



Virtualisation VMware

NetApp Solutions

NetApp
September 26, 2024

Sommaire

- Solutions NetApp pour la virtualisation avec VMware de Broadcom 1
 - VMware vSphere avec ONTAP 1
 - Fondation VMware vSphere 1
 - Socle cloud VMware 192
 - Migration de machines virtuelles 356
 - Multicloud hybride NetApp avec les solutions VMware 409
 - Cas d'usage du multicloud hybride VMware 409
 - Automatisation VMware vSphere 410
 - Postes de travail virtuels 422
 - Démos et tutoriels 464

Solutions NetApp pour la virtualisation avec VMware de Broadcom

VMware vSphere avec ONTAP

ONTAP est une solution de stockage leader pour les environnements VMware vSphere depuis près de vingt ans et continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts. Ce document présente la solution ONTAP pour vSphere, comprenant les dernières informations sur les produits et les meilleures pratiques, afin de rationaliser le déploiement, de réduire les risques et de simplifier la gestion.

Pour plus d'informations, rendez-vous sur "[VMware vSphere avec ONTAP](#)"

Fondation VMware vSphere

Guide de référence NFS pour vSphere 8

Guide de référence NFS v3 pour vSphere 8

VMware vSphere Foundation (VVF) est une plateforme haute performance capable de fournir diverses charges de travail virtualisées. VMware vCenter, l'hyperviseur ESXi, les composants réseau et divers services de ressources sont au cœur de vSphere. Combinées à ONTAP, les infrastructures virtualisées optimisées par VMware offrent une flexibilité, une évolutivité et des capacités remarquables.

Utilisation de NFS v3 avec vSphere 8 et les systèmes de stockage ONTAP

Ce document fournit des informations sur les options de stockage disponibles pour la base VMware Cloud vSphere basée sur les baies 100 % Flash NetApp. Les options de stockage prises en charge sont couvertes par des instructions spécifiques pour le déploiement des datastores NFS. Nous vous présentons également VMware Live site Recovery pour la reprise après incident des datastores NFS. Enfin, la protection anti-ransomware autonome de NetApp pour le stockage NFS est analysée.

Cas d'utilisation

Cas d'utilisation décrits dans cette documentation :

- Options de stockage pour les clients à la recherche d'environnements uniformes sur les clouds privés et publics.
- Déploiement d'infrastructure virtuelle pour les charges de travail.
- Solution de stockage évolutive et adaptée à l'évolution des besoins, même lorsqu'elle n'est pas directement alignée sur les besoins en ressources de calcul.
- Protection des machines virtuelles et des datastores à l'aide du plug-in SnapCenter pour VMware vSphere.
- Utilisation de VMware Live site Recovery pour la reprise après incident des datastores NFS.
- Stratégie de détection des ransomwares, avec plusieurs couches de protection au niveau de l'hôte ESXi et

de la machine virtuelle invitée

Public

Cette solution est destinée aux personnes suivantes :

- Architectes de solutions qui recherchent des options de stockage plus flexibles pour les environnements VMware conçus pour optimiser le TCO.
- Architectes de solutions à la recherche d'options de stockage VVF offrant des options de protection des données et de reprise d'activité avec les principaux fournisseurs cloud.
- Les administrateurs du stockage qui souhaitent des instructions spécifiques sur la configuration du VVF avec le stockage NFS.
- Les administrateurs du stockage qui souhaitent des instructions spécifiques sur la protection des VM et datastores résidant sur le stockage ONTAP

Présentation de la technologie

Le Guide de référence VVF NFS v3 pour vSphere 8 comprend les principaux composants suivants :

Fondation VMware vSphere

Composant central de vSphere Foundation, VMware vCenter est une plateforme de gestion centralisée qui assure la configuration, le contrôle et l'administration des environnements vSphere. VCenter sert de base à la gestion des infrastructures virtualisées. Les administrateurs peuvent ainsi déployer, surveiller et gérer des machines virtuelles, des conteneurs et des hôtes ESXi au sein de l'environnement virtuel.

La solution VVF prend en charge les workloads Kubernetes natifs et basés sur des machines virtuelles. Principaux composants :

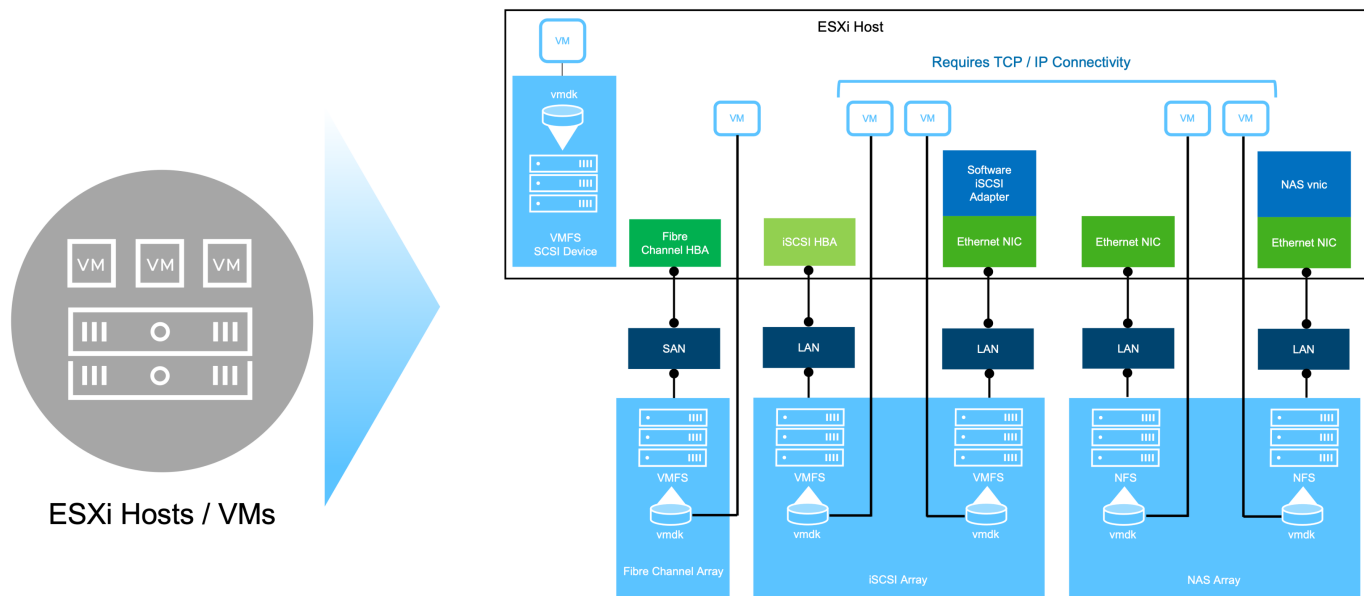
- VMware vSphere
- VMware VSAN
- ARIA Standard
- Service de grid Kubernetes VMware Tanzu pour vSphere
- Switch distribué vSphere

Pour plus d'informations sur les composants VVF inclus, reportez-vous à la section Architecture et planification, reportez-vous ["Comparaison en direct des produits VMware vSphere"](#) à la section .

