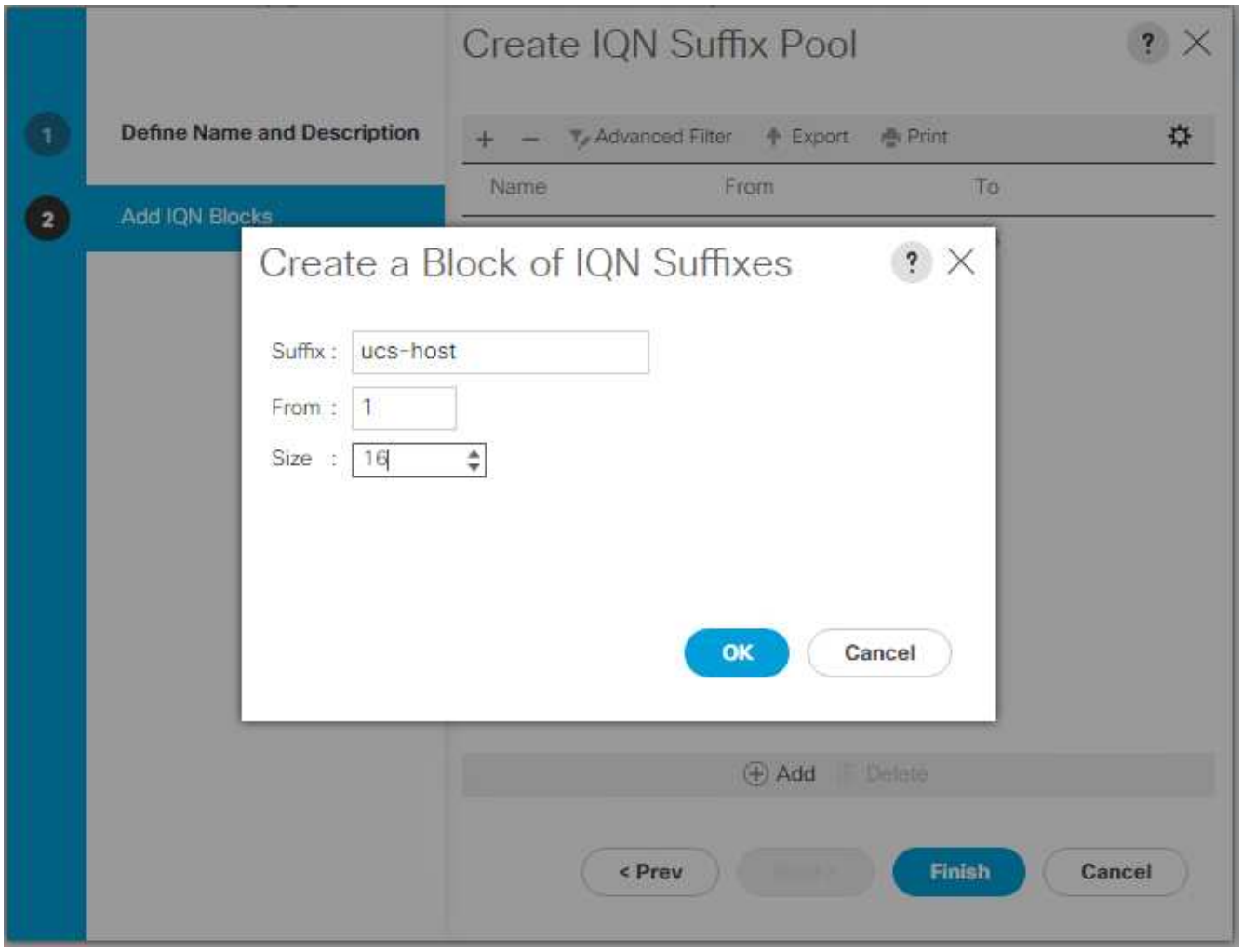
Créez le pool IQN iSCSI

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.

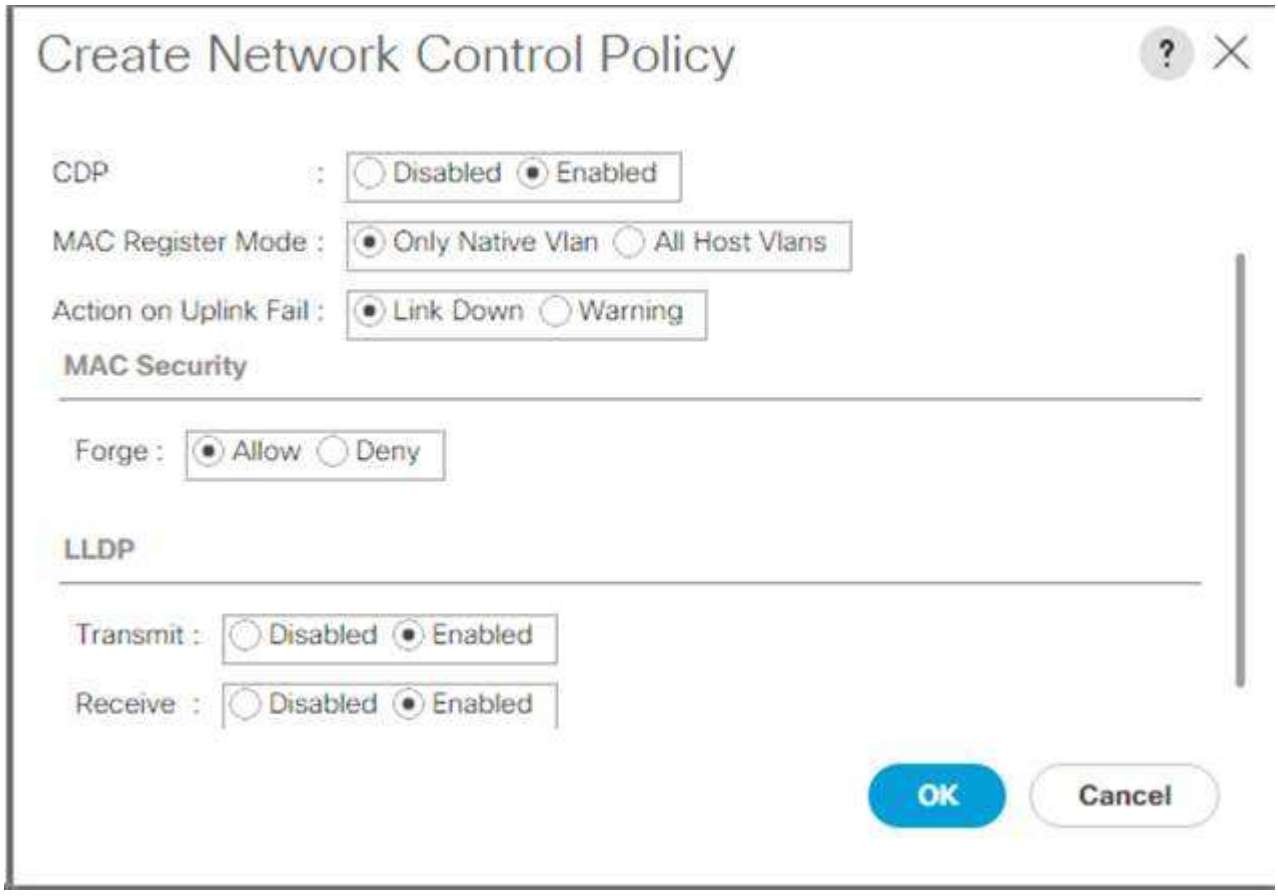
1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez pools > racine.
3. Cliquez avec le bouton droit de la souris sur pools de serveurs.

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 :

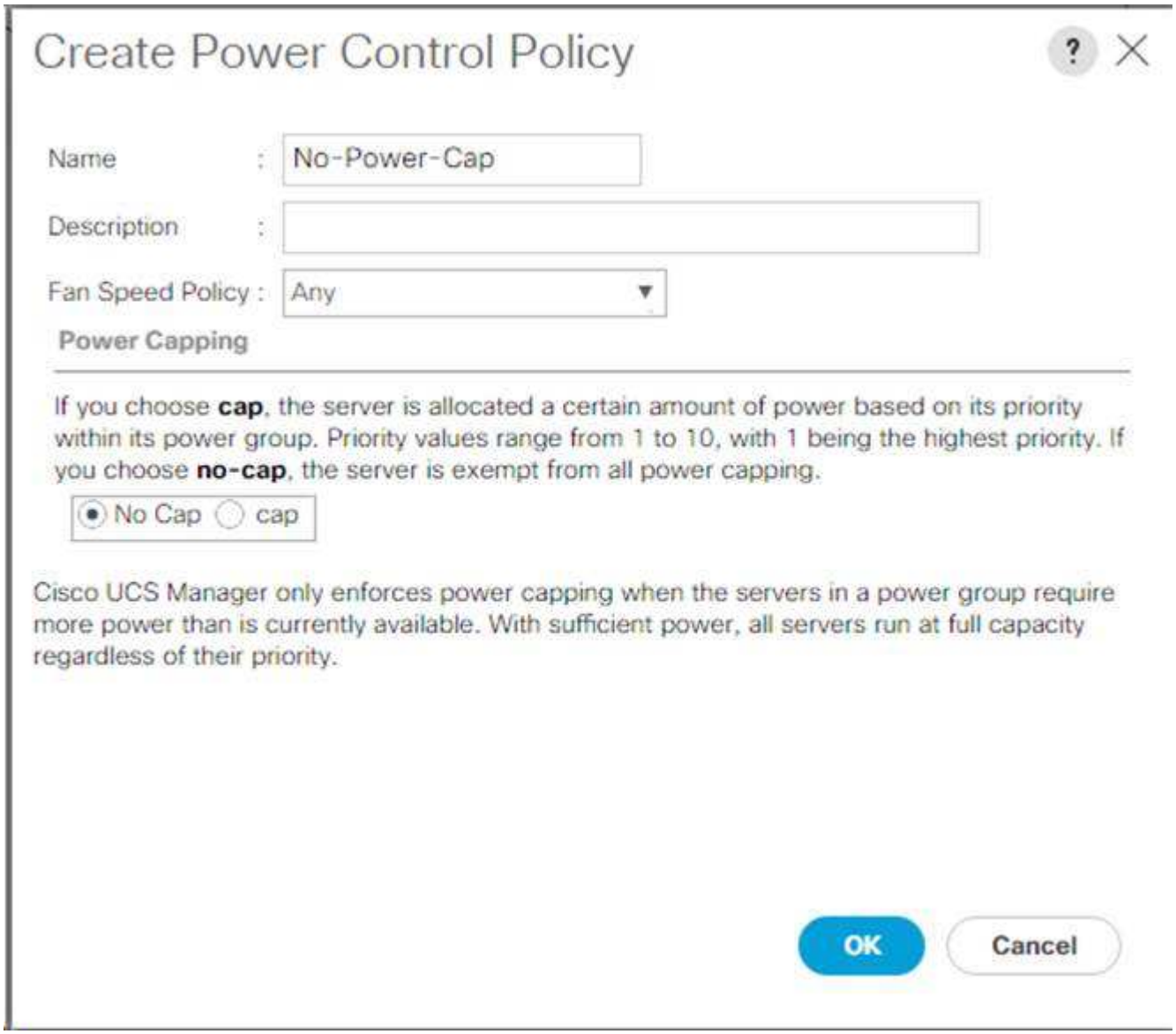
1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies de contrôle du réseau.
4. Sélectionnez Créer une stratégie de contrôle réseau.
5. Entrez le nom de la stratégie Enable-CDP-LLDP.
6. Sous CDP, sélectionnez 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.

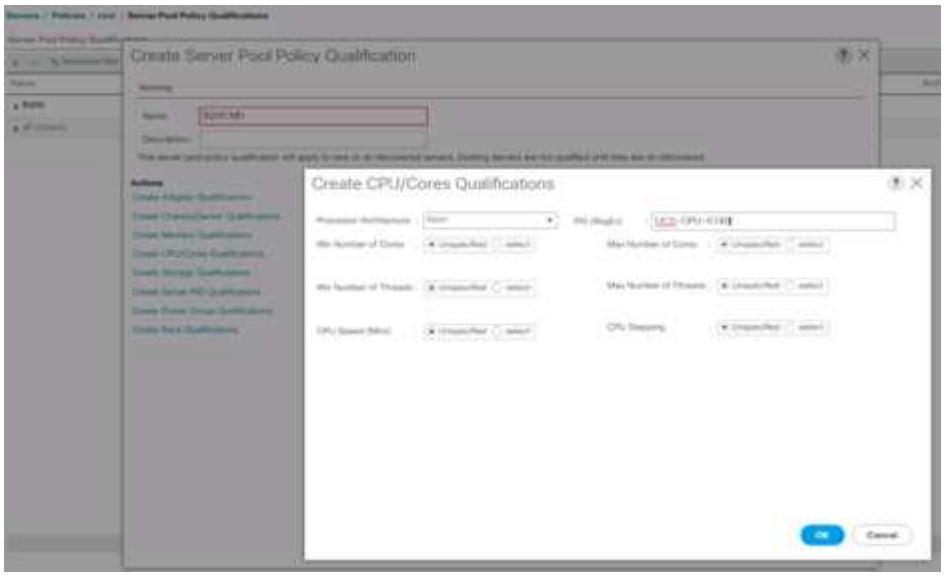


Créer une stratégie de qualification de pool de serveurs (facultatif)

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.

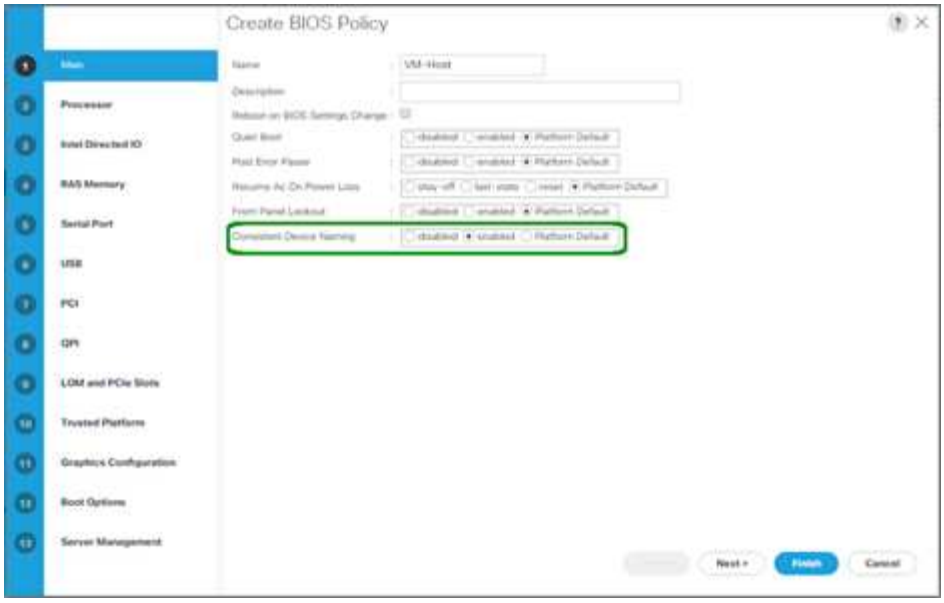
1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Sélectionnez qualifications de stratégie de pool de serveurs.
4. Sélectionnez Créer une qualification de stratégie de pool de serveurs ou Ajouter.
5. Nommez la stratégie Intel.
6. Sélectionnez Créer 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.



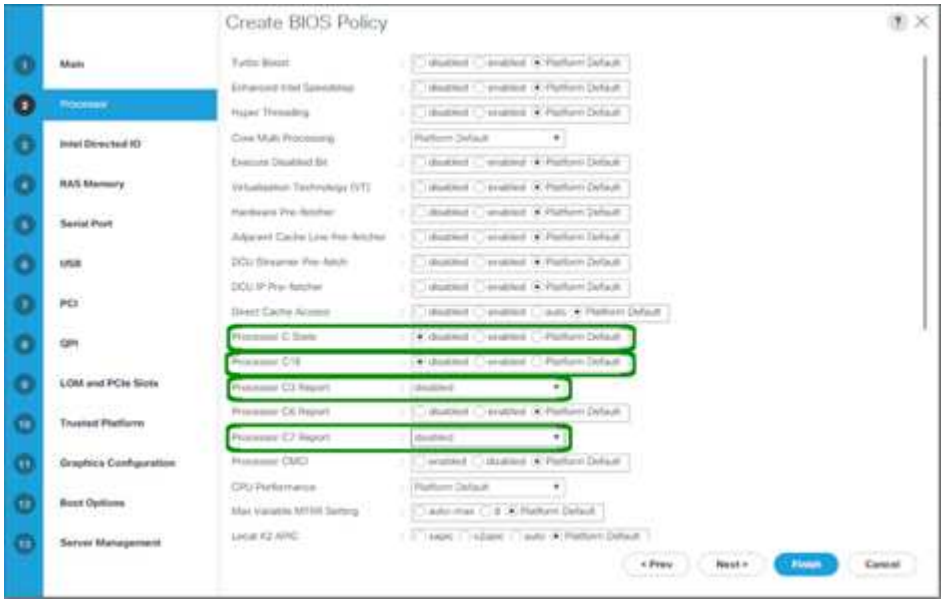
Créer une stratégie BIOS du serveur

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

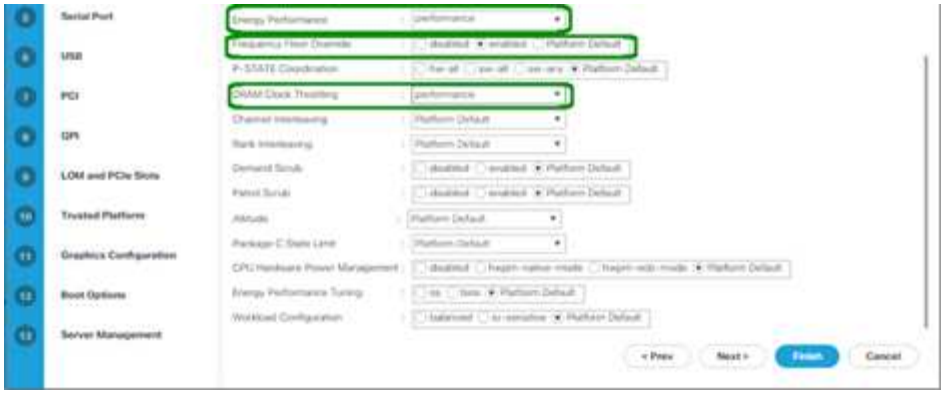
1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies BIOS.
4. Sélectionnez Créer une stratégie de BIOS.
5. Saisissez VM-Host comme nom de stratégie BIOS.
6. Définissez le paramètre de démarrage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



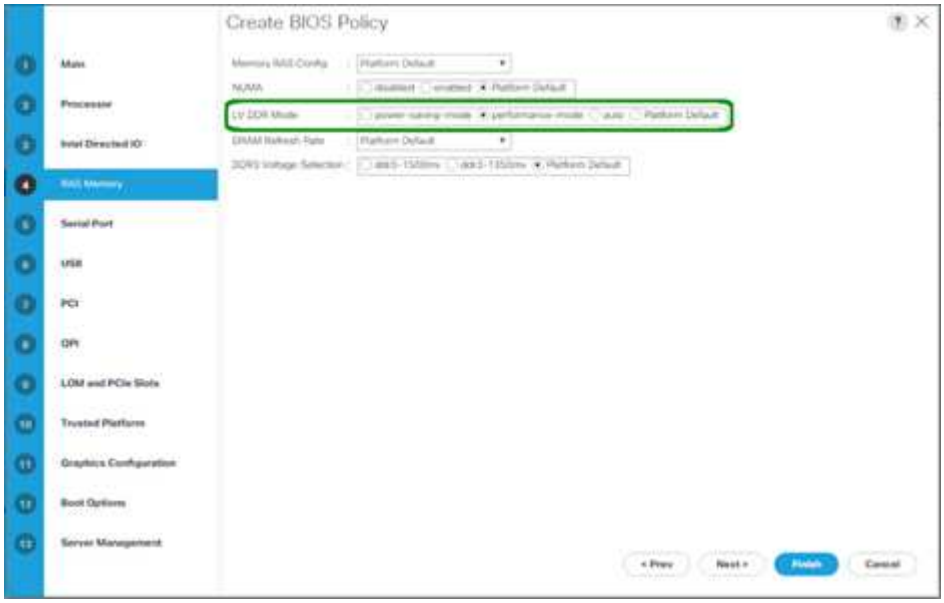
8. Sélectionnez l’onglet processeur et définissez les paramètres suivants :
   - État du processeur C : désactivé
   - Processeur C1E : désactivé
   - Rapport C3 du processeur : désactivé
   - Rapport C7 processeur : désactivé



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

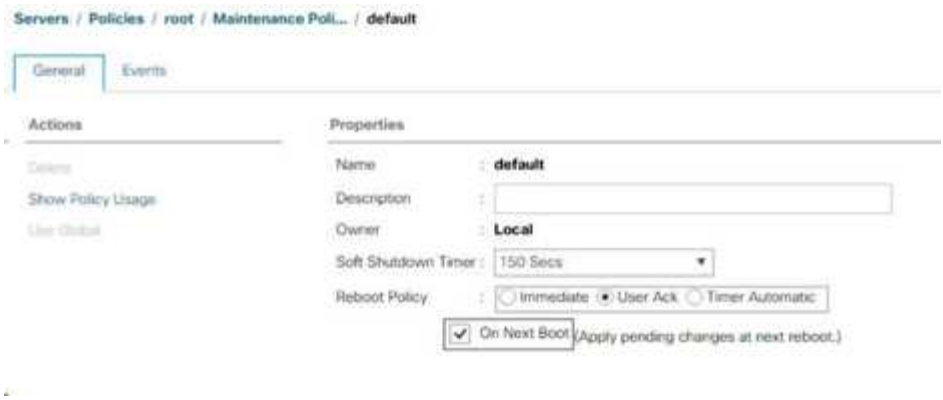


11. Cliquez sur Terminer pour créer la stratégie de BIOS.
12. Cliquez sur OK.

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.

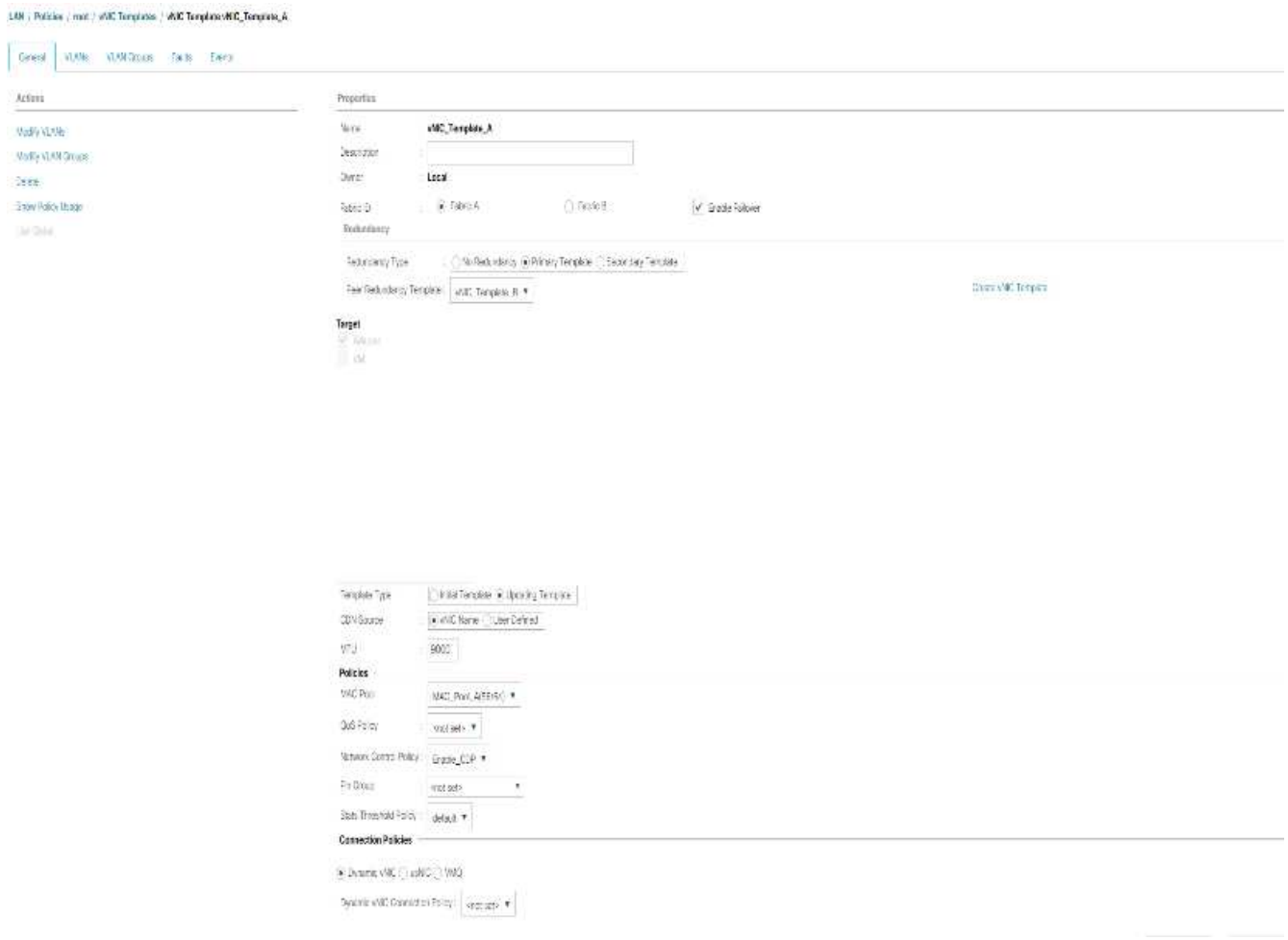
Quatre modèles vNIC au total sont créés.

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.

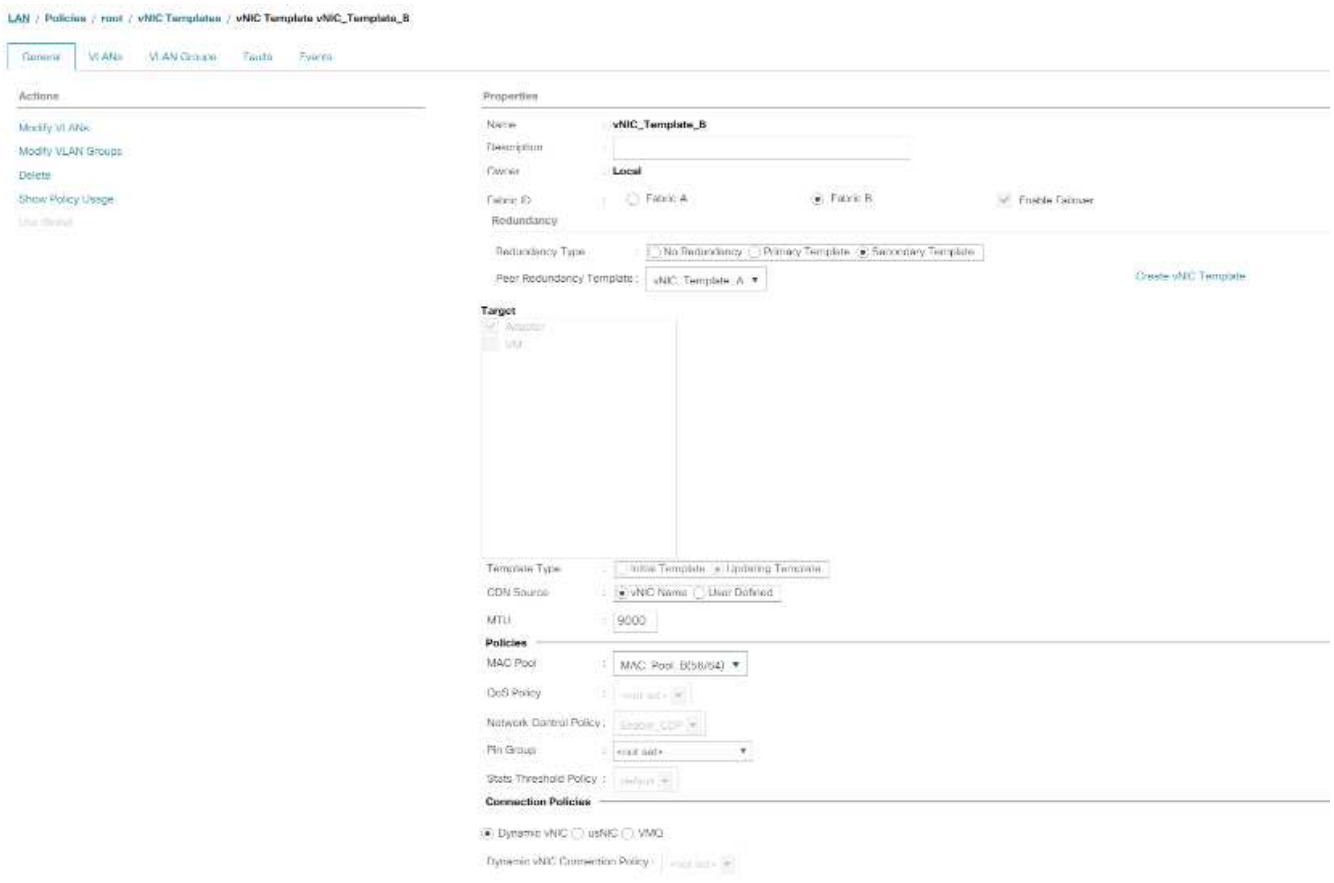


Pour créer le modèle de redondance secondaire Infra-B, procédez comme suit :

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.

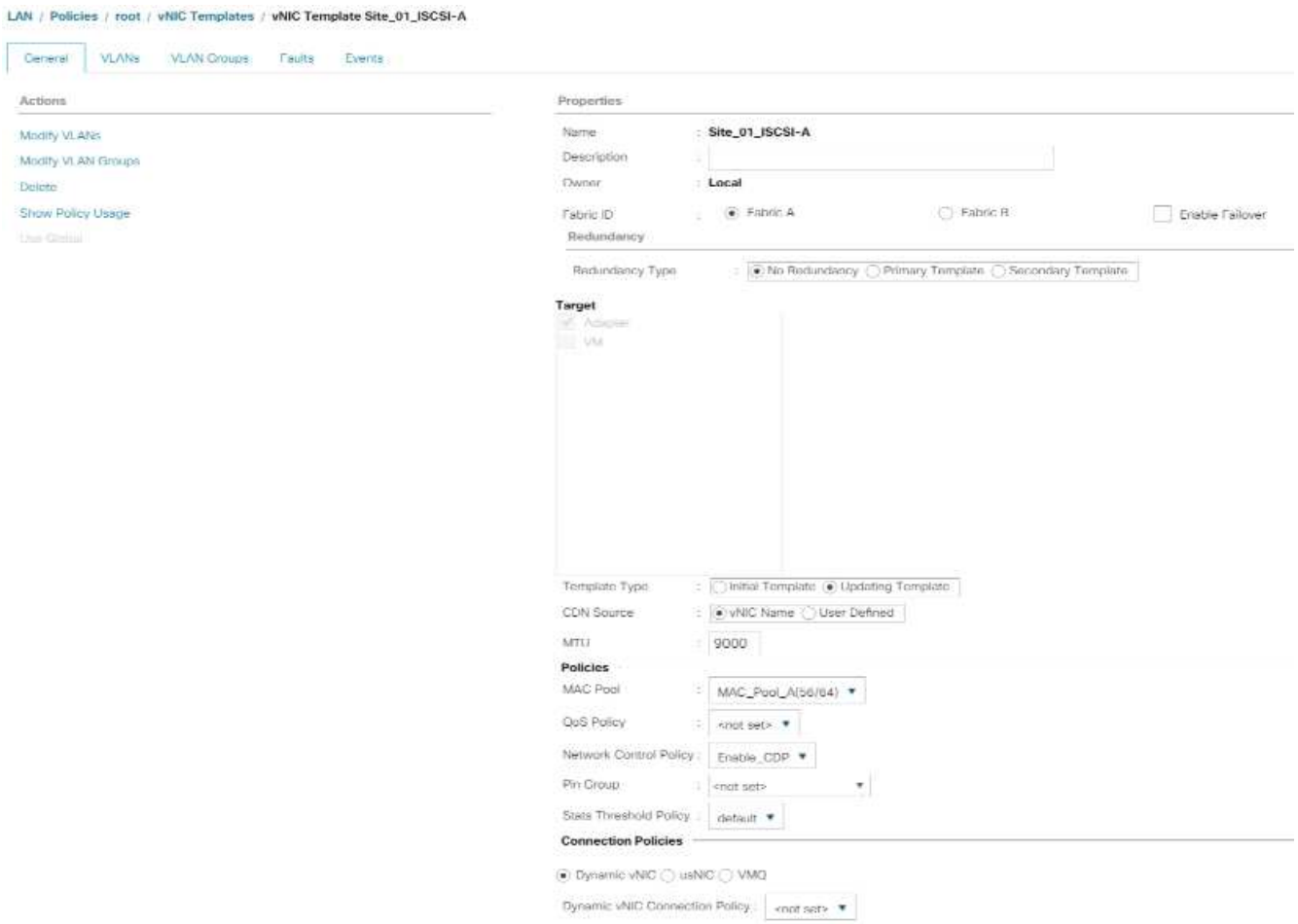


Créez des vNIC iSCSI

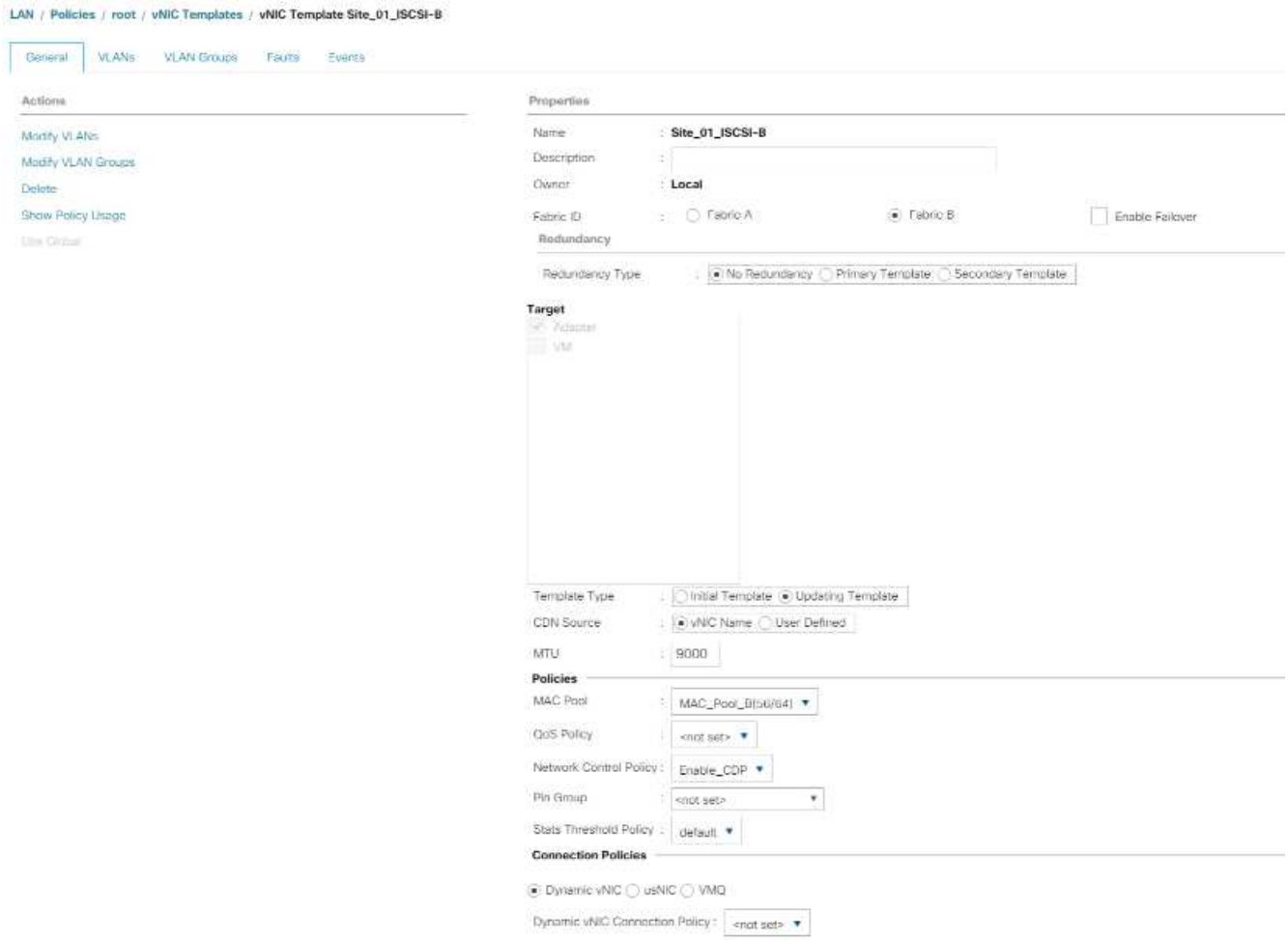
Pour créer des vNIC iSCSI, procédez comme suit :

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.



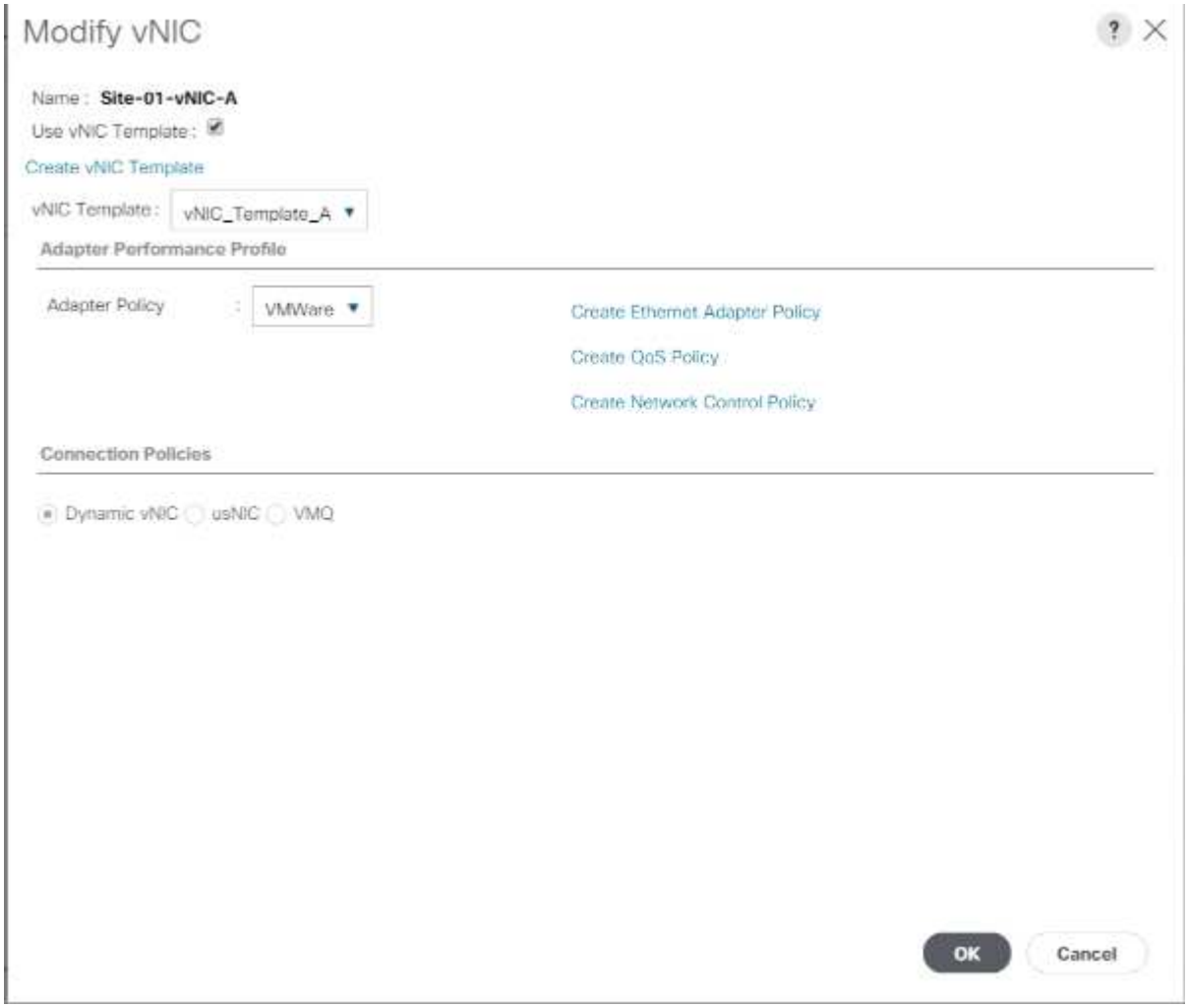
Créez une stratégie de connectivité LAN pour le démarrage iSCSI

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 :

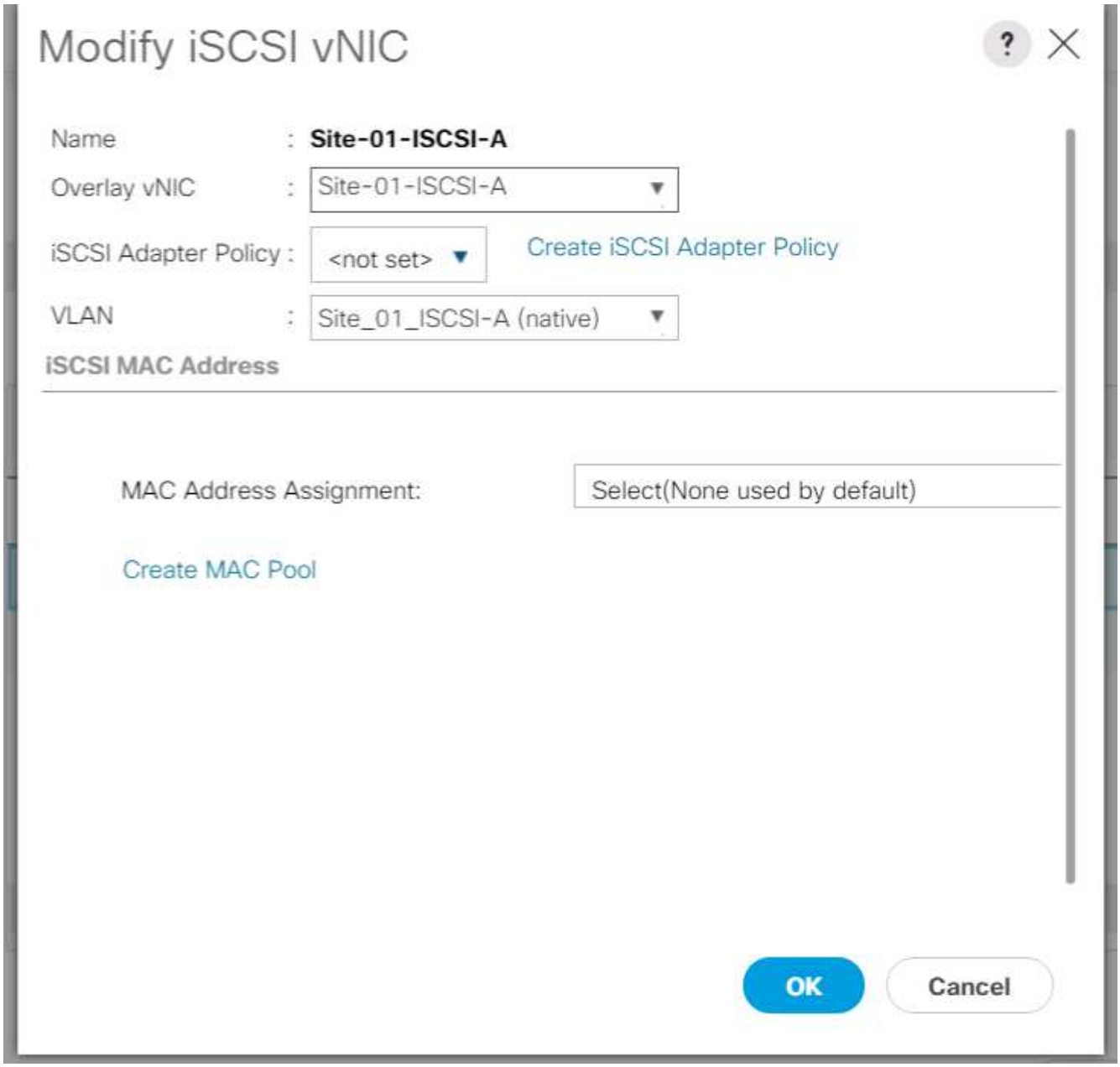
1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez LAN > stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies de connectivité LAN.
4. Sélectionnez Créer une stratégie de connectivité LAN.
5. Entrez `Site-XX-Fabric-A` comme nom de la règle.
6. Cliquez 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.

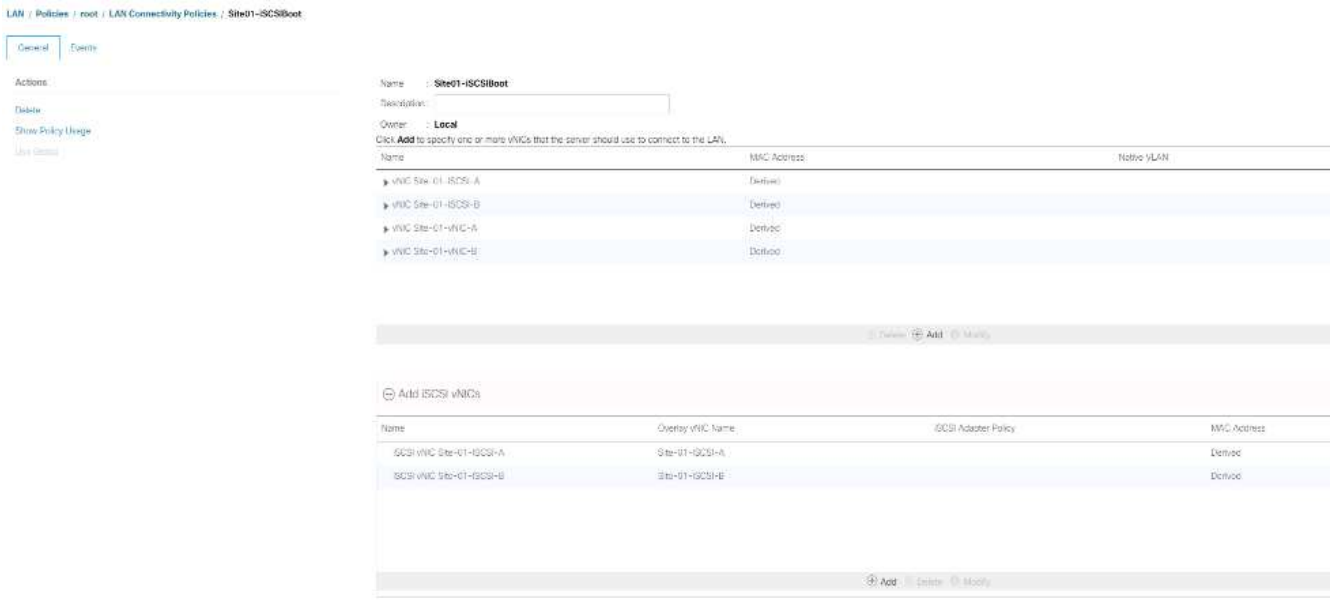


12. Cliquez sur l'option Ajouter en haut pour ajouter un vNIC.
13. Dans la boîte de dialogue Créer vNIC, entrez `Site-01-vNIC-B` Comme nom du vNIC.
14. Sélectionnez l'option utiliser le modèle vNIC.
15. Dans la liste modèle vNIC, sélectionnez `vNIC_Template_B`.
16. Dans la liste déroulante adapter Policy, 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.