Options de stockage VVF

Le stockage est au cœur d'un environnement virtuel performant. Que ce soit via les datastores VMware ou les cas d'utilisation connectés par l'invité, le système de stockage libère les fonctionnalités de vos workloads en vous permettant de choisir le meilleur prix par Go qui soit le plus avantageux tout en réduisant la sous-utilisation. ONTAP est une solution de stockage leader pour les environnements VMware vSphere depuis près de vingt ans et continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts.

Les options de stockage VMware sont généralement organisées sous la forme d'offres de stockage classiques et Software-defined. Les modèles de stockage classiques incluent le stockage local et réseau, tandis que les modèles de stockage Software-defined incluent VSAN et VMware Virtual volumes (vVols).



Pour "[Introduction au stockage dans l'environnement vSphere](#)" plus d'informations sur les types de stockage pris en charge pour VMware vSphere Foundation, reportez-vous à la section.

NetApp ONTAP

De nombreuses raisons expliquent pourquoi des dizaines de milliers de clients ont choisi ONTAP comme solution de stockage primaire pour vSphere. Ces champs d'application incluent :

1. **Système de stockage unifié** : ONTAP propose un système de stockage unifié qui prend en charge les protocoles SAN et NAS. Cette polyvalence permet l'intégration transparente de diverses technologies de stockage dans une solution unique.
2. **Protection robuste des données** : ONTAP fournit des fonctionnalités robustes de protection des données grâce à des instantanés compacts. Ces snapshots permettent de mettre en place des processus de sauvegarde et de restauration efficaces, garantissant la sécurité et l'intégrité des données d'application.
3. **Outils de gestion complets**: ONTAP offre une multitude d'outils conçus pour aider à gérer efficacement les données d'application. Ces outils rationalisent les tâches de gestion du stockage, améliorent l'efficacité opérationnelle et simplifient l'administration.
4. **Efficacité du stockage** : ONTAP inclut plusieurs fonctionnalités d'efficacité du stockage, activées par défaut, conçues pour optimiser l'utilisation du stockage, réduire les coûts et améliorer les performances globales du système.

L'utilisation de ONTAP avec VMware apporte une grande flexibilité pour répondre aux besoins des applications. Les protocoles suivants sont pris en charge comme datastore VMware avec ONTAP : * FCP * FCoE * NVMe/FC * NVMe/TCP * iSCSI * NFS v3 * NFS v4.1

En utilisant un système de stockage distinct de l'hyperviseur, vous pouvez décharger de nombreuses fonctions et optimiser votre investissement dans les systèmes hôtes vSphere. En plus de s'assurer que les ressources de vos hôtes sont concentrées sur les charges de travail applicatives, vous évitez également l'impact aléatoire sur les performances des applications en provenance des opérations de stockage.

L'association de ONTAP et de vSphere permet de réduire les dépenses liées au matériel hôte et aux logiciels VMware. Vous pouvez également protéger vos données à moindre coût grâce à des performances élevées et prévisibles. Les charges de travail virtualisées étant mobiles, vous pouvez explorer différentes approches à

l'aide de Storage vMotion afin de déplacer des ordinateurs virtuels entre des datastores VMFS, NFS ou vvolts, le tout sur un même système de stockage.

Baies 100 % Flash NetApp

NetApp AFF (FAS 100 % Flash) est une gamme de baies de stockage 100 % Flash. Des solutions de stockage hautes performances à faible latence sont conçues pour les charges de travail d'entreprise. La gamme AFF associe les avantages de la technologie Flash aux fonctionnalités de gestion des données de NetApp, offrant ainsi une plateforme de stockage puissante et efficace.

La gamme AFF comprend à la fois des modèles de la série A et des modèles de la série C.

Les baies Flash NetApp A-Series 100 % NVMe sont conçues pour les workloads haute performance. Elles offrent une latence ultra faible et une résilience élevée. Elles sont donc adaptées aux applications stratégiques.

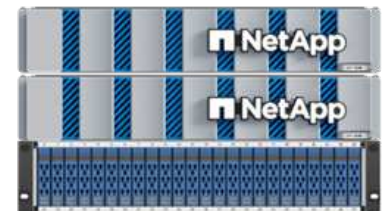
AFF A70



AFF A90



AFF A1K



Les baies Flash C-Series QLC sont destinées à des cas d'utilisation de capacité supérieure, offrant la vitesse de la technologie Flash et l'économie du Flash hybride.

AFF C250



AFF C400



AFF C800



Prise en charge des protocoles de stockage

Le système AFF prend en charge tous les protocoles standard utilisés pour la virtualisation, les data stores et le stockage connecté à l'invité, notamment NFS, SMB, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), NVME over Fabrics et S3. Les clients sont libres de choisir ce qui convient le mieux à leurs workloads et applications.

NFS - NetApp AFF prend en charge NFS, ce qui permet un accès basé sur des fichiers aux datastores VMware. Les datastores connectés par NFS depuis de nombreux hôtes ESXi dépassent de loin les limites imposées aux systèmes de fichiers VMFS. L'utilisation de NFS avec vSphere offre des avantages en termes de facilité d'utilisation et d'efficacité du stockage. ONTAP inclut des fonctionnalités d'accès aux fichiers disponibles pour le protocole NFS. Vous pouvez activer un serveur NFS et exporter des volumes ou des qtrees.

Pour obtenir des conseils de conception sur les configurations NFS, reportez-vous au ["Documentation sur la gestion du stockage NAS"](#).

iSCSI - NetApp AFF fournit une prise en charge robuste pour iSCSI, permettant un accès au niveau des blocs aux périphériques de stockage sur les réseaux IP. Il offre une intégration transparente avec les initiateurs iSCSI pour un provisionnement et une gestion efficaces des LUN iSCSI. Fonctionnalités avancées d'ONTAP, telles que les chemins d'accès multiples, l'authentification CHAP et la prise en charge ALUA.