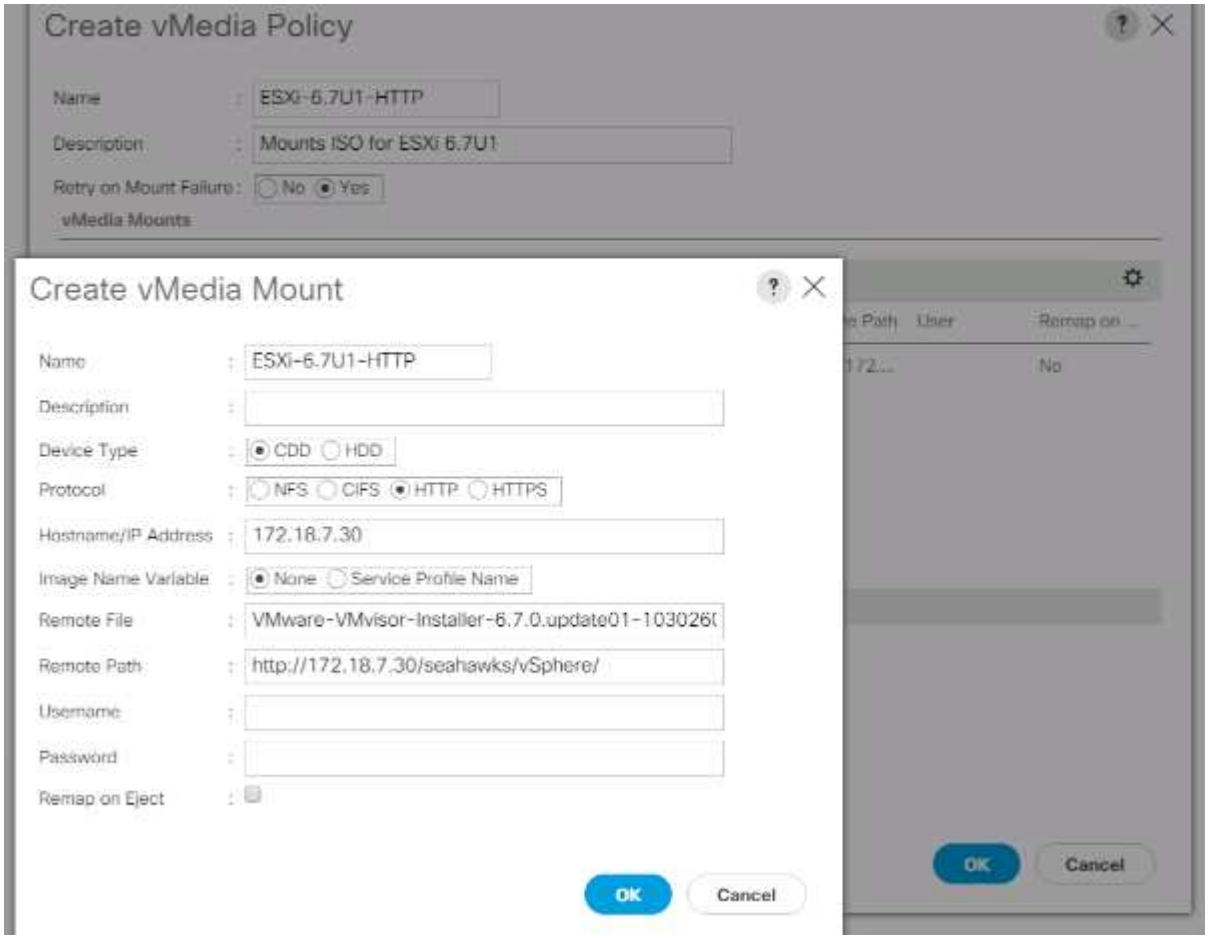
13. Entrez `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Comme nom de fichier distant.

    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

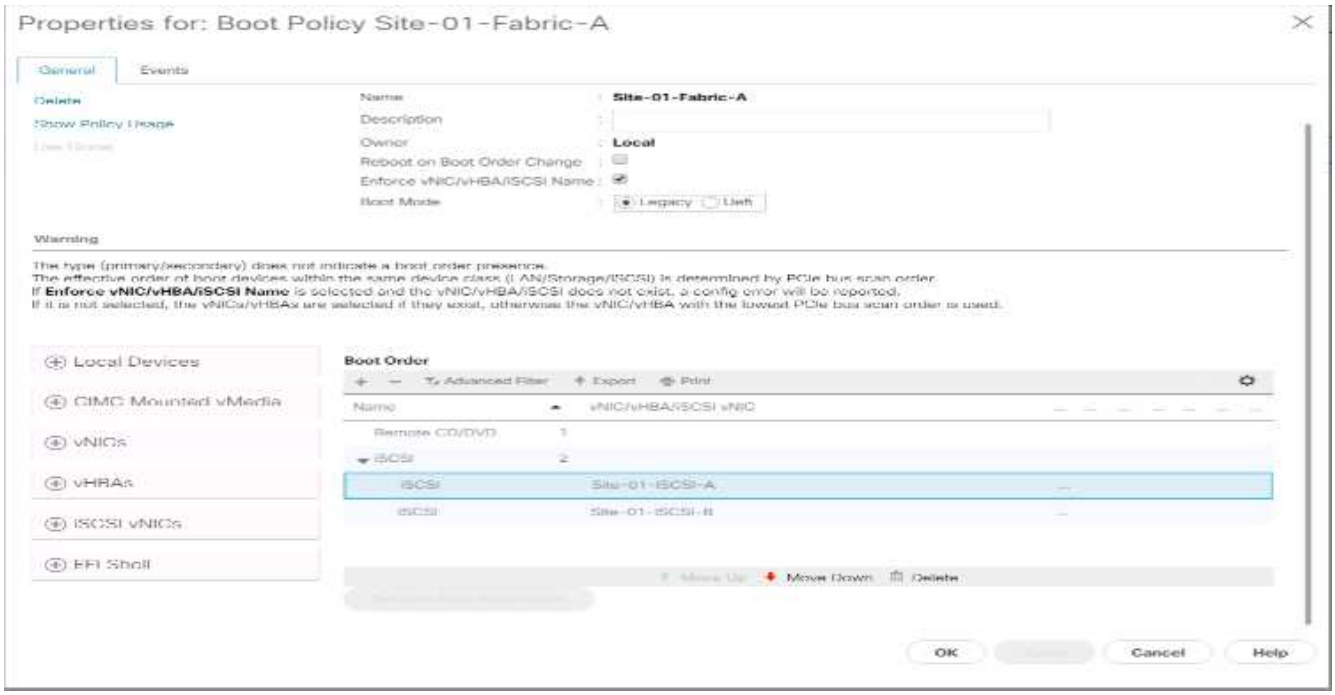
La procédure décrite dans cette section s'applique à un environnement Cisco UCS dans lequel deux interfaces logiques iSCSI (LIF) se trouvent sur le nœud de cluster 1 (`iscsi_lif01a` et `iscsi_lif01b`) Et deux LIF iSCSI sont sur le nœud de cluster 2 (`iscsi_lif02a` et `iscsi_lif02b`). On suppose également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



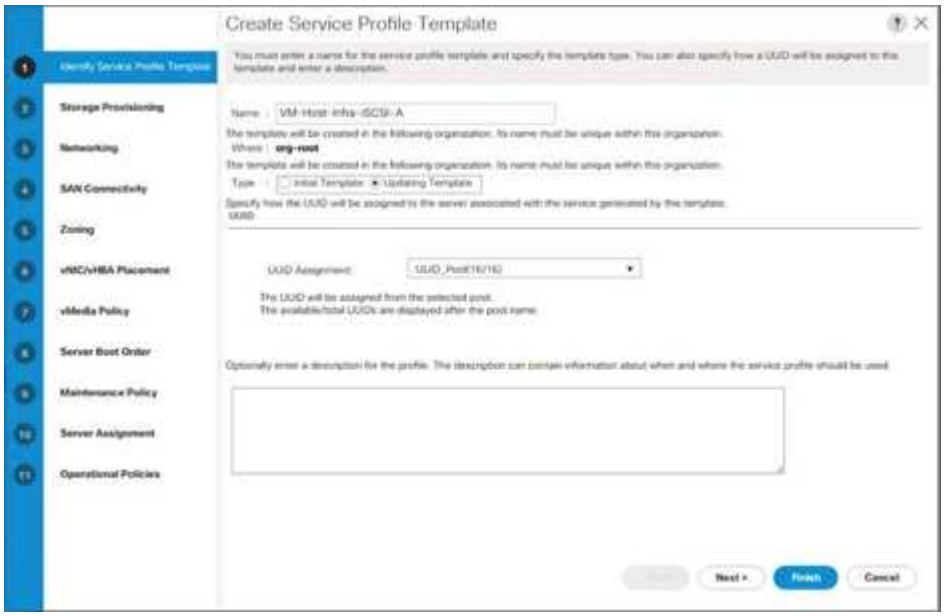
Créer un modèle de profil de service

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

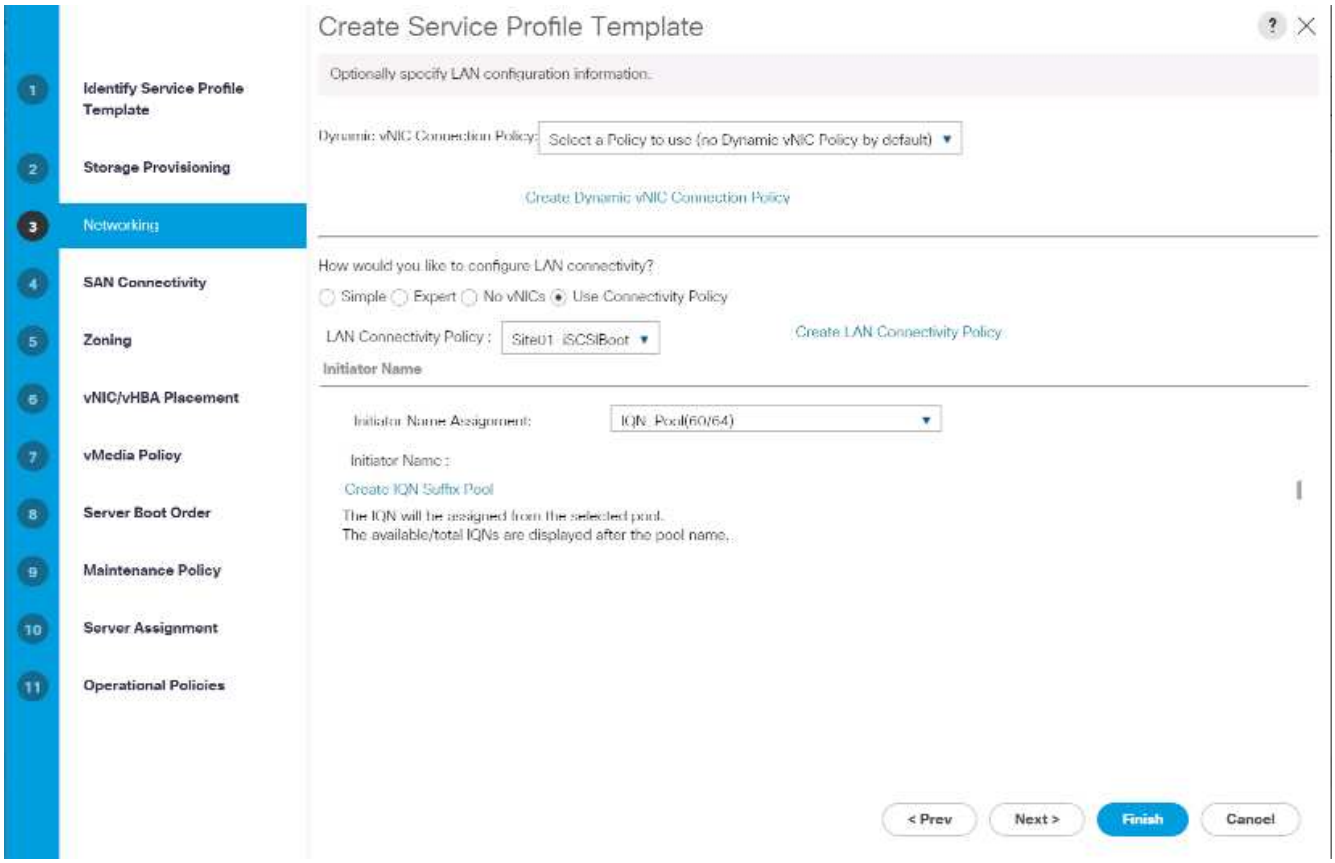
Pour configurer le provisionnement du stockage, procédez comme suit :

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

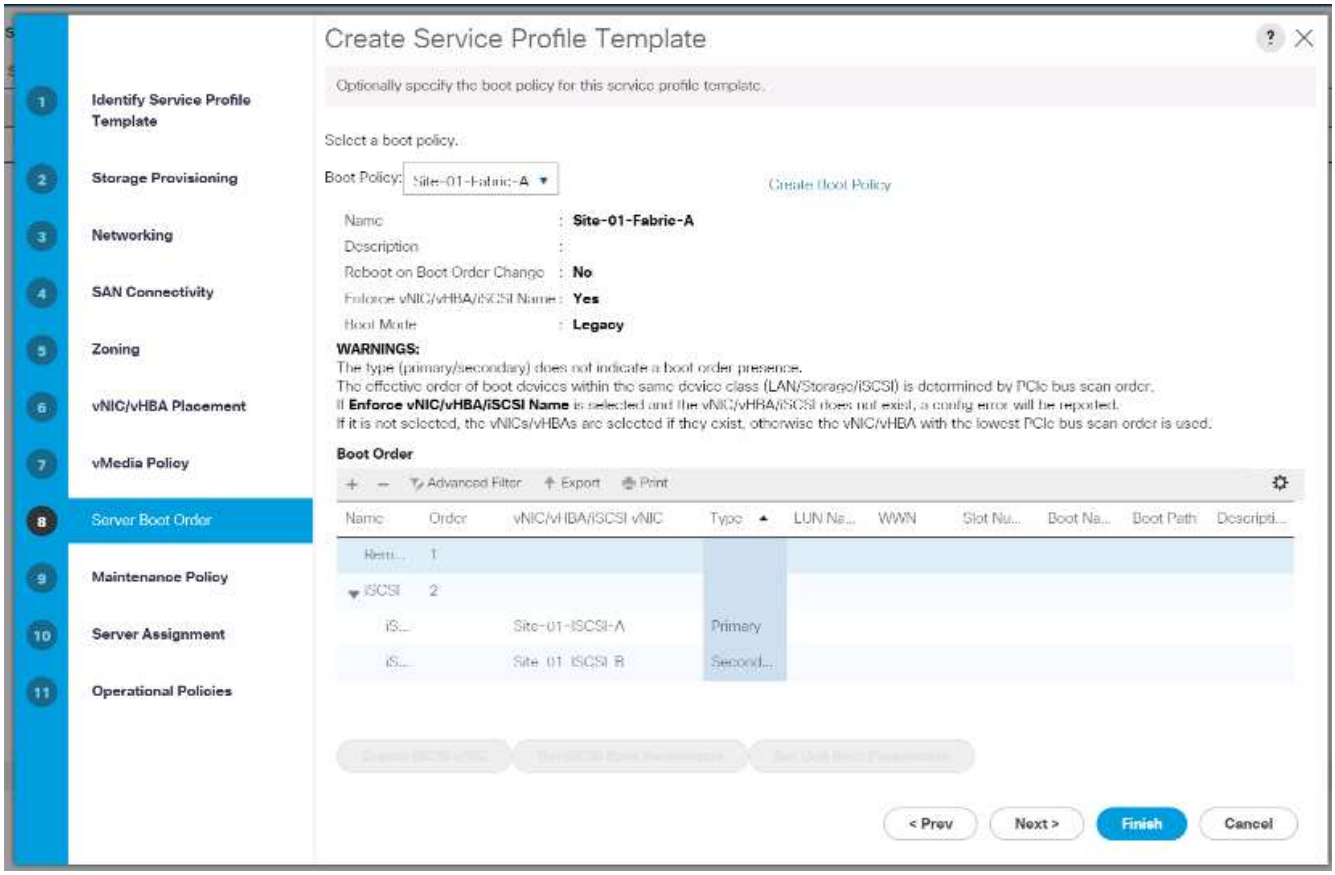
Pour configurer la stratégie vMedia, procédez comme suit :

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.



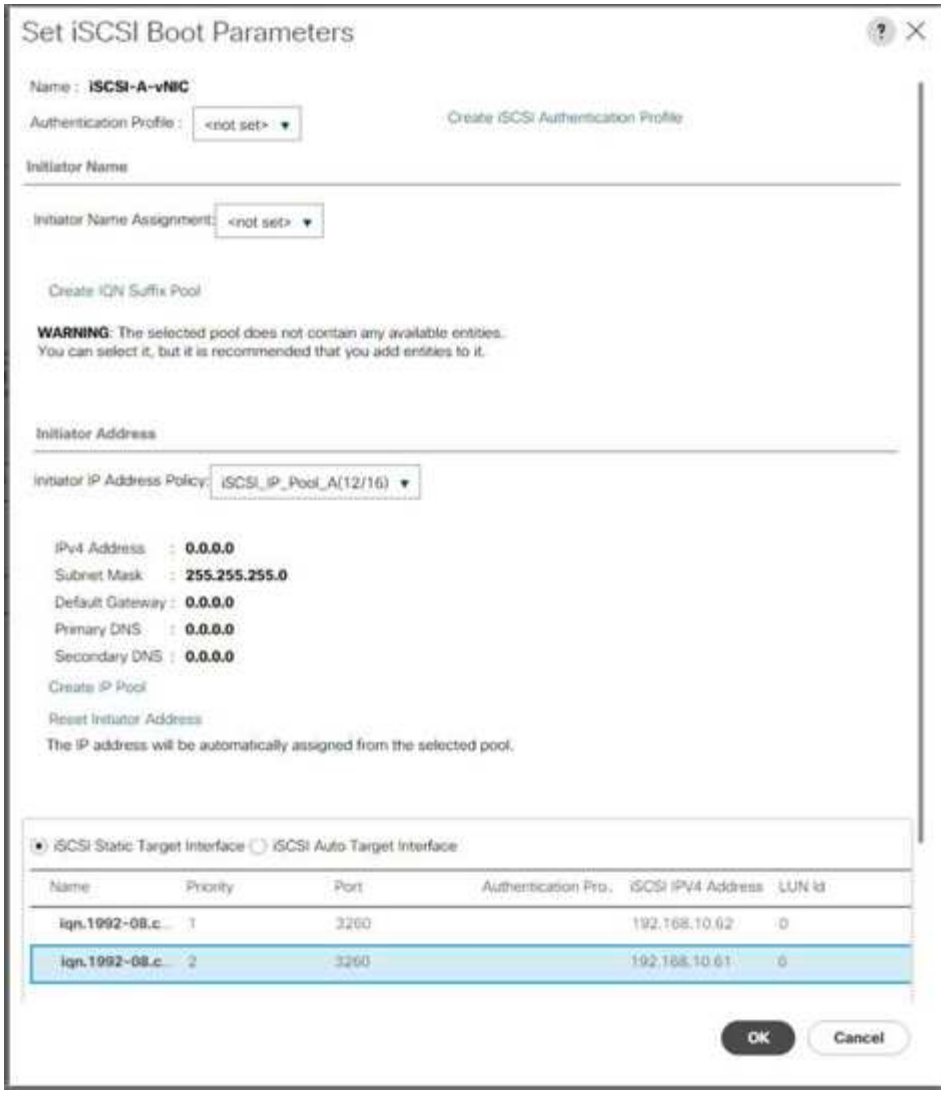
2. Dans l'ordre Boor, sélectionnez `Site-01- iSCSI-A`.
3. Cliquez sur définir les paramètres de démarrage iSCSI.
4. Dans la boîte de dialogue définir les paramètres de démarrage iSCSI, laissez l'option profil d'authentification ne pas être définie, sauf si vous avez créé un profil adapté à votre environnement 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.

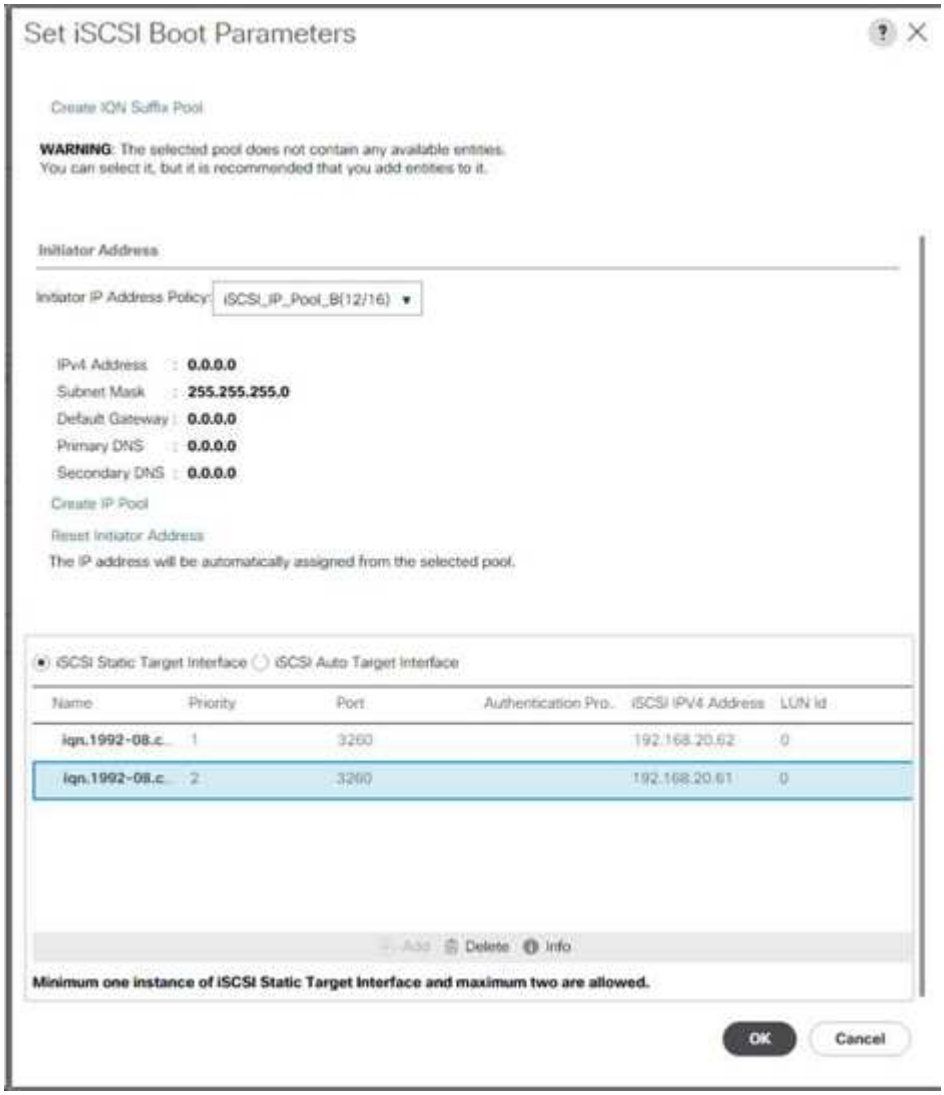
16. Dans l'ordre de démarrage, sélectionnez iSCSI-B-vNIC.
17. Cliquez sur définir les paramètres de démarrage iSCSI.
18. Dans la boîte de dialogue définir les paramètres de démarrage iSCSI, laissez l'option profil d'authentification non définie, sauf si vous avez créé un profil adapté à votre environnement 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.

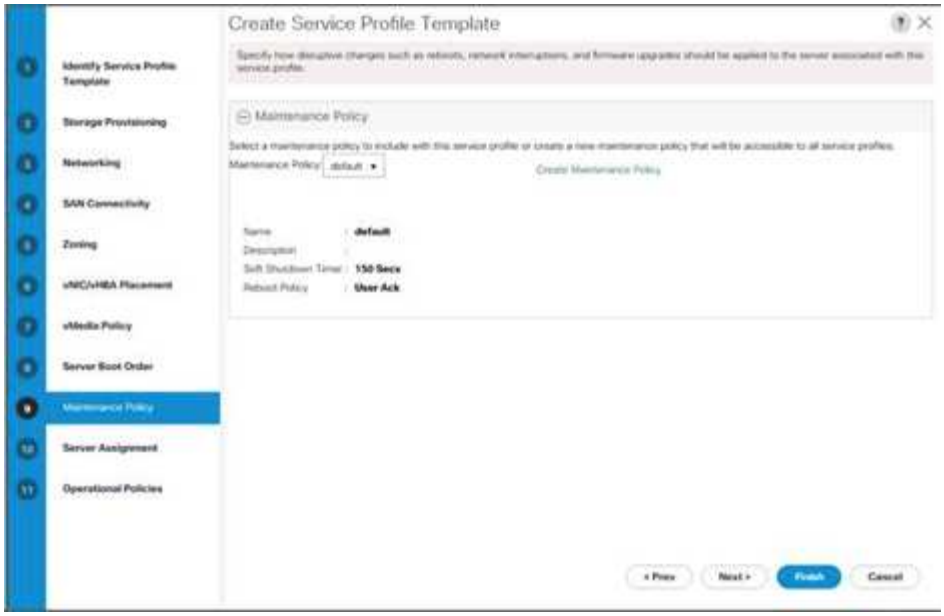


30. Cliquez sur Suivant.

Configurer la stratégie de maintenance

Pour configurer la stratégie de maintenance, procédez comme suit :

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

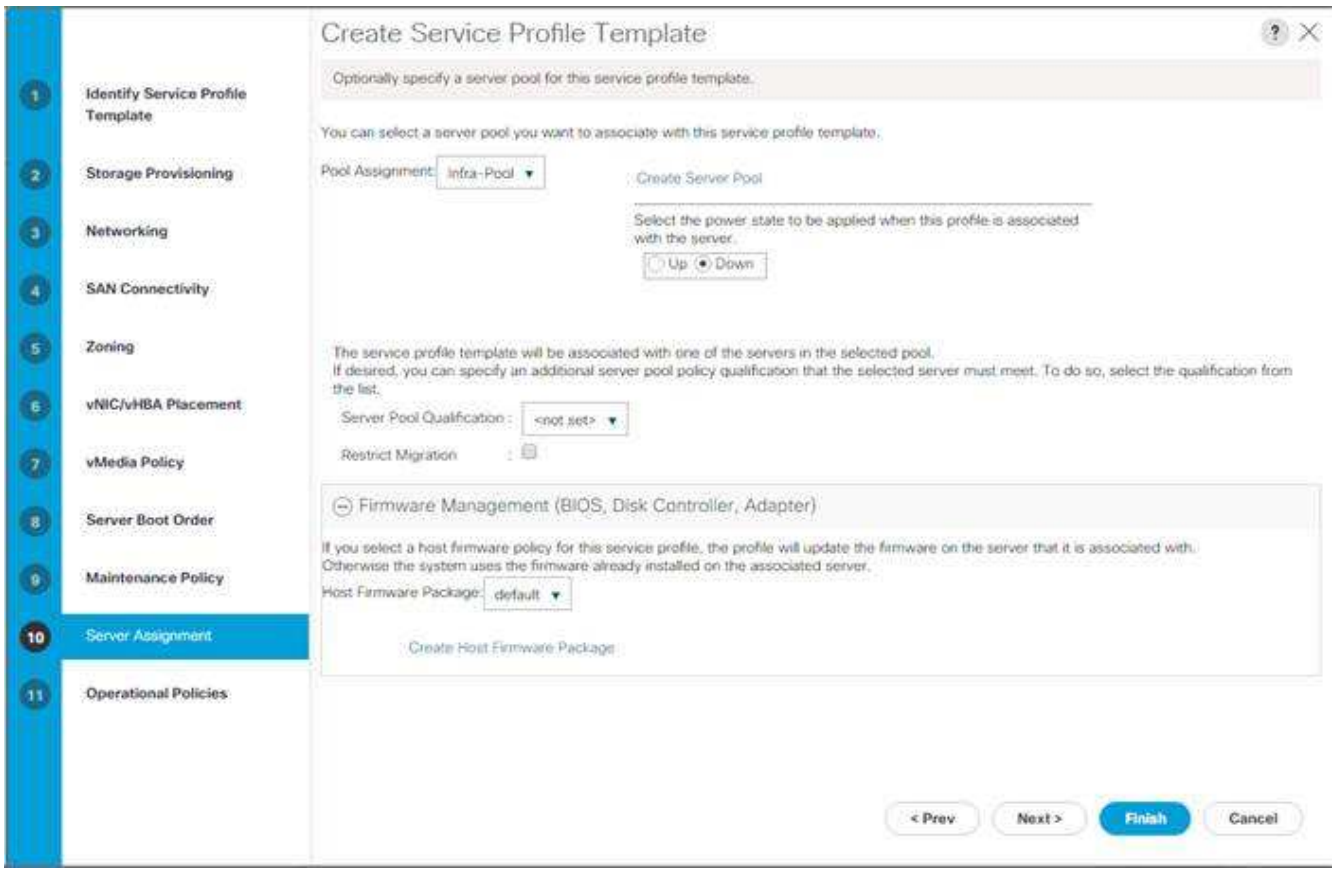


2. Cliquez sur Suivant.

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.

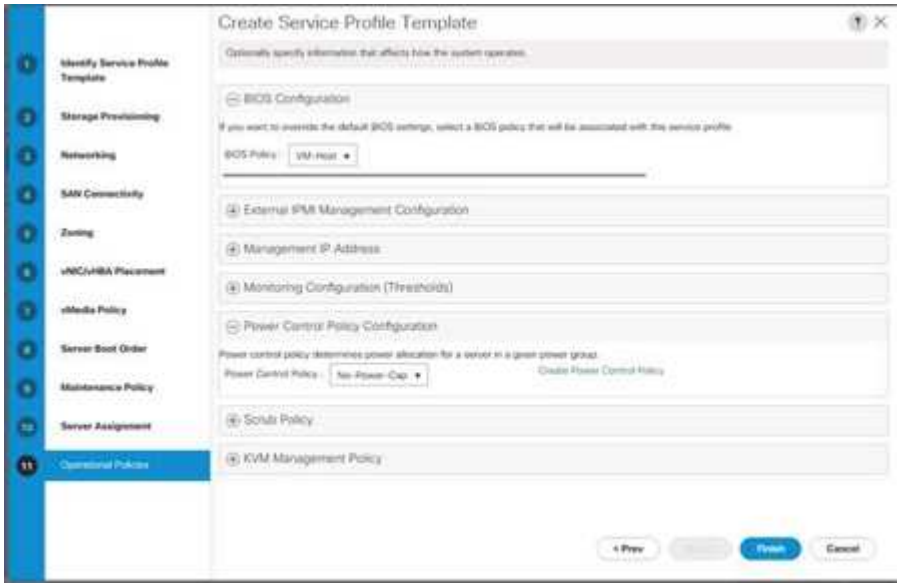


4. Cliquez sur Suivant.

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.

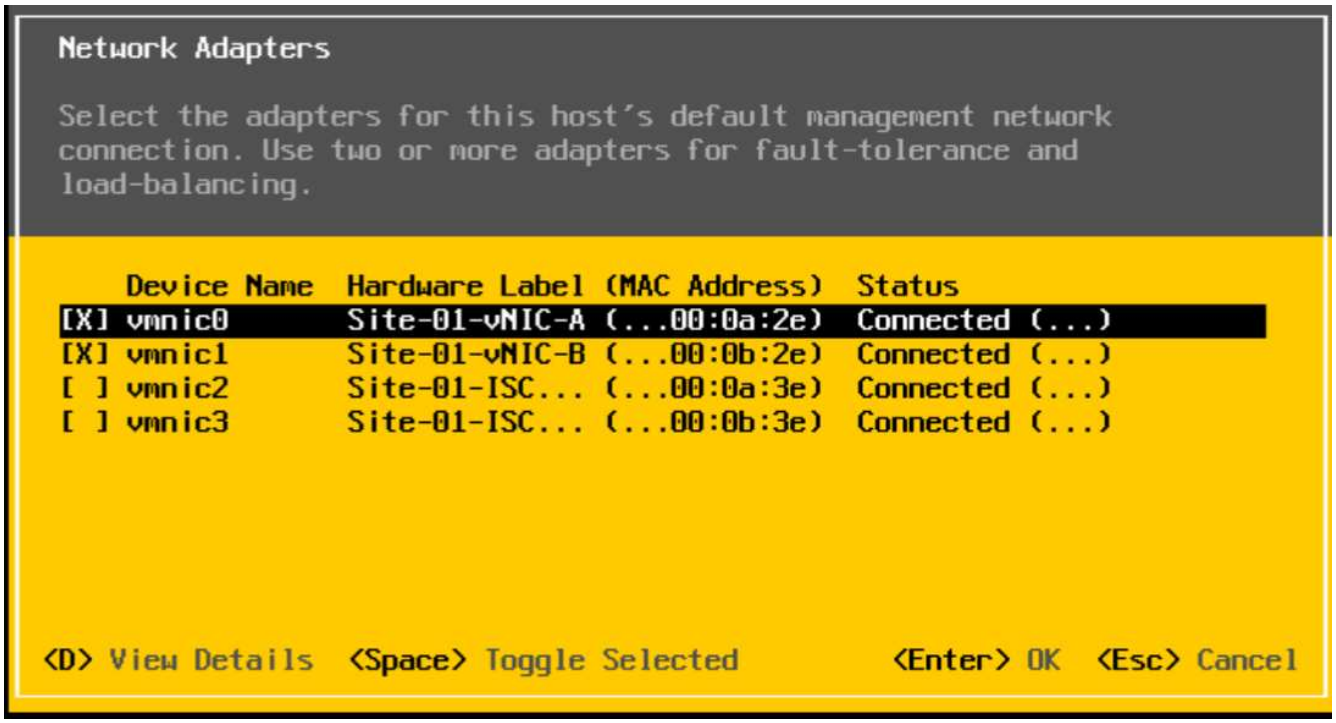
Configuration du réseau de gestion pour les hôtes ESXi

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.

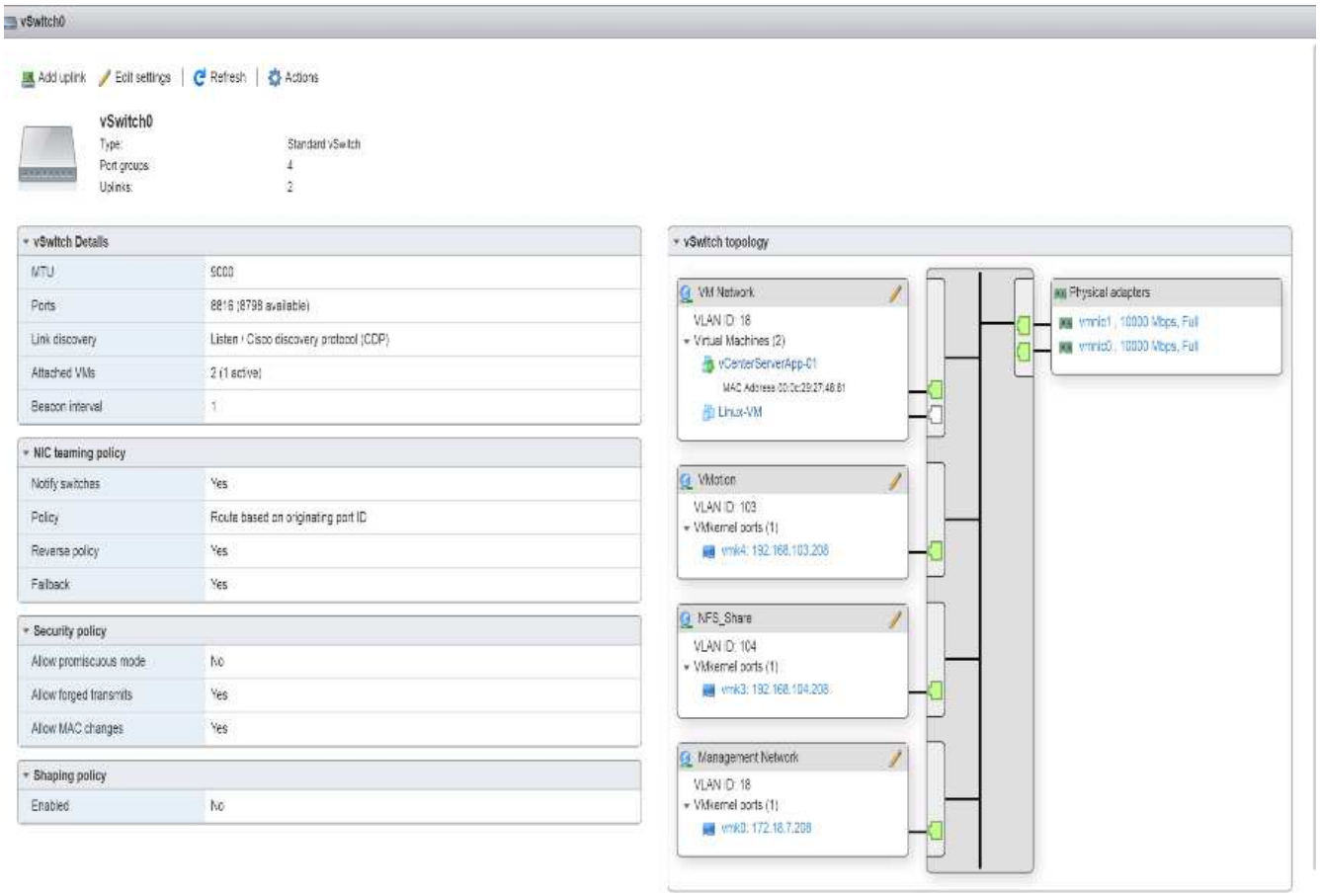
4. Sélectionnez Modifier les paramètres.
5. Remplacez la MTU par 9000.
6. Développer le regroupement de cartes réseau.
7. Dans la section ordre de basculement, sélectionnez vmnic1 et cliquez sur Marquer actif.
8. Vérifiez que vmnic1 a maintenant l'état actif.
9. Cliquez sur Enregistrer.
10. Sélectionnez 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.

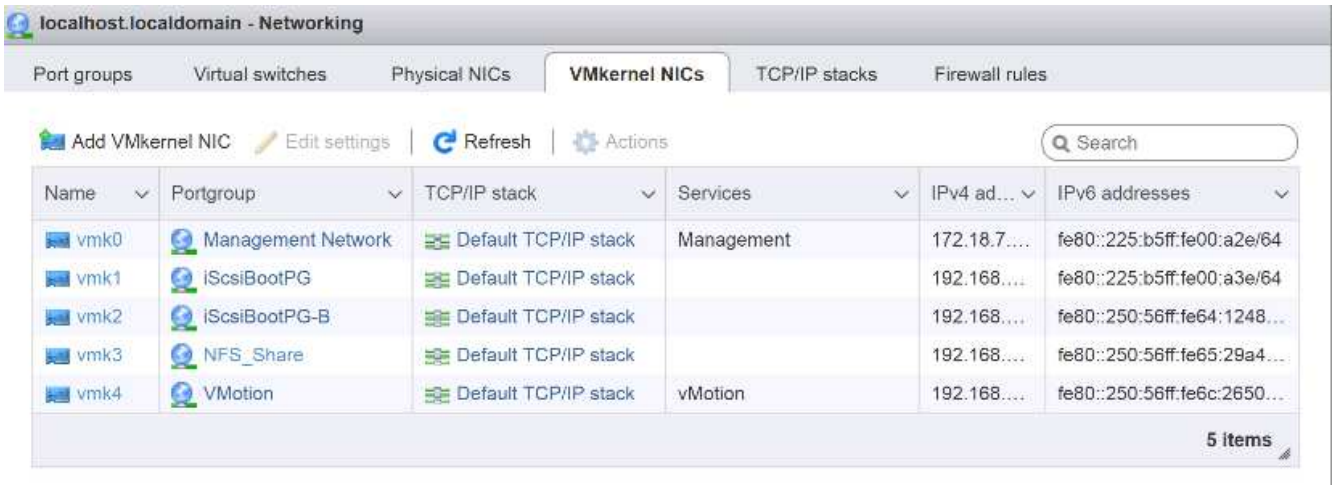
21. Cliquez sur Enregistrer.
22. Sélectionnez l'onglet commutateurs virtuels.
23. Sélectionnez le commutateur virtuel standard Add.
24. Indiquez un nom de `iScsciBootvSwitch-B` Pour le nom du vSwitch.
25. Définissez la MTU sur 9000.
26. Sélectionnez vmnic3 dans le menu déroulant Uplink 1.
27. Cliquez 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 :



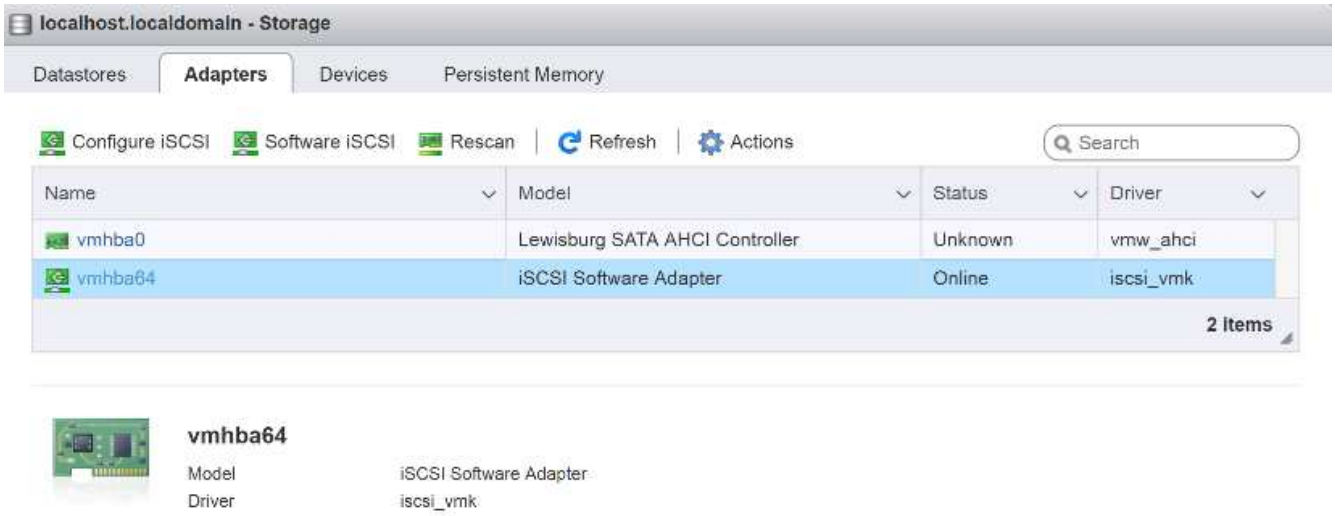
Configuration des chemins d’accès multiples iSCSI

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

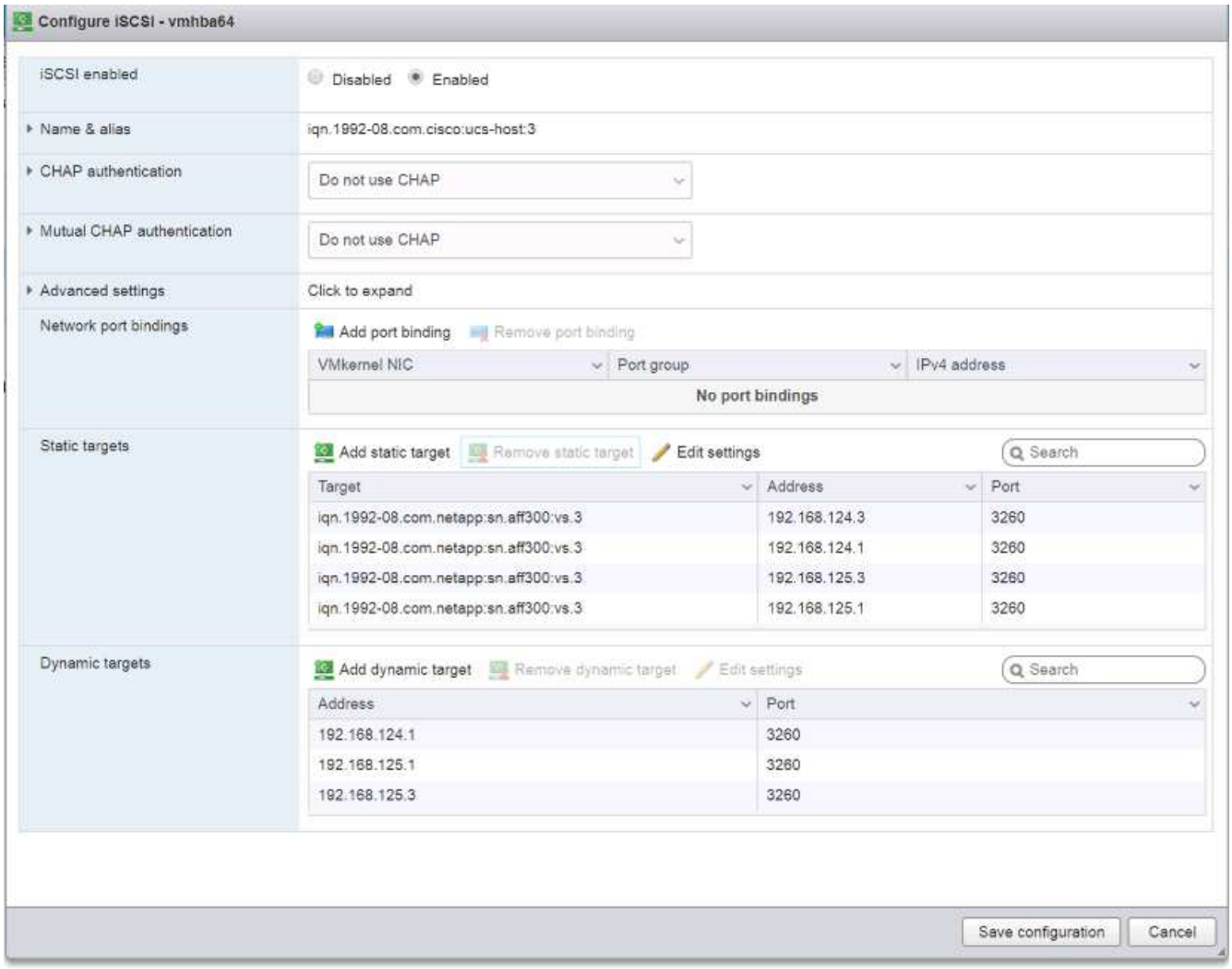
Pour configurer les chemins d’accès multiples iSCSI sur l’hôte ESXi VM-Host-Infra-01 et VM-Host-Infra-02, procédez comme suit :

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.

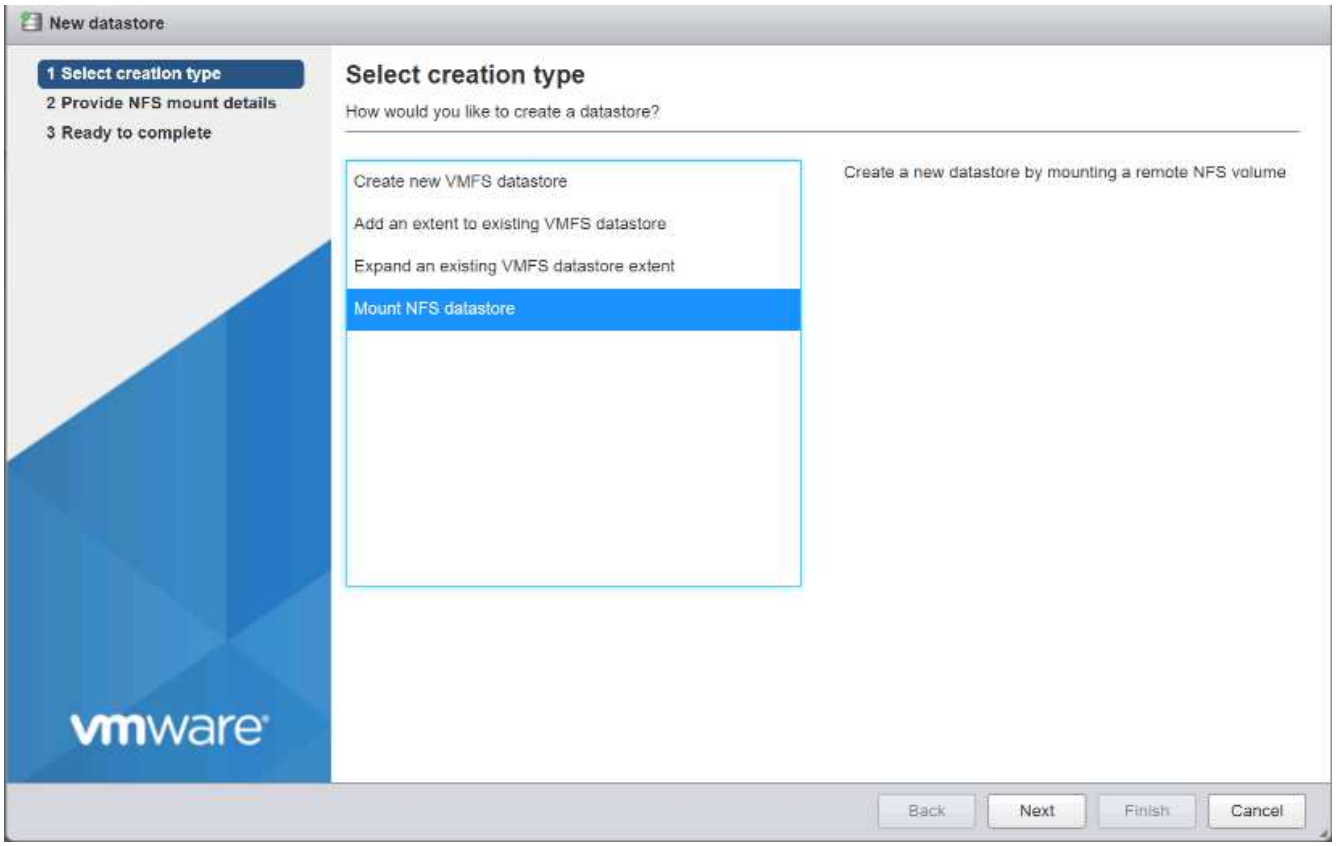
L'hôte réanalyse automatiquement l'adaptateur de stockage et les cibles sont ajoutées aux cibles statiques.

Montez les datastores requis

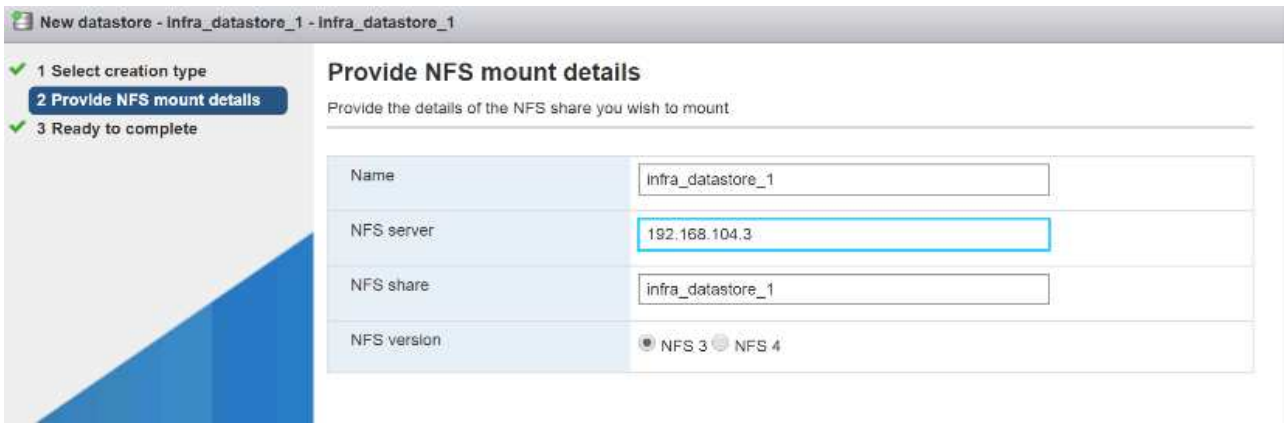
Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

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).

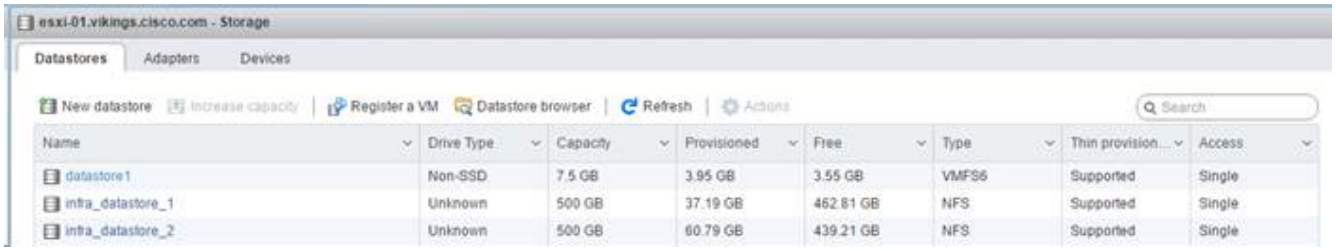


5. Sur la page Détails du montage NFS, procédez comme suit :
   a. Entrez `infra_datastore_1` nom du datastore.
   b. Entrez l'adresse IP du `nfs_lif01_a` LIF pour le serveur NFS.
   c. Entrez `/infra_datastore_1` Pour le partage NFS.
   d. Laissez la version NFS définie sur NFS 3.
   e. Cliquez sur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



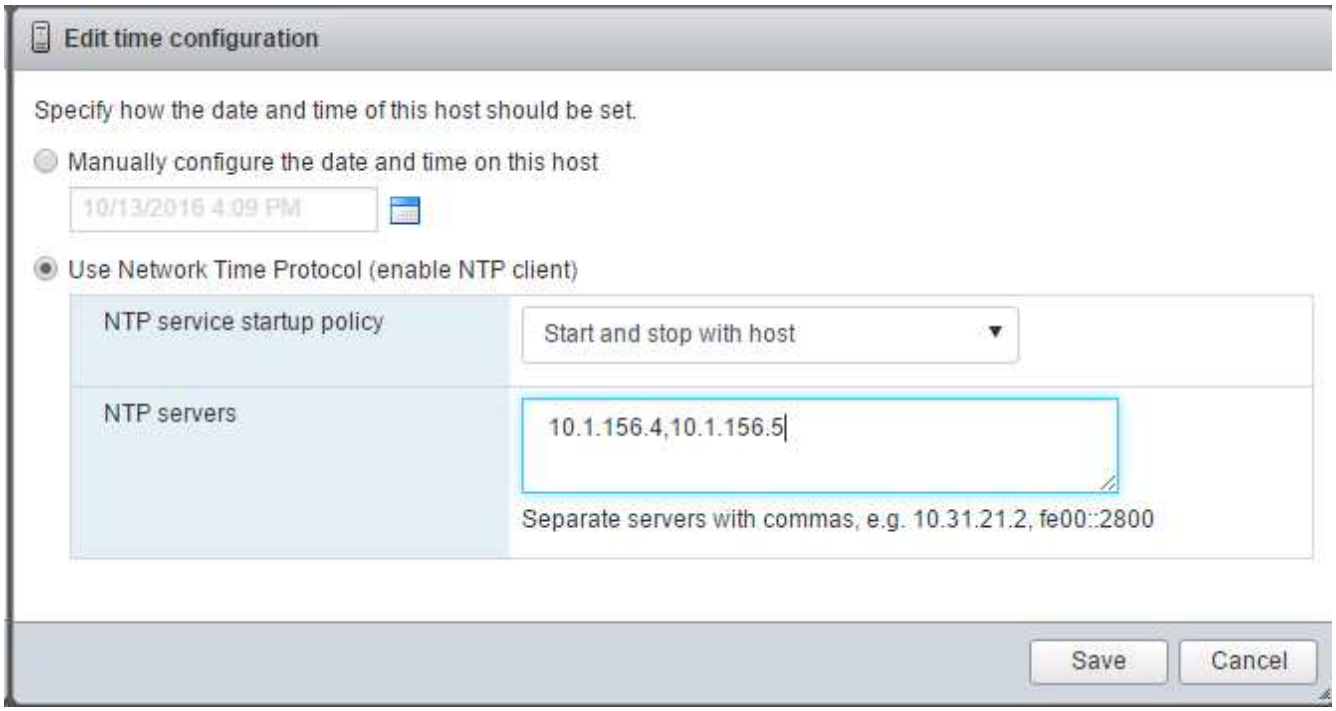
11. Montez les deux datastores sur les deux hôtes ESXi.

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

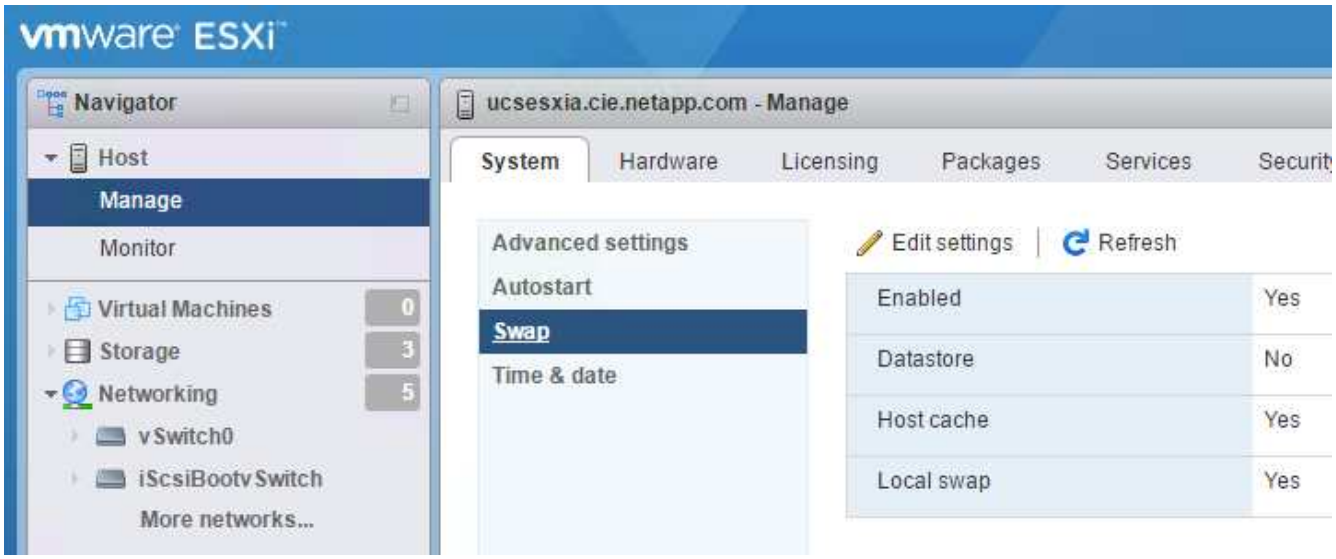
L'heure du serveur NTP peut varier légèrement par rapport à l'heure de l'hôte.

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

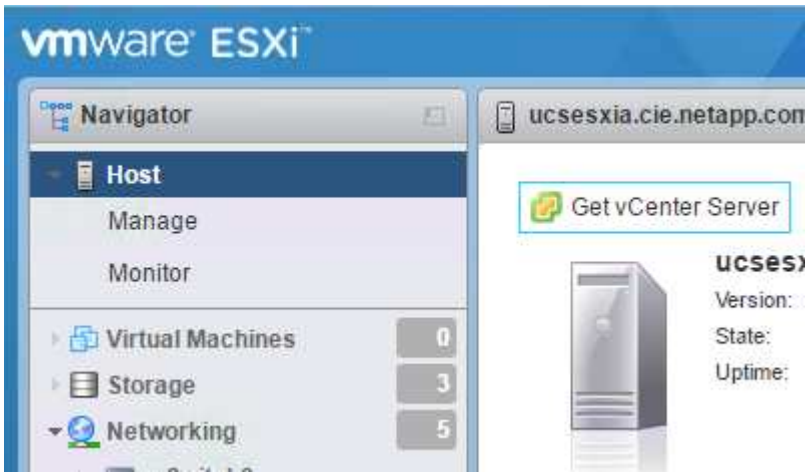
Cette section décrit les procédures détaillées d'installation de VMware vCenter Server 6.7 dans une configuration FlexPod Express.

FlexPod Express utilise VMware vCenter Server Appliance (VCSA).

Installez l'appliance de serveur VMware vCenter

Pour installer VCSA, procédez comme suit :

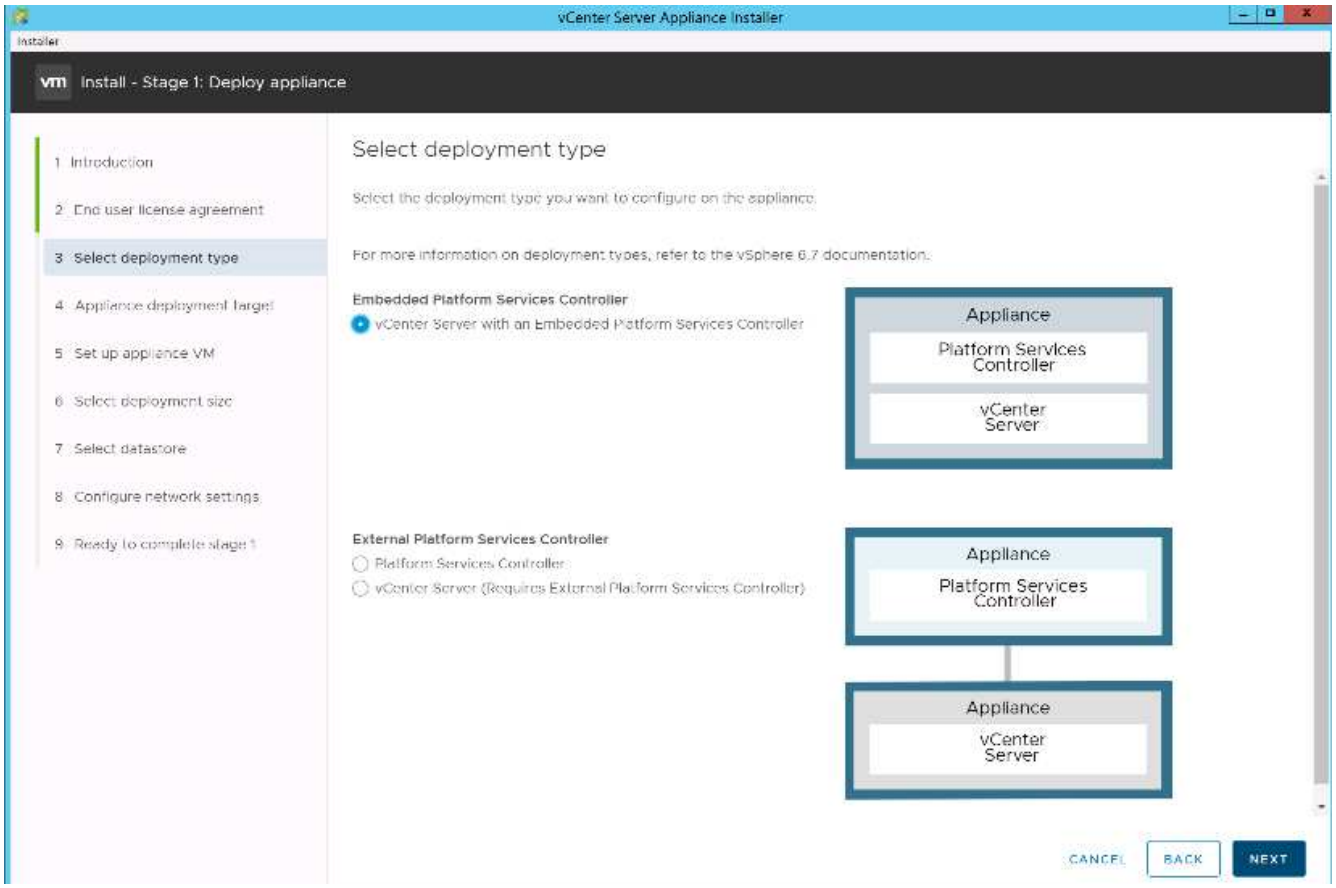
1. Téléchargez le VCSA. Accédez au lien de téléchargement en cliquant sur l'icône obtenir vCenter Server lors de la gestion de l'hôte ESXi.



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

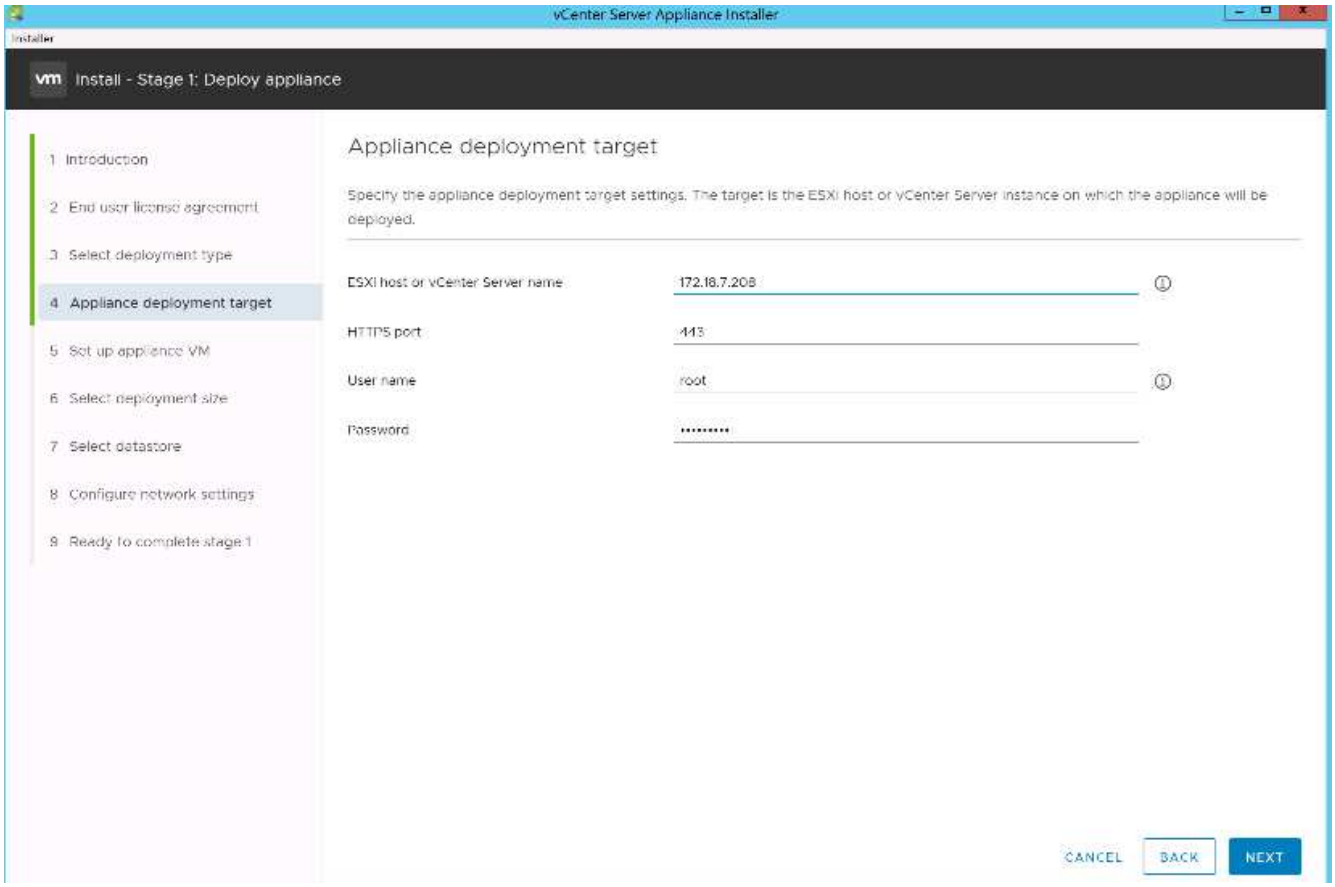
Bien que l'installation de Microsoft Windows vCenter Server soit prise en charge, VMware recommande le VCSA pour les nouveaux déploiements.

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.

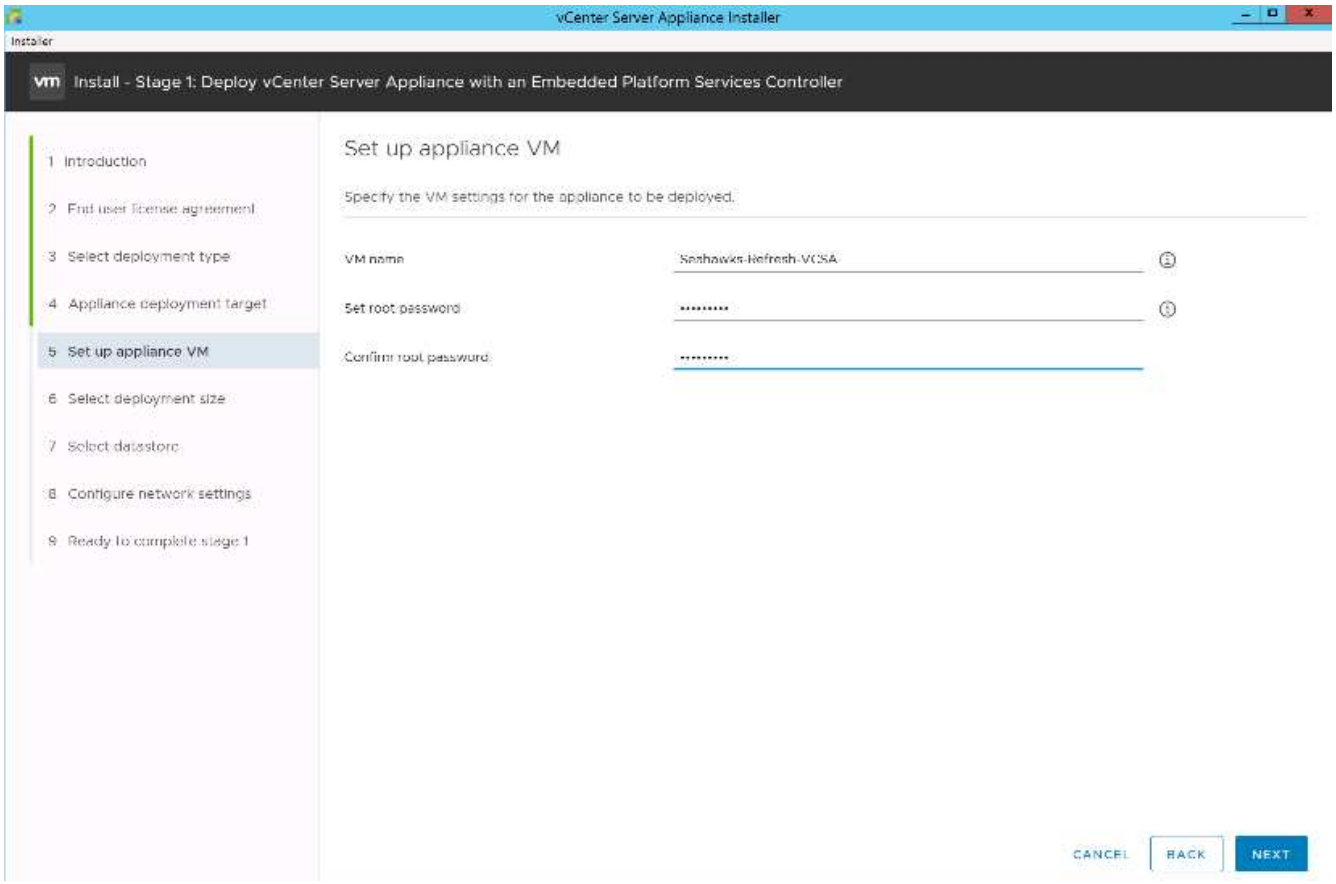


Si nécessaire, le déploiement de contrôleur de services de plateforme externe est également pris en charge dans le cadre de la solution FlexPod Express.

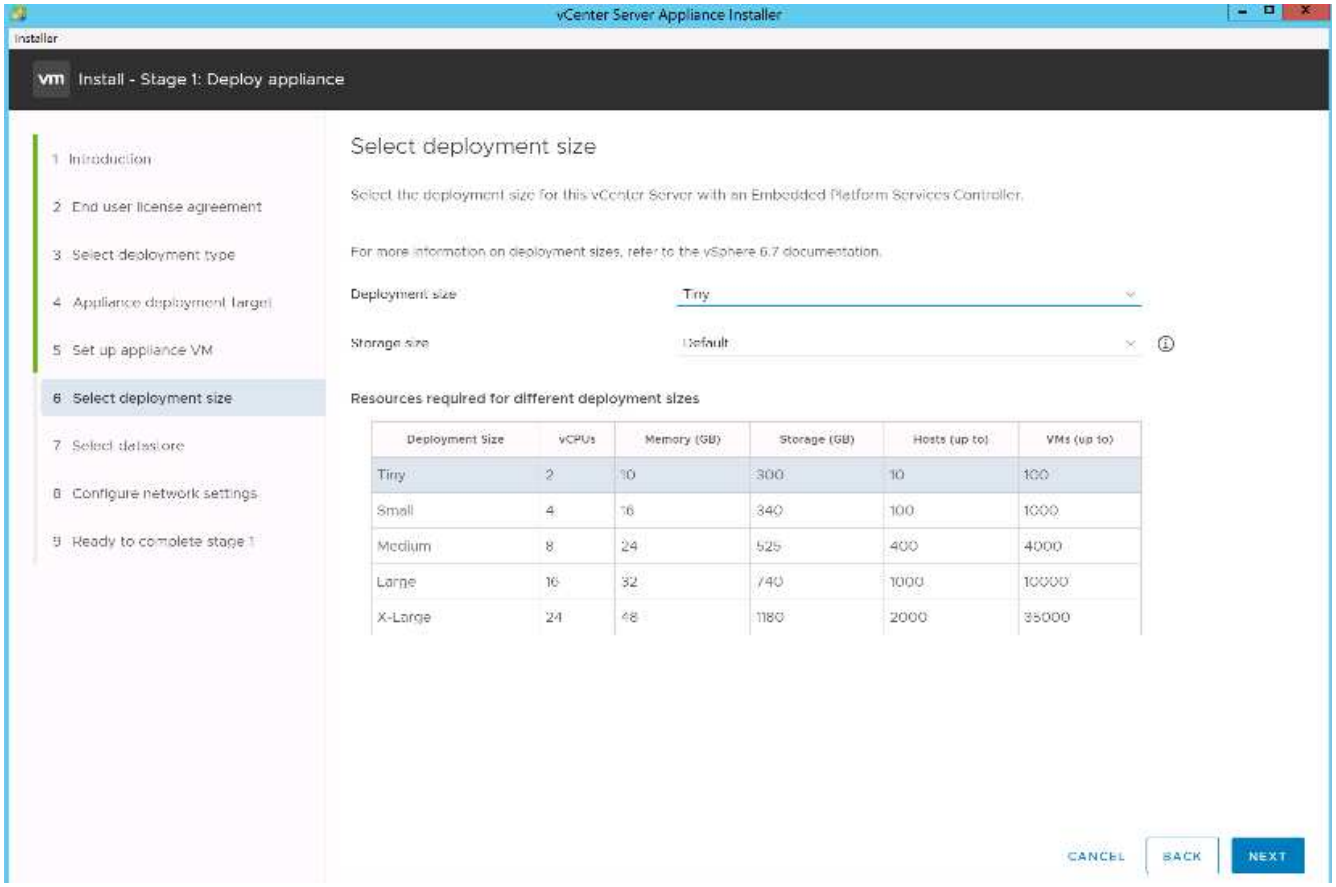
9. Sur la page cible de déploiement de l'appliance, entrez l'adresse IP d'un hôte ESXi déployé, le nom d'utilisateur root et le mot de passe root. Cliquez sur Suivant.



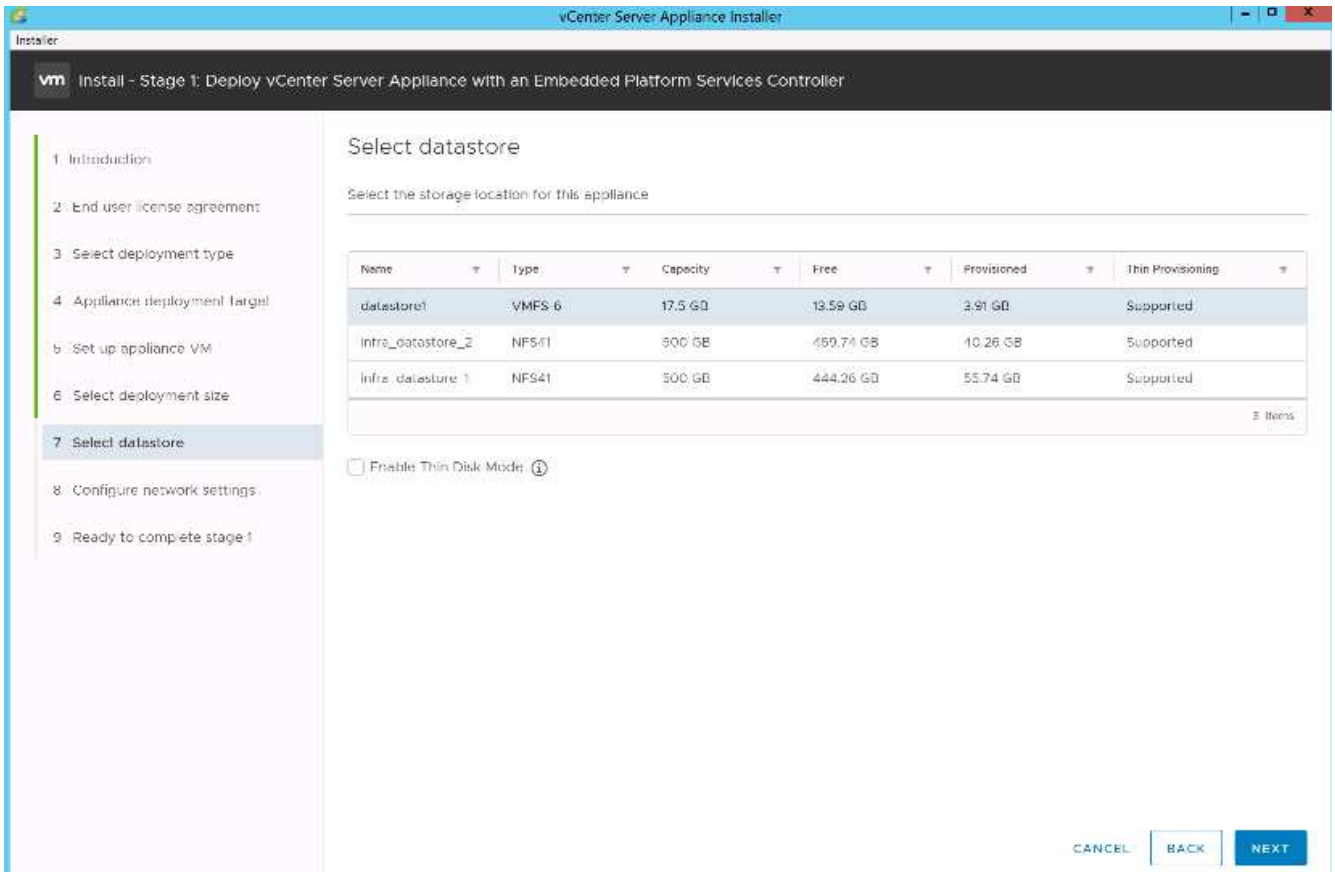
10. Définissez la machine virtuelle de l'appliance en saisissant VCSA comme nom de machine virtuelle et mot de passe root que vous souhaitez utiliser pour le VCSA. Cliquez sur Suivant.



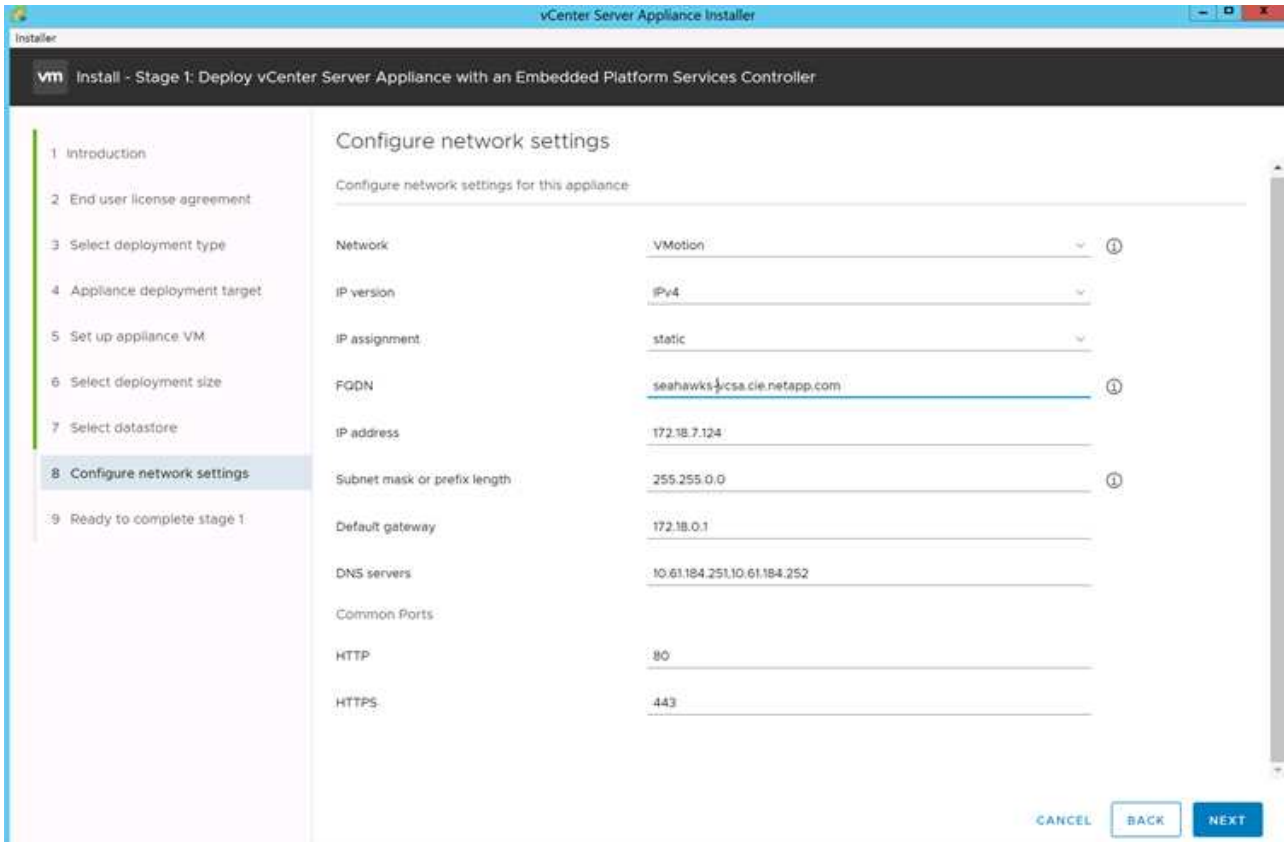
11. Choisissez la taille de déploiement qui correspond le mieux à votre environnement. Cliquez sur Suivant.



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



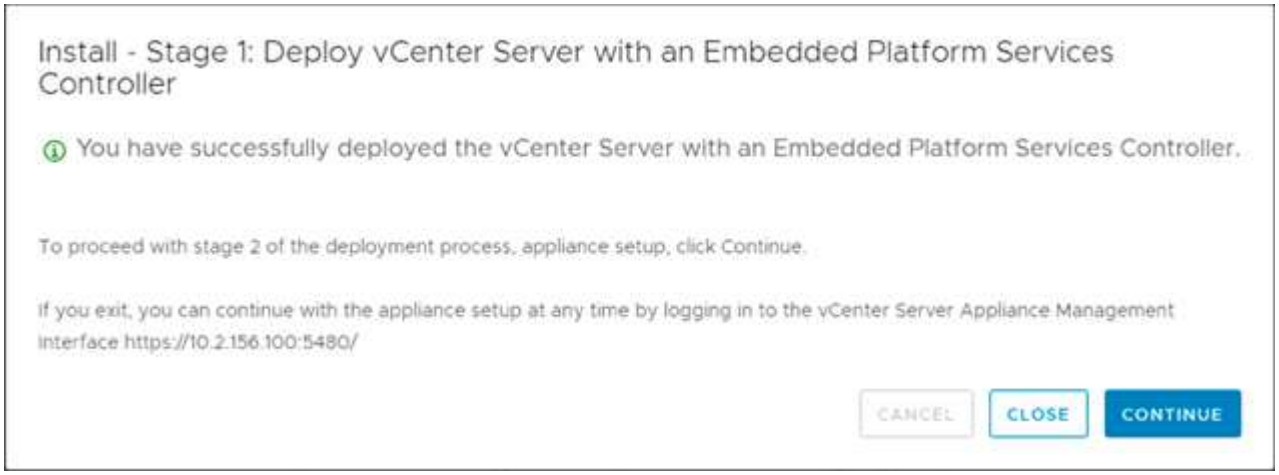
13. Entrez les informations suivantes sur la page configurer les paramètres réseau et cliquez sur Suivant.
    a. Sélectionnez MGMT-Network comme réseau.
    b. Saisissez le nom de domaine complet ou l'adresse IP à utiliser pour le VCSA.
    c. Entrez l'adresse IP à utiliser.
    d. Entrez le masque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

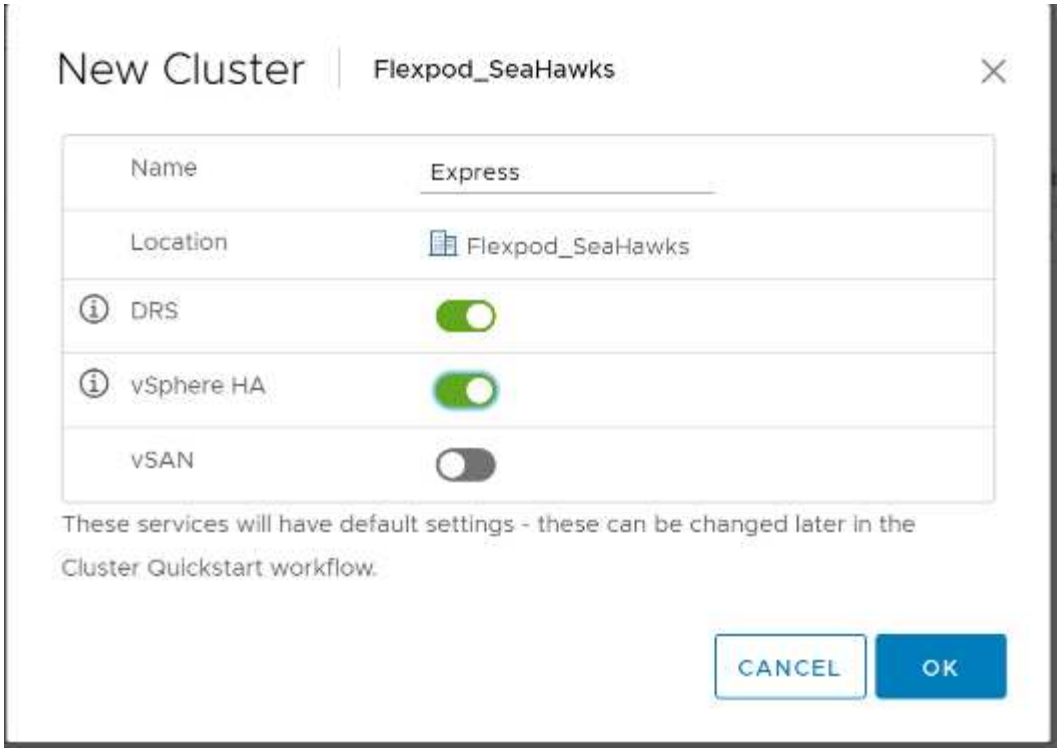
Pour configurer VMware vCenter Server 6.7 et la mise en cluster vSphere, procédez comme suit :

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 :

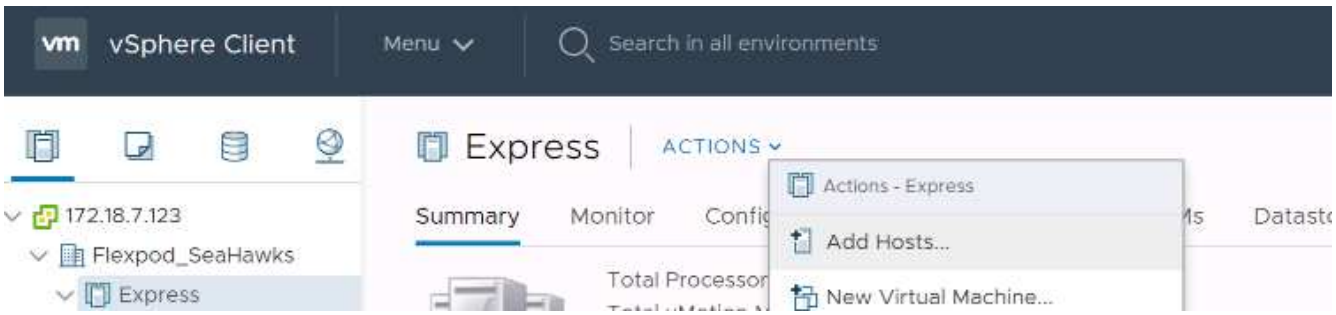
1. Cliquez avec le bouton droit de la souris sur le nouveau centre de données et sélectionnez Nouveau cluster.
2. Indiquez un nom pour le cluster.
3. Sélectionnez et activez les options HA DRS et vSphere.
4. Cliquez sur OK.



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"

FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et NetApp AFF/FAS - NVA - déploiement

Jyh-shing Chen, NetApp

La solution FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et NetApp AFF/FAS exploite des serveurs lames Cisco UCS Mini avec serveurs lames B200 M5, des interconnexions de fabric dans le châssis Cisco UCS 6324, des commutateurs Cisco Nexus 31108PC-V ou d'autres commutateurs compatibles, et NetApp AFF A220, C190 ou la paire haute disponibilité des contrôleurs FAS2700, Qui exécute le logiciel de gestion des données NetApp ONTAP 9.7. Ce document de déploiement d'architecture vérifiée NetApp (NVA) détaille les étapes nécessaires à la configuration des composants d'infrastructure et au déploiement de VMware vSphere 7.0 et des outils associés pour créer une infrastructure virtuelle FlexPod Express hautement fiable et disponible.

"FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et NetApp AFF/FAS - NVA - déploiement"

FlexPod et sécurité

FlexPod, la solution aux attaques par ransomware

Tr-4802 : FlexPod, la solution vers le ransomware

Arvind Ramakrishnan, NetApp

En partenariat avec : 

Pour comprendre un ransomware, il est nécessaire de comprendre d'abord quelques points de clé sur la cryptographie. Les méthodes Cryptographiques permettent le cryptage de données avec une clé secrète partagée (cryptage de clé symétrique) ou une paire de clés (cryptage de clé asymétrique). L'une de ces clés est une clé publique largement disponible et l'autre est une clé privée non divulguée.

Les ransomwares sont un type de malware basé sur la cryptovirologie, c'est-à-dire l'utilisation de la cryptographie pour créer des logiciels malveillants. Ce programme malveillant peut utiliser à la fois le cryptage symétrique et asymétrique des clés pour verrouiller les données d'une victime et exiger une rançon afin de fournir la clé pour décrypter les données de la victime.

Comment les attaques par ransomware fonctionnent-elles ?

Les étapes suivantes décrivent la façon dont les ransomware utilisent la cryptographie pour chiffrer les données de la victime sans recourir au décryptage ou à la restauration par la victime :

1. L'attaquant génère une paire de clés comme dans le chiffrement de clé asymétrique. La clé publique générée est placée dans le programme malveillant et le programme malveillant est ensuite libéré.
2. Une fois le programme malveillant entré dans l'ordinateur ou le système de la victime, il génère une clé symétrique aléatoire à l'aide d'un générateur de nombres pseudorandom (PRNG) ou de tout autre algorithme aléatoire viable.
3. Le programme malveillant utilise cette clé symétrique pour crypter les données de la victime. Il crypte finalement la clé symétrique en utilisant la clé publique de l'attaquant qui était intégrée dans le programme malveillant. La sortie de cette étape est un texte chiffré asymétrique de la clé symétrique chiffrée et du texte chiffré des données de la victime.
4. Le programme malveillant met à zéro (efface) les données de la victime et la clé symétrique qui a été utilisée pour crypter les données, ne laissant ainsi aucune portée pour la récupération.
5. La victime est maintenant affichée le texte chiffré asymétrique de la clé symétrique et une valeur de rançon qui doit être payée afin d'obtenir la clé symétrique qui a été utilisée pour crypter les données.
6. La victime paie la rançon et partage le texte chiffré asymétrique avec l'attaquant. L'attaquant décrypte le texte du corps avec sa clé privée, ce qui donne une clé symétrique.
7. L'attaquant partage cette clé symétrique avec la victime, qui peut être utilisée pour décrypter toutes les données et ainsi récupérer de l'attaque.

À relever

Les individus et les organisations sont confrontés aux challenges suivants lorsqu'ils sont attaqués par des ransomware :

- Le défi le plus important est qu'il a un impact immédiat sur la productivité de l'organisation ou de l'individu. Il faut du temps pour revenir à un état de normalité, car tous les fichiers importants doivent être retrouvés et les systèmes sécurisés.
- Cela pourrait mener à une violation des données qui contient des informations sensibles et confidentielles appartenant à des clients ou clients et entraîner une situation de crise qu'une entreprise veut clairement éviter.
- Il y a de très bonnes chances que les données se trouvent entre de mauvaises mains ou soient effacées complètement, ce qui engendre un point de non-retour qui pourrait être désastreux pour les entreprises et les particuliers.
- Après avoir payé la rançon, il n'y a aucune garantie que l'attaquant fournira la clé pour restaurer les données.
- Il n'y a aucune assurance que l'attaquant s'abstiendra de diffuser les données sensibles malgré le paiement de la rançon.
- Dans les grandes entreprises, l'identification des failles qui ont conduit à une attaque par ransomware est une tâche fastidieuse et la sécurisation de tous les systèmes implique beaucoup d'efforts.

Qui est à risque ?

N'importe qui peut être attaqué par certaines personnes, y compris par des personnes et des grandes entreprises. Les entreprises qui ne mettent pas en œuvre de mesures et de pratiques de sécurité bien définies sont encore plus vulnérables à de telles attaques. L'effet de l'attaque sur une grande organisation peut être plusieurs fois plus important que ce qu'un individu peut supporter.

Les attaques par ransomware représentent environ 28 % de toutes les attaques de malware. En d'autres termes, plus d'un incident sur quatre est un ransomware. Les ransomwares peuvent se propager automatiquement et de manière discriminatoire à travers Internet, et lorsqu'il y a un retard de sécurité, ils peuvent entrer dans les systèmes de la victime et continuer de se propager à d'autres systèmes connectés. Les pirates informatiques ont tendance à cibler des personnes ou des entreprises qui effectuent énormément de partages de fichiers, à disposer de données sensibles ou essentielles, ou à conserver une protection inadéquate contre les attaques.

Les attaquants ont tendance à se concentrer sur les cibles potentielles suivantes :

- Universités et communautés d'étudiants
- Administrations et agences gouvernementales
- Hôpitaux
- Banques

Il ne s'agit pas d'une liste exhaustive des cibles. Vous ne pouvez pas vous protéger des attaques si vous vous trouvez en dehors de l'une de ces catégories.

Comment les ransomwares entrent-ils dans un système ou se propagent-ils ?

Il existe plusieurs façons dont les ransomwares peuvent entrer un système ou se propager à d'autres systèmes. Dans le monde d'aujourd'hui, presque tous les systèmes sont reliés les uns aux autres par l'intermédiaire d'Internet, de réseaux locaux, de réseaux WAN, etc. La quantité de données générées et

échangées entre ces systèmes ne cesse d'augmenter.

Parmi les méthodes les plus courantes par lesquelles les ransomwares peuvent être répartis, elles peuvent être utilisées quotidiennement pour partager ou accéder aux données :

- E-mail
- Réseaux P2P
- Téléchargements de fichiers
- Réseaux sociaux
- Appareils mobiles
- Connexion à des réseaux publics non sécurisés
- Accéder aux URL Web

Conséquences de la perte de données

Les conséquences ou les effets d'une perte de données peuvent se faire plus largement que ce que pourrait prévoir les entreprises. Les effets peuvent varier en fonction de la durée des temps d'arrêt ou de la période pendant laquelle une entreprise n'a pas accès à ses données. Plus l'attaque perdure longtemps, plus l'effet sur le chiffre d'affaires, la marque et la réputation de l'organisation est important. Une organisation peut aussi faire face à des problèmes juridiques et à un déclin important de la productivité.

Alors que ces questions persistent au fil du temps, elles commencent à s'agrandir et peuvent finir par changer la culture d'une organisation, selon la manière dont elle répond à l'attaque. Dans le monde d'aujourd'hui, l'information se répand rapidement et les nouvelles négatives sur une organisation pourraient causer des dommages permanents à sa réputation. Une entreprise peut être confrontée à de lourdes pénalités en cas de perte de données, ce qui pourrait éventuellement mener à la clôture de ses activités.

Effets financiers

Selon un récent "Rapport McAfee", Les coûts globaux encourus en raison de la cybercriminalité représentent environ 600 milliards de dollars, soit environ 0.8% du PIB mondial. Lorsque ce montant est comparé à la croissance mondiale de l'économie Internet de 4.2 billions de dollars, il équivaut à une taxe de 14% sur la croissance.

Une attaque par ransomware prend une part importante de ce coût financier. En 2018, les coûts encourus en raison d'attaques par ransomware étaient de l'ordre de 8 milliards—, un montant prévu pour atteindre 11.5 milliards de dollars en 2019.

Quelle est la solution ?

La récupération suite à une attaque par ransomware avec un temps d'indisponibilité minimal est uniquement possible grâce à la mise en œuvre d'un plan de reprise après incident proactif. Avoir la capacité de récupérer après une attaque est bon, mais la prévention d'une attaque est tout à fait idéale.

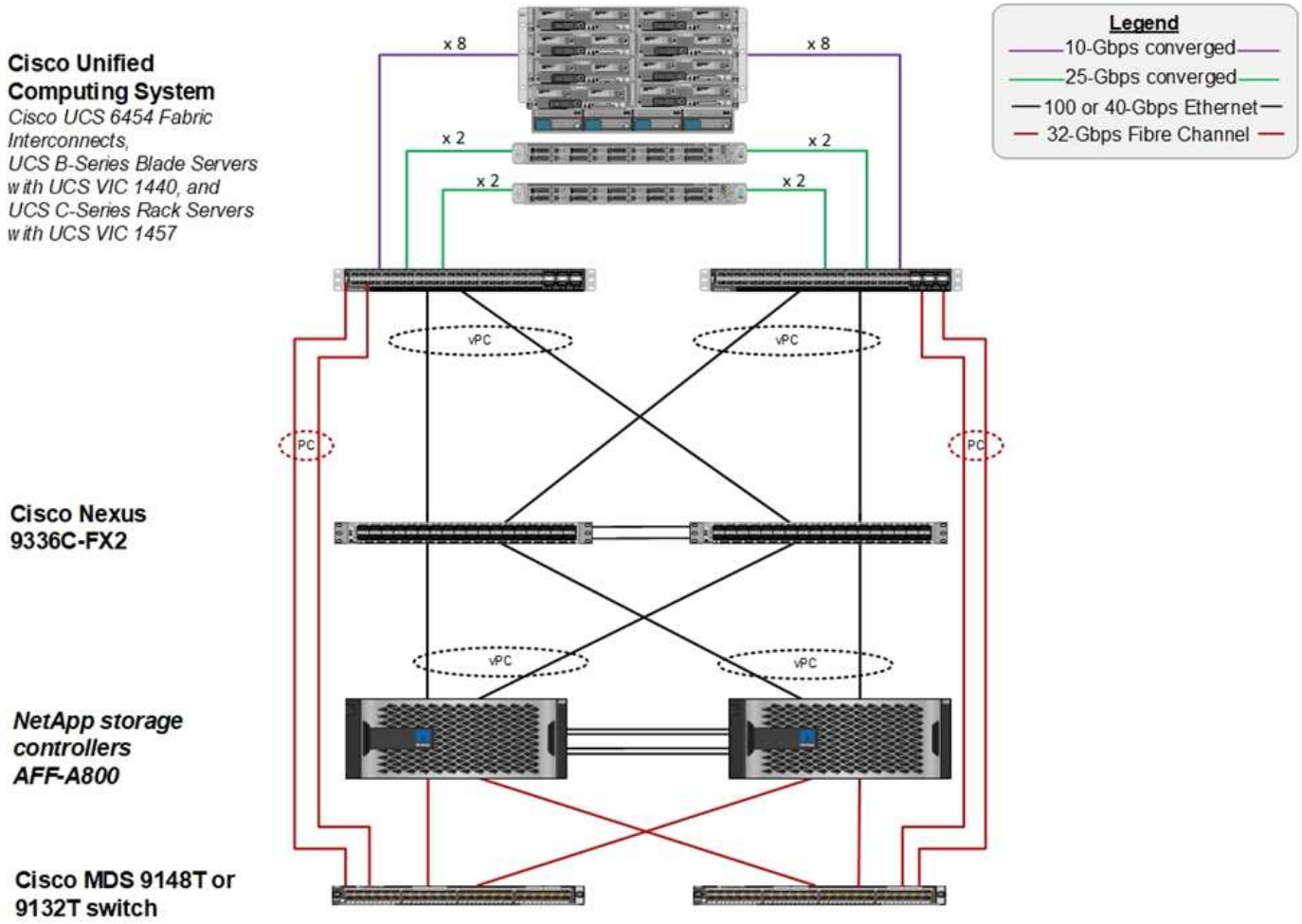
Bien que vous deviez examiner plusieurs fronts et corriger pour prévenir une attaque, le centre de données est le composant principal qui vous permet d'éviter ou de récupérer après une attaque.