Pour obtenir des conseils de conception sur les configurations iSCSI, reportez-vous au ["Documentation de référence sur la configuration SAN"](#).

Fibre Channel - NetApp AFF offre une prise en charge complète de Fibre Channel (FC), une technologie de réseau haut débit couramment utilisée dans les réseaux de stockage (SAN). ONTAP s'intègre en toute transparence à l'infrastructure FC, offrant ainsi un accès fiable et efficace au niveau des blocs aux systèmes de stockage. Elle offre des fonctionnalités telles que le zoning, les chemins d'accès multiples et la connexion à la fabric (FLOGI) pour optimiser les performances, améliorer la sécurité et assurer la connectivité transparente dans les environnements FC.

Pour obtenir des conseils de conception sur les configurations Fibre Channel ["Documentation de référence sur la configuration SAN"](#), reportez-vous au .

NVMe over Fabrics - NetApp ONTAP prend en charge NVMe over Fabrics. NVMe/FC permet d'utiliser des périphériques de stockage NVMe sur l'infrastructure Fibre Channel et NVMe/TCP sur les réseaux de stockage IP.

Pour obtenir des conseils de conception sur NVMe, reportez-vous à la section ["Configuration, prise en charge et limitations de NVMe"](#).

Technologie active/active

Les baies 100 % Flash NetApp autorisent des chemins de données actif-actif à travers les deux contrôleurs, ce qui évite au système d'exploitation hôte d'attendre la panne d'un chemin actif avant d'activer le chemin alternatif. Cela signifie que l'hôte peut utiliser tous les chemins disponibles sur tous les contrôleurs, en veillant à ce que les chemins actifs soient toujours présents, que le système soit dans un état stable ou qu'il ait subi un basculement de contrôleur.

Pour plus d'informations, reportez-vous à ["Protection des données et reprise après incident"](#) la documentation.

Garanties de stockage

NetApp propose un ensemble unique de garanties de stockage grâce aux baies 100 % Flash NetApp. Ses avantages uniques incluent :

Garantie d'efficacité du stockage : atteignez une haute performance tout en réduisant les coûts de stockage grâce à la garantie d'efficacité du stockage. Ratio de 4:1 pour les workloads SAN **Garantie de restauration ransomware** : garantie de récupération des données en cas d'attaque par ransomware.

Pour plus d'informations, reportez-vous au ["Page d'accueil NetApp AFF"](#) .

Outils NetApp ONTAP pour VMware vSphere

L'un des composants puissants de vCenter est la possibilité d'intégrer des plug-ins ou des extensions qui améliorent davantage ses fonctionnalités et fournissent des fonctionnalités et des capacités supplémentaires. Ces plug-ins étendent les fonctionnalités de gestion de vCenter et permettent aux administrateurs d'intégrer des solutions, des outils et des services tiers dans leur environnement vSphere.

Les outils NetApp ONTAP pour VMware sont une suite complète d'outils conçue pour faciliter la gestion du cycle de vie des machines virtuelles dans les environnements VMware via son architecture de plug-in vCenter.

Ces outils s'intègrent en toute transparence à l'écosystème VMware, ce qui permet un provisionnement efficace des datastores et une protection essentielle des machines virtuelles. Grâce aux outils ONTAP pour VMware vSphere, les administrateurs peuvent facilement gérer les tâches de gestion du cycle de vie du stockage.

Des ressources complètes sur les outils ONTAP 10 sont disponibles "[Ressources de documentation des outils ONTAP pour VMware vSphere](#)".

Consultez la solution de déploiement ONTAP Tools 10 à l'adresse "[Utilisez les outils ONTAP 10 pour configurer les datastores NFS pour vSphere 8](#)"

Plug-in NetApp NFS pour VMware VAAI

Le plug-in NetApp NFS pour VAAI (vStorage APIs for Array Integration) optimise les opérations de stockage en transférant certaines tâches vers le système de stockage NetApp, ce qui améliore les performances et l'efficacité. Cela inclut des opérations telles que la copie complète, la mise à zéro des blocs et le verrouillage assisté par matériel. En outre, le plug-in VAAI optimise l'utilisation du stockage en réduisant la quantité de données transférées sur le réseau lors des opérations de provisionnement et de clonage des ordinateurs virtuels.

Le plug-in NetApp NFS pour VAAI peut être téléchargé depuis le site de support NetApp, puis installé sur les hôtes ESXi à l'aide des outils ONTAP pour VMware vSphere.

Pour plus d'informations, reportez-vous à la section "[Plug-in NetApp NFS pour la documentation VMware VAAI](#)".

Plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter pour VMware vSphere (SCV) est une solution logicielle de NetApp qui protège intégralement les données dans les environnements VMware vSphere. Son objectif est de simplifier et de rationaliser le processus de protection et de gestion des machines virtuelles et des datastores. SCV utilise un snapshot basé sur le stockage et la réplication sur des baies secondaires pour atteindre des objectifs de durée de restauration plus faibles.

Le plug-in SnapCenter pour VMware vSphere offre les fonctionnalités suivantes dans une interface unifiée, intégrée au client vSphere :

Snapshots basés sur des règles - SnapCenter vous permet de définir des règles pour la création et la gestion de snapshots cohérents au niveau des applications de machines virtuelles dans VMware vSphere.

Automatisation - la création et la gestion automatisées de snapshots basées sur des règles définies permettent d'assurer une protection cohérente et efficace des données.

Protection au niveau VM - la protection granulaire au niveau VM permet une gestion et une récupération efficaces des machines virtuelles individuelles.

Fonctionnalités d'efficacité du stockage - l'intégration aux technologies de stockage NetApp fournit des fonctionnalités d'efficacité du stockage telles que la déduplication et la compression pour les snapshots, ce qui réduit les besoins en stockage.

Le plug-in SnapCenter orchestre la mise en veille des machines virtuelles en association avec des snapshots matériels sur des baies de stockage NetApp. La technologie SnapMirror permet de répliquer des copies de sauvegarde sur les systèmes de stockage secondaires, y compris dans le cloud.

Pour plus d'informations, reportez-vous à la "[Documentation du plug-in SnapCenter pour VMware vSphere](#)".

L'intégration de BlueXP active 3-2-1 stratégies de sauvegarde qui étendent les copies de données au stockage objet dans le cloud.

Pour plus d'informations sur les stratégies de sauvegarde 3-2-1 avec BlueXP, rendez-vous sur ["3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration BlueXP pour les VM"](#).

Pour obtenir des instructions de déploiement étape par étape pour le plug-in SnapCenter, reportez-vous à la solution ["Utilisez le plug-in SnapCenter pour VMware vSphere pour protéger les machines virtuelles sur les domaines de charge de travail VCF"](#).

Considérations relatives au stockage

L'utilisation des datastores ONTAP NFS avec VMware vSphere offre un environnement haute performance, facile à gérer et évolutif qui offre un ratio VM/datastore impossible avec les protocoles de stockage en mode bloc. Cette architecture peut multiplier par dix la densité des datastores, et entraîner une réduction correspondante du nombre de datastores.

NConnect for NFS: un autre avantage de l'utilisation de NFS est la possibilité de tirer parti de la fonctionnalité **nConnect**. NConnect permet de connecter plusieurs connexions TCP pour les volumes de datastores NFS v3, ce qui permet d'atteindre un débit plus élevé. Cela permet d'augmenter le parallélisme et pour les datastores NFS. Les clients qui déploient des datastores avec NFS version 3 peuvent augmenter le nombre de connexions au serveur NFS, optimisant ainsi l'utilisation des cartes d'interface réseau haut débit.

Pour plus d'informations sur nConnect, reportez-vous à ["NFS nConnect avec VMware et NetApp"](#)la .

Agrégation de session pour NFS: à partir de ONTAP 9.14.1, les clients utilisant NFSv4.1 peuvent exploiter l'agrégation de session pour établir plusieurs connexions à diverses LIFs sur le serveur NFS. Cela permet un transfert de données plus rapide et améliore la résilience grâce à l'utilisation des chemins d'accès multiples. La mise en circuits s'avère particulièrement avantageuse lors de l'exportation de volumes FlexVol vers des clients qui prennent en charge la mise en circuits, tels que des clients VMware et Linux, ou lors de l'utilisation de protocoles NFS sur RDMA, TCP ou pNFS.

Pour plus d'informations, reportez-vous à la section ["Présentation de l'agrégation NFS"](#) .

Volumes FlexVol: NetApp recommande d'utiliser des volumes **FlexVol** pour la plupart des datastores NFS. Si des datastores plus volumineux peuvent améliorer l'efficacité du stockage et les avantages opérationnels, il est conseillé d'utiliser au moins quatre datastores (volumes FlexVol) pour stocker les machines virtuelles sur un seul contrôleur ONTAP. En règle générale, les administrateurs déploient des datastores reposant sur des volumes FlexVol d'une capacité comprise entre 4 To et 8 To. Cette taille offre un bon équilibre entre performances, facilité de gestion et protection des données. Les administrateurs peuvent commencer par un déploiement de petite taille et faire évoluer le datastore en fonction des besoins (jusqu'à 100 To maximum). Des datastores plus petits accélèrent la restauration à partir de sauvegardes ou d'incidents et peuvent être facilement déplacés dans le cluster. Cette approche permet d'optimiser l'utilisation des performances des ressources matérielles et d'autoriser les datastores à appliquer différentes règles de restauration.

Volumes FlexGroup: pour les scénarios nécessitant un grand datastore, NetApp recommande l'utilisation de volumes **FlexGroup**. Les volumes FlexGroup n'ont pratiquement aucune limite de capacité ou de nombre de fichiers, ce qui permet aux administrateurs de provisionner facilement un namespace unique massif. L'utilisation de volumes FlexGroup n'entraîne pas de frais de maintenance ou de gestion supplémentaires. Avec les volumes FlexGroup, plusieurs datastores ne sont pas nécessaires pour les performances, car ils évoluent par nature. En utilisant des volumes ONTAP et FlexGroup avec VMware vSphere, vous pouvez établir des datastores simples et évolutifs exploitant toute la puissance du cluster ONTAP.

Protection par ransomware

Le logiciel de gestion des données NetApp ONTAP est doté d'une suite complète de technologies intégrées qui vous aident à protéger, détecter et restaurer vos données en cas d'attaques par ransomware. La fonctionnalité NetApp SnapLock Compliance intégrée à ONTAP empêche la suppression des données stockées dans un volume activé en utilisant la technologie WORM (write once, read many) avec une conservation avancée des données. Une fois la période de conservation établie et la copie Snapshot verrouillée, même un administrateur du stockage disposant de la Privileges complète du système ou un membre de l'équipe de support NetApp ne peut pas supprimer la copie Snapshot. Mais, plus important encore, un hacker qui a des identifiants compromis ne peut pas supprimer les données.

NetApp garantit que nous serons en mesure de récupérer vos copies NetApp® Snapshot™ protégées sur des baies éligibles, et si nous ne le pouvons pas, nous compenserons votre organisation.

Pour plus d'informations sur la garantie de restauration contre les ransomware, voir : ["Garantie de récupération par ransomware"](#).

```
https://docs.netapp.com/us-en/ontap/anti-ransomware/["Présentation de la protection autonome contre les ransomwares"]Pour plus d'informations, reportez-vous au.
```

Consultez la solution complète sur le centre de documentation des solutions NetApps : ["Protection anti-ransomware autonome pour le stockage NFS"](#)

Considérations relatives à la reprise sur incident

NetApp fournit le stockage le plus sécurisé au monde. NetApp vous aide à protéger l'infrastructure de vos données et applications, à déplacer vos données entre votre système de stockage sur site et le cloud, ainsi qu'à assurer la disponibilité des données dans les clouds. ONTAP est doté de puissantes technologies de sécurité et de protection des données qui aident à protéger les clients contre les incidents en détectant de manière proactive les menaces et en restaurant rapidement les données et les applications.

VMware Live site Recovery, anciennement VMware site Recovery Manager, offre une automatisation rationalisée basée sur des règles pour la protection des machines virtuelles au sein du client Web vSphere. Cette solution tire parti des technologies avancées de gestion des données de NetApp via Storage Replication adapter, intégrées aux outils ONTAP pour VMware. En exploitant les fonctionnalités de NetApp SnapMirror pour la réplication basée sur les baies, les environnements VMware peuvent bénéficier de l'une des technologies ONTAP les plus fiables et les plus abouties. SnapMirror assure des transferts de données sécurisés et ultra efficaces en copiant uniquement les blocs du système de fichiers modifiés, et non les machines virtuelles ou les datastores complets. De plus, ces blocs exploitent des techniques d'économie d'espace telles que la déduplication, la compression et la compaction. Avec l'introduction d'SnapMirror indépendant de la version dans les systèmes ONTAP modernes, vous avez plus de flexibilité dans le choix de vos clusters source et cible. SnapMirror s'est véritablement imposé comme un puissant outil de reprise après incident. Associé à la restauration en direct sur site, il offre une évolutivité, des performances et des économies supérieures à celles des solutions de stockage locales.