La conception du data Center et les fonctionnalités fournies pour sécuriser les terminaux de réseau, de calcul et de stockage jouent un rôle essentiel dans la mise en place d'un environnement sécurisé pour les opérations quotidiennes. Ce document explique comment les fonctions d'une infrastructure de cloud hybride FlexPod peuvent vous aider à restaurer rapidement vos données en cas d'attaque et à éviter les attaques.

Présentation de FlexPod

FlexPod est une architecture préconçue, intégrée et validée qui combine les serveurs Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus, les commutateurs Cisco MDS Fabric et les baies de stockage NetApp dans une architecture unique et flexible. Les solutions FlexPod sont conçues pour la haute disponibilité sans points de défaillance uniques, tout en garantissant à moindre coût et flexibilité de conception afin de prendre en charge un large éventail de charges de travail. Une conception FlexPod peut prendre en charge plusieurs hyperviseurs et serveurs sans système d'exploitation. Elle peut également être dimensionnée et optimisée en fonction des exigences des charges de travail des clients.

La figure ci-dessous illustre l'architecture FlexPod et met en évidence la haute disponibilité sur l'ensemble des couches de la pile. Les composants d'infrastructure du stockage, du réseau et du calcul sont configurés de telle sorte que les opérations puissent basculer instantanément vers le partenaire survivant en cas de panne de l'un des composants.



L'un des principaux avantages d'un système FlexPod est qu'il est prédéfini, intégré et validé pour plusieurs charges de travail. Des guides détaillés de conception et de déploiement sont publiés pour chaque validation des solutions. Ces documents comprennent les bonnes pratiques à suivre pour exécuter des charges de travail de façon transparente sur FlexPod. Ces solutions sont construites avec les meilleurs produits de calcul, de réseau et de stockage, ainsi qu'avec un ensemble de fonctionnalités dédiées à la sécurité et au renforcement de l'ensemble de l'infrastructure.

"Indice X-Force Threat Intelligence d'IBM" états-unis, « l'erreur humaine responsable des deux tiers des enregistrements compromis, y compris l'historique 424 % des erreurs de configuration dans l'infrastructure cloud ».

Avec un système FlexPod, vous pouvez éviter toute erreur de configuration de votre infrastructure grâce à l'automatisation, via des playbooks Ansible qui réalisent une configuration de bout en bout de l'infrastructure selon les meilleures pratiques décrites dans les conceptions validées de Cisco (CVD) et les architectures vérifiées NetApp (NVA).

Mesures de protection par ransomware

Cette section présente les principales fonctionnalités du logiciel de gestion des données NetApp ONTAP, ainsi que les outils pour Cisco UCS et Cisco Nexus que vous pouvez utiliser pour protéger et récupérer efficacement contre les attaques par ransomware.

Stockage : NetApp ONTAP

Le logiciel ONTAP offre de nombreuses fonctionnalités utiles pour la protection des données, dont la plupart sont gratuites pour les clients qui disposent d'un système ONTAP. Vous pouvez à tout moment utiliser les fonctions suivantes pour protéger les données d'attaques :

- **Technologie NetApp Snapshot.** Une copie Snapshot est une image en lecture seule d'un volume qui capture l'état d'un système de fichiers à un moment donné. Ces copies aident à protéger les données sans affecter les performances du système et elles n'occupent pas autant d'espace de stockage important. NetApp vous recommande de créer un calendrier pour la création de copies Snapshot. Vous devez également maintenir un temps de rétention long car certains programmes malveillants peuvent rester inactifs puis réactiver des semaines ou des mois après une infection. En cas d'attaque, le volume peut être restauré à l'aide d'une copie Snapshot prise avant l'infection.
- **Technologie NetApp SnapRestore.** le logiciel de restauration des données SnapRestore est extrêmement utile pour restaurer les données en cas de corruption ou pour restaurer uniquement le contenu des fichiers. SnapRestore ne rétablit pas les attributs d'un volume. Elle est bien plus rapide que ce que peut obtenir un administrateur en copiant les fichiers à partir de la copie Snapshot vers le système de fichiers actif. La vitesse à laquelle les données peuvent être restaurées est utile lorsque de nombreux fichiers doivent être restaurés aussi rapidement que possible. En cas d'attaque, ce processus de restauration hautement efficace permet de remettre rapidement les activités en ligne.
- **Technologie NetApp SnapCenter**.* le logiciel SnapCenter utilise des fonctions de sauvegarde et de réplication basées sur le stockage NetApp pour assurer une protection des données cohérente au niveau des applications. Ce logiciel s'intègre aux applications d'entreprise et fournit des flux de production spécifiques aux applications et aux bases de données afin de répondre aux besoins des administrateurs d'applications, de bases de données et d'infrastructure virtuelle. SnapCenter fournit une plateforme qui permet de coordonner et de gérer facilement et en toute sécurité la protection de vos données sur l'ensemble des applications, bases de données et systèmes de fichiers. La capacité à fournir une protection des données cohérente au niveau des applications est primordiale lors de la restauration des données, car elle permet de restaurer facilement les applications dans un état cohérent plus rapidement.
- **Technologie NetApp SnapLock.** SnapLock fournit un volume spécial dans lequel les fichiers peuvent être stockés dans un état non réinscriptibles et non effaçables. Les données de production de l'utilisateur résidant dans un volume FlexVol peuvent être mises en miroir ou archivées sur un volume SnapLock grâce respectivement à la technologie NetApp SnapMirror ou SnapVault. Les fichiers du volume SnapLock, le volume lui-même et son agrégat d'hébergement ne peuvent pas être supprimés avant la fin de la période de conservation.
- **Technologie NetApp FPolicy.** utilisez le logiciel FPolicy pour éviter les attaques en désautorisant des opérations sur des fichiers avec des extensions spécifiques. Un événement FPolicy peut être déclenché

pour des opérations de fichiers spécifiques. L'événement est lié à une politique, qui appelle le moteur qu'il doit utiliser. Vous pouvez configurer une règle avec un ensemble d'extensions de fichiers qui pourraient éventuellement contenir un ransomware. Lorsqu'un fichier doté d'une extension non autorisée tente d'effectuer une opération non autorisée, FPolicy empêche cette opération.

Réseau : Cisco Nexus

Le logiciel Cisco NX OS prend en charge la fonctionnalité NetFlow qui permet une détection améliorée des anomalies et de la sécurité du réseau. NetFlow capture les métadonnées de chaque conversation sur le réseau, les parties impliquées dans la communication, le protocole utilisé et la durée de la transaction. Une fois les informations agrégées et analysées, elles permettent de mieux comprendre le comportement normal.

Les données collectées permettent également d'identifier des modèles d'activité douteux, tels que les programmes malveillants, qui s'étendent sur le réseau, qui peuvent autrement passer inaperçues.

NetFlow utilise des flux pour fournir des statistiques sur la surveillance du réseau. Un flux est un flux unidirectionnel de paquets arrivant sur une interface source (ou VLAN) et possède les mêmes valeurs pour les clés. Une clé est une valeur identifiée pour un champ dans le paquet. Vous créez un flux à l'aide d'un enregistrement de flux pour définir les clés uniques de votre flux. Vous pouvez exporter les données collectées par NetFlow pour vos flux à l'aide d'un exportateur de flux vers un collecteur NetFlow distant, tel que Cisco StealthWatch. StealthWatch exploite ces informations pour assurer une surveillance continue du réseau et fournit une détection en temps réel des menaces et une analyse des réponses aux incidents en cas d'attaque par ransomware.

Calcul : Cisco UCS

Cisco UCS est le terminal de calcul d'une architecture FlexPod. Vous pouvez utiliser plusieurs produits Cisco qui contribuent à sécuriser cette couche de la pile au niveau du système d'exploitation.

Vous pouvez implémenter les produits clés suivants dans la couche de calcul ou d'application :

- **Cisco Advanced Malware protection (AMP) pour les noeuds finaux.** pris en charge sur les systèmes d'exploitation Microsoft Windows et Linux, cette solution intègre des capacités de prévention, de détection et de réponse. Ce logiciel de sécurité évite les failles de sécurité, bloque les programmes malveillants au point d'entrée et surveille et analyse en continu les activités des fichiers et des processus afin de détecter, de contenir et de corriger rapidement les menaces qui peuvent échapper aux défenses en première ligne.

  Le composant de protection contre les activités malveillantes (MAP) de l'AMP surveille en permanence toute l'activité des points finaux et assure la détection des temps d'exécution et le blocage du comportement anormal d'un programme en cours d'exécution sur le point final. Par exemple, lorsque le comportement de terminal indique un ransomware, les processus incriminés se terminent, ce qui empêche le chiffrement du terminal et arrête l'attaque.

- **Cisco Advanced Malware protection for Email Security.** les e-mails sont devenus le véhicule de premier choix pour la propagation des programmes malveillants et l'exécution des cyber-attaques. En moyenne, environ 100 milliards d'e-mails sont échangés en une seule journée, ce qui fournit aux pirates un excellent vecteur de pénétration dans les systèmes des utilisateurs. Par conséquent, il est absolument essentiel de se défendre contre cette ligne d'attaque.

  AMP analyse les e-mails contre les menaces, telles que les attaques sans jour et les logiciels malveillants furtifs cachés dans des pièces jointes malveillantes. Il utilise également des informations URL de pointe pour lutter contre les liens malveillants. Elle offre aux utilisateurs une protection avancée contre le phishing ciblé, les attaques par ransomware et d'autres attaques sophistiquées.

- **Système de prévention des intrusions nouvelle génération (NGIPS).** Cisco FirePOWER NGIPS peut

être déployé en tant qu'appliance physique dans le centre de données ou en tant qu'appliance virtuelle sur VMware (NGIPSv pour VMware). Ce système hautement efficace de prévention des intrusions offre des performances fiables et un faible coût total de possession. La protection contre les menaces peut être étendue avec des licences d'abonnement facultatives pour fournir AMP, visibilité et contrôle des applications, ainsi que des fonctionnalités de filtrage des URL. Le système NGIPS virtualisé inspecte le trafic entre les machines virtuelles et facilite le déploiement et la gestion des solutions NGIPS sur des sites disposant de ressources limitées, ce qui renforce la protection des ressources physiques et virtuelles.

Protégez et restaurez les données sur FlexPod

Cette section décrit comment les données d'un utilisateur final peuvent être récupérées en cas d'attaque et comment empêcher les attaques à l'aide d'un système FlexPod.

Présentation du banc d'essai

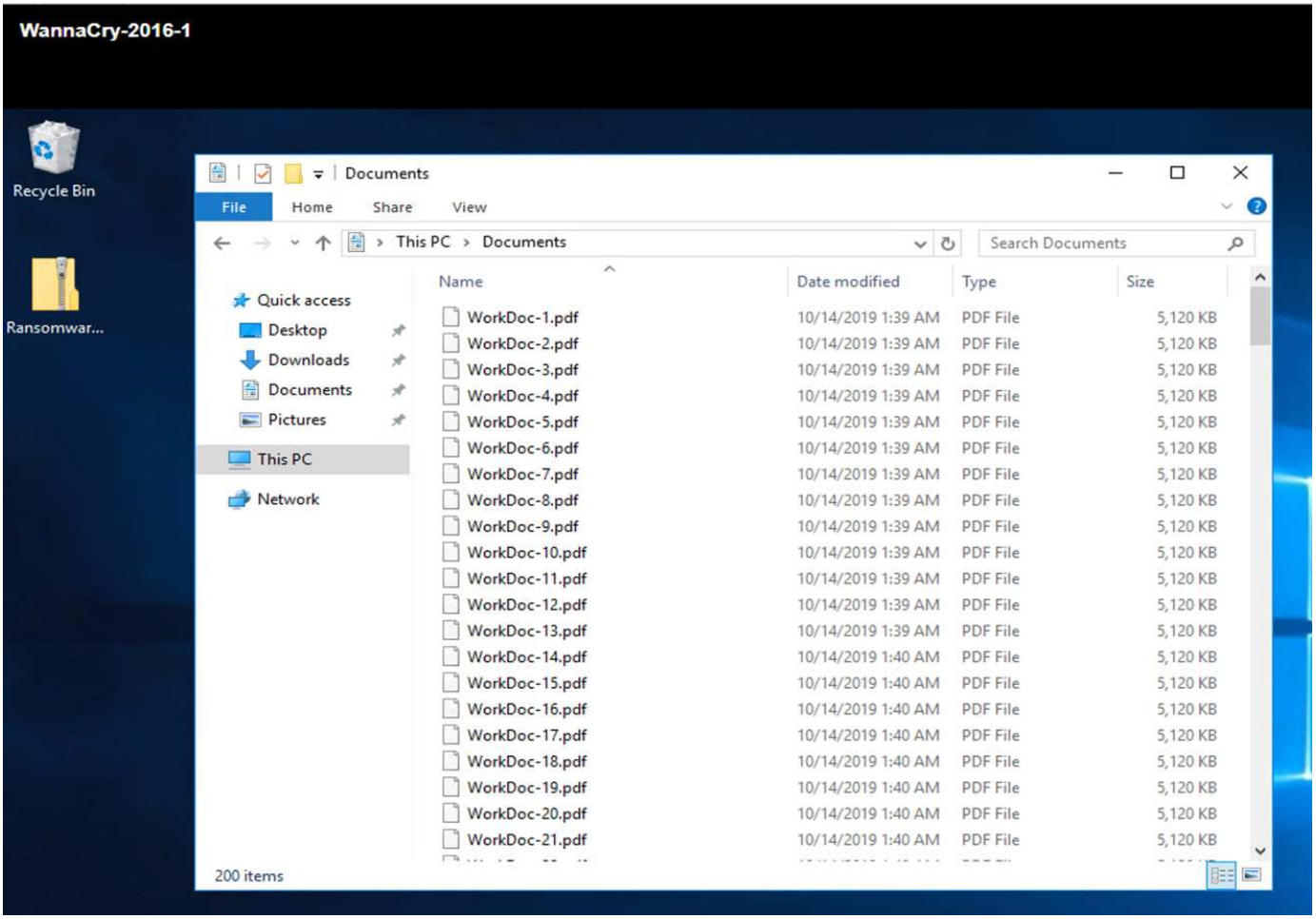
Pour mettre en avant la détection, la résolution et la prévention des problèmes liés à FlexPod, un banc d'essai a été créé à partir des directives spécifiées dans les guides CVD de la dernière plateforme disponibles au moment de l'élaboration de ce document : "CVD FlexPod Datacenter avec VMware vSphere 6.7 U1, Cisco UCS de 4e génération et NetApp AFF A-Series".

Une machine virtuelle Windows 2016, qui fournissait un partage CIFS à partir du logiciel NetApp ONTAP, a été déployée dans l'infrastructure VMware vSphere. Ensuite, NetApp FPolicy a été configuré sur le partage CIFS pour éviter l'exécution de fichiers avec certains types d'extensions. Le logiciel NetApp SnapCenter a également été déployé pour gérer les copies Snapshot des serveurs virtuels au sein de l'infrastructure afin d'offrir des copies Snapshot cohérentes au niveau des applications.

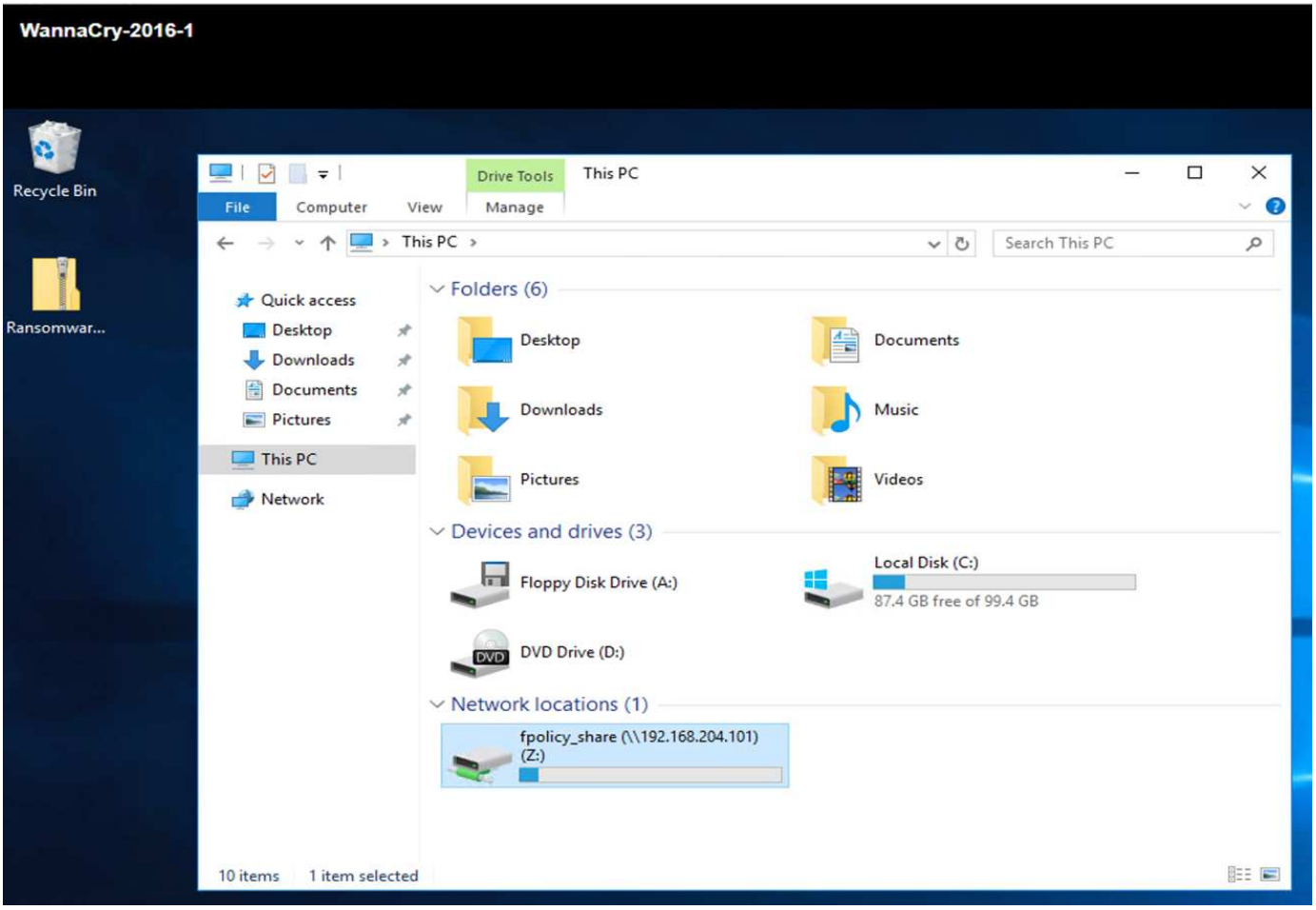
État du serveur virtuel et de ses fichiers avant une attaque

Cette section décrit l'état des fichiers avant une attaque sur la machine virtuelle et le partage CIFS qui lui a été mappé.

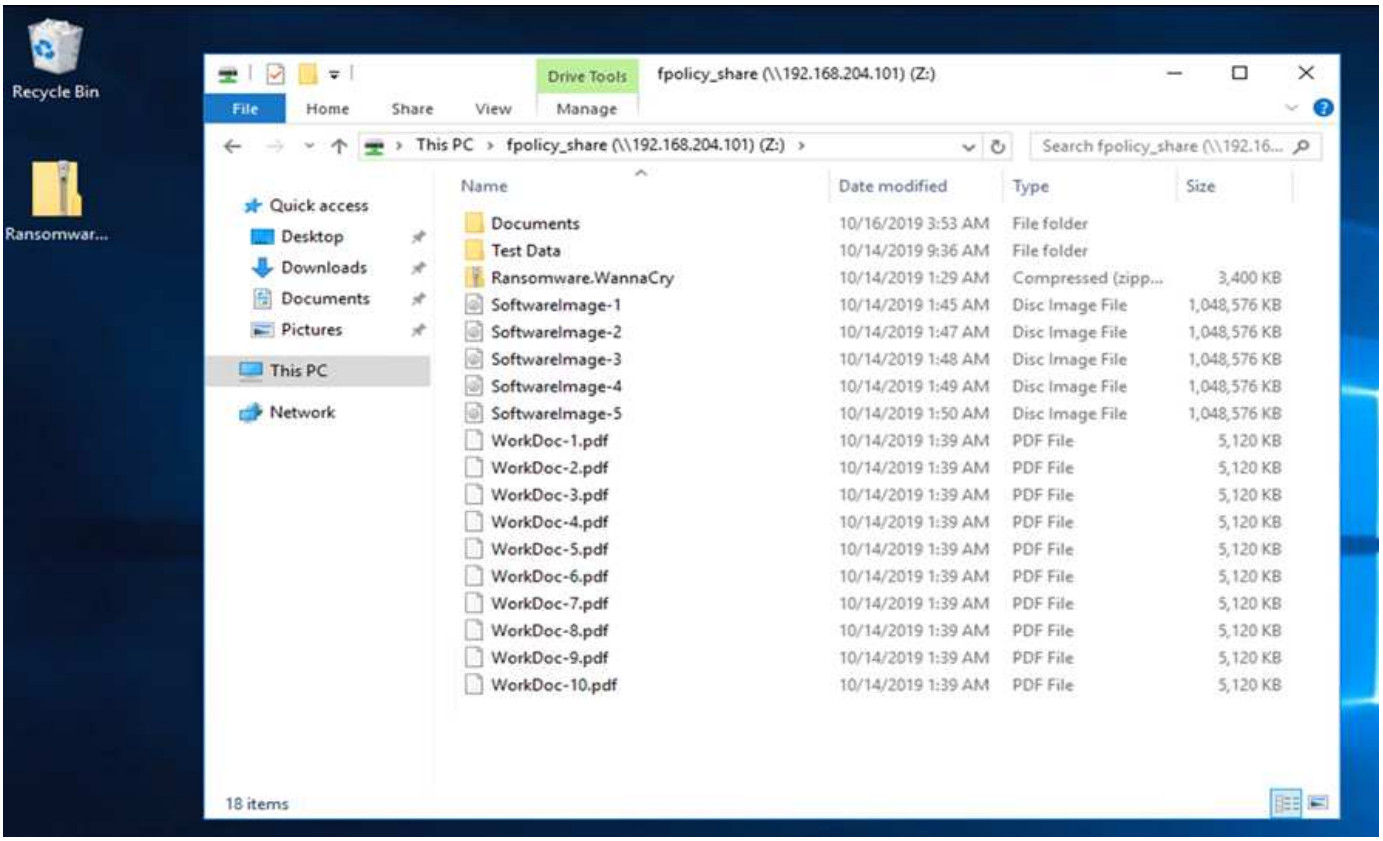
Le dossier documents de la machine virtuelle contient un ensemble de fichiers PDF qui n'ont pas encore été cryptés par le programme malveillant WannaCry.



La capture d’écran suivante montre le partage CIFS qui a été mappé sur la machine virtuelle.



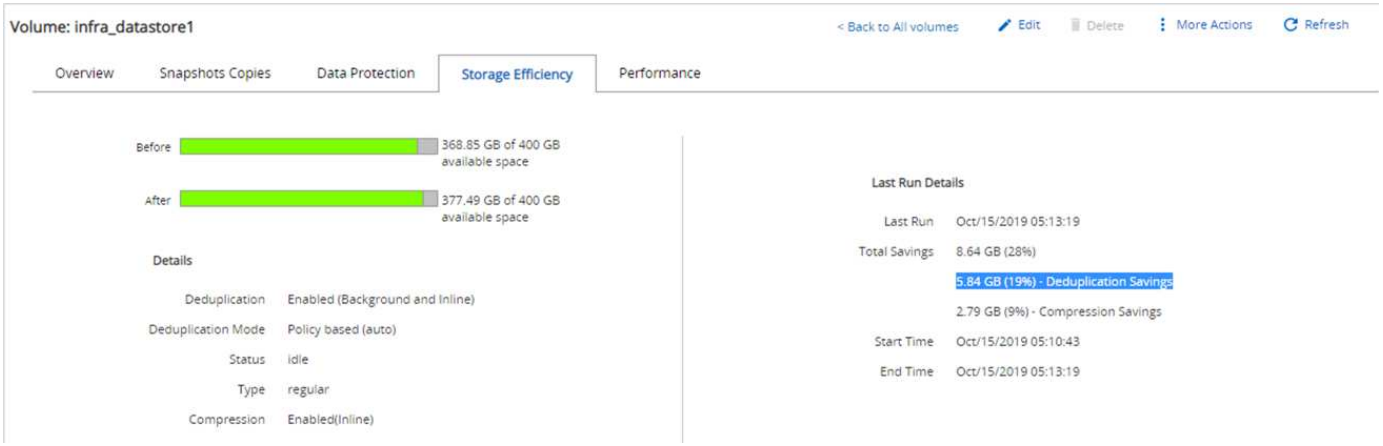
La capture d’écran suivante présente les fichiers du partage CIFS `fpolicy_share` Cela n’a pas encore été chiffré par le programme malveillant de WannaCry.



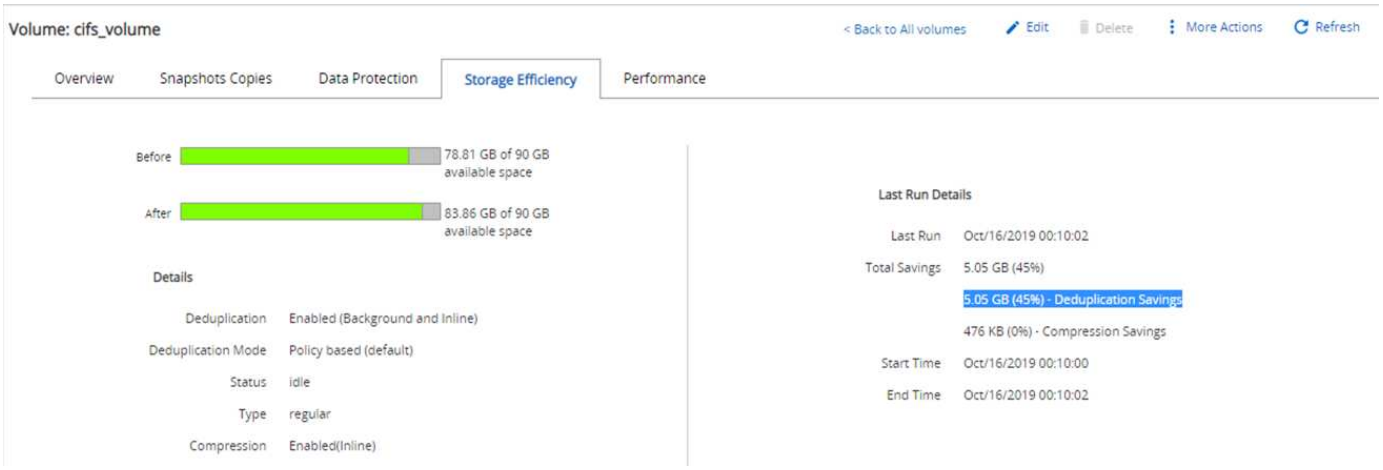
Informations relatives à la déduplication et aux snapshots avant la crise

Les détails sur l'efficacité du stockage et la taille de la copie Snapshot avant une attaque sont indiqués et utilisés comme référence lors de la phase de détection.

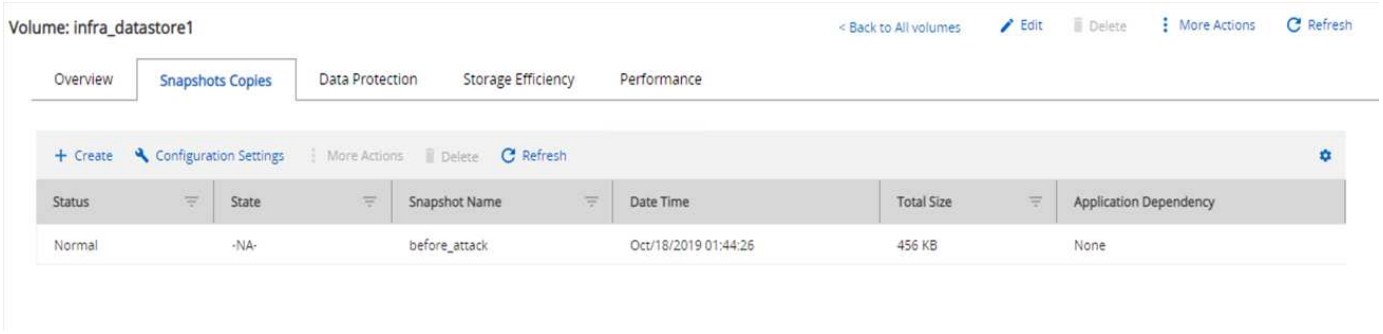
Des économies de stockage de 19 % ont été réalisées grâce à la déduplication sur le volume hébergeant la machine virtuelle.



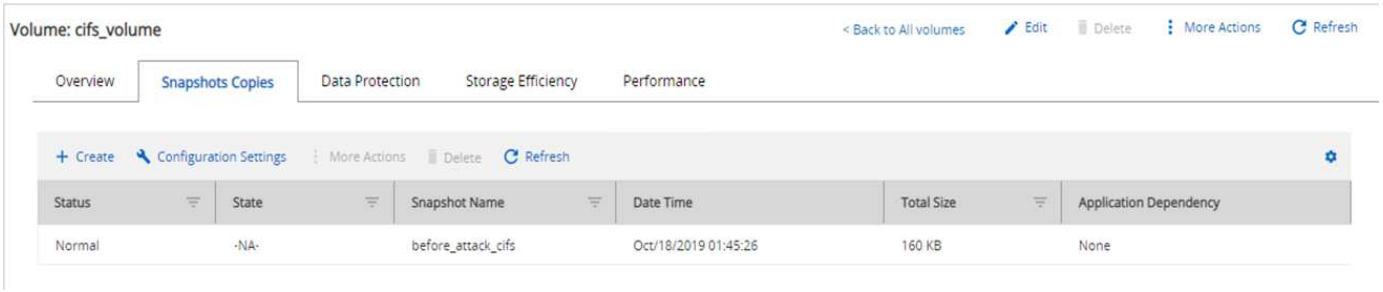
Des économies de stockage de 45 % ont été réalisées grâce à la déduplication sur le partage CIFS `fpolicy_share`.



Une taille de copie Snapshot de 456 Ko a été observée pour le volume hébergeant la machine virtuelle.



Une taille de copie Snapshot de 160 Ko a été observée pour le partage CIFS `fpolicy_share`.



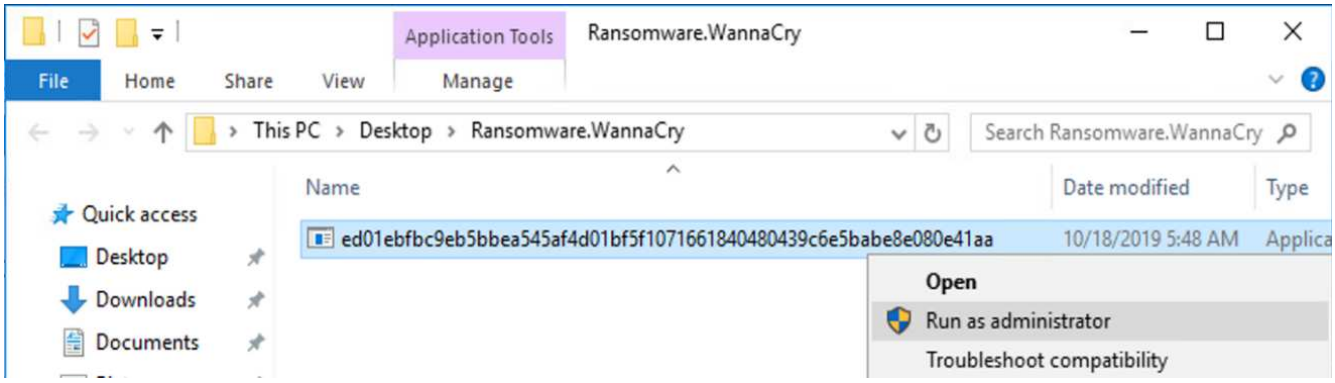
Infection de WannaCry sur VM et partage CIFS

Dans cette section, nous montrons comment le programme malveillant WannaCry a été introduit dans l'environnement FlexPod et les changements ultérieurs au système observés.

Les étapes suivantes montrent comment le binaire du programme malveillant WannaCry a été introduit dans la VM :

1. Le programme malveillant sécurisé a été extrait.

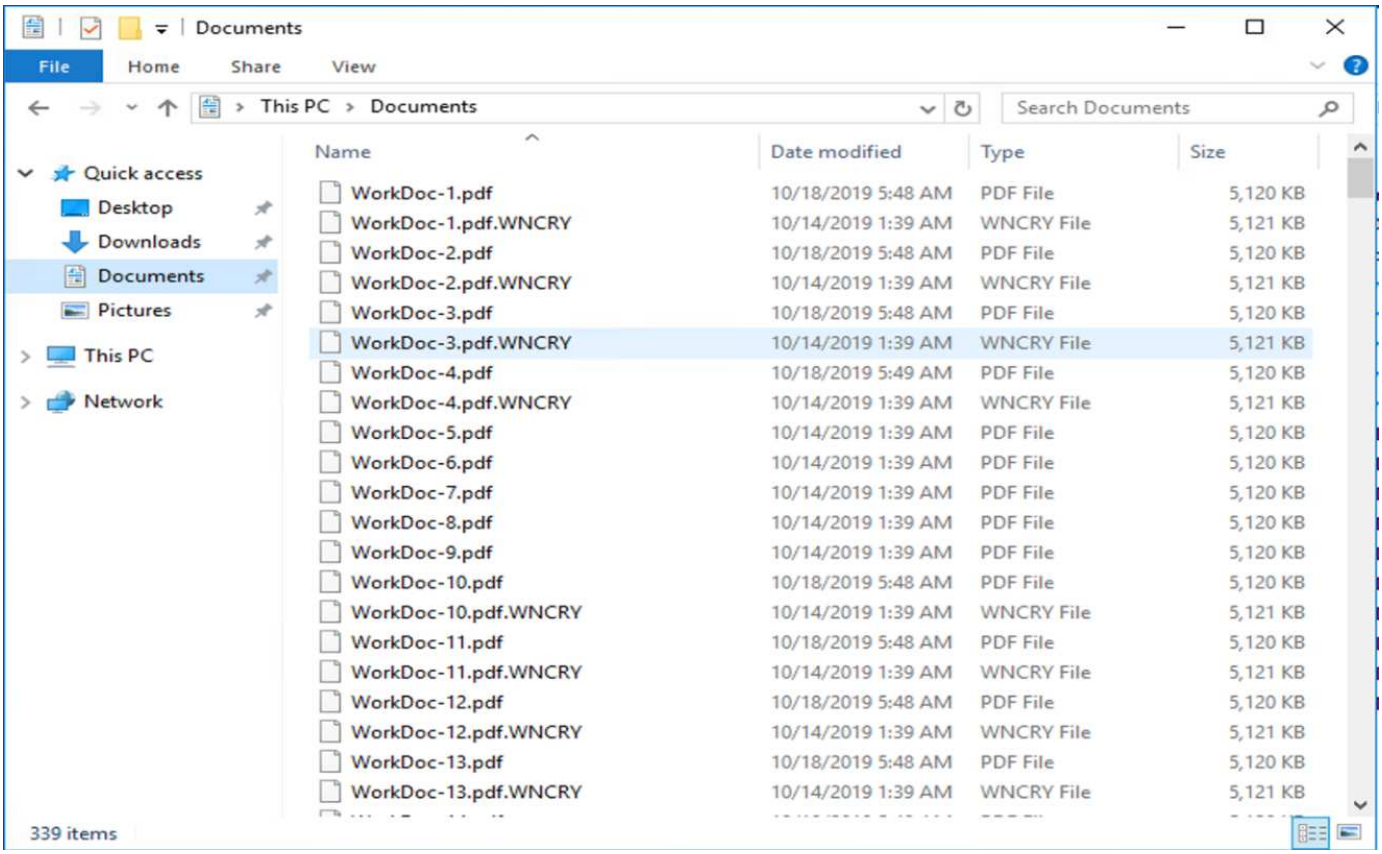
2. Le binaire a été exécuté.



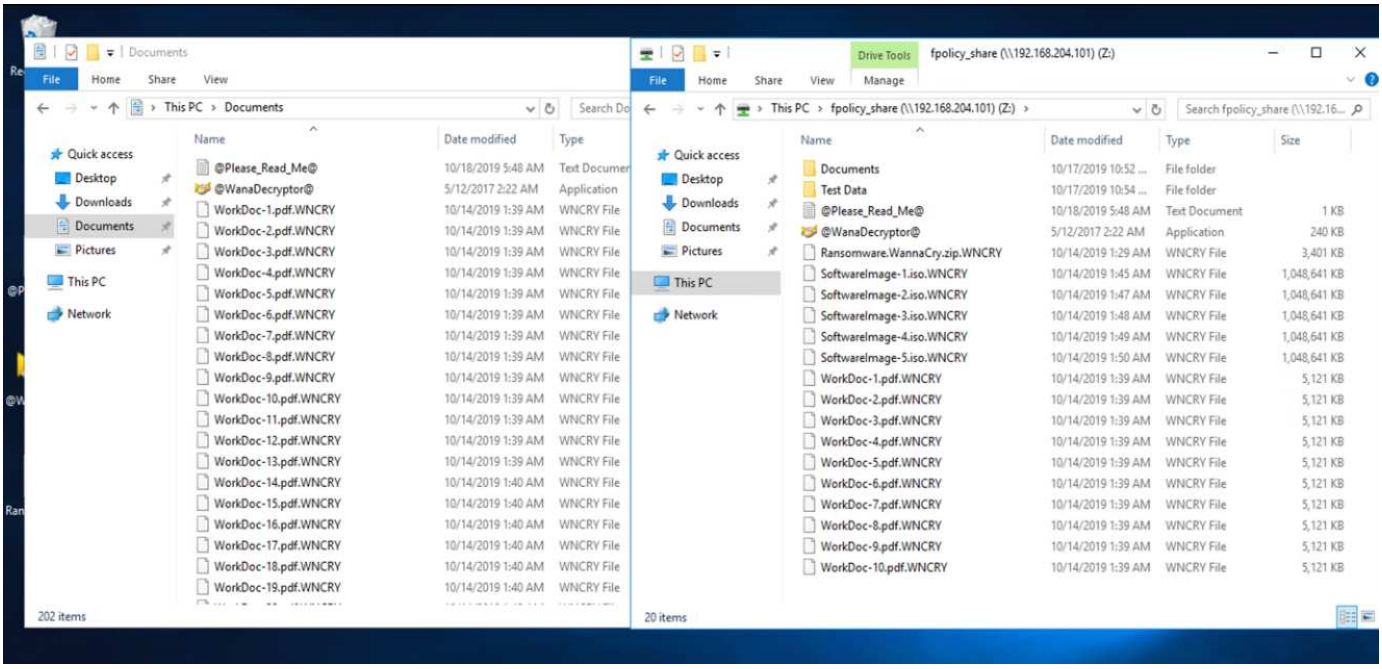
Cas 1 : WannaCry crypte le système de fichiers au sein de la machine virtuelle et le partage CIFS mappé

Le système de fichiers local et le partage CIFS mappé ont été cryptés par le programme malveillant WannaCry.

Le programme malveillant commence à crypter des fichiers avec des extensions WNCRY.



Le programme malveillant crypte tous les fichiers de la machine virtuelle locale et le partage mappé.

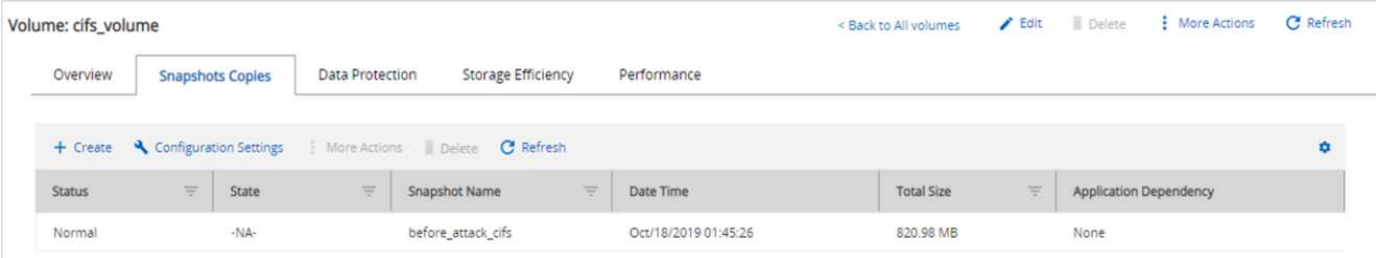


Détection

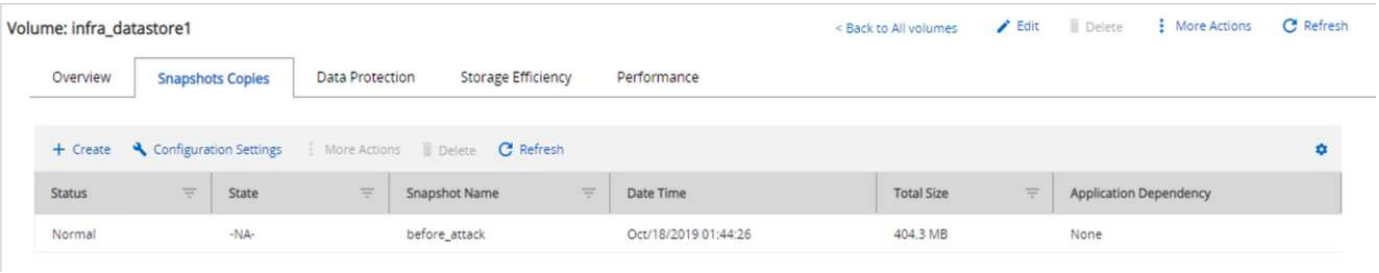
Au moment où le programme malveillant a commencé à chiffrer les fichiers, il a déclenché une augmentation exponentielle de la taille des copies Snapshot et une diminution exponentielle du pourcentage d'efficacité du stockage.

Nous avons détecté une augmentation spectaculaire de la taille de l'instantané à 820.98MB pour le volume

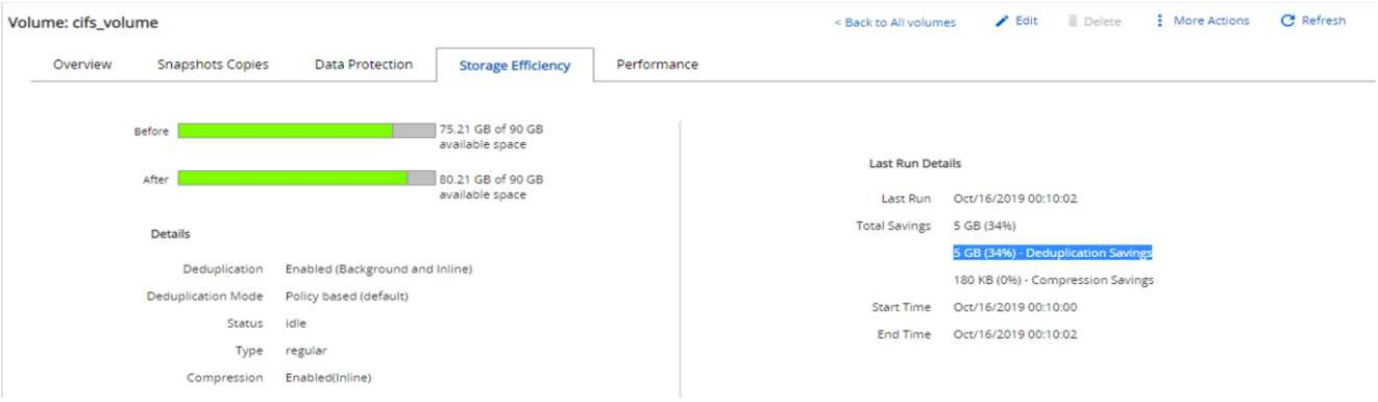
hébergeant le partage CIFS pendant l'attaque.



Nous avons détecté une augmentation de la taille de la copie Snapshot à 404,3 Mo pour le volume hébergeant la machine virtuelle.



L'efficacité du stockage pour le volume hébergeant le partage CIFS a été réduite à 34 %.



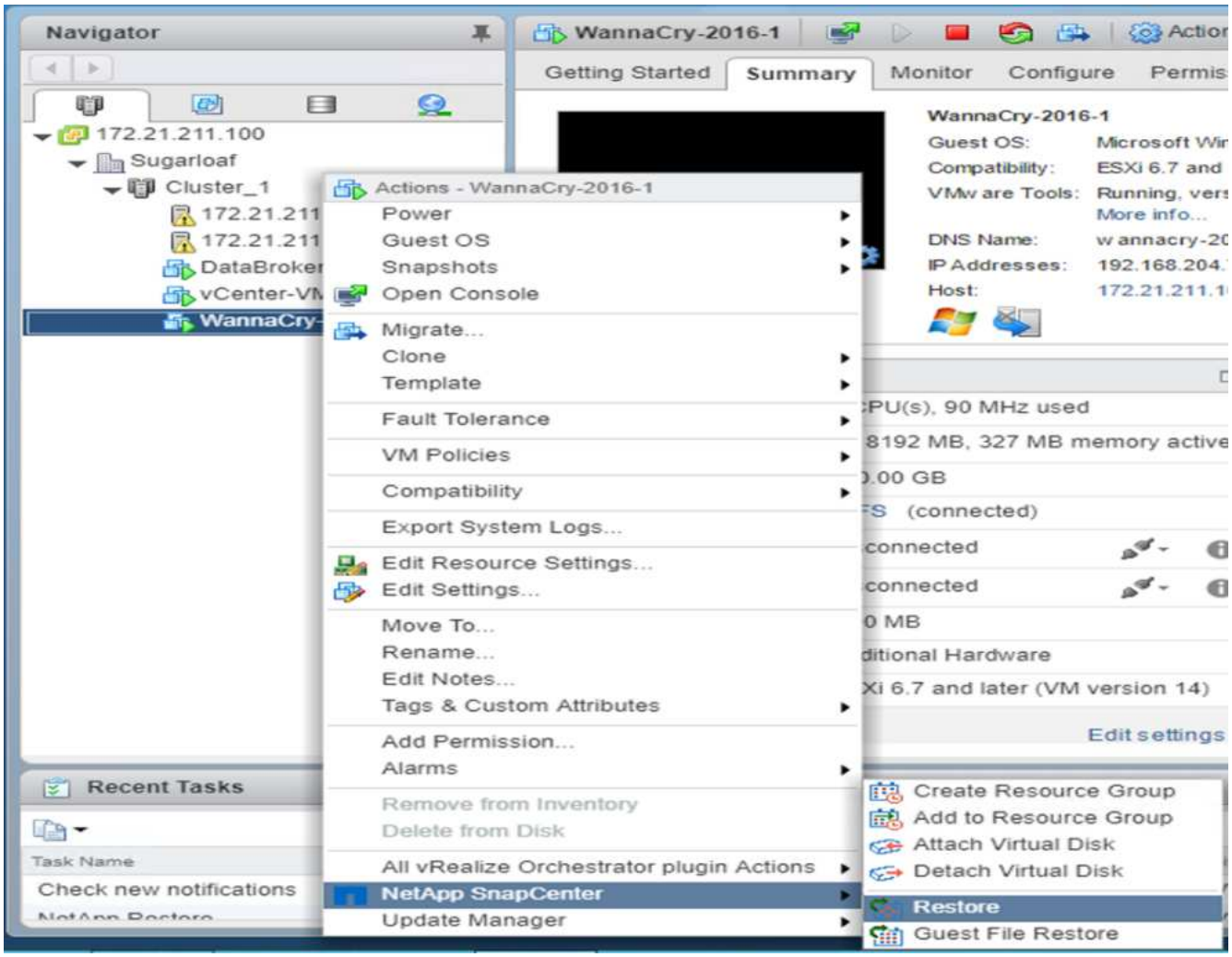
Résolution

Restaurez la machine virtuelle et le partage CIFS mappé à l'aide d'une copie Snapshot complète avant l'attaque.

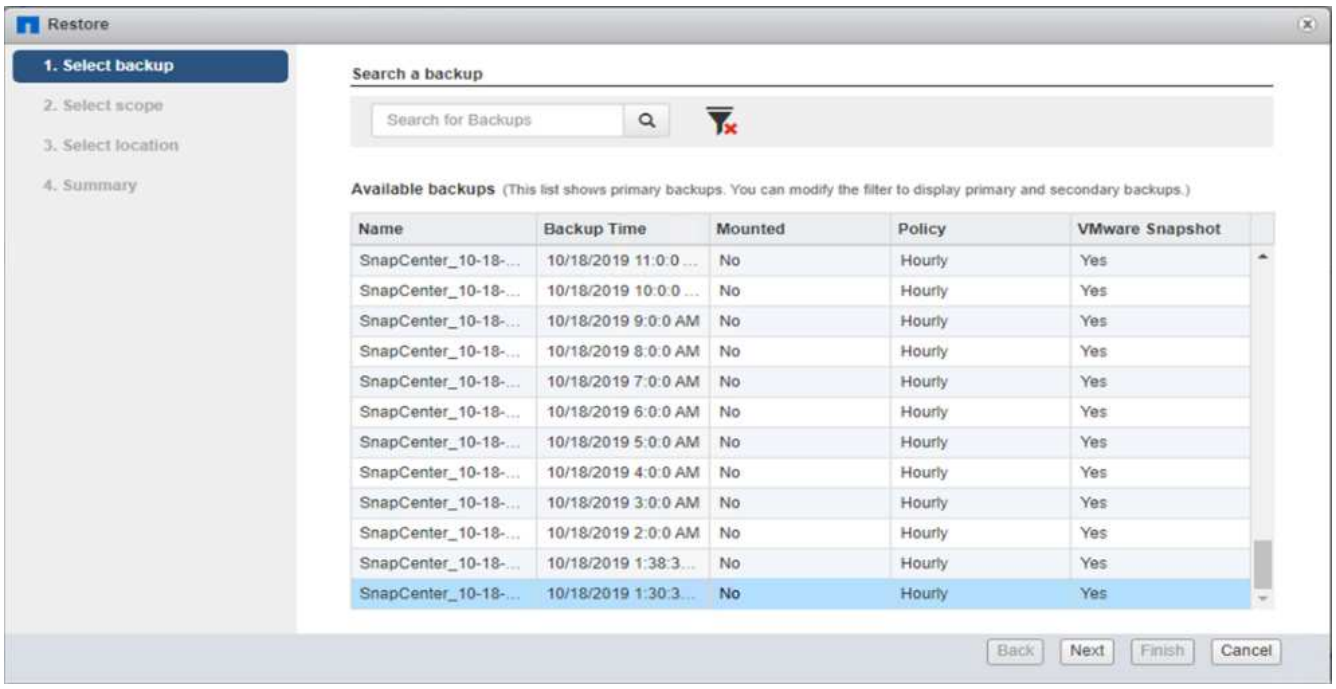
Restaurer VM

Pour restaurer la machine virtuelle, procédez comme suit :

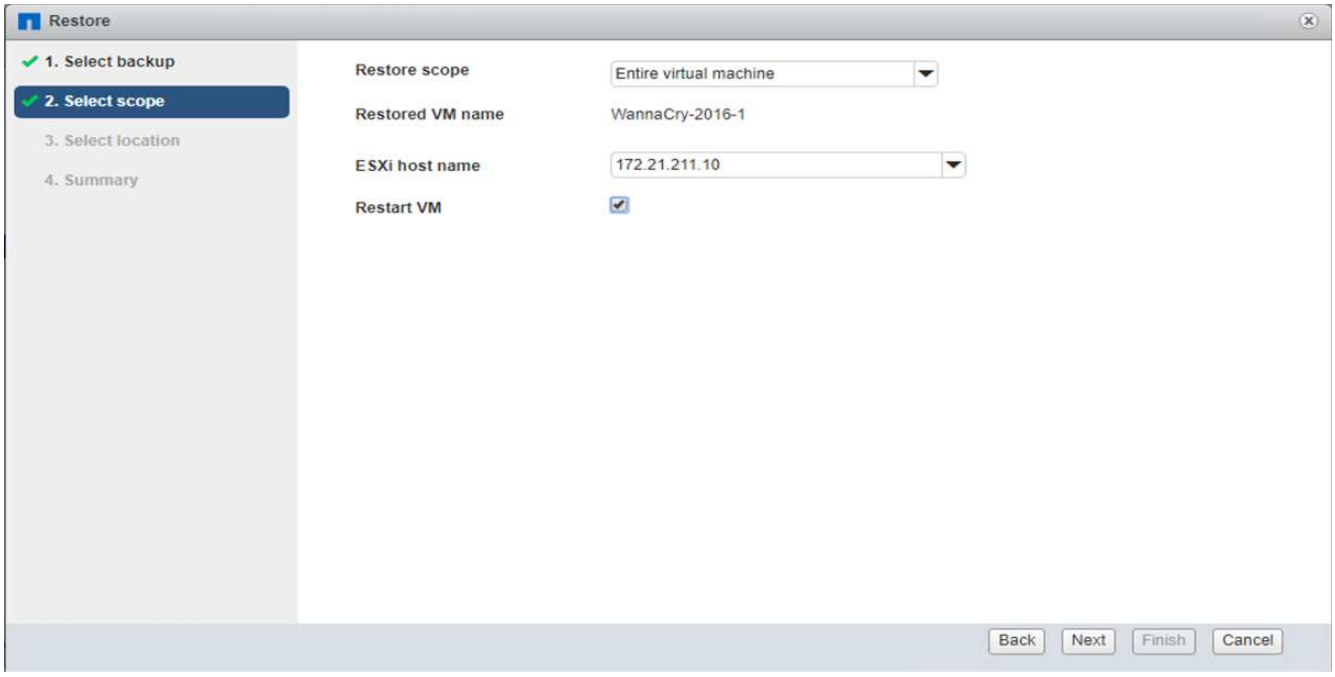
1. Utiliser la copie Snapshot que vous avez créée avec SnapCenter pour restaurer la machine virtuelle.



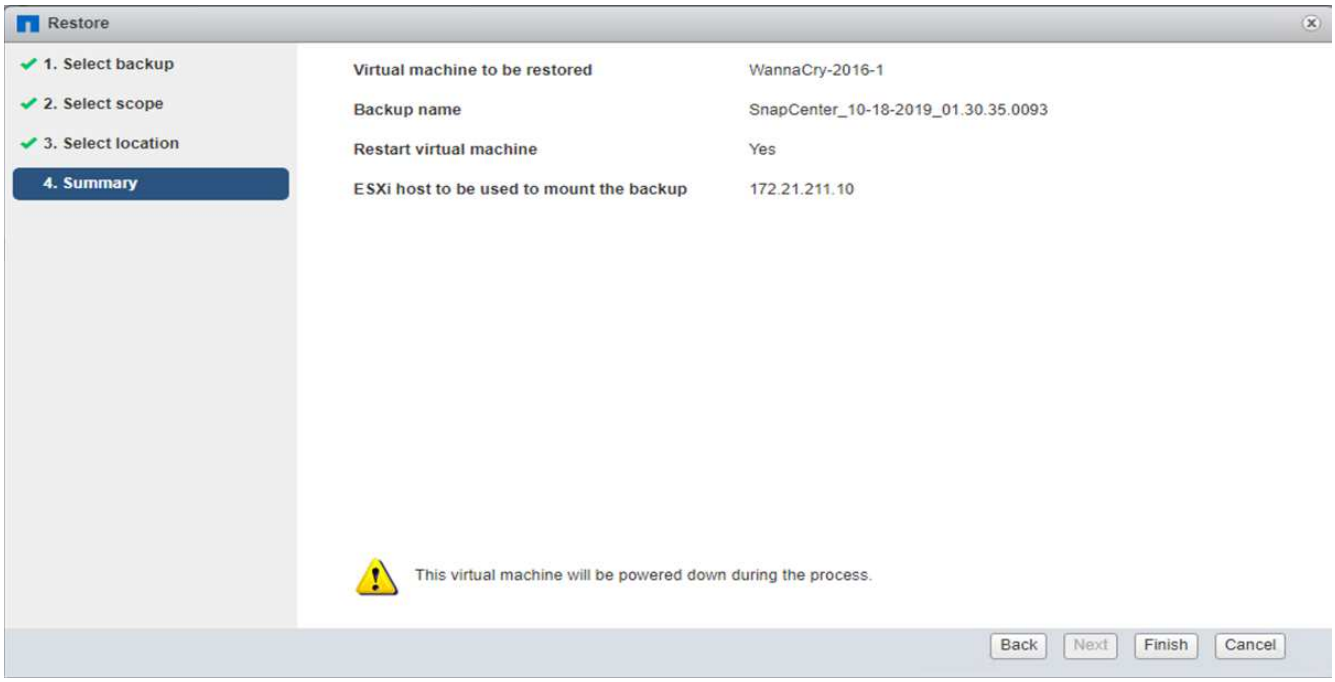
2. Sélectionnez la copie Snapshot cohérente avec VMware souhaitée pour la restauration.



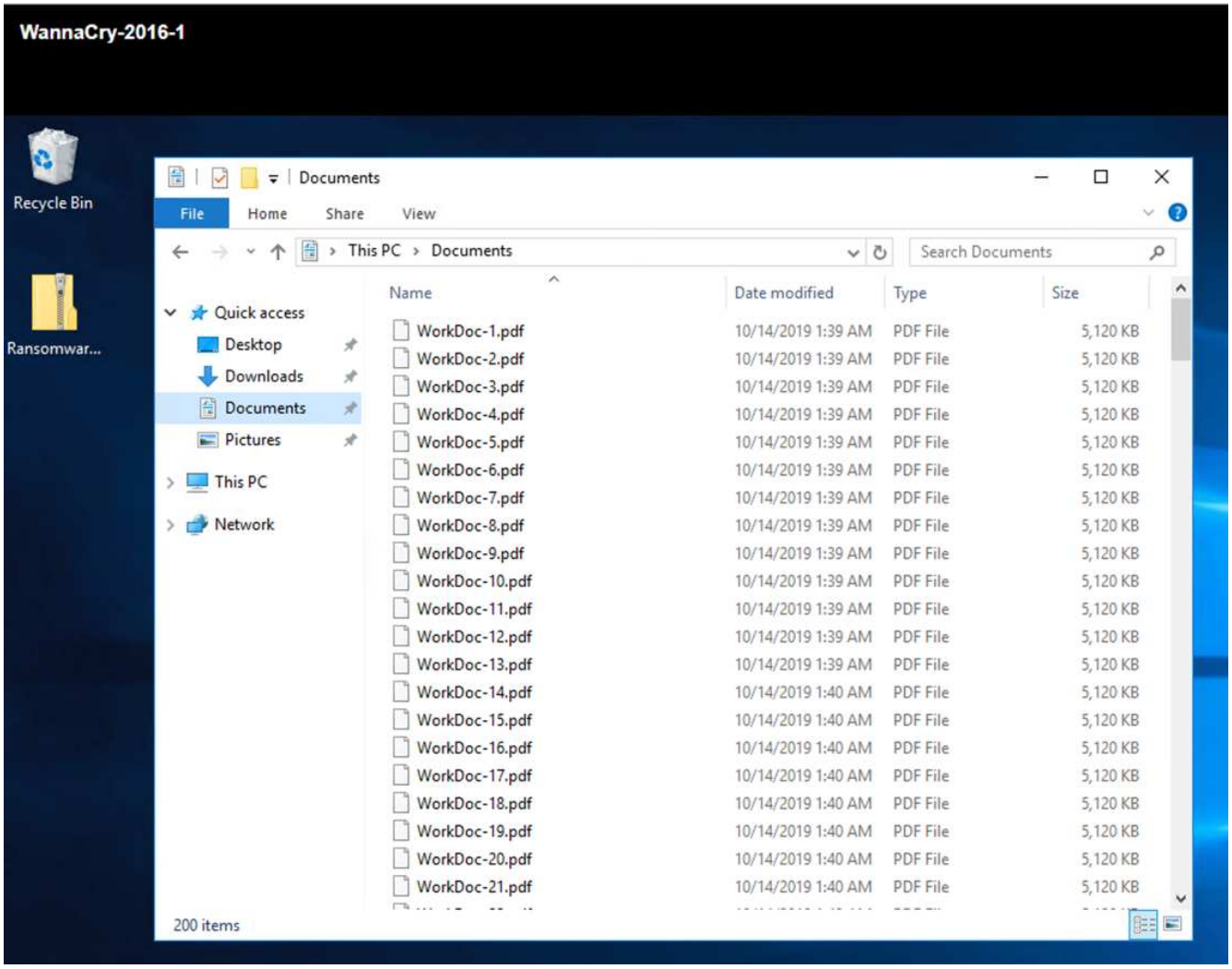
3. L’intégralité du serveur virtuel est restaurée et redémarrée.



4. Cliquez sur Terminer pour lancer le processus de restauration.



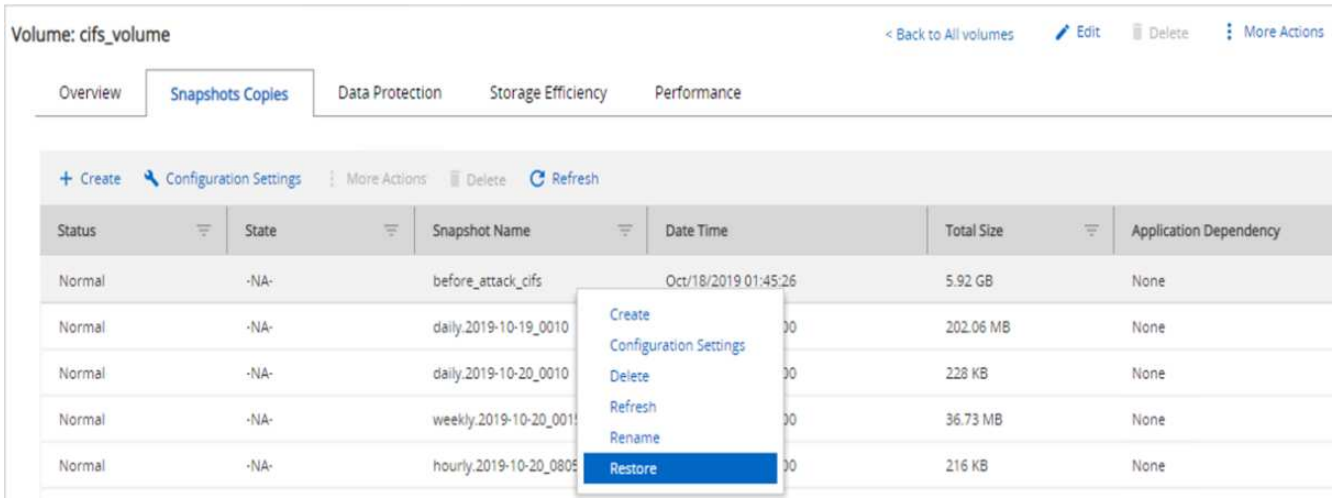
5. La machine virtuelle et ses fichiers sont restaurés.



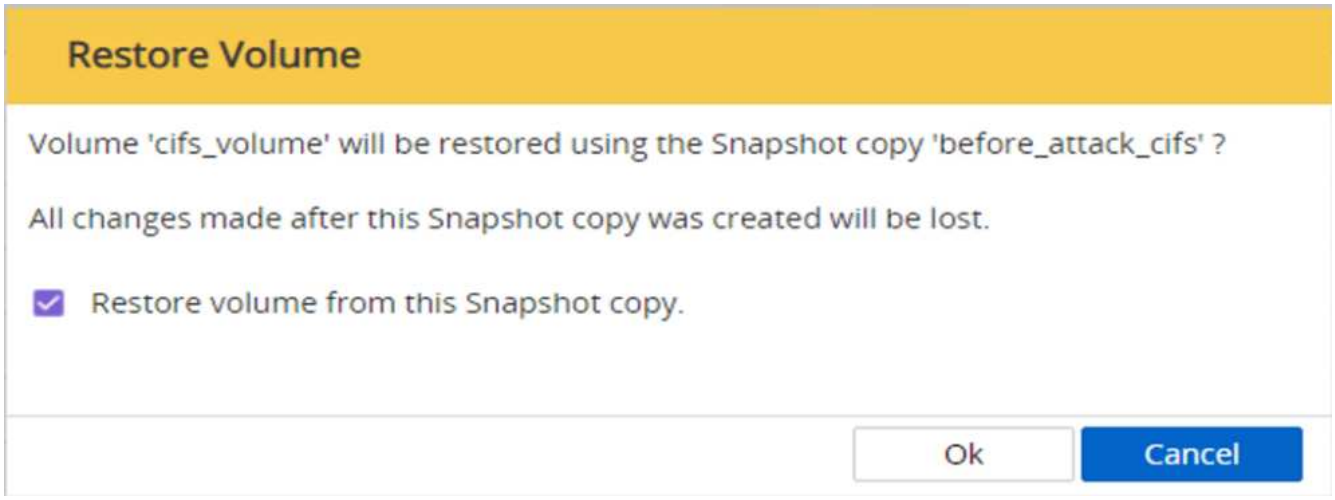
Restaurer le partage CIFS

Pour restaurer le partage CIFS, procédez comme suit :

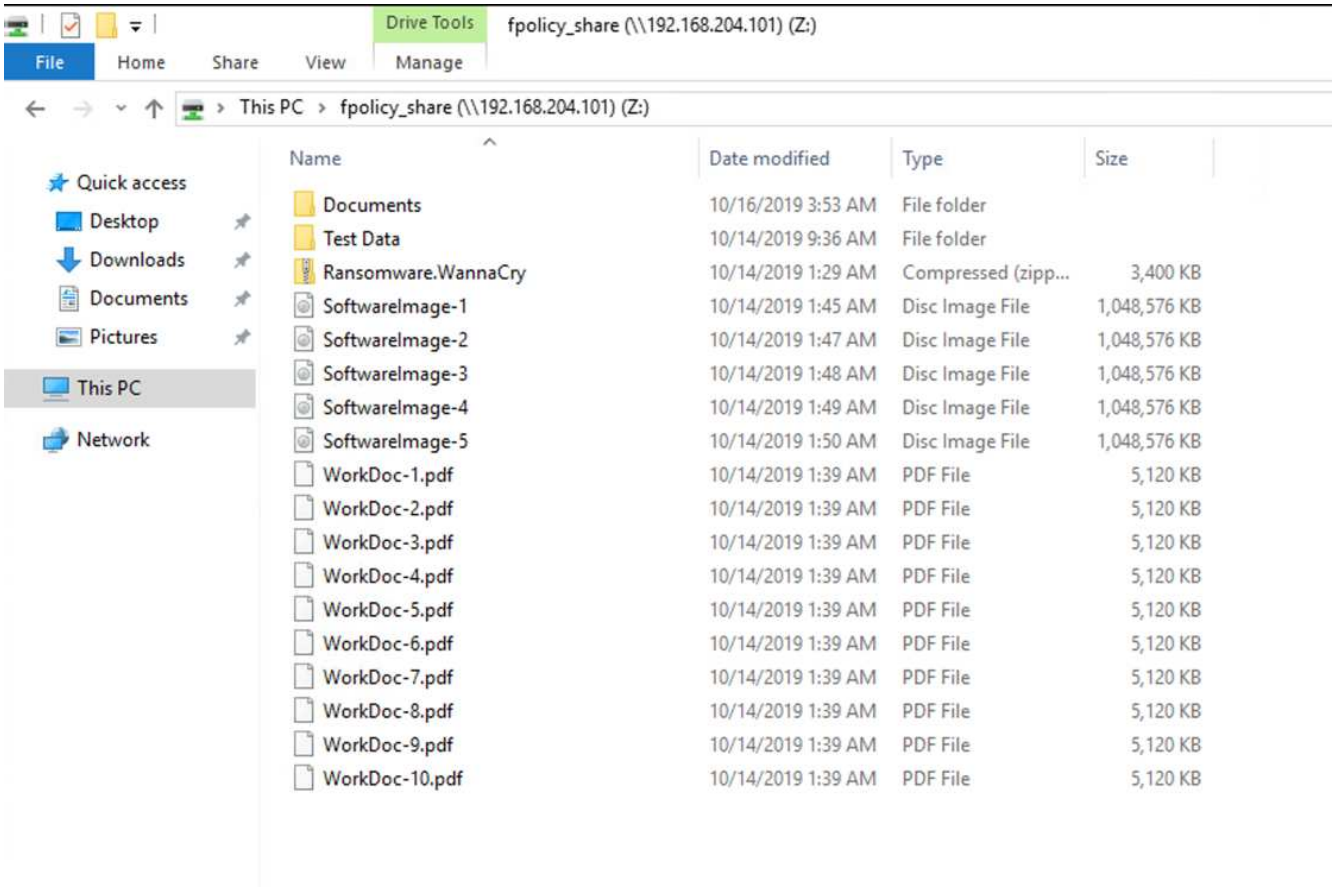
1. Utilisez la copie Snapshot du volume prise avant l'attaque pour restaurer le partage.



2. Cliquez sur OK pour lancer l'opération de restauration.



3. Afficher le partage CIFS après la restauration.



Cas 2 : WannaCry chiffre le système de fichiers au sein de la machine virtuelle et tente de chiffrer le partage CIFS mappé protégé par FPolicy

Prévention

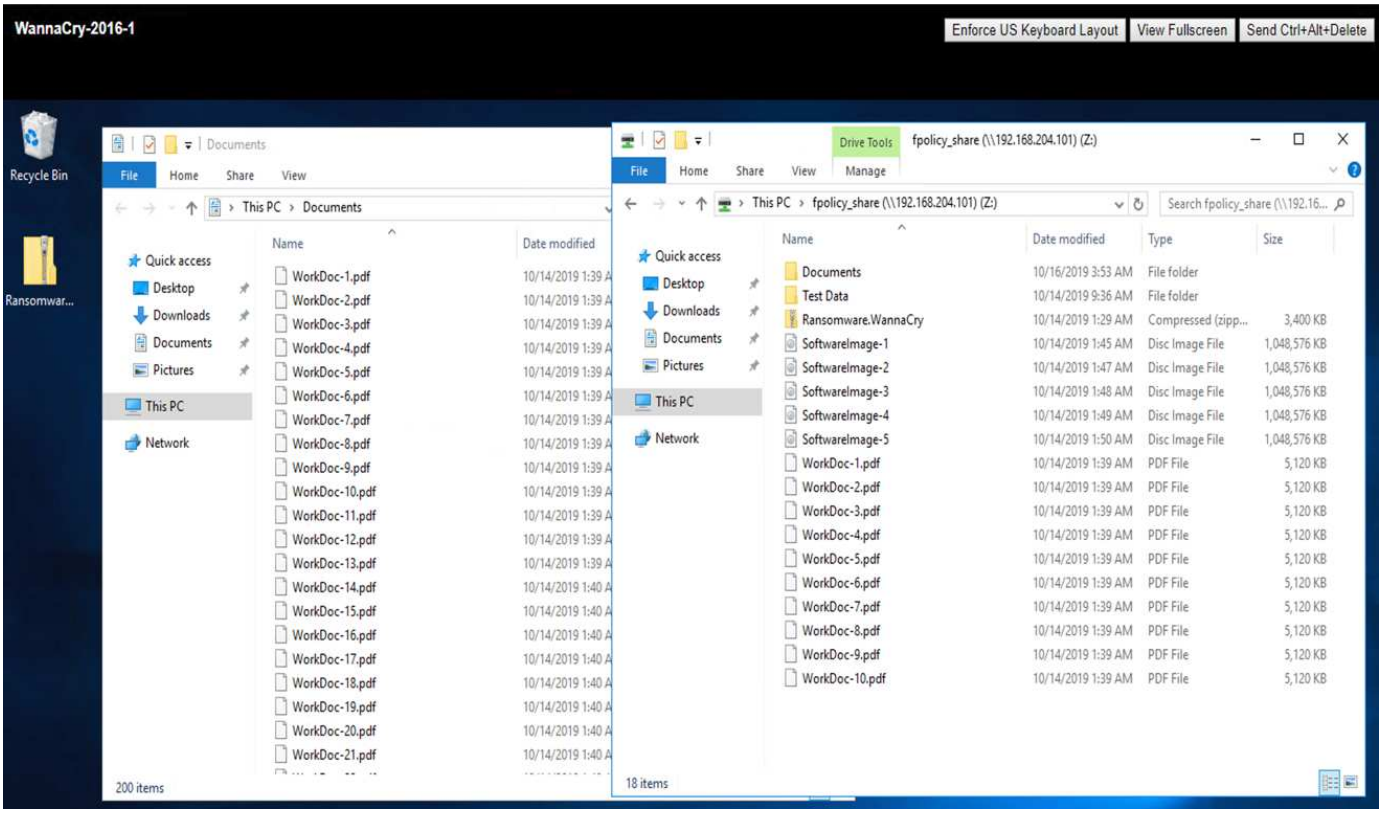
Configurer FPolicy

Pour configurer FPolicy sur le partage CIFS, exécutez les commandes suivantes sur le cluster ONTAP :

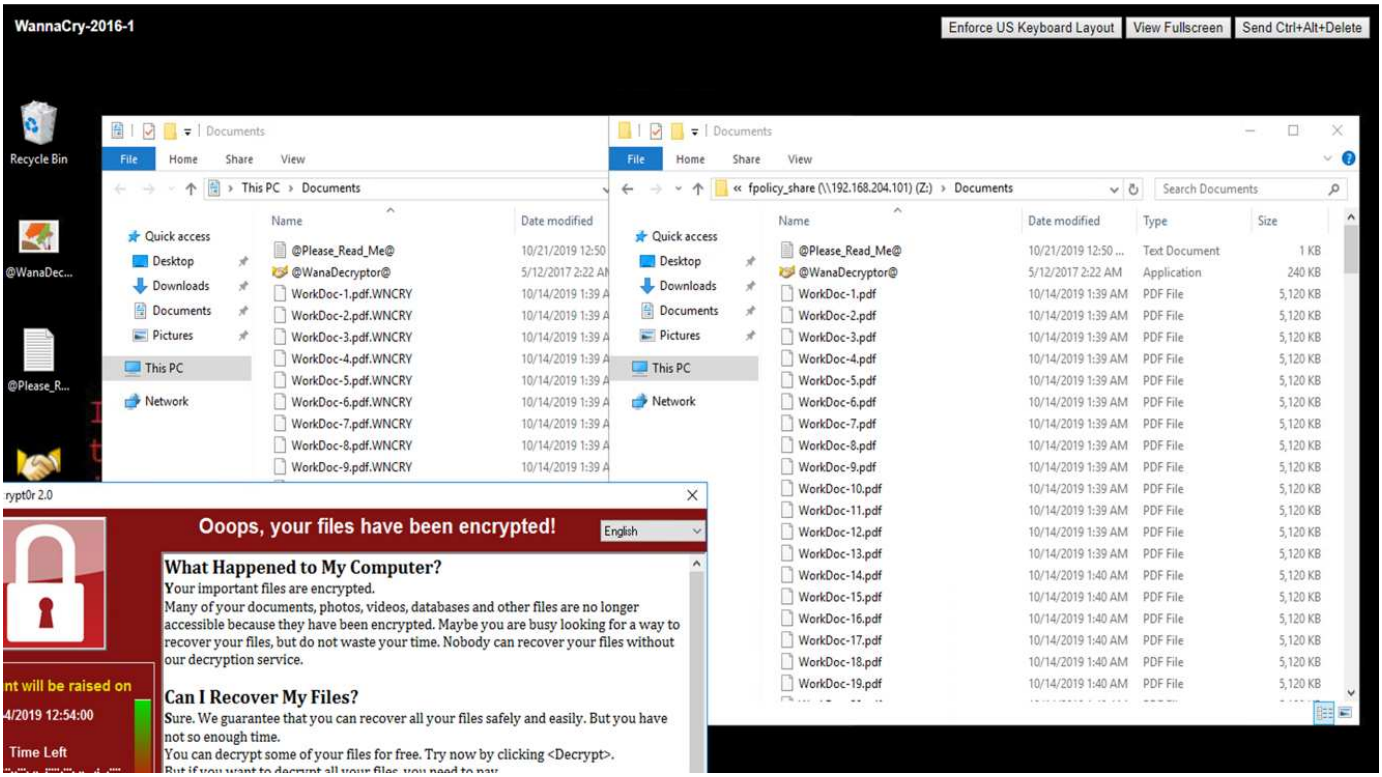
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Avec cette stratégie, les fichiers avec les extensions WNCRY, Locky et ad4c ne sont pas autorisés à effectuer les opérations de création, de renommage, d'écriture ou d'ouverture de fichiers.

Afficher l'état des fichiers avant d'attaquer, ils sont non cryptés et dans un système propre.



Les fichiers de la machine virtuelle sont chiffrés. Le programme malveillant WannaCry tente de crypter les fichiers du partage CIFS, mais FPolicy l'empêche de modifier les fichiers.



Continuez vos activités sans payer de rançon

Les fonctionnalités NetApp décrites dans ce document vous aident à restaurer les données en quelques minutes après une attaque et à éviter les attaques en premier lieu, afin de pouvoir continuer l'activité sans faire l'obstacle.

Un planning de copies Snapshot peut être défini pour atteindre l'objectif de point de récupération souhaité. Les opérations de restauration basées sur des copies Snapshot sont très rapides. Par conséquent, il est possible d'atteindre un objectif de durée de restauration (RTO) très faible.

Par-dessus tout, vous n'avez pas à payer de rançon suite à une attaque, et vous pouvez rapidement revenir à la normale.

Conclusion

Les ransomwares sont un produit de la criminalité organisée et ils n'ont pas d'ordre éthique. Ils peuvent s'abstenir de fournir la clé pour le décryptage même après avoir reçu la rançon. La victime perd non seulement ses données mais aussi une quantité importante d'argent et devra faire face à des conséquences liées à la perte de données de production.

Selon un "Article Forbes", seuls 19 % des victimes d'attaques par ransomware récupèrent leurs données pour autant. Par conséquent, les auteurs recommandent de ne pas payer une rançon en cas d'attaque, car cela renforce la foi de l'attaquant dans leur modèle d'entreprise.

Les opérations de sauvegarde et de restauration de données jouent un rôle important dans la restauration par ransomware. Par conséquent, ils doivent être inclus dans la planification des activités. La mise en œuvre de ces opérations doit être budgétisée de sorte à ce que les capacités de restauration ne puissent faire l'objet d'aucun compromis en cas d'attaque.

Il est important de choisir le partenaire technologique adéquat pour cette transition, et FlexPod propose la plupart des fonctionnalités de manière native, sans frais supplémentaires dans un système FAS 100 % Flash.

Remerciements

L'auteur tient à remercier les personnes suivantes pour leur soutien à la création de ce document :

- Jorge Gomez Navarret, NetApp
- Ganesh Kamath, NetApp

Informations supplémentaires

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

- Logiciel NetApp Snapshot

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- Gestion des sauvegardes SnapCenter

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- Conformité des données SnapLock

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- Documentation produit NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- Protection avancée contre les programmes malveillants Cisco (AMP)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

Solution FlexPod conforme à la norme FIPS 140-2 pour le secteur de la sécurité dans le secteur de la santé

Tr-4892 : solution FlexPod conforme à la norme FIPS 140-2 pour le secteur de la santé

JayaKishore Esanakula, NetApp John McAbel, Cisco

La loi HITECH (Health information Technology for Economic and Clinical Health Act) requiert le cryptage certifié FIPS (Federal information Processing Standard) 140-2 des informations de santé électroniques protégées (ePHI). Les applications et logiciels HIT

(Health information Technology) doivent être conformes à la norme FIPS 140-2 pour obtenir la certification « promotion Interoperability Program » (anciennement « Gsignificative Use Incentive Program »). Les prestataires admissibles et les hôpitaux sont tenus d'utiliser un RÉSULTAT conforme à la norme FIPS 140-2 (niveau 1) pour bénéficier d'incentives Medicare et Medicaid et pour éviter les pénalités de remboursement du Centre for Medicare and Medicaid (CMS). Les algorithmes de chiffrement certifiés FIPS 140-2 sont éligibles en tant que dispositifs de sécurité techniques requis conformément au "Règle de sécurité" De la loi américaine sur la transférabilité et la responsabilité en matière d'information médicale (HIPAA).

FIPS 140-2 est une loi américaine norme gouvernementale qui définit les exigences de sécurité pour les modules cryptographiques dans les matériels, les logiciels et les firmwares afin de protéger les informations sensibles. La conformité à la norme est obligatoire pour toute utilisation par les États-Unis les administrations publiques, et elles sont aussi souvent utilisées dans des secteurs réglementés tels que les services financiers et les soins de santé. Ce rapport technique aide le lecteur à comprendre à un niveau élevé la norme de sécurité FIPS 140-2-2. Il aide également le public à comprendre les diverses menaces auxquelles les organismes de santé sont confrontés. Enfin, le rapport technique permet de comprendre comment un système FlexPod conforme à la norme FIPS 140-2 permet de sécuriser les ressources de santé lorsqu'il est déployé sur une infrastructure convergée FlexPod.

Portée

Ce document présente une présentation technique des infrastructures Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS et FlexPod basées sur NetApp ONTAP pour héberger une ou plusieurs applications OU solutions INFORMATIQUES de santé conformes à la norme FIPS 140-2-2.

Public

Ce document est destiné aux leaders techniques du secteur de la santé, aux ingénieurs solutions partenaires Cisco et NetApp et aux équipes des services professionnels. NetApp suppose que le lecteur connaît bien les concepts de dimensionnement du stockage et du calcul, ainsi que la connaissance technique des menaces médicales, de la sécurité sanitaire, des systèmes IT de santé, de Cisco UCS et des systèmes de stockage NetApp.

"Suivant : les menaces de cybersécurité dans le domaine de la santé."

Cyber-menaces dans le secteur de la santé

"Précédent : introduction."

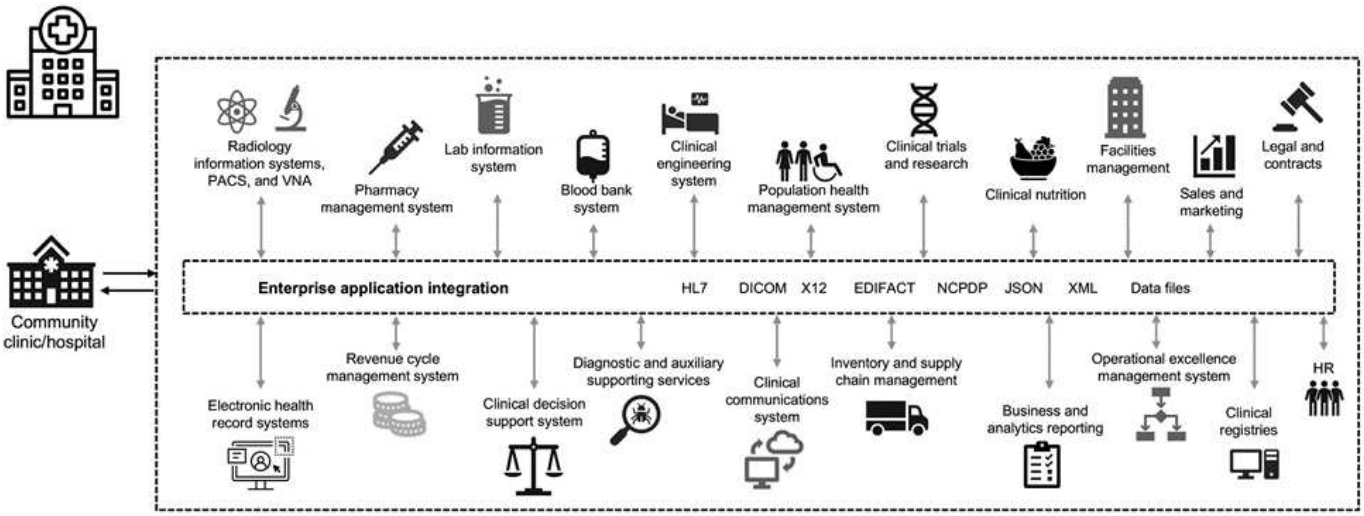
Chaque problème représente une nouvelle opportunité : la pandémie de COVID donne un exemple. Selon un "rapport" Par le programme de cybersécurité du ministère de la Santé et des Services sociaux (HHS), la réponse de la COVID a entraîné l'augmentation du nombre d'attaques par ransomware. Il y avait 6,000 nouveaux domaines Internet enregistrés juste au cours de la troisième semaine de mars 2020. Plus de 50 % des domaines ont hébergé des programmes malveillants. Les attaques par ransomware étaient responsables de près de 50 % de l'ensemble des violations de données de santé en 2020 et touchent plus de 630 organismes de santé et environ 29 millions de dossiers médicaux. Dix-neuf béchers/sites ont doublé l'extorsion. Avec un taux de 24.5 %, le secteur de la santé a été considéré comme la plus forte violation de données en 2020.

Les agents malveillants ont tenté de violer la sécurité et la confidentialité des informations médicales protégées (PHI) en vendant ces informations ou en menaçant de les détruire ou de les exposer. Des tentatives ciblées et de diffusion en masse sont fréquemment effectuées pour obtenir un accès non autorisé à l'ePHI. Environ 75 % des dossiers patient exposés au cours de la seconde moitié de 2020 étaient dus à des relations professionnelles compromises.

La liste suivante des organismes de soins de santé était ciblée par les agents malveillants :

- Systèmes hospitaliers
- Laboratoires de sciences de la vie
- Laboratoires de recherche
- Installations de réhabilitation
- Hôpitaux et cliniques communautaires

La diversité des applications qui constituent une organisation de soins de santé est indéniable et de plus en plus complexe. Les bureaux de la sécurité de l'information doivent assurer la gouvernance d'une grande variété de systèmes ET ressources IT. La figure suivante illustre les capacités cliniques d'un système hospitalier type.



Les données patient sont au cœur de cette image. La perte de données sur les patients et la stigmatisation associée aux affections médicales sensibles sont très réelles. Parmi les autres questions sensibles figurent le risque d'exclusion sociale, le chantage, le profilage, la vulnérabilité au marketing ciblé, l'exploitation et la responsabilité financière potentielle envers les payeurs à propos de l'information médicale au-delà des privilèges du payeur.

Les menaces pour les soins de santé sont multidimensionnelles dans la nature et dans l'impact. Les gouvernements du monde entier ont adopté diverses dispositions pour sécuriser les renseignements médicaux personnels. Les effets néfastes et la nature évolutive des menaces qui pèsent sur les soins de santé rendent difficile la défense de toutes les menaces.

Voici une liste de menaces courantes identifiées dans le domaine de la santé :

- Attaques par ransomware
- Perte ou vol d'équipement ou de données contenant des informations sensibles
- Attaques de phishing

- Attaques contre des dispositifs médicaux connectés pouvant affecter la sécurité du patient
- Envoyez un e-mail aux attaques de phishing
- Perte ou vol d'équipement ou de données
- Compromis sur le protocole des postes de travail à distance
- Vulnérabilité logicielle

Les établissements de santé opèrent dans un environnement juridique et réglementaire aussi complexe que leurs écosystèmes numériques. Cet environnement inclut, sans s'y limiter, les éléments suivants :

- Bureau du coordonnateur national (pour la technologie des soins de santé) normes d'interopérabilité des technologies de l'information en santé électroniques certifiées ONC
- Accès à l'assurance-santé et Loi sur la réautorisation du Programme d'assurance-santé pour enfants (MACRA)/utilisation significative
- Obligations multiples en vertu de la Food and Drug Administration (FDA)
- Les processus d'accréditation de la Commission mixte
- Exigences HIPAA
- Exigences HITECH
- Normes de risque minimales acceptables pour les payeurs
- Règles de confidentialité et de sécurité
- Loi fédérale sur la modernisation de la sécurité de l'information exigences intégrées aux contrats fédéraux et aux subventions de recherche par l'intermédiaire d'organismes comme les National Institutes of Health
- Norme de sécurité de l'industrie des cartes de paiement (PCI-DSS)
- Exigences relatives à la gestion des services de santé mentale et de toxicomanie (SAMHSA)
- Loi Gramm-Leach-Bliley pour le traitement financier
- La loi Stark en ce qui concerne la prestation de services aux organisations affiliées
- Loi sur les droits à l'éducation familiale et la protection des renseignements personnels (FERPA) pour les institutions qui participent à l'enseignement supérieur
- Loi sur la non-discrimination en matière d'information génétique (GINA)
- Le nouveau Règlement général sur la protection des données (RGPD) dans l'Union européenne

Les normes d'architecture de sécurité évoluent rapidement pour empêcher les acteurs malveillants d'affecter les systèmes d'information de santé. L'une de ces normes est la norme FIPS 140-2, définie par l'Institut national des normes et de la technologie (NIST). La publication FIPS 140-2 détaille le niveau américain exigences gouvernementales pour un module cryptographique. Les exigences de sécurité couvrent les domaines liés à la conception et à l'implémentation sécurisées d'un module cryptographique et peuvent être appliqués à HIT. Les frontières cryptographiques bien définies facilitent la gestion de la sécurité tout en restant à jour avec les modules cryptographiques. Ces limites permettent d'éviter les faibles modules de cryptage qui peuvent être facilement exploités par des acteurs malveillants. Ils permettent également d'éviter les erreurs humaines lors de la gestion de modules cryptographiques standard.

Le NIST, de concert avec le Centre de sécurité des communications (CSE), a mis en place le Programme de validation du module cryptographique (CMVP) pour certifier les modules cryptographiques des niveaux de validation FIPS 140-2. Grâce à un module certifié FIPS 140-2-2, les organismes fédéraux doivent protéger leurs données sensibles ou précieuses tout en transit. En raison de sa réussite dans la protection des informations sensibles ou précieuses, de nombreux systèmes de santé ont choisi de crypter les informations médicales confidentielles à l'aide de modules cryptographiques FIPS 140-2 au-delà du niveau de sécurité

minimum requis par la loi.

L'exploitation et la mise en œuvre des fonctionnalités FlexPod FIPS 140-2 ne prennent que des heures (et non plusieurs jours). La plupart des organismes de santé, quelle que soit leur taille, sont à la portée de la conformité avec la norme FIPS. Avec des limites de chiffrement clairement définies et des étapes de mise en œuvre simples et bien documentées, une architecture FlexPod conforme à la norme FIPS 140-2 peut constituer une base de sécurité solide pour l'infrastructure. De plus, des améliorations simples permettent d'améliorer encore la protection contre les menaces de sécurité.

"Présentation de la norme FIPS 140-2."

Présentation de la norme FIPS 140-2

"Précédent : cyber-menaces dans le domaine de la santé."

"FIPS 140-2" spécifie les exigences de sécurité pour un module cryptographique utilisé dans un système de sécurité qui protège les informations sensibles dans les systèmes informatiques et de télécommunication. Un module cryptographique doit être un ensemble de matériel, de logiciels, de micrologiciels ou une combinaison. FIPS s'applique aux algorithmes cryptographiques, à la génération de clés et aux gestionnaires de clés contenus dans une limite cryptographique. Il est important de comprendre que la norme FIPS 140-2 s'applique spécifiquement au module cryptographique et non au produit, à l'architecture, aux données ou à l'écosystème. Le module cryptographique, qui est défini dans les termes clés plus loin dans ce document, est le composant spécifique (qu'il s'agisse du matériel, du logiciel et/ou du micrologiciel) qui implémente des fonctions de sécurité approuvées. La norme FIPS 140-2 spécifie également quatre niveaux. Les algorithmes cryptographiques approuvés sont communs à tous les niveaux. Voici les éléments clés et exigences de chaque niveau de sécurité :

- **Niveau de sécurité 1**
  - Spécifie les exigences de sécurité de base pour un module cryptographique (au moins un algorithme ou une fonction de sécurité approuvé est nécessaire).
  - Aucun mécanisme de sécurité physique spécifique n'est requis pour le niveau 1 au-delà des exigences de base pour les composants de qualité de production.
- **Niveau de sécurité 2**
  - Améliore les mécanismes de sécurité physique en ajoutant la nécessité de preuves d'inviolabilité en utilisant des solutions inviolables telles que des revêtements ou des joints, des verrous sur des capots ou portes amovibles des modules cryptographiques.
  - Exige, au minimum, que le contrôle d'accès basé sur des rôles (RBAC) dans lequel le module cryptographique authentifie l'autorisation d'un opérateur ou d'un administrateur d'assumer un rôle spécifique et exécute un ensemble de fonctions correspondant.
- **Niveau de sécurité 3**
  - S'appuie sur les exigences inviolables du niveau 2 et tente d'empêcher un accès plus poussé aux paramètres de sécurité critiques (CSP) au sein du module cryptographique.
  - Les mécanismes de sécurité physique requis au niveau 3 sont destinés à avoir une forte probabilité de détecter et de répondre aux tentatives d'accès physique ou à toute utilisation ou modification du module cryptographique. Il peut s'agir, par exemple, de boîtiers forts, d'une détection d'autosurveillance et de circuits de réponse qui zéros tous les CSP en texte clair lorsqu'un capot

amovible sur le module cryptographique est ouvert.

  - Nécessite des mécanismes d'authentification basés sur les identités pour renforcer la sécurité des mécanismes RBAC spécifiés au niveau 2. Un module cryptographique authentifie l'identité d'un opérateur et vérifie que celui-ci est autorisé à utiliser un rôle et à exécuter les fonctions du rôle.

- **Niveau de sécurité 4**
  - Le plus haut niveau de sécurité de la norme FIPS 140-2.
  - Le niveau le plus utile pour les opérations dans les environnements physiquement non protégés.
  - À ce niveau, les mécanismes de sécurité physique sont conçus pour fournir une protection complète autour du module cryptographique, qui est responsable de détecter et de répondre à toute tentative non autorisée d'accès physique.
  - La pénétration ou l'exposition du module cryptographique devrait avoir une forte probabilité de détection et entraîner la mise à zéro immédiate de tous les CSP non sécurisés ou en texte clair.

"Ensuite, plan de contrôle et plan de données."

Plan de contrôle et plan de données

"Précédent : présentation de la norme FIPS 140-2."

Lors de la mise en œuvre d'une stratégie FIPS 140-2-2, il est important de comprendre ce qui est protégé. Elle peut facilement être divisée en deux zones : le plan de contrôle et le plan de données. Un plan de contrôle se réfère aux aspects ayant un impact sur le contrôle et le fonctionnement des composants au sein du système FlexPod : par exemple, accès administratif aux contrôleurs de stockage NetApp, commutateurs Cisco Nexus et serveurs Cisco UCS. La protection à cette couche est assurée par la limitation des protocoles et des gestionnaires cryptographiques que les administrateurs peuvent utiliser pour se connecter aux périphériques et apporter des modifications. Un plan de données fait référence aux informations réelles, telles que les informations médicales personnelles, dans le système FlexPod. Ces données sont protégées par chiffrement des données au repos, puis à nouveau pour la norme FIPS, garantissant ainsi que les modules de chiffrement utilisés respectent les normes.

"Nœuds de calcul FlexPod Cisco UCS et FIPS 140-2"

Les ressources de calcul FlexPod Cisco UCS et FIPS 140-2

"Précédent : plan de contrôle par rapport au plan de données."

Une architecture FlexPod peut être conçue avec un serveur Cisco UCS conforme à la norme FIPS 140-2-2. Conformément à la norme U. S. Le serveur Cisco UCS, NIST, peut fonctionner en mode de conformité FIPS 140-2 de niveau 1. Pour obtenir la liste complète des composants Cisco compatibles FIPS, reportez-vous à la section "La page FIPS 140 de Cisco". Cisco UCS Manager est certifié FIPS 140-2-2.

Cisco UCS et Fabric Interconnect

Cisco UCS Manager est déployé et s'exécute à partir des interconnexions de fabric Cisco (IF).

Pour plus d'informations sur Cisco UCS et sur l'activation de FIPS, reportez-vous au "Documentation Cisco UCS Manager".

Pour activer le mode FIPS sur le Cisco Fabric Interconnect sur chaque structure A et B, exécutez les commandes suivantes :

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> Pour remplacer un SYSTÈME DE CLUSTER sur Cisco UCS Manager version 3.2(3) par UN FI disponible dans une version antérieure à Cisco UCS Manager version 3.2(3), désactivez le mode FIPS (désactivez-les `fips-mode`) Sur le FI existant avant d'ajouter le FI de remplacement au cluster. Une fois le cluster formé, dans le cadre du démarrage de Cisco UCS Manager, le mode FIPS est automatiquement activé.