Pour plus d'informations, reportez-vous au ["Présentation de VMware site Recovery Manager"](#).

Consultez la solution complète sur le centre de documentation des solutions NetApps : ["Protection anti-ransomware autonome pour le stockage NFS"](#)

BlueXP DRaaS (Disaster Recovery as a Service) pour NFS est une solution économique de reprise d'activité conçue pour les workloads VMware qui s'exécutent sur des systèmes ONTAP sur site avec des datastores

NFS. Il exploite la réplication NetApp SnapMirror pour se protéger contre les pannes de site et les corruptions de données, telles que les attaques par ransomware. Intégré à la console NetApp BlueXP, ce service facilite la gestion et la découverte automatisée des vCenter VMware et du stockage ONTAP. Les entreprises peuvent créer et tester des plans de reprise d'activité, et atteindre un objectif de point de restauration (RPO) de 5 minutes maximum grâce à la réplication au niveau des blocs. La DRaaS de BlueXP exploite la technologie FlexClone de ONTAP pour réaliser des tests compacts sans affecter les ressources de production. Ce service orchestre les processus de basculement et de rétablissement, permettant ainsi d'installer des serveurs virtuels protégés sur le site de reprise d'activité désigné en toute simplicité. Par rapport à d'autres solutions connues, la DRaaS de BlueXP offre ces fonctionnalités pour un coût inférieur, ce qui en fait une solution efficace pour les entreprises qui peuvent configurer, tester et exécuter les opérations de reprise après incident dans leurs environnements VMware à l'aide de systèmes de stockage ONTAP.

Consultez la solution complète sur le centre de documentation des solutions NetApps : ["Reprise après incident à l'aide de la DRaaS BlueXP pour les datastores NFS"](#)

Présentation des solutions

Solutions décrites dans cette documentation :

- **Fonctionnalité NFS nConnect avec NetApp et VMware.** Cliquez sur ["ici"](#) pour les étapes de déploiement.
 - **Utilisez les outils ONTAP 10 pour configurer les datastores NFS pour vSphere 8.** Cliquez sur ["ici"](#) pour les étapes de déploiement.
 - **Déployer et utiliser le plug-in SnapCenter pour VMware vSphere pour protéger et restaurer les machines virtuelles.** Cliquez sur ["ici"](#) pour les étapes de déploiement.
 - **Reprise après incident des datastores NFS avec VMware site Recovery Manager.** Cliquez sur ["ici"](#) pour les étapes de déploiement.
 - **Protection anti-ransomware autonome pour le stockage NFS.** Cliquez sur ["ici"](#) pour les étapes de déploiement.

Fonctionnalité NFS nConnect avec NetApp et VMware

À partir de VMware vSphere 8.0 U1 (sous forme de Tech-preview), la fonctionnalité nconnect permet d'effectuer plusieurs connexions TCP pour les volumes de datastore NFS v3 afin d'atteindre un débit supérieur. Les clients qui utilisent le datastore NFS peuvent désormais augmenter le nombre de connexions au serveur NFS, optimisant ainsi l'utilisation de cartes d'interface réseau haut débit.



Cette fonctionnalité est généralement disponible pour NFS v3 avec 8.0 U2. Reportez-vous à la section stockage sur ["Notes de version de VMware vSphere 8.0 Update 2"](#). NFS v4.1 est pris en charge avec vSphere 8.0 U3. Pour plus d'informations, vérifiez ["Notes de version de vSphere 8.0 mise à jour 3"](#)

Cas d'utilisation

- Héberger plus de machines virtuelles par datastore NFS sur le même hôte.
- Boostez les performances des datastores NFS.
- Offre de service à un Tier supérieur pour les applications basées sur des machines virtuelles et des conteneurs.