Cisco propose les produits clés suivants pouvant être implémentés au niveau de la couche de calcul ou d'application :

- **Cisco Advanced Malware protection (AMP) pour les noeuds finaux.** pris en charge sur les systèmes d'exploitation Microsoft Windows et Linux, cette solution intègre des capacités de prévention, de détection et de réponse. Ce logiciel de sécurité évite les failles de sécurité, bloque les programmes malveillants au point d'entrée et surveille et analyse en continu les activités des fichiers et des processus afin de détecter, de contenir et de corriger rapidement les menaces qui peuvent échapper aux défenses en première ligne. Le composant de protection contre les activités malveillantes (MAP) de l'AMP surveille en permanence toute l'activité des points finaux et assure la détection des temps d'exécution et le blocage du comportement anormal d'un programme en cours d'exécution sur le point final. Par exemple, lorsque le comportement de terminal indique un ransomware, les processus incriminés se terminent, ce qui empêche le chiffrement du terminal et arrête l'attaque.
- **AMP pour la sécurité des e-mails** les e-mails sont devenus le véhicule principal pour propager des programmes malveillants et mener à bien des cyberattaques. En moyenne, environ 100 milliards d'e-mails sont échangés en une seule journée, ce qui fournit aux pirates un excellent vecteur de pénétration dans les systèmes des utilisateurs. Par conséquent, il est absolument essentiel de se défendre contre cette ligne d'attaque. AMP analyse les e-mails contre les menaces, telles que les attaques sans jour et les logiciels malveillants furtifs cachés dans des pièces jointes malveillantes. Il utilise également des informations URL de pointe pour lutter contre les liens malveillants. Elle offre aux utilisateurs une protection avancée contre le phishing ciblé, les attaques par ransomware et d'autres attaques sophistiquées.
- **Système de prévention des intrusions nouvelle génération (NGIPS).** Cisco FirePOWER NGIPS peut être déployé en tant qu'appliance physique dans le centre de données ou en tant qu'appliance virtuelle sur VMware (NGIPSv pour VMware). Ce système hautement efficace de prévention des intrusions offre des performances fiables et un faible coût total de possession. La protection contre les menaces peut être étendue avec des licences d'abonnement facultatives pour fournir AMP, visibilité et contrôle des applications, ainsi que des fonctionnalités de filtrage des URL. Le système NGIPS virtualisé inspecte le trafic entre les machines virtuelles et facilite le déploiement et la gestion des solutions NGIPS sur des sites disposant de ressources limitées, ce qui renforce la protection des ressources physiques et virtuelles.

"FlexPod : connectivité réseau Cisco et FIPS 140-2."

Les réseaux FlexPod Cisco et FIPS 140-2

"Précédent : calcul FlexPod Cisco UCS et FIPS 140-2."

Cisco MDS

La plateforme Cisco MDS 9000 avec logiciel 8.4.x est "Conforme à la norme FIPS 140-2". Cisco MDS implémente des modules cryptographiques et les services suivants pour SNMPv3 et SSH.

- Établissement de session prenant en charge chaque service
- Tous les algorithmes cryptographiques sous-jacents prenant en charge les fonctions de dérivation des clés de service
- Hachage pour chaque service
- Chiffrement symétrique pour chaque service

Avant d'activer le mode FIPS, effectuez les tâches suivantes sur le commutateur MDS :

1. Faites de vos mots de passe un minimum de huit caractères.
2. Désactivez Telnet. Les utilisateurs doivent se connecter à l'aide de SSH uniquement.
3. Désactivez l'authentification à distance via RADIUS/TACACS+. Seuls les utilisateurs locaux du commutateur peuvent être authentifiés.
4. Désactivez SNMP v1 et v2. Tout compte utilisateur existant sur le commutateur qui a été configuré pour SNMPv3 doit être configuré uniquement avec SHA pour l'authentification et AES/3DES pour la confidentialité.
5. Désactivez VRRP.
6. Supprimez toutes les règles IKE qui ont soit MD5 pour l'authentification, soit DES pour le cryptage. Modifiez les règles de sorte qu'elles utilisent SHA pour l'authentification et 3DES/AES pour le cryptage.
7. Supprimez tous les types de clés RSA1 du serveur SSH.

Pour activer le mode FIPS et afficher l'état FIPS sur le commutateur MDS, procédez comme suit :

1. Affiche le statut FIPS.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Configurez la clé SSH 2048 bits.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Activez le mode FIPS.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Affiche le statut FIPS.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Enregistrez la configuration dans la configuration en cours d'exécution.

```
MDSSwitch(config)# copy ru st
[##################################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Redémarrez le commutateur MDS

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Affiche le statut FIPS.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

Pour plus d'informations, voir "Activation du mode FIPS".

Commutateurs Cisco Nexus

Les commutateurs de la gamme Cisco Nexus 9000 (version 9.3) sont "Conforme à la norme FIPS 140-2". Cisco Nexus implémente des modules cryptographiques et les services suivants pour SNMPv3 et SSH.

- Établissement de session prenant en charge chaque service
- Tous les algorithmes cryptographiques sous-jacents prenant en charge les fonctions de dérivation des clés de service
- Hachage pour chaque service
- Chiffrement symétrique pour chaque service

Avant d'activer le mode FIPS, effectuez les tâches suivantes sur le commutateur Cisco Nexus :

1. Désactivez Telnet. Les utilisateurs doivent se connecter à l'aide de Secure Shell (SSH) uniquement.
2. Désactivez SNMPv1 et v2. Tout compte utilisateur existant sur le périphérique qui a été configuré pour SNMPv3 doit être configuré uniquement avec SHA pour l'authentification et AES/3DES pour la confidentialité.
3. Supprimez toutes les paires de clés RSA1 du serveur SSH.
4. Activez le contrôle d'intégrité des messages (MIC) HMAC-SHA1 à utiliser lors de la négociation du protocole SAP (Security Association Protocol) de Cisco TrustSec. Pour ce faire, entrez l'algorithme de hachage sap `HMAC-SHA-1` de la commande `cts-manual` ou `cts-dot1x` mode.

Pour activer le mode FIPS sur le commutateur Nexus, effectuez les opérations suivantes :

1. Configurez la clé SSH 2048 bits.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Configurez la clé SSH 2048 bits.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Activez le mode FIPS.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Redémarrez le commutateur Nexus.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Affiche le statut FIPS.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

De plus, le logiciel Cisco NX OS prend en charge la fonctionnalité NetFlow qui permet une détection améliorée des anomalies et de la sécurité du réseau. NetFlow capture les métadonnées de chaque conversation sur le réseau, les parties impliquées dans la communication, le protocole utilisé et la durée de la transaction. Une fois les informations agrégées et analysées, elles permettent de mieux comprendre le comportement normal. Les données collectées permettent également d'identifier des modèles d'activité douteux, tels que les programmes malveillants, qui s'étendent sur le réseau, qui peuvent autrement passer inaperçues. NetFlow utilise des flux pour fournir des statistiques sur la surveillance du réseau. Un flux est un flux unidirectionnel de paquets arrivant sur une interface source (ou VLAN) et possède les mêmes valeurs pour les clés. Une clé est une valeur identifiée pour un champ dans le paquet. Vous créez un flux à l'aide d'un enregistrement de flux pour définir les clés uniques de votre flux. Vous pouvez exporter les données collectées par NetFlow pour vos flux à l'aide d'un exportateur de flux vers un collecteur NetFlow distant, tel que Cisco StealthWatch. StealthWatch exploite ces informations pour assurer une surveillance continue du réseau et fournit une détection en temps réel des menaces et une analyse des réponses aux incidents en cas d'attaque par ransomware.

"FlexPod : stockage NetApp ONTAP et FIPS 140-2."

Stockage FlexPod ONTAP et FIPS 140-2

"Précédent : réseau FlexPod Cisco et FIPS 140-2."

NetApp propose toute une gamme de matériel, de logiciels et de services, qui peuvent inclure divers composants des modules cryptographiques validés selon la norme. NetApp a donc recours à diverses approches de conformité à la norme FIPS 140-2 pour le plan de contrôle et le plan de données :

- NetApp inclut des modules cryptographiques qui ont obtenu une validation de niveau 1 pour les données en transit et le chiffrement des données au repos.
- NetApp acquiert à la fois des modules matériels et logiciels ayant été validés par la norme FIPS 140-2 par les fournisseurs de ces composants. Par exemple, la solution NetApp Storage Encryption exploite des disques validés conformes à la norme FIPS de niveau 2.
- Les produits NetApp peuvent utiliser un module validé conformément à la norme, même si le produit ou la fonctionnalité ne se trouve pas aux limites de la validation. Par exemple, NetApp Volume Encryption (NVE) est conforme à la norme FIPS 140-2-2. Bien qu'il ne soit pas validé séparément, il exploite le module cryptographique de NetApp, qui est validé au niveau 1. Pour comprendre les spécificités de la conformité de votre version de ONTAP, contactez votre expert technique FlexPod.

Les modules cryptographiques NetApp sont certifiés conformes à la norme FIPS 140-2 de niveau 1

- NetApp Cryptographic Security module (NCSM) est certifié conforme à la norme FIPS 140-2 de niveau 1.

Les disques à autochiffrement de NetApp sont validés par la norme FIPS 140-2 de niveau 2

NetApp achète des disques à autocryptage (SED) qui ont été validés par la norme FIPS 140-2 par le fabricant d'équipement d'origine ; les clients qui les recherchent doivent les spécifier lors de la commande. Les disques sont validés au niveau 2. Les produits NetApp suivants peuvent utiliser les disques SED validés :

- AFF A-Series et les systèmes de stockage FAS
- Systèmes de stockage E-Series et EF-Series

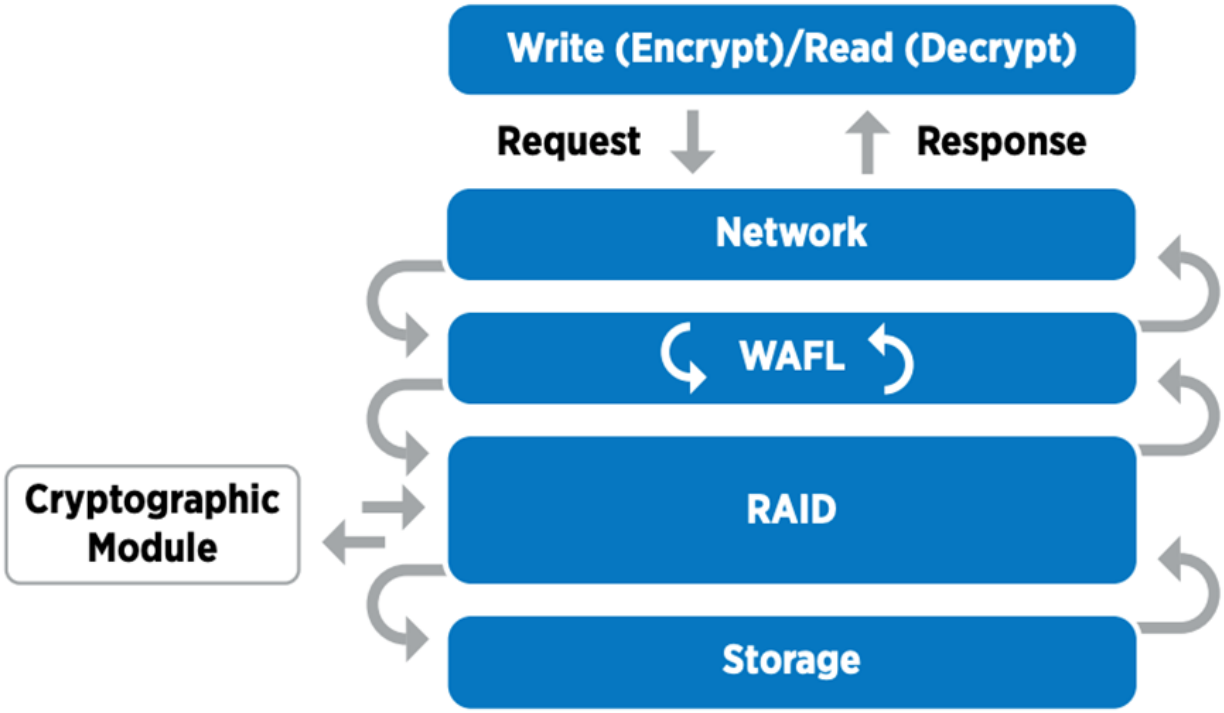
NetApp Aggregate Encryption et NetApp Volume Encryption

Les technologies NVE et NetApp Aggregate Encryption (NAE) permettent de chiffrer les données au niveau des volumes et des agrégats, de manière à ce qu'elles soient indépendantes du disque physique.

Mécanisme de chiffrement logiciel des données au repos, disponible à partir de ONTAP 9.1, conforme à la norme FIPS 140-2-2 depuis ONTAP 9.2. NVE permet à ONTAP de chiffrer les données pour chaque volume pour la granularité. NAE, disponible avec ONTAP 9.6, est une solution de plus en plus croissante de NVE. Il permet au ONTAP de chiffrer les données pour chaque volume et aux volumes de partager les clés dans l'ensemble de l'agrégat. NVE et NAE utilisent tous deux le chiffrement AES 256 bits. Les données peuvent également être stockées sur disque sans disques SED. Avec NVE et NAE, vous pouvez utiliser des fonctionnalités d'efficacité du stockage même lorsque le chiffrement est activé. Un chiffrement au niveau des applications uniquement résout tous les avantages de l'efficacité du stockage. Avec NVE et NAE, les fonctionnalités d'efficacité du stockage sont maintenues, car les données proviennent du réseau via NetApp WAFL et de la couche RAID qui détermine si les données doivent être chiffrées. Pour une meilleure efficacité du stockage, il est possible d'utiliser la déduplication globale avec NAE. Les volumes NVE et NAE peuvent coexister sur un même agrégat NAE. Les agrégats NAE ne prennent pas en charge les volumes non chiffrés.

Voici comment fonctionne le processus : lorsque les données sont cryptées, elles sont envoyées au module cryptographique validé FIPS 140-2 de niveau 1. Le module cryptographique crypte les données et les renvoie

à la couche RAID. Les données cryptées sont alors envoyées au disque. Par conséquent, avec la combinaison de NVE et de NAE, les données sont déjà chiffrées sur le disque. Les lectures suivent la trajectoire inverse. En d'autres termes, les données quittent le disque chiffré, sont envoyées au RAID, elles sont déchiffrées par le module cryptographique et sont ensuite envoyées le reste de la pile, comme illustré dans la figure suivante.



NVE utilise un module cryptographique logiciel conforme à la norme FIPS 140-2 de niveau 1.

Pour plus d'informations sur NVE, consultez le "Fiche technique NVE".

NVE protège les données dans le cloud. Cloud Volumes ONTAP et Azure NetApp Files peuvent assurer le chiffrement des données au repos conforme à la norme FIPS 140-2-2.

Depuis ONTAP 9.7, les volumes et les agrégats nouvellement créés sont chiffrés par défaut lorsque vous disposez d'une licence NVE et d'une gestion des clés intégrée ou externe. Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes. Les volumes que vous créez dans l'agrégat sont chiffrés par défaut. Vous pouvez remplacer la valeur par défaut lorsque vous chiffrez le volume.

COMMANDES CLI ONTAP NAE

Avant d'exécuter les commandes CLI suivantes, vérifiez que le cluster possède la licence NVE requise.

Pour créer un agrégat et le chiffrer, exécutez la commande suivante (lorsqu'elle s'exécute sur ONTAP 9.6 et version ultérieure de l'interface de ligne de commandes du cluster) :

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

Pour convertir un agrégat non-NAE en agrégat, exécutez la commande suivante (lorsqu'il s'exécute sur un ONTAP 9.6 et une interface de ligne de commande de cluster ultérieure) :

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

Pour convertir un agrégat NAE en agrégat non-NAE, exécutez la commande suivante (lorsqu'il s'exécute sur un ONTAP 9.6 et l'interface de ligne de commande du cluster par la suite) :

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

COMMANDES CLI ONTAP NVE

Depuis ONTAP 9.6, vous pouvez utiliser le chiffrement au niveau de l'agrégat pour attribuer des clés à l'agrégat contenant afin de chiffrer les volumes. Les volumes que vous créez dans l'agrégat sont chiffrés par défaut.

Pour créer un volume sur un agrégat NAE activé, exécutez la commande suivante (lorsqu'elle s'exécute sur ONTAP 9.6 et versions ultérieures de l'interface de ligne de commande du cluster) :

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

Pour activer le chiffrement d'un volume existant « inplace » sans déplacement du volume, exécutez la commande suivante (lorsqu'elle est exécutée sur un ONTAP 9.6 et version ultérieure de l'interface de ligne de commande du cluster) :

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

Pour vérifier que les volumes sont activés pour le chiffrement, exécutez la commande CLI suivante :

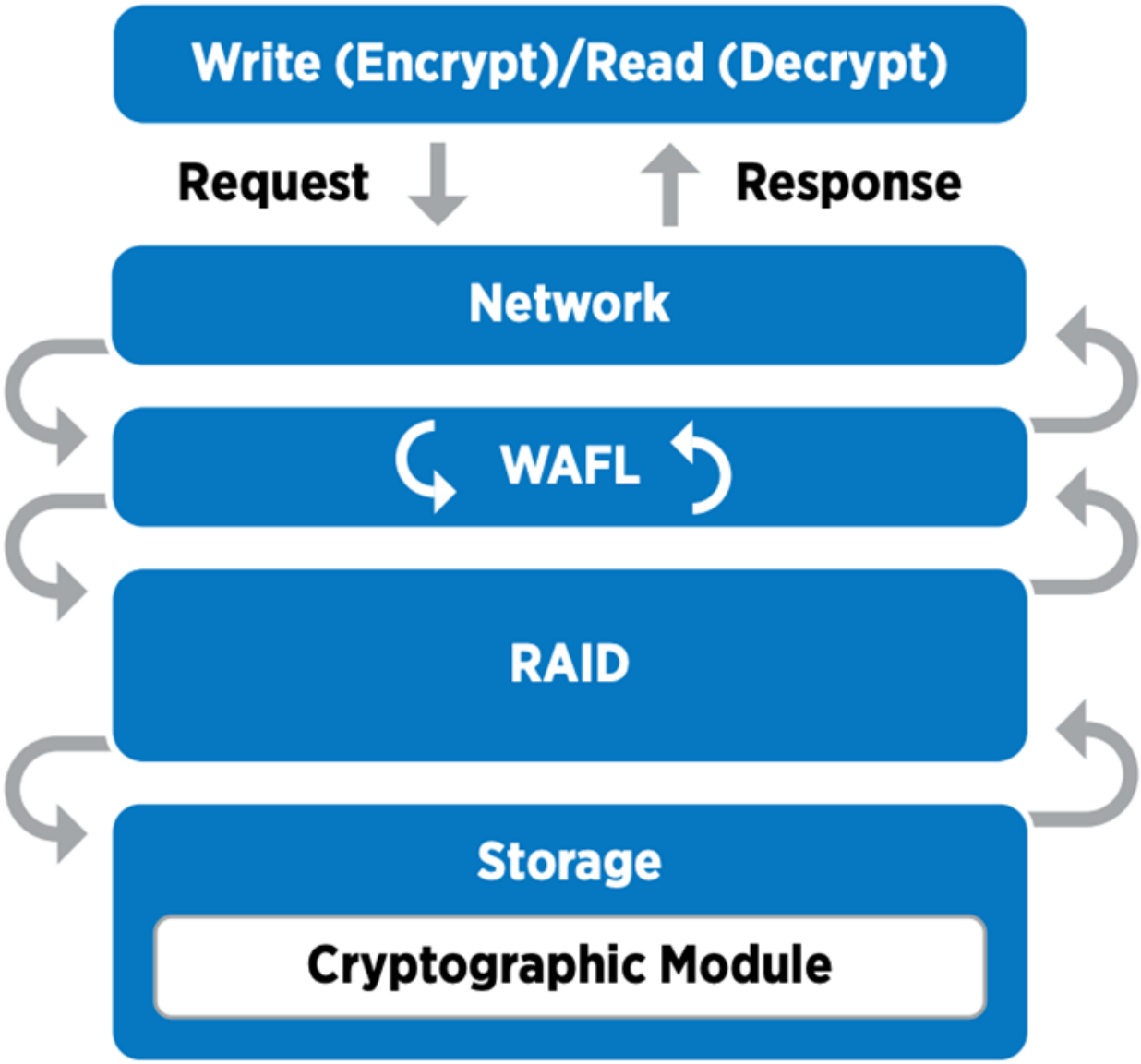
```
fp-health::> volume show -is-encrypted true
```

NSE

NSE utilise les disques SED pour effectuer le chiffrement des données à l'aide d'un mécanisme à accélération matérielle.

NSE est configuré pour utiliser des disques à autochiffrement FIPS 140-2 de niveau 2 pour faciliter la conformité et les retours de disques de secours, en assurant la protection des données au repos via le chiffrement de disque transparent AES 256 bits. Ces disques effectuent toutes les opérations de chiffrement des données en interne, comme illustré dans la figure ci-dessous, notamment la génération de clés de chiffrement. Pour empêcher tout accès non autorisé aux données, le système de stockage doit s'authentifier

auprès du disque à l'aide d'une clé d'authentification établie lors de la première utilisation du disque.



NSE utilise un chiffrement matériel sur chaque disque certifié conforme à la norme FIPS 140-2 de niveau 2.

Pour plus d'informations sur NSE, reportez-vous au "Fiche technique NSE".

Gestion des clés

La norme FIPS 140-2 s'applique au module cryptographique, tel que défini par la limite, comme illustré dans la figure suivante.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

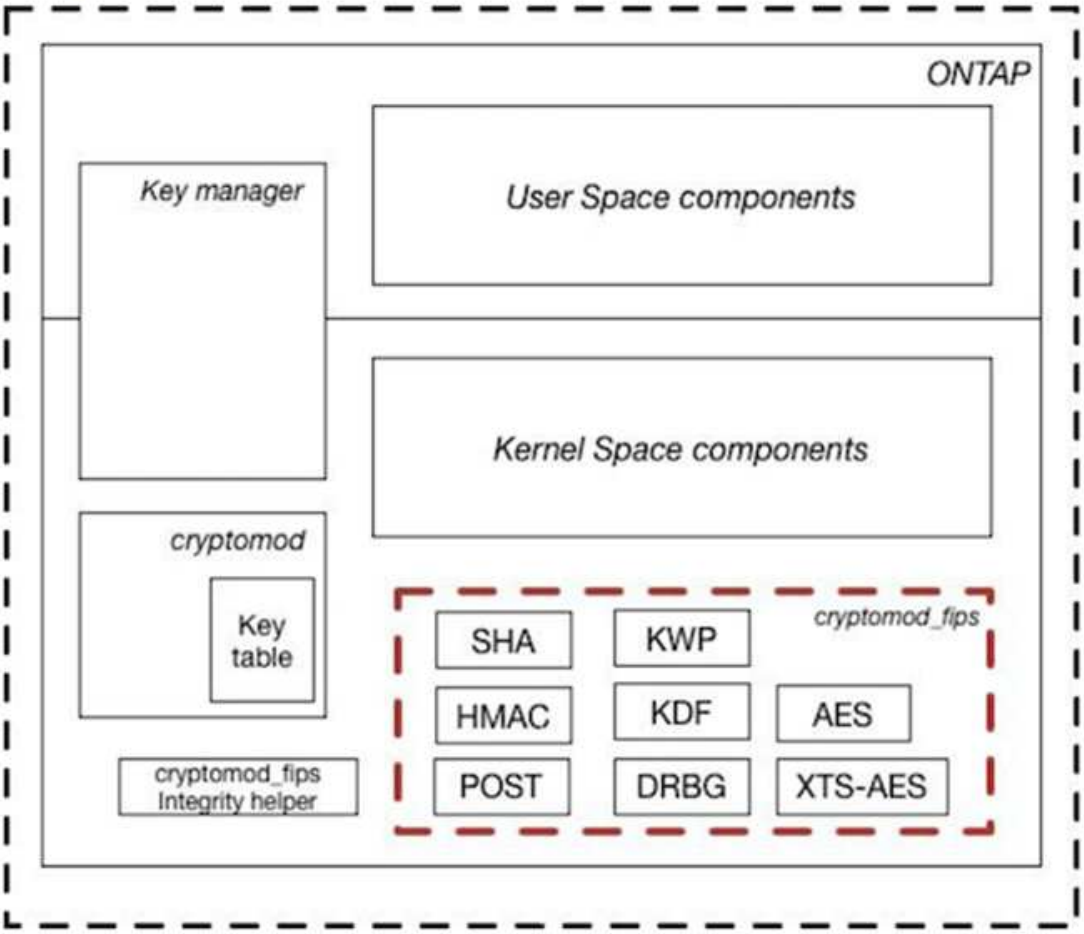


Figure 1 - Block Diagram

Le gestionnaire de clés assure le suivi de toutes les clés de cryptage utilisées par ONTAP. Les disques SED NSE utilisent le gestionnaire de clés pour définir les clés d'authentification pour les disques SED NSE. Avec le gestionnaire de clés, la solution combinée NVE et NAE est composée d'un module cryptographique logiciel, de clés de chiffrement et d'un gestionnaire de clés. Pour chaque volume, NVE utilise une clé de chiffrement des données XTS-AES 256 unique, qui stocke le gestionnaire de clés. La clé utilisée pour un volume de données est unique pour le volume de données du cluster et est générée lors de la création du volume chiffré. De même, un volume NAE utilise des clés de chiffrement des données XTS-AES 256 uniques par agrégat, ce que le gestionnaire de clés stocke également. Les clés NAE sont générées lors de la création de l'agrégat chiffré. ONTAP ne prégénère pas de clés, ne les réutilisez pas ou ne les affiche pas en texte clair : elles sont stockées et protégées par le gestionnaire de clés.

Prise en charge d'un gestionnaire de clés externe

Depuis la version ONTAP 9.3, les gestionnaires de clés externes sont pris en charge dans les solutions NVE et NSE. La norme FIPS 140-2 s'applique au module cryptographique utilisé dans la mise en œuvre du fournisseur spécifique. Le plus souvent, les clients FlexPod et ONTAP utilisent l'une des solutions suivantes validées (selon le "Matrice d'interopérabilité NetApp") gestionnaires clés :

- Gemalto ou SafeNet À L'ADRESSE
- Vormetric (Thales)
- IBM SKLM
- Utimaco (anciennement Microfocus, HPE)

La clé d'authentification NSE et NVMe SED est sauvegardée dans un gestionnaire de clés externe à l'aide du protocole KMIP (OASIS Key Management Interoperability Protocol), une norme du secteur. Seuls le système de stockage, le disque et le gestionnaire de clés ont accès à la clé et le disque ne peut pas être déverrouillé s'il est déplacé en dehors du domaine de sécurité, empêchant ainsi les fuites de données. Le gestionnaire de clés externe stocke également des clés de chiffrement de volume NVE et des clés de chiffrement d'agrégat NAE. Si le contrôleur et les disques sont déplacés et qu'ils n'ont plus accès au gestionnaire de clés externe, les volumes NVE et NAE ne sont plus accessibles et ne peuvent pas être déchiffrés.

L'exemple de commande suivant ajoute deux serveurs de gestion des clés à la liste des serveurs utilisés par le gestionnaire de clés externe pour stocker une machine virtuelle (SVM) `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

Dans le FlexPod cas d'une colocation, ONTAP permet aux utilisateurs d'utiliser la colocation pour des raisons de sécurité au niveau de la SVM.

Pour vérifier la liste des gestionnaires de clés externes, exécutez la commande CLI suivante :

```
fp-health::> security key-manager external show
```

Combinaison du cryptage pour le double cryptage (protection en couches)

Si vous devez isoler l'accès aux données et veiller à ce qu'elles soient protégées en permanence, les disques SED NSE peuvent être combinés avec un cryptage au niveau du réseau ou de la structure. Les disques SED NSE agissent comme un backstop si un administrateur oublie de configurer ou de configurer un cryptage de niveau supérieur. Pour deux couches de chiffrement distinctes, vous pouvez combiner les disques SED NSE avec NVE et NAE.

Plan de contrôle NetApp ONTAP en mode FIPS au niveau du cluster

Le logiciel de gestion de données NetApp ONTAP est doté d'une configuration FIPS-mode qui instancie un niveau de sécurité supplémentaire pour le client. Ce mode FIPS s'applique uniquement au plan de contrôle. Lorsque le mode FIPS est activé, conformément aux éléments clés de FIPS 140-2, transport Layer Security v1 (TLSv1) et SSLv3 sont désactivés et seuls TLS v1.1 et TLS v1.2 restent activés.

> Le panneau de contrôle ONTAP en mode FIPS est conforme à la norme FIPS 140-2 de niveau 1. Le mode FIPS sur l'ensemble du cluster utilise un module cryptographique logiciel fourni par NCSM.

Le mode de conformité FIPS 140-2 pour le plan de contrôle à l'échelle du cluster sécurise toutes les interfaces de contrôle de ONTAP. Par défaut, le mode FIPS 140-2 uniquement est désactivé. Cependant, vous pouvez activer ce mode en configurant le `is- fips-enabled` paramètre à `true` pour le `security config modify` commande.

Pour activer le mode FIPS sur le cluster ONTAP, exécutez la commande suivante :

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP vers les composants client ou serveur externes en dehors de ONTAP utilise le chiffrement des plaintes FIPS pour SSL.

Pour afficher le statut FIPS pour l'ensemble du cluster, exécutez les commandes suivantes :

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"Ensuite, les avantages de l'infrastructure convergée FlexPod."

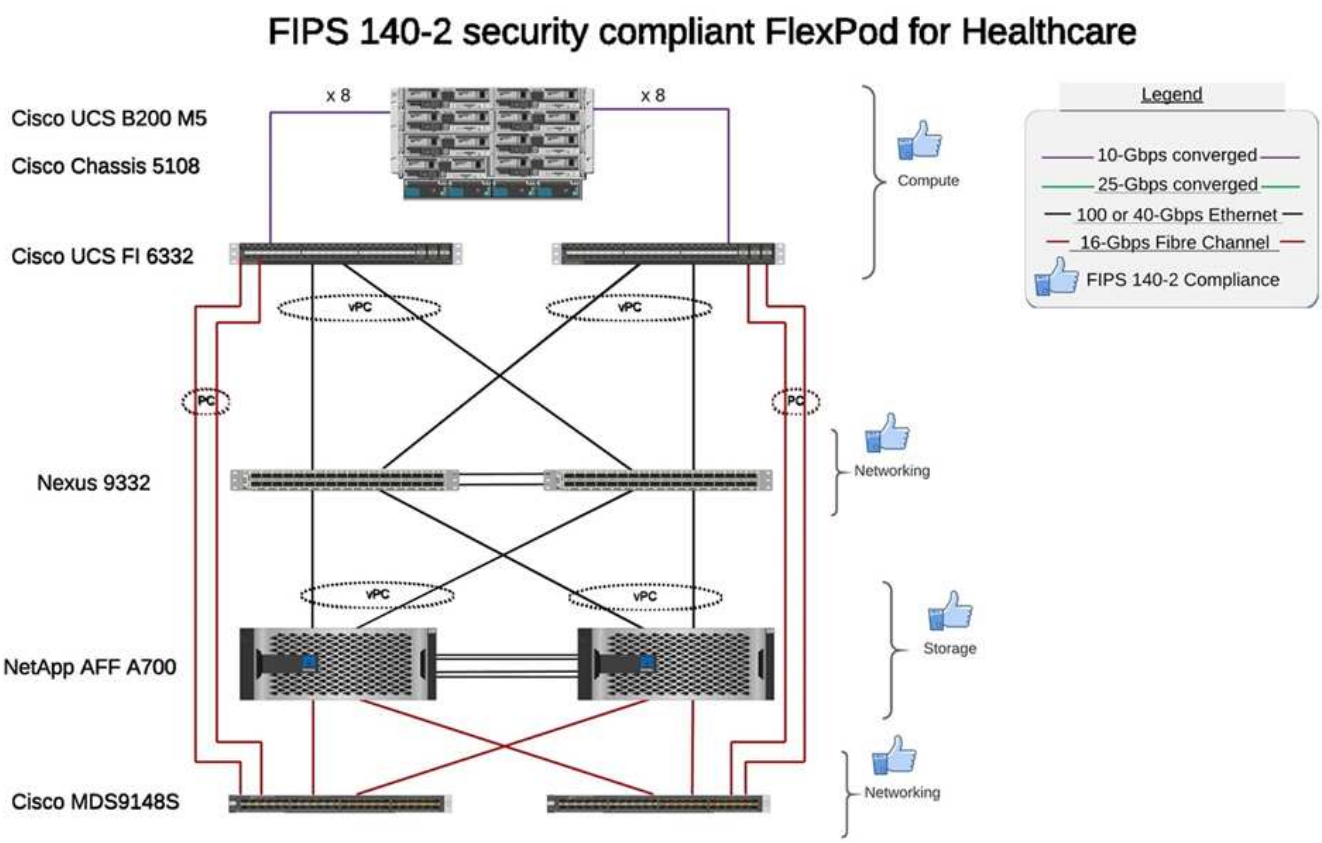
Avantages de la solution de l'infrastructure convergée FlexPod

"Précédent : stockage NetApp ONTAP de FlexPod et FIPS 140-2."

Les organismes de santé disposent de plusieurs systèmes stratégiques. Deux des systèmes les plus critiques sont les systèmes de dossiers médicaux électroniques (DME) et les systèmes d'imagerie médicale. Pour démontrer la configuration FIPS sur un système FlexPod, nous avons utilisé un système de DME open source et un système de communication et d'archivage des images open source pour la configuration en laboratoire et la validation des charges de travail sur le système FlexPod. Pour obtenir la liste complète des fonctionnalités EHR, des composants d'application logique EHR et les avantages des systèmes EHR lorsqu'ils sont implémentés sur un système FlexPod, consultez la section "Tr-4881 : FlexPod pour les systèmes de dossiers de santé électroniques". Pour obtenir la liste complète des fonctionnalités d'un système d'imagerie médicale, des composants d'application logique et des avantages des systèmes d'imagerie médicale lorsqu'ils sont implémentés sur FlexPod, consultez la section "Tr-4865 : FlexPod pour l'imagerie médicale".

Lors de la configuration de FIPS et de la validation des charges de travail, nous avons exercé les caractéristiques de workloads représentatives d'un organisme de santé typique. Par exemple, nous avons exercé un système open source EHR afin d'inclure des scénarios réalistes d'accès aux données des patients et de changement. Par ailleurs, nous avons exercé les charges de travail d'imagerie médicale incluant l'imagerie numérique et les communications dans des objets médicaux (DICOM) dans un `*. dcm` format de fichier. Les objets DICOM avec métadonnées étaient stockés dans le stockage de fichiers et en blocs. De plus, nous avons mis en œuvre des fonctionnalités de chemins d'accès multiples à partir d'un serveur virtualisé RedHat Enterprise Linux (RHEL). Nous stockons des objets DICOM sur un système NFS, des LUN montées à l'aide d'iSCSI et des LUN montées à l'aide de FC. Lors de la configuration et de la validation FIPS, nous avons observé que l'infrastructure convergée FlexPod dépassait nos attentes.

La figure suivante décrit le système FlexPod utilisé pour la configuration et la validation de FIPS. Nous avons utilisé "FlexPod Datacenter avec VMware vSphere 7.0 et NetApp ONTAP 9.7 conception validée par Cisco (CVD)" pendant le processus de configuration.



Composants matériels et logiciels de l'infrastructure de la solution

Les deux figures suivantes illustrent respectivement les composants matériels et logiciels utilisés lors du test FIPS lors de l'activation sur un FlexPod. Les recommandations présentées dans ces tableaux sont des exemples. Vous devez collaborer avec votre expert technique NetApp pour vous assurer que les composants sont adaptés à votre entreprise. Assurez-vous également que les composants et versions sont pris en charge dans le "Matrice d'interopérabilité NetApp" (IMT) et "Liste de compatibilité matérielle Cisco (HCL)".

Calque	Famille de produits	Quantité et modèle	Détails
Calcul	Châssis Cisco UCS 5108	1 ou 2	
	Les serveurs lames Cisco UCS	3 B200 M5	Chacun doté de 2 20 cœurs ou plus, de 2,7 GHz et de 128 Go de RAM
	Carte d'interface virtuelle Cisco UCS (VIC)	Cisco UCS 1440	Voir la
	2 interconnexions de fabric Cisco UCS	6332	-
Le réseau	Commutateurs Cisco Nexus	2 x Cisco Nexus 9332	-

Calque	Famille de produits	Quantité et modèle	Détails
Réseau de stockage	Réseau IP pour l'accès au stockage via les protocoles SMB/CIFS, NFS ou iSCSI	Mêmes commutateurs réseau que ci-dessus	-
	Accès au stockage via FC	2 x Cisco MDS 9148S	-
Stockage	Système de stockage 100 % Flash NetApp AFF A700	1 Cluster	Cluster à deux nœuds
	Tiroir disque	Un tiroir disque DS224C ou NS224	Plein avec 24 disques
	SSD	Pour 24, 1,2 To ou plus	-

Logiciel	Famille de produits	Version ou version	Détails
Divers	Linux	RHEL 7.X.	-
	Répertoires de base	Windows Server 2012 R2 (64 bits)	-
	NetApp ONTAP	ONTAP 9.7 ou version ultérieure	-
	Fabric Interconnect Cisco UCS	Cisco UCS Manager 4.1 ou version ultérieure	-
	Switchs Cisco Ethernet 3000 ou 9000	Pour la série 9000, 7.0(3)I7(7) ou ultérieure pour la série 3000, 9.2(4) ou ultérieure	-
	Cisco FC : Cisco MDS 9132T	8.4(1a) ou ultérieure	-
	Hyperviseur	VMware vSphere ESXi 6.7 U2 ou version ultérieure	-
Stockage	Système de gestion de l'hyperviseur	VMware vCenter Server 6.7 U3 (vCSA) ou version ultérieure	-
Le réseau	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	-
	NetApp SnapCenter	SnapCenter 4.3 ou version ultérieure	-
	Cisco UCS Manager	4.1(1c) ou ultérieure	
Hyperviseur	VMware ESXi		

Logiciel	Famille de produits	Version ou version	Détails
Gestion	Système de gestion de l'hyperviseur VMware vCenter Server 6.7 U3 (vCSA) ou version ultérieure		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 ou version ultérieure	
	NetApp SnapCenter	SnapCenter 4.3 ou version ultérieure	
	Cisco UCS Manager	4.1(1c) ou ultérieure	

"Ensuite, d'autres considérations relatives à la sécurité FlexPod."

Autres considérations relatives à la sécurité FlexPod

"Précédent : avantages de la solution pour l'infrastructure convergée FlexPod."

L'infrastructure FlexPod est une plateforme modulaire, convergée, évolutive (scale-out et scale-up) et économique. Avec la plateforme FlexPod, vous pouvez faire évoluer indépendamment les ressources de calcul, de réseau et de stockage pour accélérer le déploiement de vos applications. En outre, l'architecture modulaire garantit la continuité de l'activité, même lors des activités de mise à niveau et d'évolutivité horizontale de votre système.

Les différents composants d'un système HIT nécessitent que les données soient stockées dans des systèmes de fichiers SMB/CIFS, NFS, Ext4 et NTFS. Par conséquent, l'infrastructure doit fournir un accès aux données via les protocoles NFS, CIFS et SAN. Un système de stockage NetApp unique peut prendre en charge tous ces protocoles, ce qui évite la pratique existante de systèmes de stockage spécifiques au protocole. Un système de stockage NetApp unique peut également prendre en charge plusieurs charges DE travail HIT (DME, PACS ou VNA), génomique, VDI, etc. avec des niveaux de performance garantis et configurables.

Lorsqu'elle est déployée dans un système FlexPod, HIT offre plusieurs avantages spécifiques au secteur de la santé. La liste suivante fournit une description générale de ces avantages :

- **Sécurité FlexPod**. La sécurité est à la base même d'un système FlexPod. Ces dernières années, les attaques par ransomware sont devenues une menace. Les ransomwares sont un type de malware basé sur la cryptovirologie, l'utilisation de la cryptographie pour créer des logiciels malveillants. Ce programme malveillant peut utiliser à la fois un cryptage symétrique et asymétrique pour verrouiller les données d'une victime et exiger une rançon afin de fournir la clé de chiffrement des données. Pour découvrir comment la solution FlexPod permet de réduire les menaces telles que les ransomware, rendez "Tr-4802 : la solution aux attaques par ransomware"-vous sur . Les composants de l'infrastructure FlexPod sont également "Conforme à la norme FIPS 140-2".
- **Cisco Intersight** Cisco Intersight est une plateforme de gestion à la demande basée sur le cloud et innovante, qui offre une fenêtre unique pour la gestion et l'orchestration FlexPod de la pile complète. La plateforme Intersight utilise des modules cryptographiques conformes à la norme FIPS 140-2. L'architecture de gestion hors bande de la plate-forme la rend hors de portée pour certaines normes ou certains audits comme HIPAA. Aucune information d'intégrité identifiable sur le réseau n'est envoyée au portail Intersight.

- **Technologie NetApp FPolicy.** NetApp FPolicy (une évolution de l'politique de fichiers de noms) est un framework de notification d'accès aux fichiers permettant de surveiller et de gérer l'accès aux fichiers via les protocoles NFS ou SMB/CIFS. Depuis plus de dix ans, cette technologie fait partie du logiciel de gestion des données ONTAP. Elle aide à détecter les attaques par ransomware. Ce moteur Zero Trust fournit des mesures de sécurité supplémentaires au-delà des autorisations dans les listes de contrôle d'accès (ACL). FPolicy possède deux modes de fonctionnement : natif et externe :
  - Le mode natif fournit à la fois la liste noire et la liste blanche des extensions de fichiers.
  - Le mode externe offre les mêmes fonctionnalités que le mode natif, mais il s'intègre également à un serveur FPolicy qui s'exécute en externe au système ONTAP ainsi qu'à un système de gestion des informations de sécurité et des événements (SIEM). Pour plus d'informations sur la lutte contre les ransomwares, consultez le "Lutte contre les attaques par ransomware : troisième partie : ONTAP FPolicy, un autre outil natif puissant (ou gratuit)" blog.
- **Données au repos**. Avec ONTAP 9 et les versions ultérieures, les données au repos sont chiffrées conformes à la norme FIPS 140-2 :
  - NSE est une solution matérielle qui utilise des disques à chiffrement automatique.
  - NVE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque où il est activé avec une clé unique pour chaque volume.
  - NAE est une solution logicielle qui permet de chiffrer n'importe quel volume de données sur n'importe quel type de disque grâce à des clés uniques pour chaque agrégat.

> Depuis ONTAP 9.7, NAE et NVE sont activés par défaut si le package de licence NetApp NVE dont le nom est VE est en place.

- **Données en vol**. Depuis ONTAP 9.8, la sécurité IPSec (Internet Protocol Security) fournit une prise en charge de cryptage de bout en bout pour tout le trafic IP entre un client et un SVM ONTAP. Le cryptage de données IPSec pour tout le trafic IP inclut les protocoles NFS, iSCSI et SMB/CIFS. IPSec fournit la seule option de cryptage en vol pour le trafic iSCSI.
- **Chiffrement des données de bout en bout dans une Data Fabric hybride et multicloud**. Les clients qui utilisent des technologies de chiffrement des données au repos comme NSE ou NVE et Cluster peering Encryption (CPE) pour le trafic de réplication des données peuvent désormais utiliser le chiffrement de bout en bout entre les clients et le stockage dans leur structure de données multicloud hybride en effectuant une mise à niveau vers ONTAP 9.8 ou version ultérieure et en utilisant IPSec. À partir de ONTAP 9, vous pouvez activer le mode de conformité FIPS 140-2 pour les interfaces du plan de contrôle au niveau du cluster. Par défaut, le mode FIPS 140-2 uniquement est désactivé. À partir de ONTAP 9.6, CPE assure la prise en charge du cryptage TLS 1.2 AES-256 GCM pour les fonctionnalités de réplication des données ONTAP telles que les technologies NetApp SnapMirror, NetApp SnapVault et NetApp FlexCache. Le chiffrement est configuré au moyen d'une clé pré-partagée (PSK) entre deux pairs de cluster.
- **Colocation sécurisée**. Prend en charge les besoins accrus de l'infrastructure partagée de serveurs et de stockage virtualisés, ce qui permet une colocation sécurisée des informations spécifiques aux sites, notamment si vous hébergez plusieurs instances de bases de données et de logiciels.

"Suivant: Conclusion."

Conclusion

"Précédent : autres considérations de sécurité FlexPod."

En exécutant votre application médicale sur une plateforme FlexPod, votre organisme de santé est mieux protégé par une plateforme compatible FIPS 140-2. FlexPod propose

une protection à plusieurs couches pour chaque composant : calcul, réseau et stockage. Les fonctionnalités de protection des données de FlexPod protègent les données au repos ou à la volée. Les sauvegardes restent sécurisées et prêtes à l'emploi, selon les besoins.

Évitez les erreurs humaines en tirant parti des designs prévalidés de FlexPod soumis à des tests rigoureux d'infrastructures convergées issues du partenariat stratégique de Cisco et de NetApp. Un système FlexPod conçu et conçu pour fournir des performances prévisibles avec une faible latence des systèmes et une haute disponibilité avec un impact minimal, même lorsque la norme FIPS 140-2 est activée dans les couches de calcul, de réseau et de stockage. Cette approche permet d'améliorer l'expérience utilisateur et de bénéficier d'un temps de réponse optimal pour les utilisateurs de votre système HIT.

"Suivant : Remerciements, historique des versions, et où trouver des informations supplémentaires."

Remerciements, historique des versions et où trouver des informations supplémentaires

"Précédent: Conclusion."

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

- Guide de configuration de la sécurité de la gamme Cisco MDS 9000 NX-OS

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Guide de configuration de la sécurité Cisco Nexus série 9000 NX-OS, version 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- Publication NetApp and Federal information Processing Standard (FIPS) 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- Guide NetApp ONTAP 9 sur le renforcement du partenariat

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- Guide d'alimentation du cryptage NetApp

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- Fiche produit NVE et NAE

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- Fiche technique NSE

https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- Centre de documentation ONTAP 9

  http://docs.netapp.com

- Publication NetApp and Federal information Processing Standard (FIPS) 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Conformité Cisco et FIPS 140-2

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- Module de chiffrement NetApp

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Cybersécurité pour les moyennes et grandes organisations dans le domaine de la santé

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Programme de validation Cisco et module cryptographique (CMVP)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp Storage Encryption, disques avec autocryptage NVMe, NetApp Volume Encryption et NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption et chiffrement d'agrégat NetApp

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp Storage Encryption

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod pour les systèmes de dossiers médicaux électroniques

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Disponibilité immédiate des données : améliorer les performances dans les environnements de DME EPIC grâce à la technologie Flash connectée au cloud

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- FlexPod Datacenter pour infrastructure EHR Epic

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Guide de déploiement de FlexPod Datacenter pour Epic EHR

https://www.netapp.com/media/10658-tr-4693.pdf

- Infrastructure de data Center FlexPod pour le logiciel MEDITECH

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- La norme FlexPod s'étend au logiciel MEDITECH

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- FlexPod pour MEDITECH : Guide de dimensionnement

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- FlexPod pour l'imagerie médicale

  https://www.netapp.com/media/19793-tr-4865.pdf

- L'IA dans le domaine de la santé

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- FlexPod pour le secteur de la santé facilite votre transformation

  https://flexpod.com/solutions/verticals/healthcare/

- FlexPod de Cisco et NetApp

  https://flexpod.com/

Remerciements

- Abhinav Singh, Ingénieur marketing et technique, NetApp
- Brian O'Mehony, architecte de solutions au sein du secteur de la santé (Epic), NetApp
- Brian Pruitt, responsable du développement commercial chez NetApp
- Arvind Ramakrishnan, architecte de solutions senior, NetApp
- Michael Hommer, Directeur technique mondial chez FlexPod, NetApp

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Avril 2021	Version initiale

Cisco Intersight avec le stockage ONTAP NetApp

Guide de démarrage rapide de Cisco Intersight avec le stockage NetApp

En partenariat avec : 

Introduction

NetApp et Cisco se sont associés pour offrir Cisco Intersight, une vue centralisée de l'écosystème FlexPod. Cette intégration simplifiée crée une plateforme de gestion unifiée pour tous les composants de l'infrastructure FlexPod et de la solution FlexPod. Cisco Intersight permet de surveiller le stockage NetApp, les ressources de calcul Cisco et les inventaires VMware. Elle vous permet également d'orchestrer ou d'automatiser des flux de travail pour accomplir conjointement des tâches de stockage et de virtualisation.

Informations associées

Pour en savoir plus, consultez ces documents et sites web :

"Tr 4883 : FlexPod Datacenter avec ONTAP 9.8, ONTAP Storage Connector for Cisco Intersight et Cisco Intersight Managed mode"

"Centre d'aide de Cisco Intersight"

"Présentation de Cisco Intersight Getting Started"

"Guide d'installation et de mise à niveau d'Intersight Appliance"

Quoi de neuf

Cette section répertorie les nouvelles fonctionnalités disponibles pour Cisco Intersight avec le stockage NetApp ONTAP.

Janvier 2024

- Orchestration du stockage NetApp à l'aide de workflows de référence désormais disponibles au téléchargement dans GitHub via "Référentiel de flux de travail FlexPod Intersight". Pour plus d'informations sur les nouveaux flux de travail de référence dans GitHub, voir "Cas d'utilisation 2 : orchestration du stockage NetApp à l'aide des workflows de référence".

Novembre 2023

- Ajout de la page Namespaces NVMe dans la section Inventory de l'interface utilisateur.

Août 2023

Une mise à niveau vers NetApp Active IQ Unified Manager 9.13GA est nécessaire pour garantir la compatibilité et l'intégralité des fonctionnalités avec la dernière version.

- Amélioration de la tâche New NetApp Smart LUN pour indiquer clairement la disponibilité des options de sélection permettant de créer un nouveau groupe initiateur ou de sélectionner un groupe initiateur existant. Lorsque les utilisateurs sélectionnent la zone pour créer un nouveau groupe initiateur, le paramètre permettant de choisir un groupe initiateur existant n'est plus disponible. Si les utilisateurs désélectionnez la case pour créer un nouveau groupe initiateur, le paramètre du groupe initiateur existant devient disponible.
- Amélioration des tâches Nouveau mappage de LUN NetApp et Supprimer le mappage de LUN NetApp - effectué. La nouvelle relation entre la LUN et le groupe initiateur est maintenant mise à jour. L'inventaire de l'interface utilisateur est immédiatement mis à jour pour la LUN et le groupe initiateur lors de l'exécution de la tâche.
- La page vérifications se charge maintenant correctement lors de la première connexion des utilisateurs et ne nécessite plus d'actualisation.

Juillet 2023

Une mise à niveau vers NetApp Active IQ Unified Manager 9.13GA est nécessaire pour garantir la compatibilité et l'intégralité des fonctionnalités avec la dernière version.

- Noms mis à jour pour les tâches de stockage NetApp. Voir cas d'utilisation 3 flux de travail personnalisés à l'aide d'un formulaire sans concepteur pour la liste complète des tâches renommées.
- L'adresse IP de l'interface NFS a été ajoutée en tant que sortie de la tâche Nouveau volume intelligent NAS NetApp.
- Vérifiez que le transport ASUP est HTTPS a été ajouté à l'onglet vérifications.
- Le type de niveau correct pour tous les niveaux s'affiche désormais correctement sous l'interface utilisateur tiers.
- Toutes les licences compatibles s'affichent désormais correctement dans la page licences.
- La valeur exacte des partages CIFS sans ou sans répertoire personnel s'affiche désormais sur la page partages.
- Le tri et le filtrage sont désormais activés pour la colonne mappée sur la page LUN.
- Le tri et le filtrage ont maintenant activé la colonne authentification activée sur la page serveurs NTP.
- Ajout de nouvelles vérifications et des catégories correspondantes suivantes à l'onglet vérifications.
  - Sécurité
  - Anti-ransomware
  - Disponibilité
  - Autre
- Dans la vue détaillée Inventaire, le rapport est maintenant utilisé au lieu de la capacité physique utilisée.

Juin 2023

Une mise à niveau vers NetApp Active IQ Unified Manager 9.13RC1 est nécessaire pour garantir la compatibilité et l'intégralité des fonctionnalités avec la dernière version.

- Noms mis à jour pour les tâches de stockage NetApp. Voir "Cas d'utilisation 3 workflows personnalisés à

l'aide d'un formulaire sans concepteur" pour la liste complète des tâches renommées.

Avril 2023

- Ajout des onglets protection Policies (SnapMirror) et Snapshot Policies dans la page Policies de la section Inventory de l'interface utilisateur.
- Ajout de la page clients NFS sous la section Inventaire de l'interface utilisateur.
- Ajout de la colonne protégé dans la page machines virtuelles de stockage sous la section Inventaire de l'interface utilisateur.
- Modification du mode de rapport et d'affichage des informations de réduction des données.
- Ajout des onglets local Tier et Cloud Tier sous la page tiers dans la section Inventaire de l'interface utilisateur.
- La colonne nœud s'affiche désormais après la colonne Nom sous la page ports de la section Inventaire de l'interface utilisateur.

Janvier 2023

Une mise à niveau vers NetApp Active IQ Unified Manager 9.12 GA est nécessaire pour garantir la compatibilité et l'intégralité des fonctionnalités de la dernière version. Pour obtenir la liste des problèmes connus liés à cette version, reportez-vous à la section Problèmes connus.

- Les contrôles d'interopérabilité Intersight permettent désormais de distinguer les modes de microprogramme de l'UCSM et de l'IMM lors de l'exécution des contrôles de compatibilité.
- Les relations de protection ne s'afficheront pas dans Intersight pour ONTAP 9.7. Ce problème a été résolu dans la version ONTAP 9.8RC1.

Août 2022

Une mise à niveau vers NetApp Active IQ Unified Manager 9.11 GA est nécessaire pour garantir la compatibilité et l'intégralité des fonctionnalités de la dernière version. Pour obtenir la liste des problèmes connus liés à cette version, reportez-vous à la section Problèmes connus.

- Calcul de la capacité disponible du cluster mis à jour pour correspondre à System Manager
- Page général du cluster mise à jour pour masquer le récapitulatif des mesures de performances jusqu'à ce que les données de performances soient renseignées
- Résolution d'un problème lié à l'interface utilisateur de la page générale du cluster qui a occasionnellement provoqué l'arrêt de la page
- Ajout de partages CIFS, de services CIFS, de qtrees et de règles SnapMirror SVM à l'inventaire interne.
- Partages et qtrees ajoutés au menu de navigation de l'interface utilisateur, sous la section Logical Inventory (Inventaire logique)
- Partages ajoutés sous forme d'onglet à partir d'une VM de stockage sélectionnée
- Ajout d'informations sur le service CIFS dans l'onglet général de la machine virtuelle de stockage si la machine virtuelle de stockage est activée par CIFS
- Ajout d'une page de vérification de cluster qui permet aux utilisateurs de valider la configuration des systèmes de stockage NetApp conformément aux meilleures pratiques

Juillet 2022

- Des graphismes améliorés pour le ratio de réduction des données du cluster sont désormais disponibles dans le widget capacité
- Ajout de l'onglet interfaces FC à la page interfaces réseau
- La création d'un nouveau volume à l'aide de la tâche générique "Nouveau volume de stockage" définit maintenant la garantie d'espace volume sur aucun et le pourcentage de réserve snapshot sur 0%
- Le champ Commentaire de la tâche Modifier la stratégie Snapshot est maintenant facultatif et n'est plus obligatoire
- Inventaire de l'interface et cohérence de l'orchestration améliorées
- Les informations de capacité Intersight sous capacité du cluster sont désormais cohérentes avec System Manager
- Case à cocher ajoutée sous la tâche Nouvelle machine virtuelle de stockage pour afficher tous les paramètres lors de la création d'une nouvelle interface de gestion afin d'améliorer la convivialité
- Protocoles déplacés en dessous de la correspondance du client, désormais compatibles avec System Manager
- Page générale de la règle d'exportation affichant maintenant le ou les protocoles d'accès
- suppression d'igroup désormais enregistrée de manière conditionnelle
- Ajout des paramètres « Failover Policy » et « autorevert » pour NAS sous Nouvelle interface de données Storage NAS et Nouvelle interface de données Storage iSCSI
- La restauration de la tâche New Storage NAS Smart Volume supprime désormais la stratégie d'exportation si aucun autre volume n'est associé
- Améliorations apportées aux tâches Smart Volume et Smart LUN

Avril 2022

Pour assurer la compatibilité et une fonctionnalité complète avec les prochaines versions, il est recommandé de mettre à niveau votre Active IQ Unified Manager vers la version 9.10P1.

- Ajout de la page Broadcast Domain à Ethernet Port Detail
- A modifié le terme « agrégat » en « Tier » pour l'agrégat et la SVM au sein de l'interface utilisateur
- Le terme « État du cluster » est passé à « État de la baie »
- Le filtre MTU fonctionne maintenant pour les caractères <,>,=,⇐,>=
- Ajout de la page d'interface réseau à l'inventaire du cluster
- Ajout de AutoSupport à l'inventaire du cluster
- Ajouté `cdpd.enable` option vers le nœud
- Ajout d'un objet pour le voisin CDP
- Ajout des tâches de stockage des flux de travail NetApp dans Cisco InterSight. Voir "Cas d'utilisation 3 workflows personnalisés à l'aide d'un formulaire sans concepteur" Vous trouverez une liste complète des tâches de stockage NetApp.

Janvier 2022

- Ajout d'alarmes Intersight basées sur les événements pour NetApp Active IQ Unified Manager 9.10 ou version ultérieure.

> Pour assurer la compatibilité et une fonctionnalité complète dans les prochaines versions, nous vous recommandons de mettre à niveau votre Active IQ Unified Manager NetApp vers la version 9.10.

- Définissez explicitement chaque protocole activé (vrai ou faux) pour Storage Virtual machine
- État clusterHealthStatus mappé ok-avec suppression sur OK
- Colonne Santé renommée dans la colonne État du cluster, sous la page de liste Cluster List
- Affichage de la matrice de stockage « inaccessible » si le cluster est arrêté ou inaccessible
- Colonne Santé renommée dans la colonne État de la matrice sous la page général du cluster
- Le SVM dispose désormais d'un onglet « volumes » qui affiche tous les volumes du SVM
- Le volume dispose d'une section de capacité de snapshot
- Les licences s'affichent maintenant correctement

Octobre 2021

- Liste mise à jour des tâches de stockage NetApp disponibles dans Cisco Intersight. Voir "Cas d'utilisation 3 workflows personnalisés à l'aide d'un formulaire sans concepteur" Vous trouverez une liste complète des tâches de stockage NetApp.
- Ajout de la colonne Santé sous la page liste des clusters.
- Des détails étendus sont désormais disponibles sous la page général pour un groupe sélectionné.
- Le tableau du serveur NTP est désormais accessible via le volet de navigation.
- Ajout d'un nouvel onglet capteurs contenant la page général de la machine virtuelle de stockage.
- Résumé des groupes VLAN et d'agrégation de liens maintenant disponible sous la page Port General.
- Capacité totale des données ajoutée sous le tableau Volume Total Capacity.
- Colonnes latence, IOPS et débit ajoutées sous Statistiques de volume moyennes, Statistiques de LUN moyennes, Statistiques moyennes sur l'agrégat, Statistiques moyennes sur les machines virtuelles de stockage et statistiques moyennes sur les nœuds

> Les metrics de performance ci-dessus ne sont disponibles que pour les baies de stockage contrôlées par le biais de NetApp Active IQ Unified Manager 9.9 ou version ultérieure.

Problèmes connus

- Si vous utilisez une version d'AIQUM 9.11 ou antérieure, un écart se produit entre les valeurs affichées sur la page liste de stockage et le graphique à barres de capacité de la page général de stockage. Pour résoudre ce problème, passez à AIQUM 9.12 ou supérieur pour garantir la précision des valeurs de capacité affichées.
- Si vous utilisez AIQUM 9.11 ou une version antérieure, toute vérification effectuée par l'onglet « interopérabilité » de la page « systèmes intégrés » ne permettra pas de distinguer précisément les composants IMM et UCSM Cisco. Pour résoudre ce problème, passez à AIQUM 9.12 pour vous assurer que tous les composants sont correctement identifiés.

- Pour garantir que les données d'inventaire du stockage Intersight ne sont pas affectées pendant le processus de collecte des données, tous les clusters ONTAP non pris en charge (c'est-à-dire les versions inférieures à ONTAP 9.7P1) doivent être supprimés de l'application Active IQ Unified Manager (AIQUM).
- Pour que toutes les cibles revendiquées puissent être correctement exécutées, il faut au moins une version AIQUM de 9.11 pour que les requêtes d'interopérabilité du système intégré FlexPod soient exécutées.
- La page vérifications de l'inventaire de stockage ne s'affiche pas si le cluster ONTAP est ajouté à AIQUM à l'aide d'un nom de domaine complet. Les utilisateurs doivent ajouter des clusters ONTAP à AIQUM à l'aide d'une adresse IP.

De formation

Vérifiez que vous respectez les exigences en matière de matériel, de logiciels et de licences pour l'intégration du stockage NetApp ONTAP dans Cisco Intersight.

Configuration matérielle et logicielle requise

Il s'agit des composants matériels et logiciels minimum requis pour implémenter la solution. Ils peuvent varier selon la mise en œuvre de la solution et les besoins du client.

Composant	Détails de l'exigence
NetApp ONTAP	ONTAP 9.7P1 et versions ultérieures
NetApp Active IQ Unified Manager	La dernière version de NetApp Active IQ Unified Manager est requise (actuellement 9.14RC1)
Baie de stockage NetApp	Toutes les baies de stockage ONTAP ASA, AFF et FAS sont prises en charge pour ONTAP 9.7P1 et versions ultérieures
Hyperviseur de virtualisation	VSphere 7.0 et versions ultérieures

Reportez-vous à la section "Systèmes pris en charge par Cisco Intersight" Pour les exigences minimales des composants de calcul Cisco UCS et de la version UCSM.

Conditions requises pour les licences Cisco Intersight

Cisco Intersight propose des services tels que le service d'infrastructure et le service d'orchestration cloud pour gérer, automatiser et optimiser le stockage physique (stockage NetApp). Vous pouvez utiliser ces services pour gérer le serveur Cisco UCS et le système Cisco HyperFlex. Le service d'infrastructure et le service Cloud Orchestrator utilisent un modèle de licence par abonnement avec plusieurs tiers. Vous pouvez choisir le niveau de volume de serveur Cisco UCS requis pour la période d'abonnement sélectionnée.

Modèle de licence

Le modèle de licence des services d'infrastructure Cisco Intersight a été simplifié et offre désormais les deux tiers suivants :

- **Cisco Intersight Infrastructure Services Essentials** - le niveau de licence Essentials offre la gestion du serveur, y compris la fonctionnalité de surveillance de l'état global, l'inventaire, la prise en charge proactive via l'intégration Cisco TAC, l'authentification multifacteur, ainsi que l'accès au SDK et à l'API.
- **Cisco Intersight Infrastructure Services Advantage** - le niveau de licence Advantage offre une gestion

avancée des serveurs avec une visibilité étendue, l'intégration de l'écosystème, l'automatisation du matériel et des logiciels Cisco et tiers, ainsi que des solutions multi-domaines.

Pour plus d'informations sur les fonctionnalités couvertes par les différents niveaux de licence, accédez à "Licence Infrastructure Services".

Avant de commencer

Pour contrôler et orchestrer le stockage NetApp depuis Cisco InterSight, vous avez besoin d'une appliance virtuelle NetApp Active IQ Unified Manager et Cisco Intersight installée dans l'environnement vCenter.

Installez ou mettez à niveau NetApp Active IQ Unified Manager

Installer ou mettre à niveau vers Active IQ Unified Manager (la dernière version est requise, actuellement 9.14RC1) si vous ne l'avez pas fait. Pour obtenir des instructions, reportez-vous au "Documentation NetApp Active IQ Unified Manager".

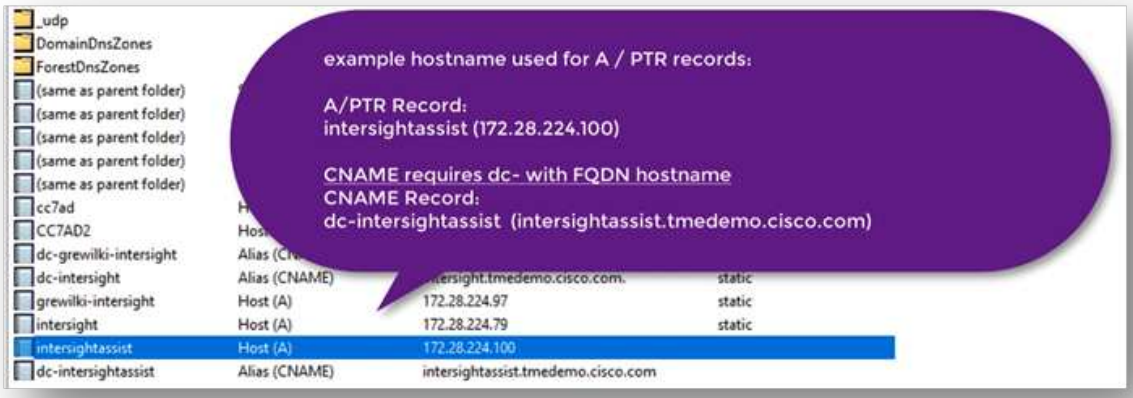
Installation de l'appliance virtuelle Cisco InterSight Assist

Assurez-vous que vous rencontrez le "Exigences relatives aux licences, aux systèmes et au réseau pour les appliances virtuelles Cisco Intersight".

Étapes

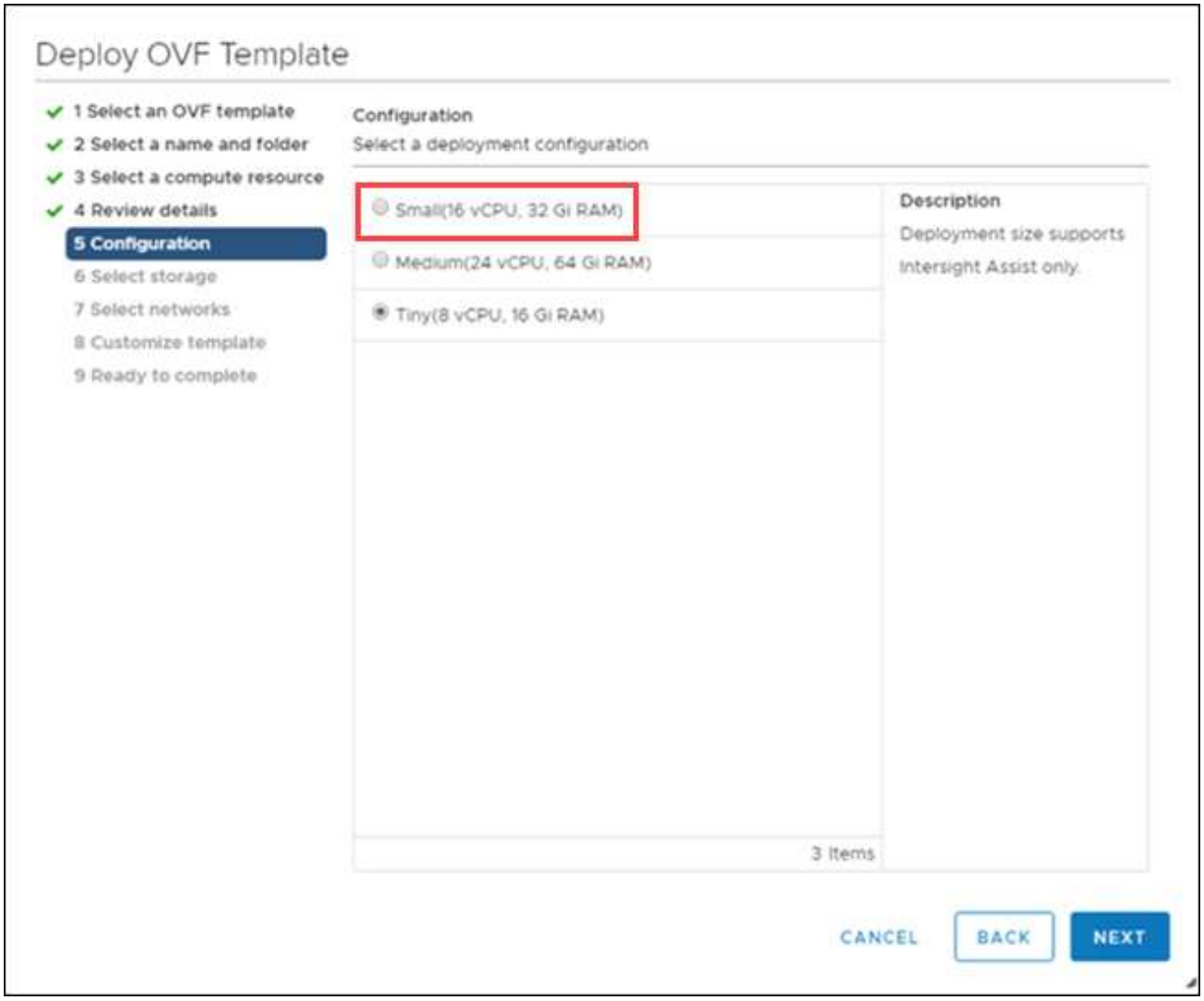
1. Créez un compte Cisco InterSight. Visitez "https://intersight.com/" Pour créer votre compte InterSight. Vous devez disposer d'un ID Cisco valide pour créer un compte Cisco Intersight.
2. Téléchargez l'appliance virtuelle Intersight sur "software.cisco.com". Pour plus d'informations, consultez le "Guide d'installation et de mise à niveau d'Intersight Appliance".
3. Déployer l'OVA. DNS et NTP sont nécessaires pour déployer le fichier OVA.

   a. Configurez DNS avec Des enregistrements a/PTR et CNAME alias avant de déployer l'OVA. Voir l'exemple ci-dessous.

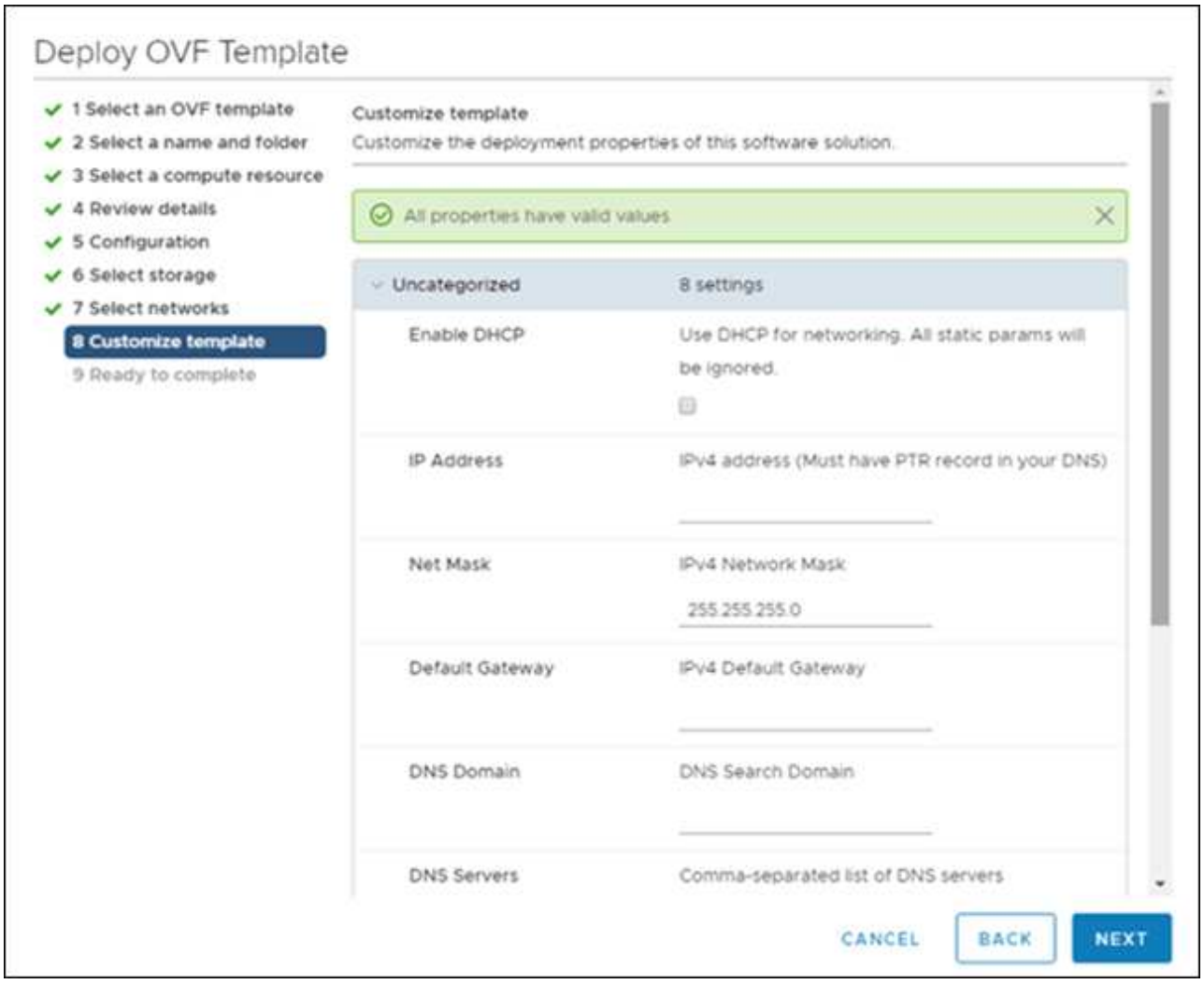


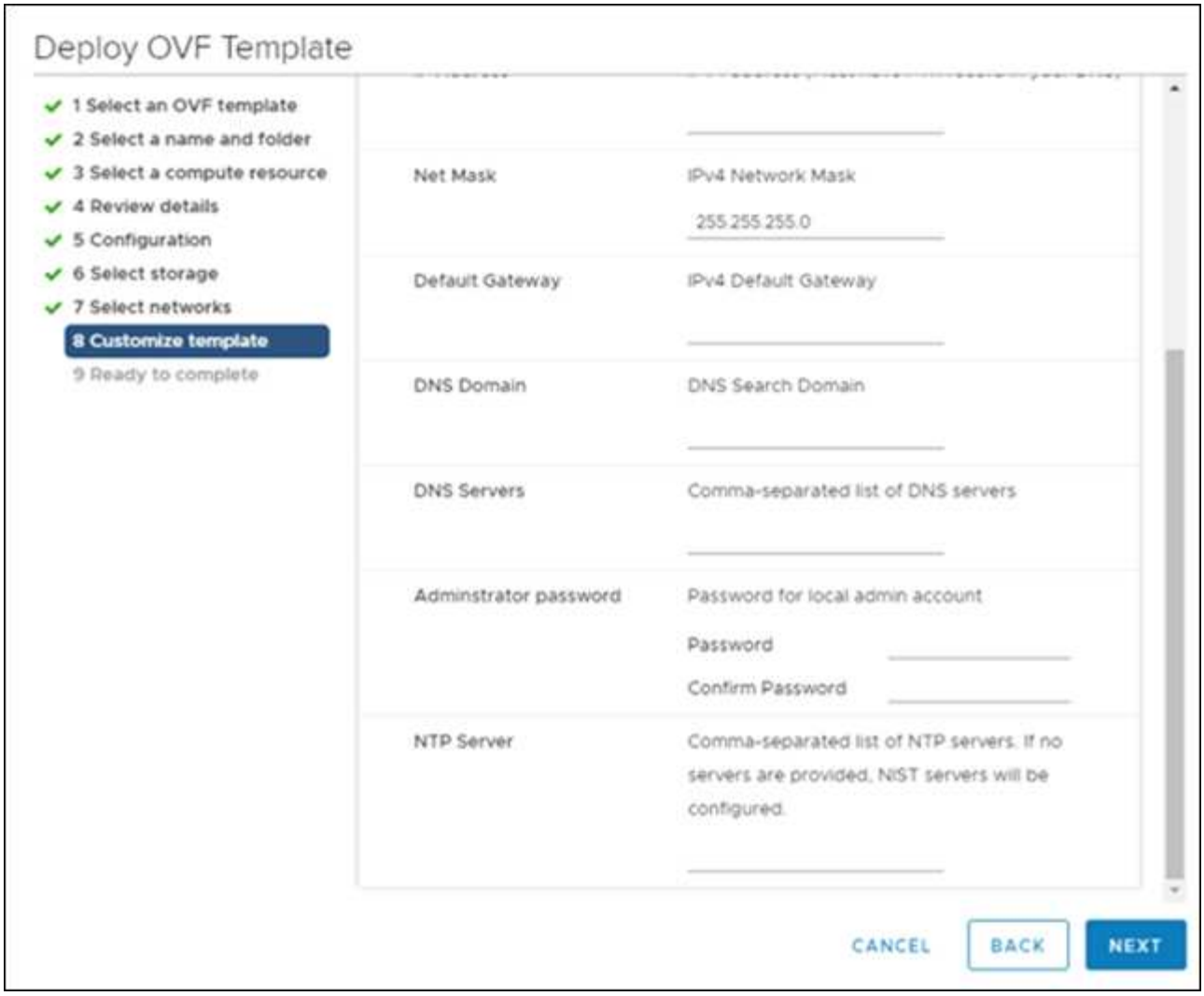
   b. Choisissez la taille de configuration appropriée (petite, petite ou moyenne) en fonction de vos besoins de déploiement OVA pour Intersight Virtual Appliance.

CONSEIL : pour un cluster ONTAP à deux nœuds avec un grand nombre d'objets de stockage, NetApp vous recommande d'utiliser l'option petite (16 vCPU, 32 Gi RAM).



c. Sur la page **Personnaliser le modèle**, personnalisez les propriétés de déploiement du modèle OVF. Le mot de passe administrateur est utilisé pour les utilisateurs locaux : admin(`webUI/cli/ssh`).


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Configuration
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Uncategorized
8 settings
Enable DHCP
Use DHCP for networking. All static params will be ignored.
IP Address
IPv4 address (Must have PTR record in your DNS)
Net Mask
IPv4 Network Mask
255.255.255.0
Default Gateway
IPv4 Default Gateway
DNS Domain
DNS Search Domain
DNS Servers
Comma-separated list of DNS servers
CANCEL
BACK
NEXT



a. Cliquez sur **Suivant**.

4. Post-déploiement de l'appareil InterSight Assist.

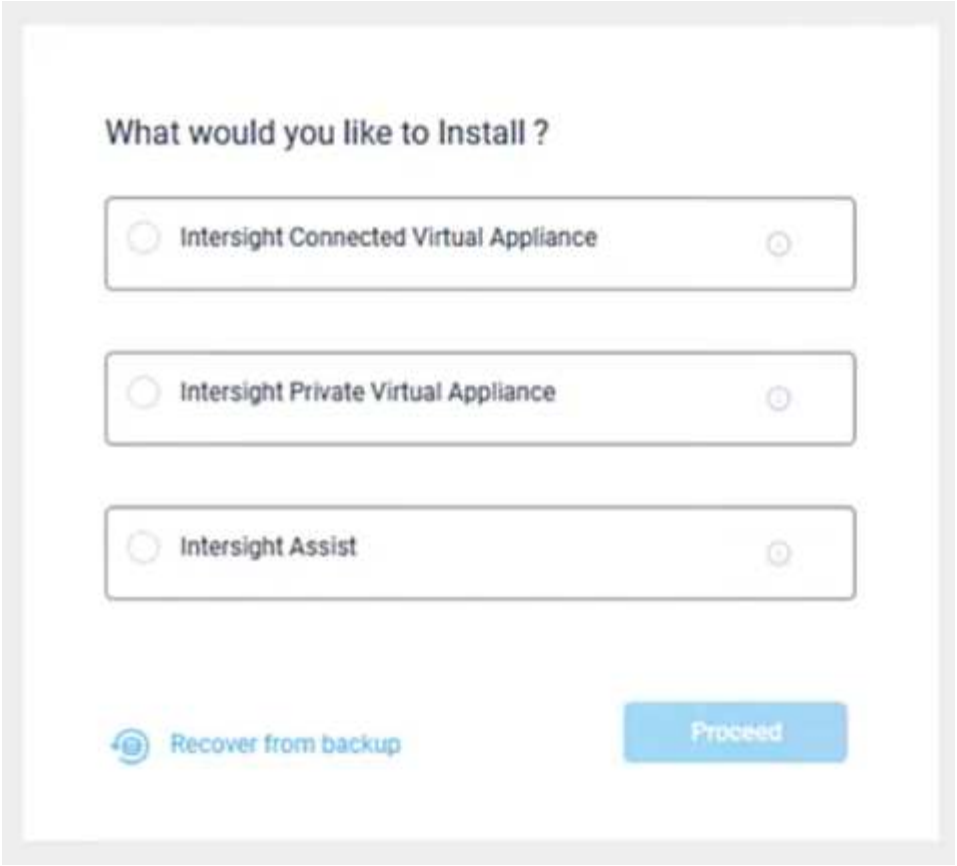
   a. Accédez à https://FQDN-of-your-appliance pour terminer la configuration post-installation de votre appareil.

      Le processus d'installation démarre automatiquement. L'installation peut prendre jusqu'à une heure selon la bande passante jusqu'à Intersight.com. Le site sécurisé peut également être opérationnel en quelques secondes après la mise sous tension de la machine virtuelle.

   b. Pendant le processus post-déploiement, sélectionnez l'option suivante :

      - **Intersight Assist.** ce déploiement permet au modèle SaaS de se connecter à Cisco Intersight.

      Lorsque vous sélectionnez Intersight Assist, notez l'ID et le code de demande de l'appareil avant de continuer.



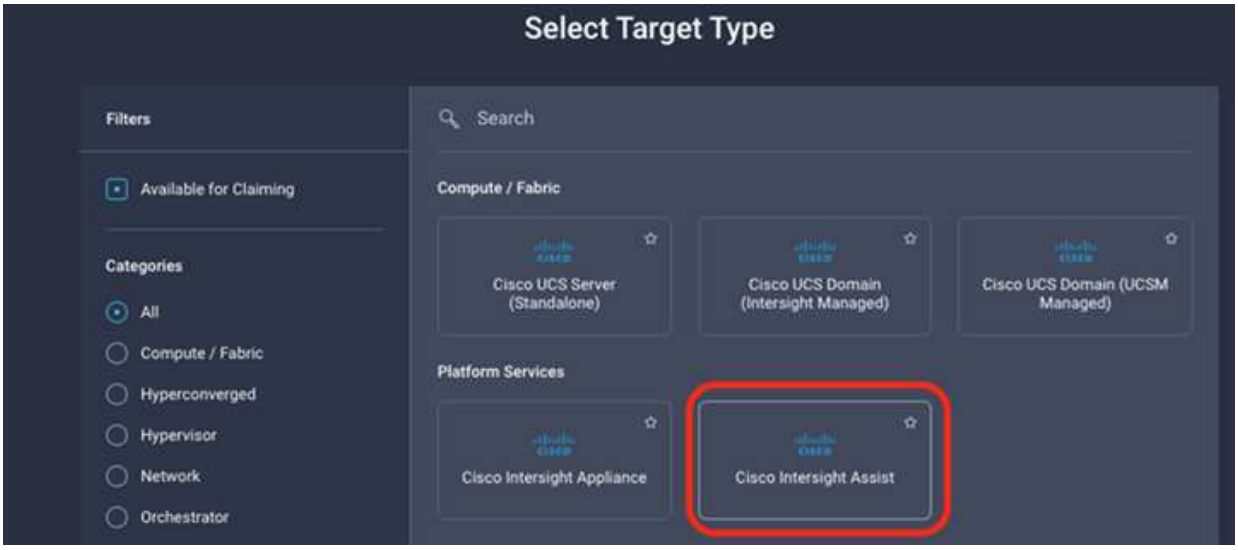
a. Cliquez sur **Continuer**.

b. Sélectionnez **Intersight** et procédez comme suit :

   i. Accédez à votre compte SaaS Intersight à l'adresse "https://intersight.com".

   ii. Cliquez sur **Targets**, **Cisco Intersight**, puis sur **Start**.

   iii. Demandez l'appareil **Cisco Intersight** en copiant et en collant l'ID de l'appareil et le code de demande depuis votre nouvelle appliance virtuelle Intersight déployée.



   iv. Retournez à l'appareil **Cisco Intersight** et cliquez sur **Continuer.** il se peut que vous deviez actualiser le navigateur.

Le téléchargement et l'installation commencent. Les binaires sont transférés d'Intersight Cloud vers votre appliance sur site. Le temps de fin varie en fonction de la bande passante que vous utilisez pour Intersight Cloud.

Configurez le serveur proxy AIQ UM pour le service IMT

Si vous utilisez un serveur proxy avec AIQ UM pour Cisco Intersight avec le stockage ONTAP NetApp, vous devez configurer la configuration via l'interface de ligne de commande pour utiliser le service IMT (matrice d'interopérabilité). Le service IMT est disponible sous l'onglet **interopérabilité** de la page **systèmes intégrés**. Vous devez utiliser le shell Diag de la machine virtuelle Active IQ Unified Manager (OVA) pour configurer les paramètres du serveur proxy AIQ UM.

Pour plus d'informations sur l'accès au shell Diag MU UM, reportez-vous à la section "Comment accéder à la coque DIAG Active IQ Unified Manager Virtual machine (OVA)"

Étapes

1. Connectez-vous au terminal AIQ UM et exécutez la commande suivante pour vous connecter à UM.

```
um cli login -u <um maintenance user name>
```

Exemple

```
um cli login -u admin
```

2. Réglez le `imt_proxy_host` et `imt_proxy_port` en exécutant les commandes suivantes.

Le proxy IMT est une configuration distincte des configurations proxy AutoSupport (ASUP).

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

Exemple

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

Les configurations du serveur proxy IMT ne prennent pas en charge l'authentification.

3. Affichez les détails du proxy IMT pour vérifier `proxy_host` et `proxy_port` paramètres via la commande suivante.