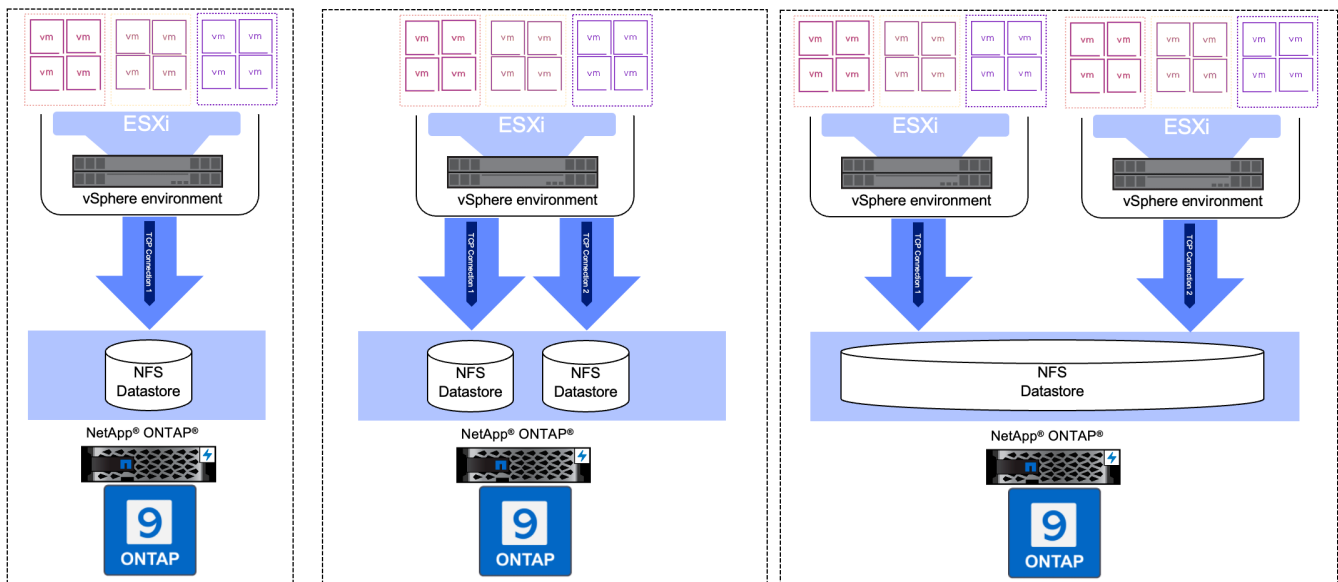
Détails techniques

L'objectif de nconnect est de fournir plusieurs connexions TCP par datastore NFS sur un hôte vSphere. Cela permet d'augmenter le parallélisme et les performances des datastores NFS. Dans ONTAP, lorsqu'un montage NFS est établi, un ID de connexion (CID) est créé. Ce CID fournit jusqu'à 128 opérations en vol simultanées. Lorsque ce nombre est dépassé par le client, ONTAP agit comme une forme de contrôle de flux jusqu'à ce qu'il puisse libérer certaines ressources disponibles à mesure que d'autres opérations sont terminées. Ces pauses ne prennent généralement que quelques microsecondes, mais au-delà de millions d'opérations, elles peuvent s'additionner et engendrer des problèmes de performance. NConnect peut prendre la limite de 128 et la multiplier par le nombre de sessions nconnect sur le client, ce qui fournit plus d'opérations simultanées par CID et peut potentiellement améliorer les performances. Pour plus d'informations, reportez-vous à la section "[Guide d'implémentation et des meilleures pratiques NFS](#)"

Datastore NFS par défaut

Pour résoudre les limites de performances d'une connexion unique au datastore NFS, des datastores supplémentaires sont montés ou des hôtes supplémentaires sont ajoutés pour augmenter la connexion.

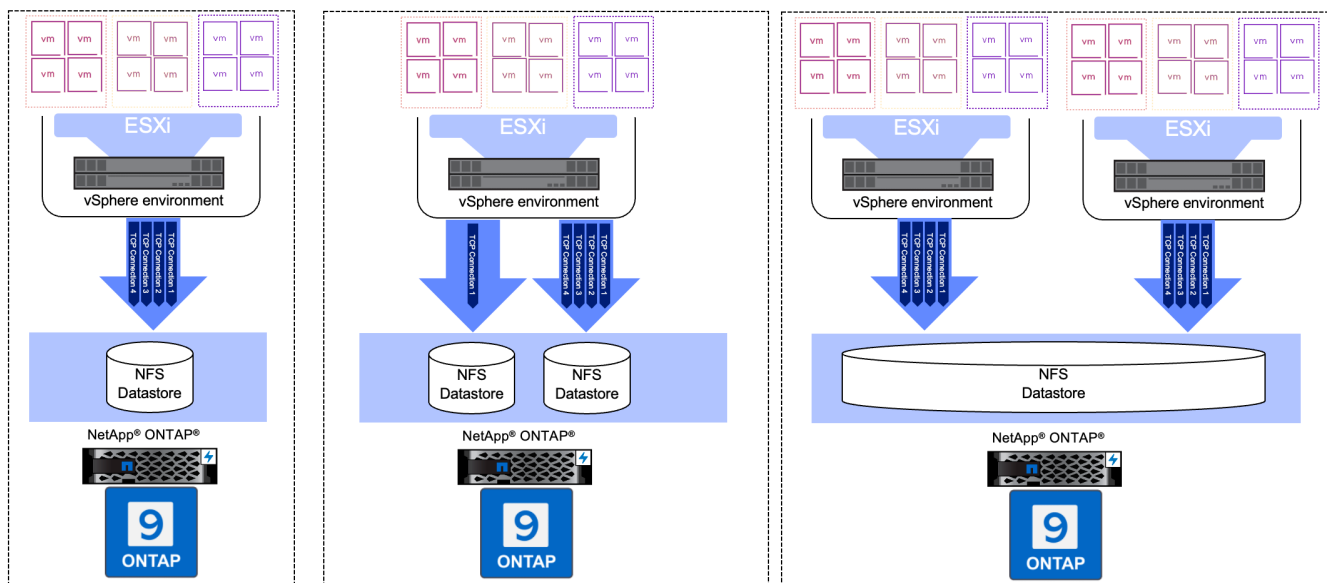
Without nConnect feature with NetApp and VMware



Avec le datastore nConnect NFS

Une fois le datastore NFS créé à l'aide des outils ONTAP ou d'autres options, le nombre de connexions par datastore NFS peut être modifié à l'aide de l'interface de ligne de commande vSphere, de PowerCLI, de l'outil govc ou d'autres options d'API. Pour éviter tout problème de performances avec vMotion, conservez le même nombre de connexions pour le datastore NFS sur tous les hôtes vSphere faisant partie du cluster vSphere.

With nConnect feature with NetApp and VMware



Condition préalable

Pour utiliser la fonctionnalité nconnect, les dépendances suivantes doivent être satisfaites.

| Version ONTAP | Version vSphere | Commentaires |
|---------------|-----------------|---|
| 9.8 ou plus | 8 mise à jour 1 | Aperçu technique avec option pour augmenter le nombre de connexions. |
| 9.8 ou plus | 8 mise à jour 2 | Généralement disponible avec option pour augmenter ou diminuer le nombre de connexions. |
| 9.8 ou plus | 8 mise à jour 3 | NFS 4.1 et prise en charge de chemins d'accès multiples. |

Mettre à jour le numéro de connexion au datastore NFS

Une seule connexion TCP est utilisée lorsqu'un datastore NFS est créé avec les outils ONTAP ou avec vCenter. Pour augmenter le nombre de connexions, il est possible d'utiliser l'interface de ligne de commande vSphere. La commande de référence est illustrée ci-dessous.

```

# Increase the number of connections while creating the NFS v3 datastore.
esxcli storage nfs add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To specify the number of connections while mounting the NFS 4.1
datastore.
esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the number of connections for existing NFSv3
datastore.
esxcli storage nfs param set -v <datastore_name> -c
<number_of_connections>
# For NFSv4.1 datastore
esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# To set VMkernel adapter for an existing NFS 4.1 datastore
esxcli storage nfs41 param set -I <NFS_Server_FQDN_or_IP>:vmk2 -v
<datastore_name> -c <number_of_connections>

```

Ou utilisez PowerCLI comme illustré ci-dessous

```

$datastoreSys = Get-View (Get-VMHost host01.vsphere.local).ExtensionData
.ConfigManager.DatastoreSystem
$nfSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfSpec.RemoteHost = "nfs_server.ontap.local"
$nfSpec.RemotePath = "/DS01"
$nfSpec.LocalPath = "DS01"
$nfSpec.AccessMode = "readWrite"
$nfSpec.Type = "NFS"
$nfSpec.Connections = 4
$datastoreSys.CreateNasDatastore($nfSpec)