```
um option list |grep imt
```

Objectifs de demande de remboursement

Une fois Cisco InterSight Assist installé, vous pouvez demander vos systèmes de stockage et de virtualisation NetApp. Revenez à la page **Intersights Targets** et ajoutez vos cibles Active IQ Unified Manager vCenter et NetApp.

Assurez-vous que la passerelle d'API NetApp Active IQ Unified Manager (AIQ MU) est activée.

Depuis NetApp IQ Unified Manager, accédez à **Paramètres > général > Paramètres des fonctionnalités**.

L'exemple suivant montre la cible de demande NetApp AIQ UM faisant l'objet d'une demande auprès de Cisco Intersight.

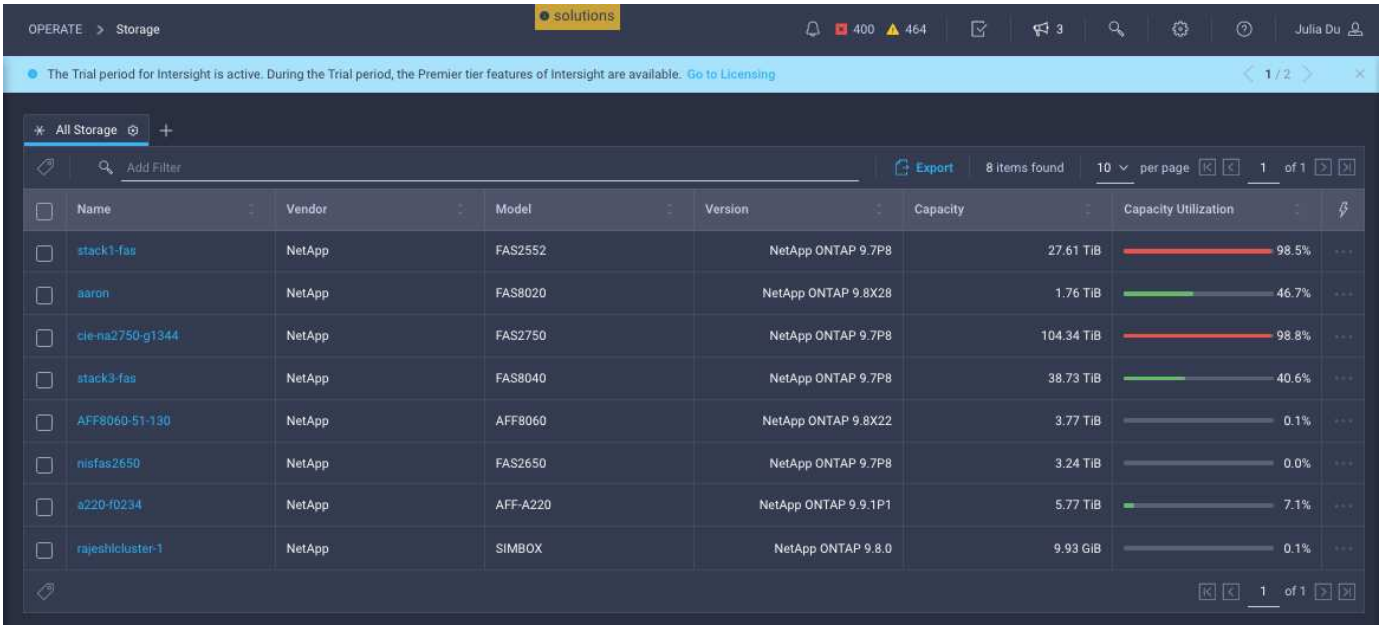
Lorsque vous demandez la cible UM NetApp AIQ, tous les clusters gérés par Active IQ Unified Manager sont automatiquement ajoutés à InterSight.

Surveiller le stockage NetApp depuis Cisco InterSight

Une fois les cibles réclamées, les widgets de stockage NetApp, l'inventaire du stockage et les onglets de virtualisation deviennent disponibles si vous disposez d'une licence Advantage Tier. Des onglets d'orchestration sont disponibles si vous disposez d'une licence Premier Tier.

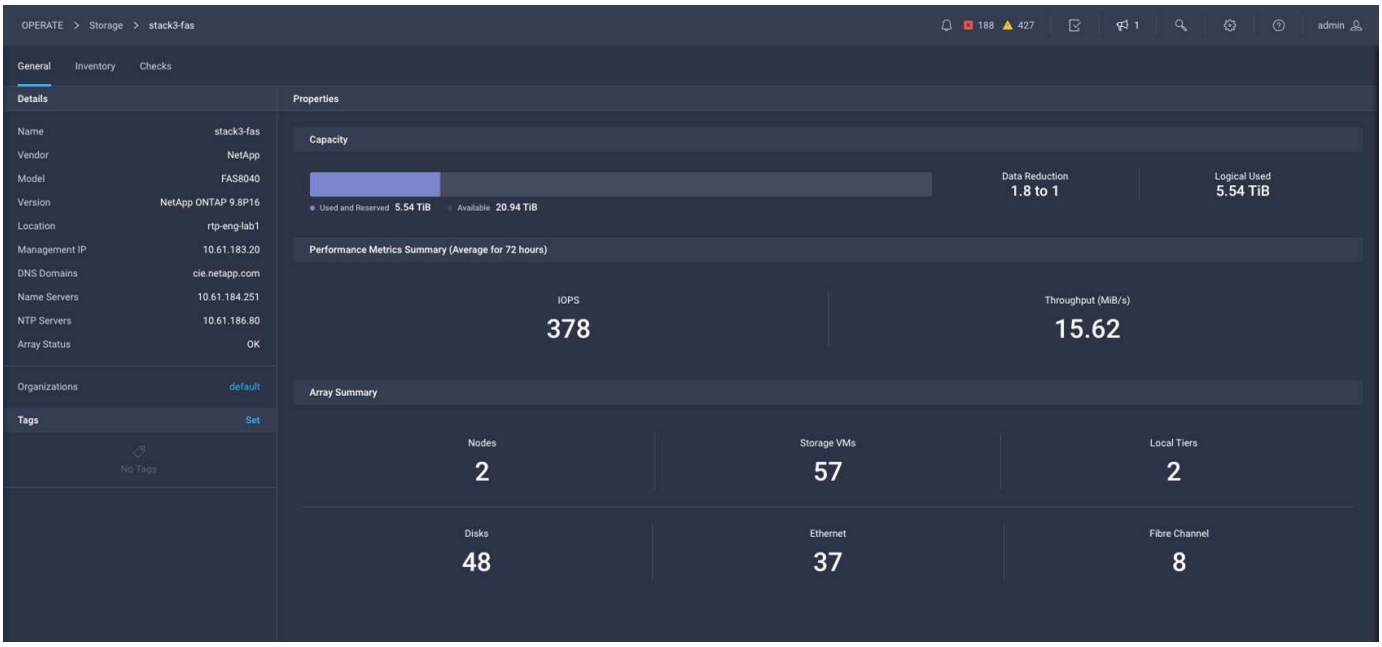
Présentation de l'inventaire du stockage

La capture d'écran suivante affiche l'écran * opération > stockage*.



La capture d'écran ci-dessous présente la présentation du cluster de stockage.

Le récapitulatif des mesures de performance suivantes n'apparaît que si la baie de stockage est contrôlée par NetApp Active IQ Unified Manager 9.9 ou version ultérieure.

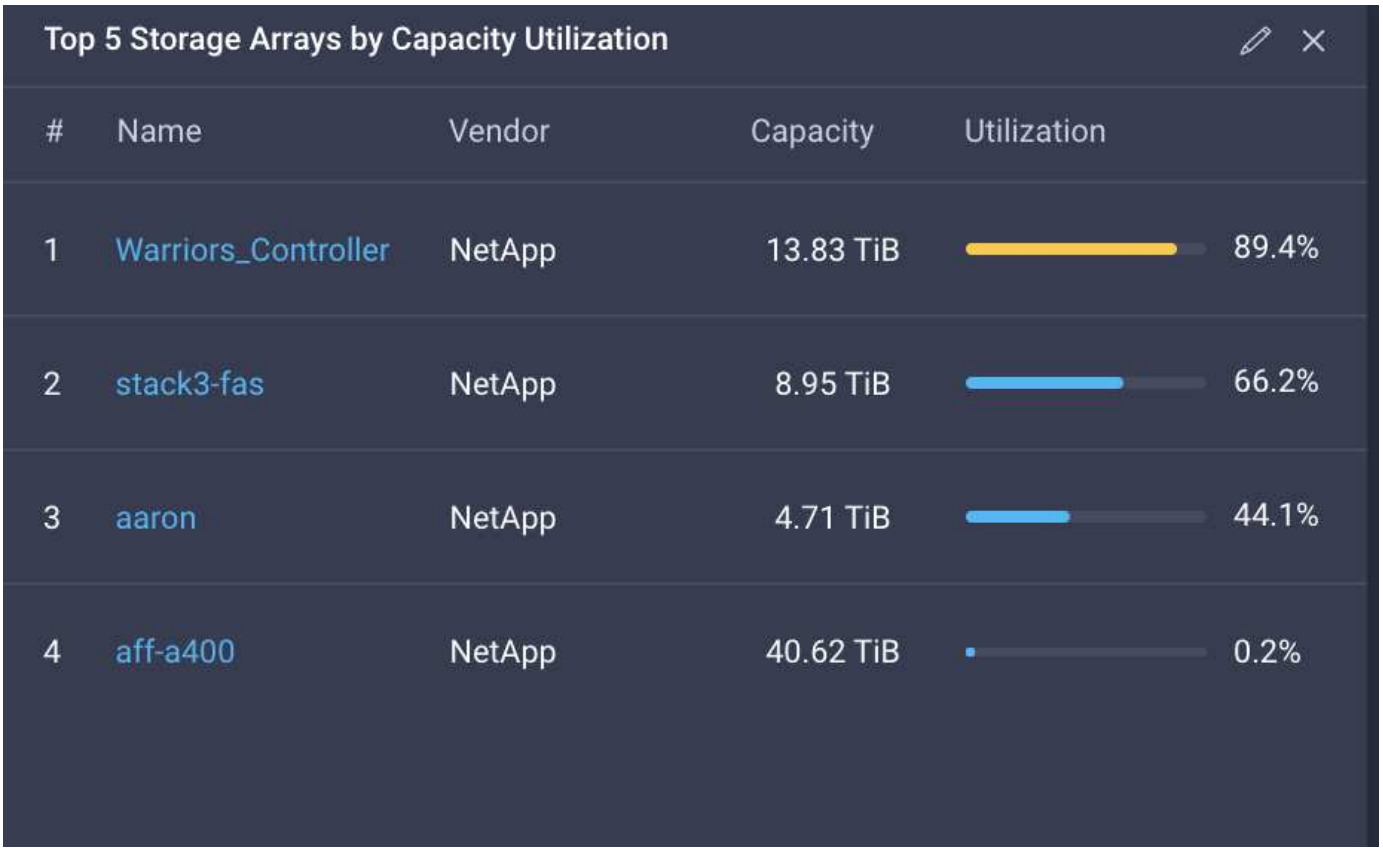


Widgets de stockage

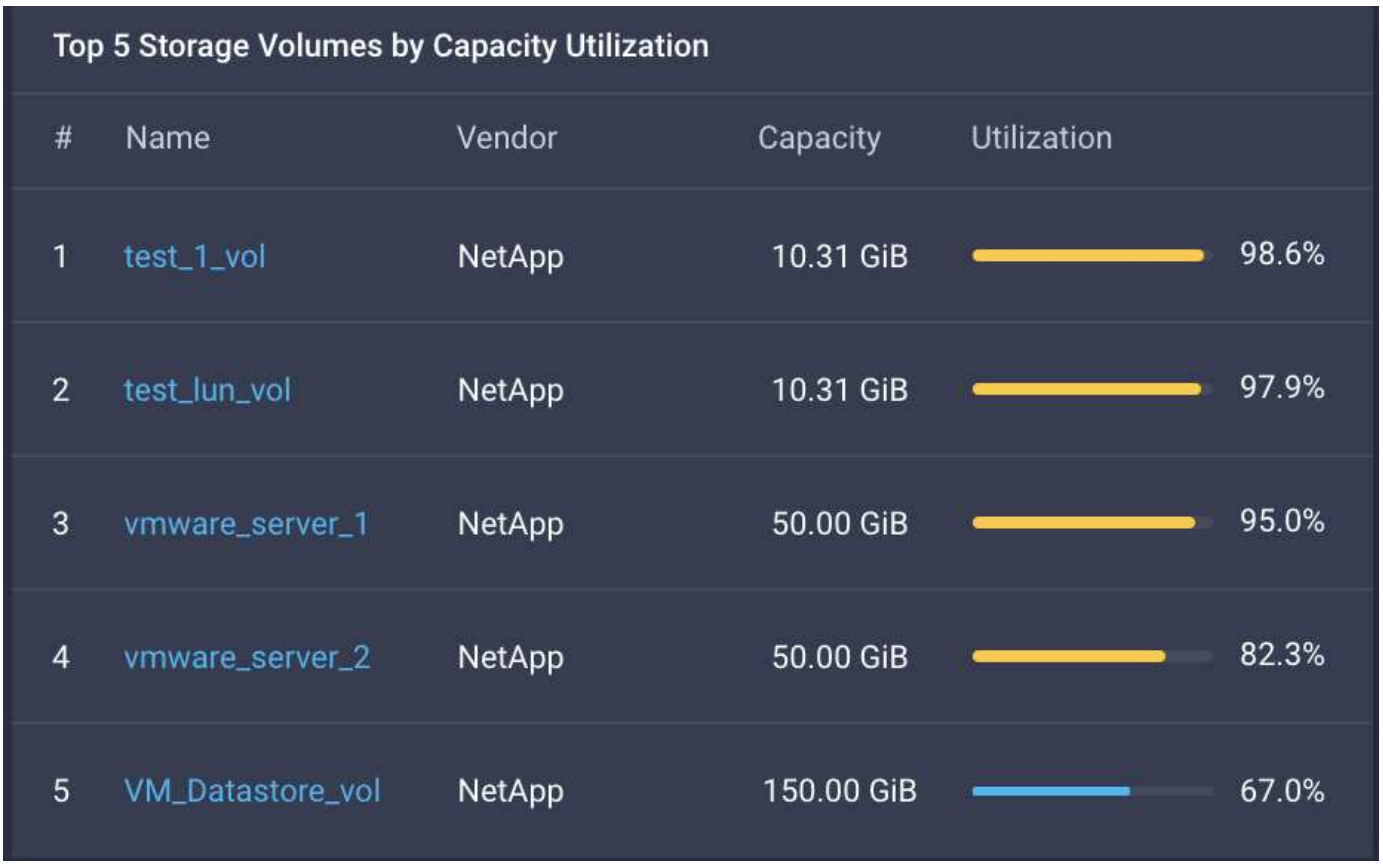
Pour afficher les widgets de stockage, accédez à **surveillance > tableaux de bord > Afficher les widgets de stockage NetApp**.

- La capture d'écran suivante affiche le widget Récapitulatif de la version de stockage.

- Cette capture d'écran présente le widget Capacity Utilization des 5 baies de stockage les plus populaires.



- Cette capture d'écran présente le widget Capacity Utilization des 5 premiers volumes de stockage.



Cas d’utilisation

Il s’agit de quelques exemples de cas d’utilisation pour le contrôle et l’orchestration du stockage NetApp auprès de Cisco Intersight.

Cas d’utilisation 1 : surveillance de l’inventaire du stockage NetApp et des widgets

Lorsque l’environnement de stockage NetApp est disponible dans Cisco Intersight, vous pouvez surveiller les objets de stockage NetApp en détail à partir de l’inventaire du stockage et obtenir une vue d’ensemble à partir des widgets de stockage.

1. Déployer InterSight Assist OVA (tâche Onsite dans l’environnement vCenter).
2. Ajouter des systèmes NetApp AIQ MU dans InterSight Assist.
3. Accédez à **stockage** et naviguez dans l’inventaire du stockage NetApp.
4. Ajoutez **Widgets** pour le stockage NetApp à votre **Monitor Dashboard**.

Cas d’usage n°2 : orchestration du stockage NetApp à l’aide de workflows de référence

Lorsque le stockage NetApp et les environnements vCenter sont disponibles dans Cisco Intersight, vous pouvez utiliser des workflows de référence de bout en bout disponibles dans GitHub via le "Référentiel de flux de travail FlexPod Intersight".

Les workflows de référence incluent les tâches de stockage et de virtualisation. Le fichier README du référentiel fournit les prérequis nécessaires à l’exécution des flux de travail, des liens vers des ressources utiles (y compris de la documentation sur l’importation d’un flux de travail) et des liens de documentation pour chaque flux de travail de référence.

Chaque flux de travail comporte un dossier dans le référentiel contenant deux fichiers :

- Le fichier JSON à télécharger et à importer dans Intersight,
- Fichier de documentation qui fournit une vue des tâches du flux de travail, des entrées de flux de travail et un exemple d’exécution du flux de travail.

Pour importer et utiliser un flux de travail de référence, procédez comme suit :

1. Déployer InterSight Assist OVA (tâche Onsite dans l’environnement vCenter).
2. Ajouter des systèmes NetApp AIQ MU dans InterSight Assist.
3. Ajoutez la cible vCenter à InterSight via InterSight Assist.
4. Téléchargez le fichier JSON pour un workflow de référence depuis le référentiel FlexPod-Intersight-Workflow.
5. Importez le flux de travail dans Intersight, puis exécutez-le.

Voici la liste des workflows disponibles dans le référentiel GitHub FlexPod-Intersight-Workflow :

- Ajouter des initiateurs au groupe initiateur NetApp
- Nouvelle règle d’export pour volume NetApp
- Nouveau datastore NAS à l’aide du volume intelligent NetApp

- Nouvelle interface de données FC NetApp
- Nouveau groupe initiateur NetApp
- Nouvelle interface de données iSCSI NetApp
- Nouvelle interface de données NAS NetApp
- Nouvelle machine virtuelle de stockage NetApp
- Nouveau datastore VMFS avec LUN intelligente NetApp
- Supprimer les initiateurs du groupe initiateur NetApp
- Supprimez le datastore NAS à l'aide du volume intelligent NetApp
- Supprimer la règle d'export NetApp
- Supprimer le groupe initiateur NetApp
- Supprimez un datastore VMFS à l'aide de la LUN intelligente NetApp
- Mettez à jour le datastore NAS à l'aide du volume intelligent NetApp
- Mettre à jour un datastore VMFS à l'aide de la LUN intelligente NetApp

Cas d'utilisation 3 : flux de travail personnalisés utilisant un format sans design

Lorsque les environnements NetApp Storage et vCenter sont disponibles dans Cisco InterSight, vous pouvez créer des flux de travail personnalisés en utilisant les tâches de stockage et de virtualisation NetApp.

1. Déployer InterSight Assist OVA (tâche Onsite dans l'environnement vCenter)
2. Ajouter des systèmes NetApp AIQ MU dans InterSight Assist.
3. Ajoutez la cible vCenter à InterSight via InterSight Assist.
4. Accédez à l'onglet **orchestration** dans Intersight.
5. Sélectionnez **Créer un flux de travail**.
6. Ajoutez des tâches de stockage et de virtualisation à vos flux de production.

   Les tâches de stockage NetApp sont disponibles auprès de Cisco Intersight :

   - Ajouter une liste de contrôle d'accès au partage CIFS NetApp
   - Ajouter la correspondance client à la règle de stratégie d'exportation NetApp
   - Ajouter une règle d'export au volume NetApp
   - Ajouter des initiateurs au groupe initiateur NetApp
   - Ajouter une règle à la stratégie d'exportation NetApp
   - Ajouter une planification à la règle NetApp Snapshot
   - Confirmez l'état de la licence NetApp
   - Confirmez l'état du protocole FCP de la machine virtuelle de stockage NetApp
   - Modifiez les agrégats NetApp pour Storage Virtual machine
   - Modifier la règle de SnapMirror asynchrone NetApp
   - Modifier l'autorisation ACL du partage CIFS NetApp
   - Modifier la règle de stratégie d'exportation NetApp
   - Modifier la règle de snapshot NetApp

- Modifier la planification de la règle de snapshot NetApp
- Modifier le style de sécurité du volume NetApp
- Modifier la règle de snapshot du volume NetApp
- Activez les services NetApp CIFS
- Développez NetApp LUN
- Nouvelle règle NetApp relative aux SnapMirror asynchrones
- Nouveau serveur CIFS NetApp
- Nouveau partage CIFS NetApp
- Recherchez NetApp Initiator Group LUN Map
- Recherchez LUN NetApp par ID
- Recherchez NetApp Volume par ID
- Nouvelle politique d’exportation NetApp
- Nouvelle interface de données FC NetApp
- Nouveau groupe initiateur NetApp
- Nouvelle interface de données iSCSI NetApp
- Nouveaux miroirs de partage de charge NetApp pour le volume racine du SVM
- Nouveau LUN NetApp
- Nouveau mappage de LUN NetApp
- Nouvelle interface de données NAS NetApp
- Nouveau volume intelligent NAS NetApp
- Nouveau LUN intelligent NetApp
- Nouvelle relation NetApp SnapMirror pour Volume
- Nouvelle règle NetApp Snapshot
- Nouvelle machine virtuelle de stockage NetApp
- Nouveau volume NetApp
- Nouveau snapshot de volume NetApp
- Enregistrez le serveur DNS pour la machine virtuelle de stockage NetApp
- Supprimez la liste de contrôle d’accès du partage CIFS NetApp
- Supprimer la correspondance client de la règle de stratégie d’exportation NetApp
- Supprimez la règle d’export du volume NetApp
- Supprimer l’initiateur du groupe initiateur NetApp
- Supprimez le serveur CIFS NetApp
- Supprimer le partage CIFS NetApp
- Supprimer la règle d’export NetApp
- Retirez l’interface de données FC NetApp
- Supprimer le groupe initiateur NetApp
- Retirez l’interface IP NetApp

- Supprimez les miroirs de partage de charge NetApp pour le volume racine du SVM
- Supprimer la LUN NetApp
- Supprimer le mappage de LUN NetApp
- Supprimez le volume intelligent NAS NetApp
- Supprimez la LUN intelligente NetApp
- Supprimez la relation NetApp SnapMirror pour Volume
- Supprimer la règle SnapMirror NetApp
- Supprimer la règle de snapshot NetApp
- Retirez la machine virtuelle de stockage NetApp
- Supprimez le volume NetApp
- Supprimer l'instantané de volume NetApp
- Supprimer la règle de la règle d'export NetApp
- Supprimer la planification de la règle NetApp Snapshot
- Renommer le snapshot de volume NetApp
- Mettre à jour les miroirs de partage de charge NetApp pour le volume racine du SVM
- Mettre à jour la capacité du volume NetApp

Infrastructures

NVMe de bout en bout pour FlexPod avec Cisco UCSM, VMware vSphere 7.0 et NetApp ONTAP 9

Tr-4914 : NVMe de bout en bout pour FlexPod avec Cisco UCSM, VMware vSphere 7.0 et NetApp ONTAP 9

Chris Schmitt et Kamini Singh, NetApp

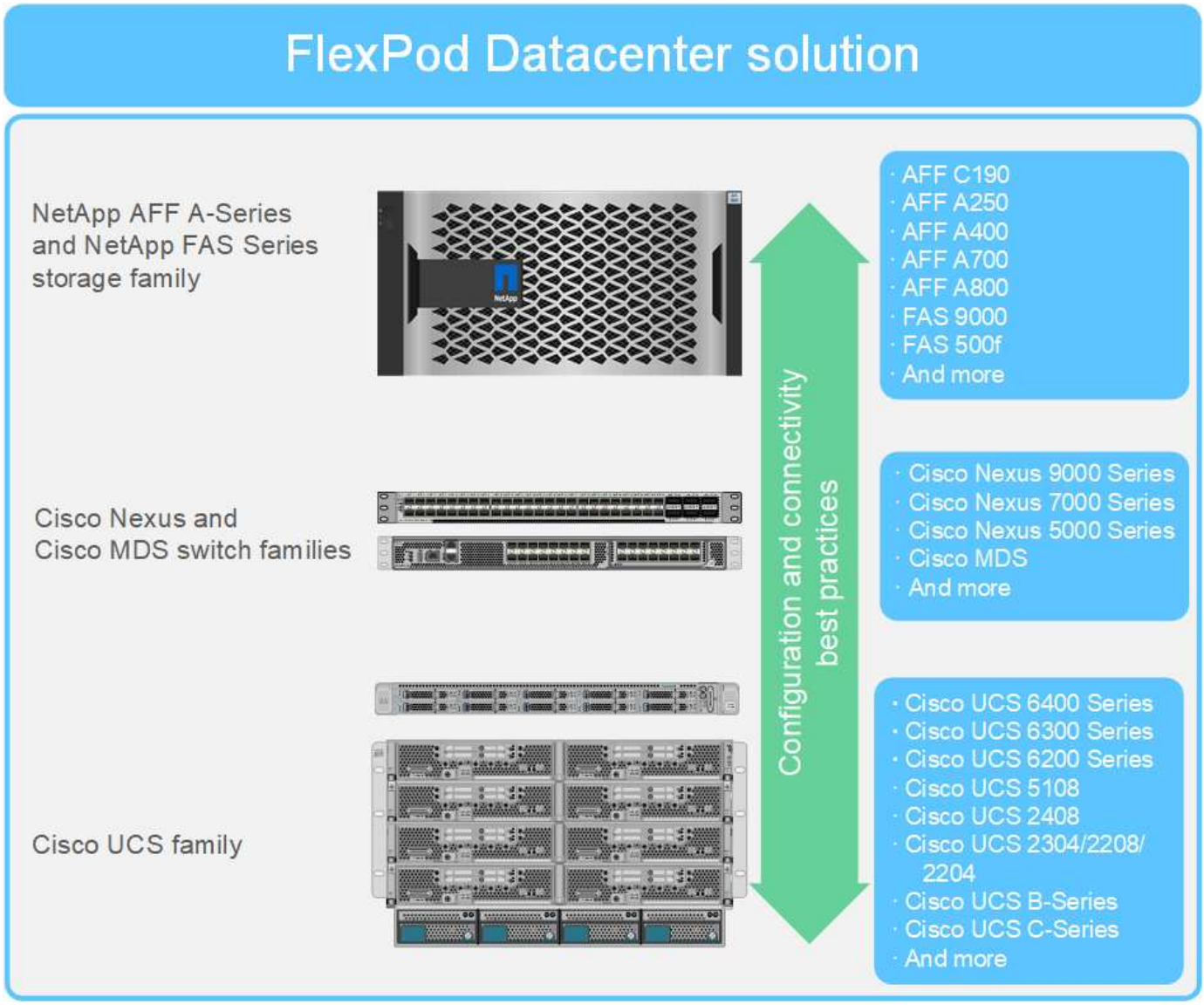
En partenariat avec : 

La norme de stockage de données NVMe, technologie de cœur émergente, transforme l'accès au stockage et le transport des données en fournissant une bande passante très élevée et un accès au stockage à faible latence pour les technologies de mémoire actuelles et futures. NVMe remplace le jeu de commandes SCSI par le jeu de commandes NVMe.

La technologie NVMe a été conçue pour fonctionner avec les disques Flash non volatiles, les processeurs multicœurs et des gigaoctets de mémoire. Il tire également parti des avancées significatives de l'informatique depuis les années 1970, permettant ainsi à des jeux de commandes rationalisés d'analyser et de manipuler plus efficacement les données. Une architecture NVMe complète permet également aux administrateurs de data Center de repenser la mesure dans laquelle ils peuvent pousser leurs environnements virtualisés et conteneurisés, ainsi que l'évolutivité que peuvent prendre en charge leurs bases de données orientées transactions.

L'architecture de data Center FlexPod est une pratique exemplaire, incluant Cisco Unified Computing System (Cisco UCS), les switchs Cisco Nexus, les commutateurs Cisco MDS et les systèmes NetApp AFF. Ces composants sont connectés et configurés conformément aux meilleures pratiques recommandées par Cisco et NetApp pour fournir une excellente plateforme pour exécuter en toute confiance une variété de charges de travail d'entreprise. FlexPod peut évoluer verticalement pour de meilleures performances et une plus grande capacité (ajout individuel de ressources de calcul, de réseau ou de stockage en fonction des besoins), ou horizontalement dans le cadre d'environnements nécessitant plusieurs déploiements cohérents (tels que le déploiement de piles FlexPod supplémentaires).

La figure suivante présente les familles de composants FlexPod.



FlexPod est la plateforme idéale pour présenter FC-NVMe. Il peut être pris en charge avec l'ajout de la carte Cisco UCS VIC 1400 Series et de la carte d'extension de port dans les serveurs Cisco UCS B200 M5 ou M6 existants ou les serveurs rack Cisco UCS C-Series M5 ou M6, ainsi que des mises à niveau logicielles simples et sans interruption du système Cisco UCS, les commutateurs Cisco MDS 32 Gbit/s, Et les baies de stockage NetApp AFF. Une fois le matériel et les logiciels pris en charge en place, la configuration FC-NVMe est similaire à la configuration FCP.

NetApp ONTAP 9.5 et versions ultérieures fournissent une solution FC-NVMe complète. Une mise à jour logicielle non disruptive pour les baies AFF A300, AFF A400, ONTAP AFF A700, AFF A700s et AFF A800 permet à ces dispositifs de prendre en charge une pile de stockage NVMe de bout en bout. Par conséquent, les serveurs avec adaptateurs de bus hôte (HBA) de sixième génération et la prise en charge des pilotes NVMe peuvent communiquer avec ces baies à l'aide du protocole NVMe natif.

Objectif

Cette solution fournit une synthèse générale des performances FC-NVMe avec VMware vSphere 7 sur FlexPod. La solution a été vérifiée pour passer avec succès le trafic FC-NVMe, et des schémas de performances ont été capturés pour FC-NVMe avec différentes tailles de blocs de données.

Avantages de la solution

La technologie NVMe complète pour FlexPod offre une valeur ajoutée exceptionnelle aux clients car elle apporte plusieurs avantages :

- NVMe repose sur l'architecture PCIe, un protocole matériel haut débit à large bande passante beaucoup plus rapide que les normes plus anciennes comme SCSI, SAS et SATA. Une connectivité à large bande passante et à latence ultra faible entre Cisco UCS Server et la baie de stockage NetApp pour la plupart des applications les plus exigeantes.
- Une solution FC-NVMe ne subit aucune perte et peut gérer les exigences d'évolutivité d'applications nouvelle génération. Ces nouvelles technologies incluent l'intelligence artificielle (IA), le machine learning (ML), le deep learning (DL), l'analytique en temps réel et d'autres applications stratégiques.
- Réduit le coût INFORMATIQUE en utilisant efficacement toutes les ressources de la pile.
- Elle réduit considérablement les temps de réponse et améliore les performances des applications, ce qui correspond à une augmentation des IOPS et du débit avec une latence réduite. La solution augmente les performances d'environ 60 % et réduit la latence d'environ 50 % pour les charges de travail existantes.
- FC-NVMe est un protocole optimisé doté d'excellentes fonctionnalités de mise en file d'attente, en particulier dans les cas où davantage d'opérations d'E/S par seconde (IOPS, davantage de transactions) et d'activités parallèles sont exécutées.
- Permet des mises à niveau logicielles sans interruption vers les composants FlexPod, tels que Cisco UCS, Cisco MDS et les baies de stockage NetApp AFF. Ne nécessite aucune modification des applications.

"Suivant : approche de test."

Approche de test

"Précédent : introduction."

Cette section présente un résumé général du test de validation du FC-NVMe sur FlexPod. Elle inclut à la fois l'environnement/la configuration de test et le plan de test adopté pour réaliser les tests de workloads par rapport à FC-NVMe pour FlexPod avec VMware vSphere 7.

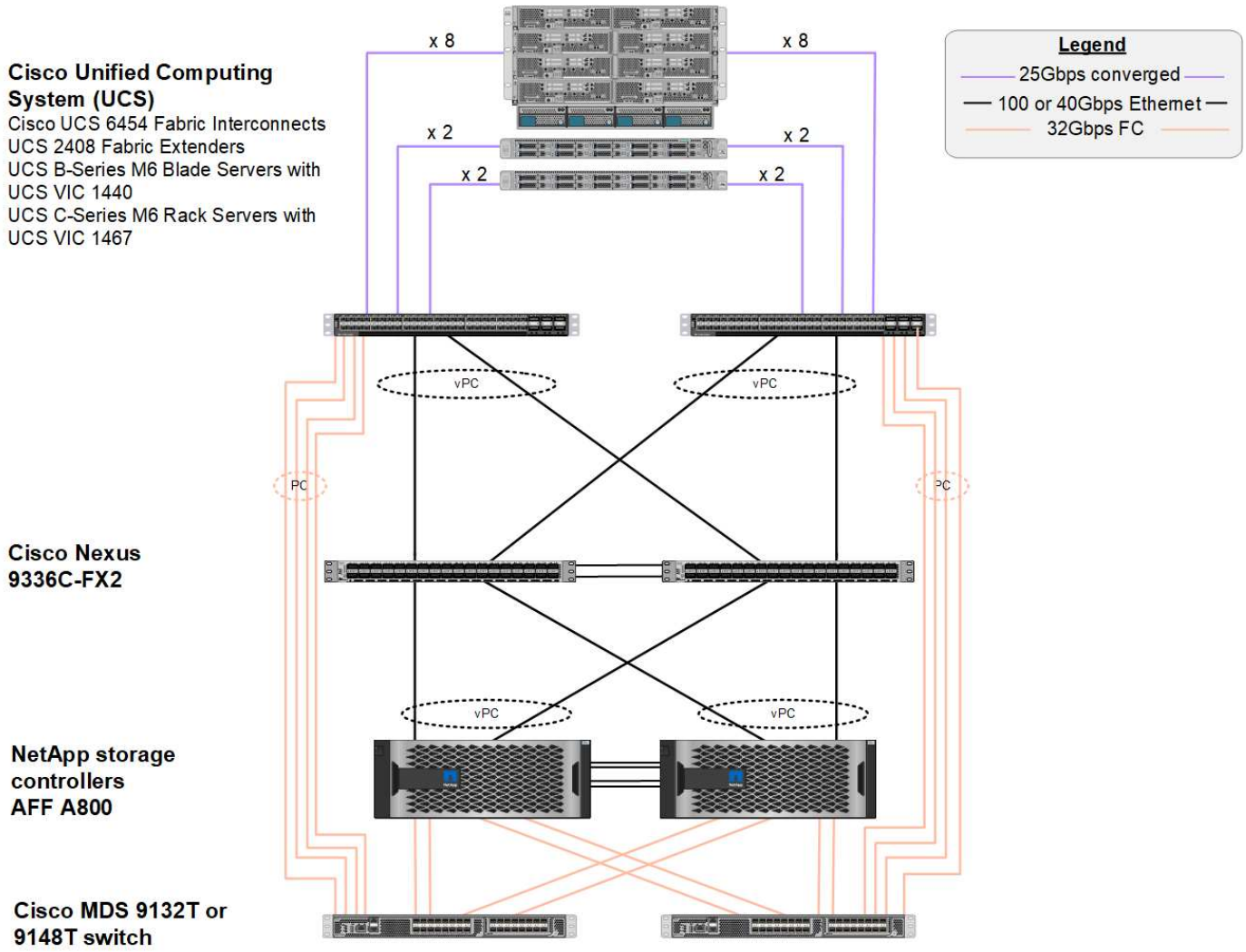
Environnement de test

Les commutateurs Cisco Nexus 9000 Series prennent en charge deux modes de fonctionnement :

- Mode autonome NX-OS, grâce au logiciel Cisco NX-OS
- Mode structure ACI (ACI) utilisant la plateforme Cisco application Centric Infrastructure (Cisco ACI)

En mode autonome, le switch fonctionne comme un switch Cisco Nexus standard avec une densité de ports accrue, une faible latence et une connectivité 40 GbE et 100 GbE.

La solution FlexPod avec NX-OS est conçue pour être totalement redondante dans les couches de calcul, de réseau et de stockage. Il n'y a pas de point de défaillance unique du point de vue d'un périphérique ou d'un chemin de trafic. La figure ci-dessous présente la connexion des différents éléments de la dernière conception FlexPod utilisée pour cette validation de FC-NVMe.



Dans un environnement SAN FC, cette conception utilise les éléments Fabric Interconnect Cisco UCS 6454 de quatrième génération et la plateforme Cisco UCS VICS 1400 avec module d'extension de ports sur les serveurs. Les serveurs lames Cisco UCS B200 M6 du châssis Cisco UCS utilisent la carte Cisco UCS VIC 1440 avec extension de port connectée au module d'extension de structure Cisco UCS 2408, et chaque adaptateur de bus hôte virtuel Fibre Channel over Ethernet (FCoE) a une vitesse de 40 Gbit/s. Les serveurs en rack Cisco UCS C220 M5 gérés par Cisco UCS utilisent le système Cisco UCS VIC 1457 avec deux interfaces de 25 Gbit/s vers chaque Fabric Interconnect. Chaque carte hôte vHBA FCoE C220 M5 possède une vitesse de 50 Gbit/s.

Les Fabric Interconnect se connectent via des canaux de port SAN 32 Gbit/s aux commutateurs FC Cisco MDS 9148T ou 9132T de dernière génération. La connectivité entre les commutateurs Cisco MDS et le cluster de stockage NetApp AFF A800 est également FC 32 Gbit/s. Cette configuration prend en charge le protocole FC 32 Gbit/s, pour le protocole FCP (Fibre Channel Protocol) et le stockage FC-NVMe entre le cluster de stockage et Cisco UCS. Pour cette validation, quatre connexions FC sont utilisées vers chaque contrôleur de stockage. Sur chaque contrôleur de stockage, les quatre ports FC sont utilisés à la fois pour les protocoles FCP et FC-NVMe.

La connectivité entre les commutateurs Cisco Nexus et le cluster de stockage NetApp AFF A800 de dernière génération est également de 100 Gbit/s avec les canaux de port sur les contrôleurs de stockage et les VPC sur les commutateurs. Les contrôleurs de stockage NetApp AFF A800 sont équipés de disques NVMe sur le bus PCIe plus rapide.

L'implémentation FlexPod utilisée dans cette validation repose sur "FlexPod Datacenter avec Cisco UCS

4.2(1) en mode géré UCS, VMware vSphere 7.0U2 et NetApp ONTAP 9.9".

Matériel et logiciels validés

Le tableau suivant répertorie les versions matérielles et logicielles utilisées lors du processus de validation de la solution. Notez que Cisco et NetApp disposent de matrices d'interopérabilité qui doivent être référencées pour déterminer la prise en charge de toute implémentation spécifique de FlexPod. Pour plus d'informations, consultez les ressources suivantes :

- "Matrice d'interopérabilité NetApp"
- "Outil d'interopérabilité matérielle et logicielle Cisco UCS"

Calque	Périphérique	Image	Commentaires
Informatique	• Deux interconnexions de fabric Cisco UCS 6454 • Un châssis lame Cisco UCS 5108 avec deux modules d'E/S Cisco UCS 2408 • Quatre serveurs lames Cisco UCS B200 M6, chacun avec un adaptateur Cisco UCS VIC 1440 et une carte d'extension de port	Version 4.2(1f)	Inclut Cisco UCS Manager, Cisco UCS VIC 1440 et port Expander
CPU	Deux processeurs Intel Xeon Gold 6330 à 2.0 GHz, avec 42 Mo de cache de couche 3 et 28 cœurs par processeur	–	–
Mémoire	1024 Go (16 DIMM de 64 Go fonctionnant à 3800 MHz)	–	–
Le réseau	Deux commutateurs Cisco Nexus 9336C-FX2 en mode autonome NX-OS	Version 9.3(8)	–
Réseau de stockage	Deux commutateurs FC 32 ports Cisco MDS 9132T 32 Gbit/s.	Version 8.4(2c)	Prise en charge de l'analytique SAN FC-NVMe
Stockage	Deux contrôleurs de stockage NetApp AFF A800 avec 24 SSD NVMe de 1,8 To	NetApp ONTAP 9.9.1P1	–
Logiciel	Cisco UCS Manager	Version 4.2(1f)	–
	VMware vSphere	7.0U2	–

Calque	Périphérique	Image	Commentaires
	VMware ESXi	7.0.2	–
	Pilote de carte réseau Fibre Channel native VMware ESXi (NFNIC)	5.0.0.12	Prise en charge du protocole FC-NVMe sur VMware
	Pilote de carte réseau Ethernet natif VMware ESXi (NENIC)	1.0.35.0	–
Outil de test	FIO	3.19	–

Plan de test

Nous avons développé un plan de test de performances pour valider NVMe sur FlexPod à l'aide d'une charge de travail synthétique. Ce workload nous a permis d'exécuter des lectures et des écritures aléatoires de 8 Ko, ainsi que des lectures et des écritures de 64 Ko. Nous avons utilisé des hôtes VMware ESXi pour exécuter nos cas de test avec la solution de stockage AFF A800.

Grâce à FIE, un outil d'E/S synthétique open source pouvant être utilisé pour mesurer les performances, nous avons généré notre charge de travail synthétique.

Pour mener à bien les tests de performances, nous avons réalisé plusieurs étapes de configuration sur le stockage et les serveurs. Les étapes détaillées de l'implémentation sont les suivantes :

1. Côté stockage, nous avons créé quatre machines virtuelles de stockage (SVM, anciennement appelées vServers), huit volumes par SVM et un espace de noms par volume. Nous avons créé des volumes de 1 To et des espaces de noms de 960 Go. Nous avons créé quatre LIF par SVM, ainsi qu'un sous-système par SVM. Les LIFs de SVM ont été réparties de manière homogène sur les huit ports FC disponibles sur le cluster.
2. Côté serveur, nous avons créé une machine virtuelle unique sur chacun de nos hôtes ESXi, pour un total de quatre machines virtuelles. Nous avons installé FIO sur nos serveurs pour exécuter les charges de travail synthétiques.
3. Après la configuration du stockage et des machines virtuelles, nous sommes parvenus à nous connecter aux espaces de noms de stockage à partir des hôtes ESXi. Cela nous a permis de créer des datastores basés sur notre espace de noms, puis de créer des disques d'ordinateurs virtuels (VMDK, Virtual machine Disks) basés sur ces datastores.

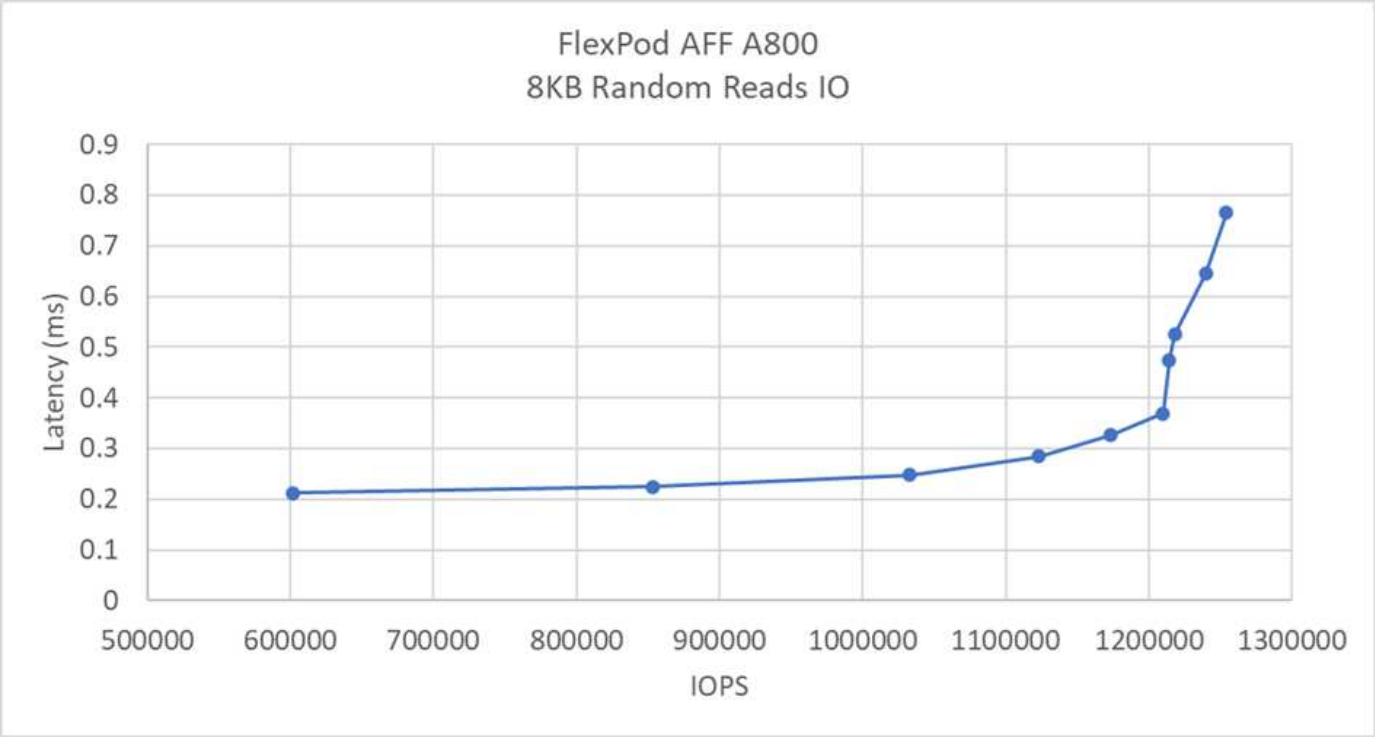
"Suivant : résultats du test."

Résultats du test

"Précédent : approche de test."

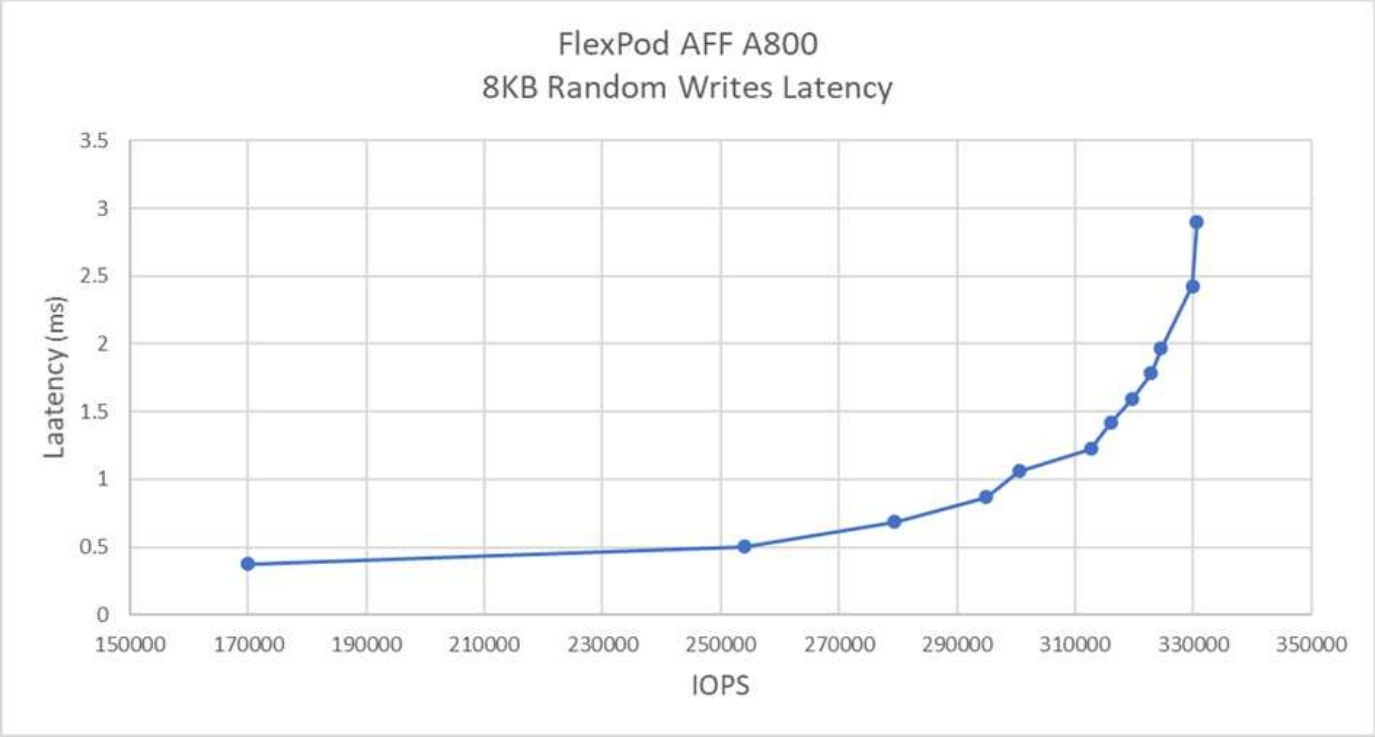
Le test a consisté à exécuter les workloads FIO pour mesurer la performance du FC-NVMe en termes d'IOPS et de latence.

Le graphique suivant illustre nos résultats lors de l'exécution d'une charge de travail de lecture aléatoire de 100 % avec des tailles de bloc de 8 Ko.



Lors de nos tests, nous avons constaté que le système a atteint plus de 1,2 million d'IOPS, tout en maintenant une latence côté serveur inférieure à 0,35 ms.

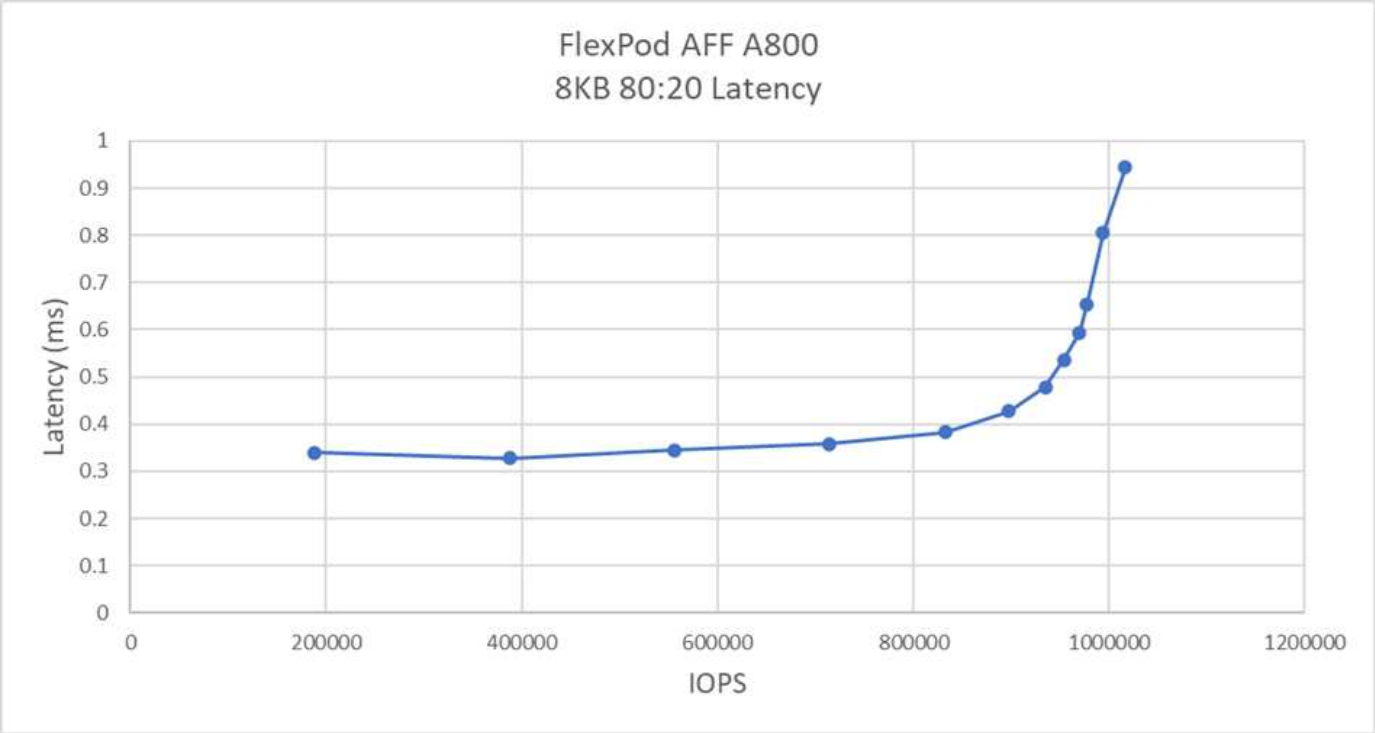
Le graphique suivant illustre nos résultats lorsque nous exécutons une charge de travail d'écriture aléatoire de 100 % avec des tailles de bloc de 8 Ko.



Lors de nos tests, nous avons constaté que le système a atteint près de 300 000 IOPS avec une latence côté serveur inférieure à 1 ms.

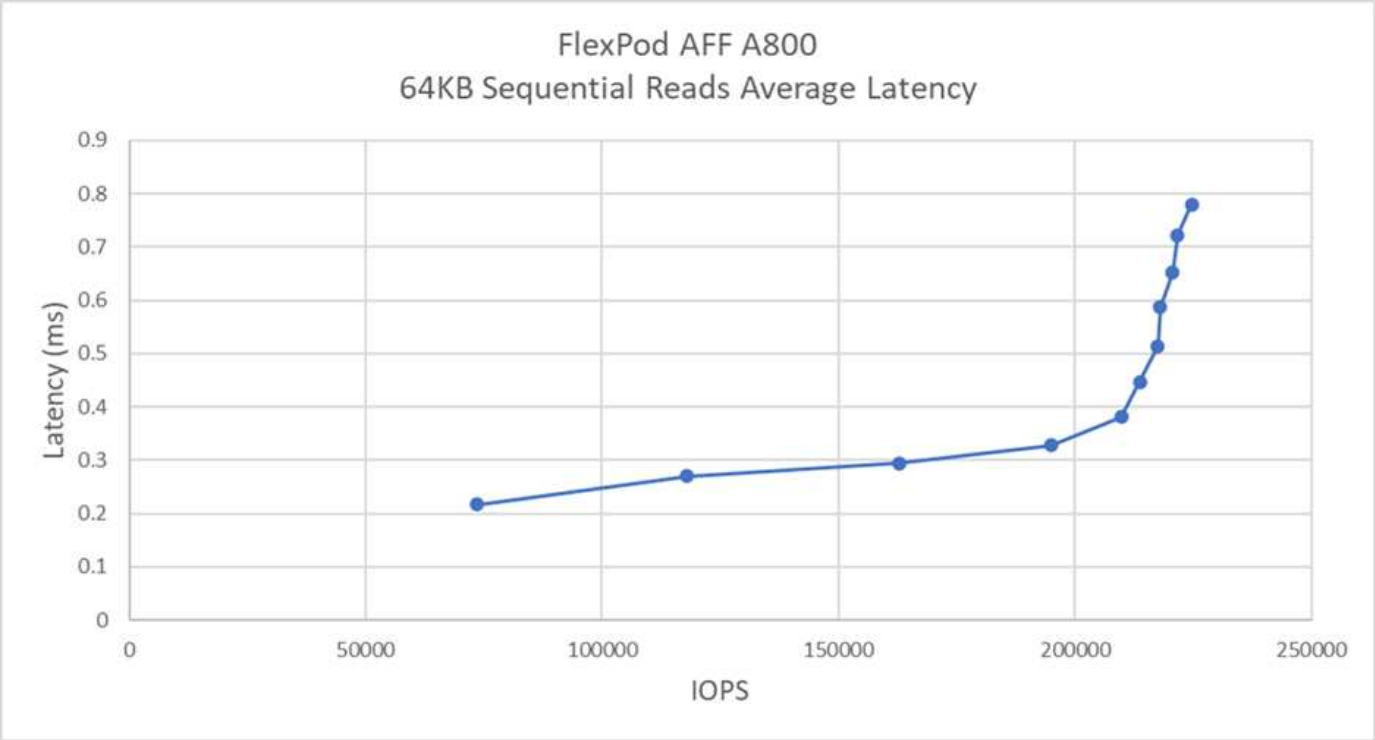
Pour une taille de bloc de 8 Ko avec des lectures aléatoires à 80 % et des écritures de 20 %, nous avons

observé les résultats suivants :



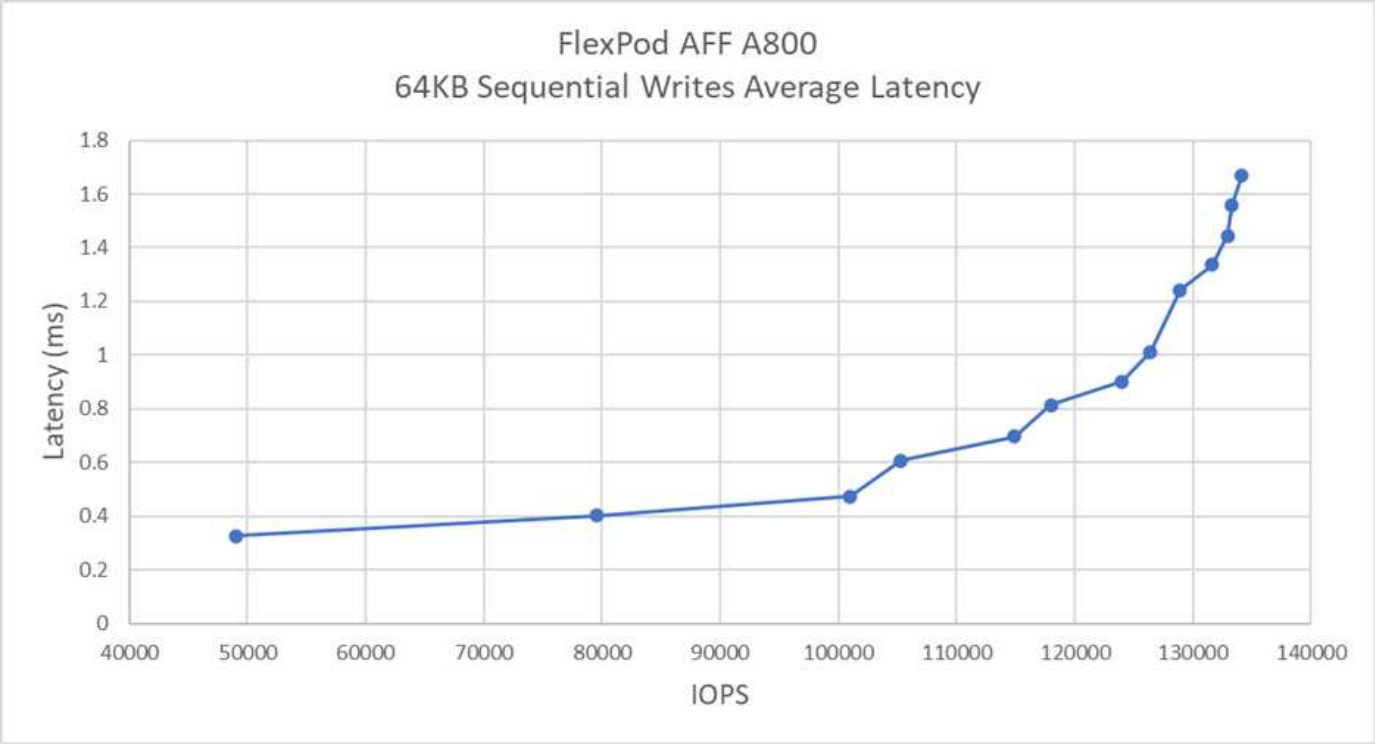
Lors de nos tests, nous avons constaté que le système a atteint plus d'un million d'IOPS avec une latence côté serveur inférieure à 1 ms.

Pour la taille de bloc de 64 Ko et les lectures séquentielles 100 %, nous avons observé les résultats suivants :



Lors de nos tests, nous avons constaté que le système a atteint environ 250 000 IOPS tout en maintenant une latence côté serveur inférieure à 1 ms.

Pour la taille de bloc de 64 Ko et les écritures séquentielles de 100 %, nous avons observé les résultats suivants :



Lors de nos tests, nous avons constaté que le système avait atteint environ 120 000 IOPS, tout en maintenant une latence côté serveur inférieure à 1 ms.

"Suivant: Conclusion."

Conclusion

"Précédent : résultats du test."

Le débit observé pour cette solution était de 14 Gbit/s et de 220 000 IOPS pour une charge de travail de lecture séquentielle inférieure à 1 ms. Pour les workloads de lecture aléatoire, nous avons atteint un débit de 9,5 Gbit/s et de 1,25 millions d'IOPS. La capacité de FlexPod à fournir cette performance avec FC-NVMe répond aux besoins de toutes les applications stratégiques.

FlexPod Datacenter avec VMware vSphere 7.0 U2 est une base d'infrastructure partagée optimale pour déployer du FC-NVMe pour diverses charges DE travail IT. Il fournit ainsi un accès au stockage haute performance pour les applications qui en ont besoin. Au fur et à mesure que le FC-NVMe évolue pour inclure la haute disponibilité, les chemins d'accès multiples et une prise en charge supplémentaire du système d'exploitation, FlexPod convient aussi bien à la plateforme de choix, offrant l'évolutivité et la fiabilité nécessaires pour prendre en charge ces fonctionnalités.

Grâce à FlexPod, Cisco et NetApp ont créé une plateforme à la fois flexible et évolutive pour de nombreux cas d'utilisation et applications. Grâce aux technologies FC-NVMe, FlexPod ajoute une autre fonctionnalité qui permet aux entreprises de prendre en charge de manière efficace et efficace des applications stratégiques s'exécutant simultanément à partir de la même infrastructure partagée. La flexibilité et l'évolutivité de FlexPod permettent également aux clients de démarrer avec une infrastructure correctement dimensionnée qui peut évoluer en fonction de leurs besoins.

Informations supplémentaires

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

- Serveurs Cisco Unified Computing System (UCS)

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Cisco UCS 6400 Series Fabric Interconnect Fiche technique

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Châssis de serveur lame Cisco UCS 5100 Series

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Serveurs lames Cisco UCS B-Series

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Serveurs en rack Cisco UCS C-Series

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Adaptateurs système Unified Computing System de Cisco

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Cisco UCS Manager

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Commutateurs Cisco Nexus 9000 Series

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Commutateurs de fabric multicouche Cisco MDS 9000

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Commutateur Fibre Channel Cisco MDS 9132T 32 Gbits/s à 32 ports

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF A-Series

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere

"https://www.vmware.com/products/vsphere"

- Serveur VMware vCenter

  "http://www.vmware.com/products/vcenter-server/overview.html"

- Meilleures pratiques pour le SAN moderne

  "https://www.netapp.com/us/media/tr-4080.pdf"

- Introduction à la technologie NVMe de bout en bout pour FlexPod

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

Matrices d'interopérabilité

- Matrice d'interopérabilité NetApp

  "http://support.netapp.com/matrix/"

- Matrice de compatibilité matérielle Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility"

Remerciements

Les auteurs remercient John George de Cisco, Scott Lane et Bobby Oommen de NetApp pour l'aide et les conseils offerts lors de l'exécution du projet.

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"