```

Voici l'exemple de l'augmentation du nombre de connexions avec l'outil govc.

```

$env.GOVc_URL = 'vcenter.vsphere.local'
$env.GOVc_USERNAME = 'administrator@vsphere.local'
$env.GOVc_PASSWORD = 'XXXXXXXXXX'
$env.GOVc_Datastore = 'DS01'
# $env.GOVc_INSECURE = 1
$env.GOVc_HOST = 'host01.vsphere.local'
# Increase number of connections while creating the datastore.
govc host.esxcli storage nfs add -H nfs_server.ontap.local -v DS01 -s
/DS01 -c 2
# For NFS 4.1, replace nfs with nfs41
govc host.esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v
<datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
govc host.esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the connections for existing datastore.
govc host.esxcli storage nfs param set -v DS01 -c 4
# For NFSv4.1 datastore
govc host.esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# View the connection info
govc host.esxcli storage nfs list

```

Reportez-vous à ["Article 91497 de la base de connaissances VMware"](#) pour en savoir plus.

Considérations relatives à la conception

Le nombre maximal de connexions pris en charge par ONTAP dépend du modèle de plateforme de stockage. Recherchez `exec_ctx` activé ["Guide d'implémentation et des meilleures pratiques NFS"](#) pour en savoir plus.

Plus le nombre de connexions par datastore NFSv3 augmente, plus le nombre de datastores NFS pouvant être montés sur cet hôte vSphere diminue. Le nombre total de connexions prises en charge par hôte vSphere est de 256. Voir ["Article 91481 de la base de connaissances VMware"](#) Pour les limites de datastores par hôte vSphere.



Le datastore vVol ne prend pas en charge la fonctionnalité nConnect. Toutefois, les terminaux de protocole comptent pour atteindre la limite de connexion. Un terminal de protocole est créé pour chaque lif de données du SVM lors de la création du datastore vVol.

Utilisez les outils ONTAP 10 pour configurer les datastores NFS pour vSphere 8

Les outils ONTAP pour VMware vSphere 10 disposent d'une architecture nouvelle génération qui offre une haute disponibilité et une évolutivité natives pour le fournisseur VASA (prenant en charge les vVols iSCSI et NFS). Cela simplifie la gestion de plusieurs serveurs VMware vCenter et clusters ONTAP.

Dans ce scénario, nous allons vous montrer comment déployer et utiliser les outils ONTAP pour VMware vSphere 10 et configurer un datastore NFS pour vSphere 8.

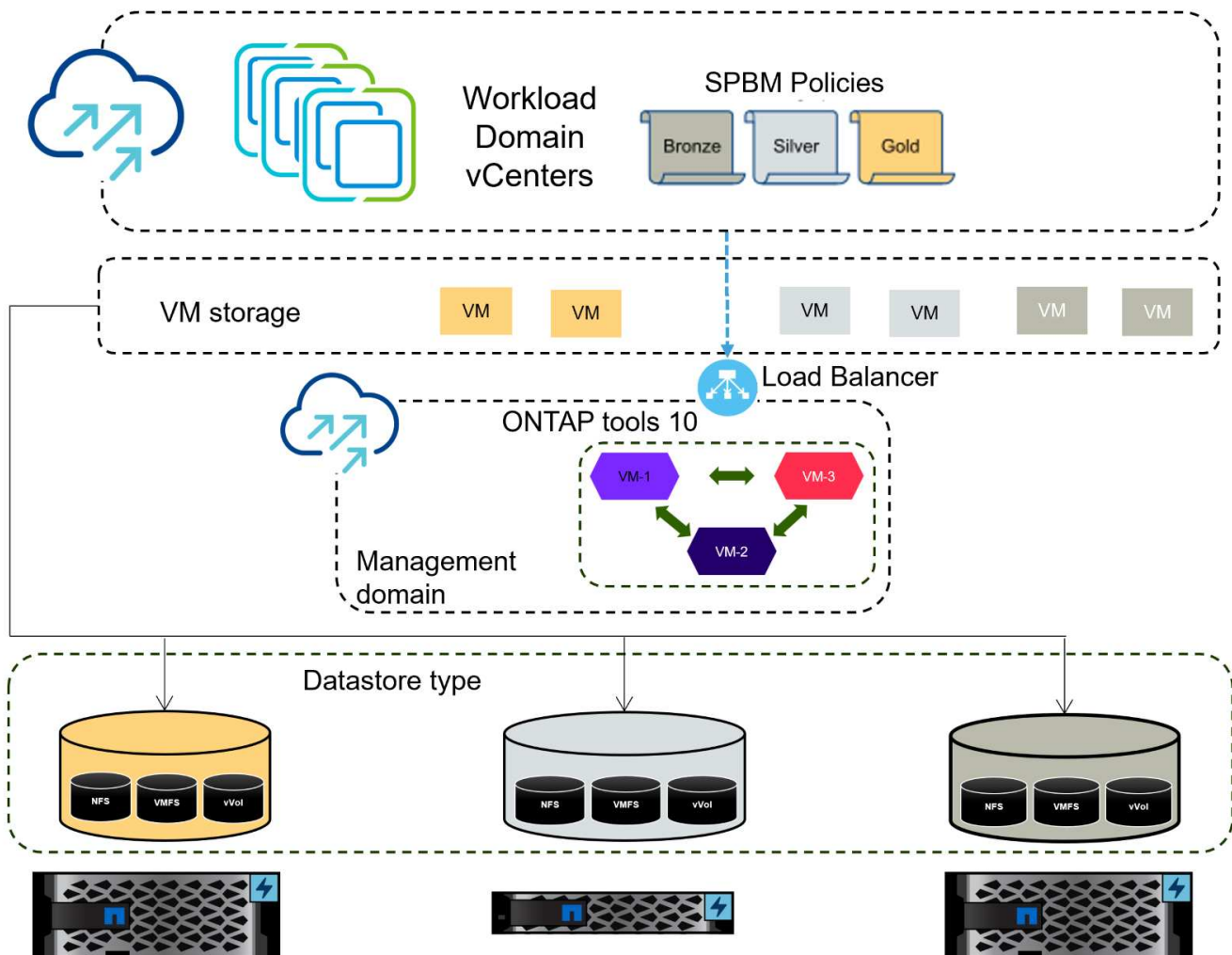
Présentation de la solution

Ce scénario couvre les étapes générales suivantes :

- Créez un SVM (Storage Virtual machine) avec des interfaces logiques (LIF) pour le trafic NFS.
- Créez un port group distribué pour le réseau NFS sur le cluster vSphere 8.
- Créez un adaptateur vmkernel pour NFS sur les hôtes ESXi du cluster vSphere 8.
- Déployer les outils ONTAP 10 et les enregistrer sur le cluster vSphere 8.
- Créez un datastore NFS sur le cluster vSphere 8.

Architecture

Le diagramme suivant présente les composants architecturaux des outils ONTAP pour l'implémentation de VMware vSphere 10.



Prérequis

Cette solution requiert les configurations et composants suivants :

- Un système de stockage ONTAP AFF doté de ports de données physiques sur des commutateurs ethernet dédiés au trafic de stockage.
- Le déploiement du cluster vSphere 8 est terminé et le client vSphere est accessible.
- Le modèle OVA des outils ONTAP pour VMware vSphere 10 a été téléchargé à partir du site de support NetApp.

NetApp recommande un réseau redondant pour NFS, offrant une tolérance aux pannes pour les systèmes de stockage, les switchs, les adaptateurs réseau et les systèmes hôtes. Il est courant de déployer NFS avec un ou plusieurs sous-réseaux, selon les exigences architecturales.

Reportez-vous à la section "[Meilleures pratiques pour l'exécution de NFS avec VMware vSphere](#)" Pour obtenir des informations détaillées spécifiques à VMware vSphere.

Pour obtenir des conseils réseau sur l'utilisation de ONTAP avec VMware vSphere, reportez-vous au "[Configuration réseau - NFS](#)" De la documentation des applications d'entreprise NetApp.

Des ressources complètes sur les outils ONTAP 10 sont disponibles "[Ressources de documentation des outils ONTAP pour VMware vSphere](#)".

Étapes de déploiement

Pour déployer les outils ONTAP 10 et l'utiliser pour créer un datastore NFS sur le domaine de gestion VCF, procédez comme suit :

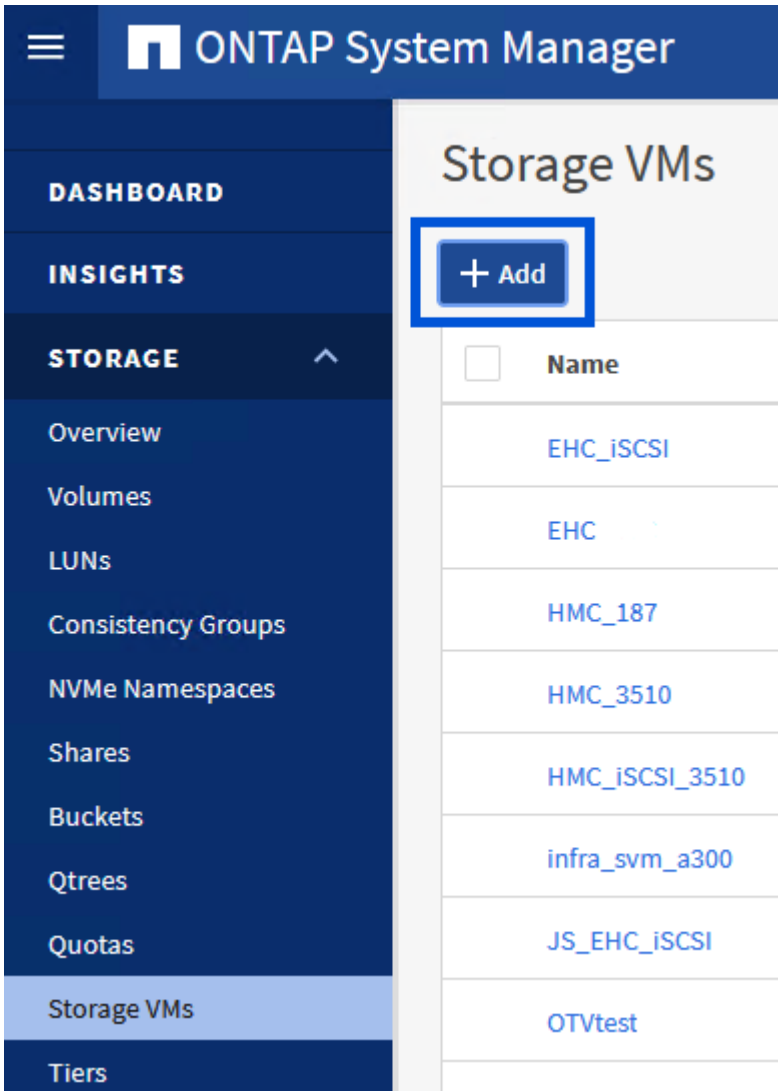
Créez un SVM et des LIF sur un système de stockage ONTAP

L'étape suivante s'effectue dans ONTAP System Manager.

Créez la VM de stockage et les LIF

Effectuer les étapes suivantes pour créer un SVM avec plusieurs LIF pour le trafic NFS.

1. Dans le Gestionnaire système ONTAP, accédez à **Storage VMs** dans le menu de gauche et cliquez sur **+ Add** pour démarrer.



2. Dans l'assistant **Add Storage VM**, indiquez un **Name** pour le SVM, sélectionnez **IP Space**, puis, sous **Access Protocol**, cliquez sur l'onglet **SMB/CIFS, NFS, S3** et cochez la case **Enable NFS**.

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default


Access Protocol

SMB/CIFS, NFS, S3 [iSCSI](#) [FC](#) [NVMe](#)

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



Il n'est pas nécessaire de cliquer ici sur le bouton **Autoriser l'accès client NFS** car les outils ONTAP pour VMware vSphere seront utilisés pour automatiser le processus de déploiement du datastore. Cela inclut l'accès client pour les hôtes ESXi. Et no 160 ;

3. Dans la section **interface réseau**, remplissez les champs **adresse IP**, **masque de sous-réseau** et **domaine de diffusion et Port** pour la première LIF. Pour les LIF suivantes, la case à cocher peut être activée pour utiliser des paramètres communs à toutes les LIF restantes ou pour utiliser des paramètres distincts.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

- Indiquez si vous souhaitez activer le compte Storage VM Administration (pour les environnements en colocation) et cliquez sur **Save** pour créer le SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

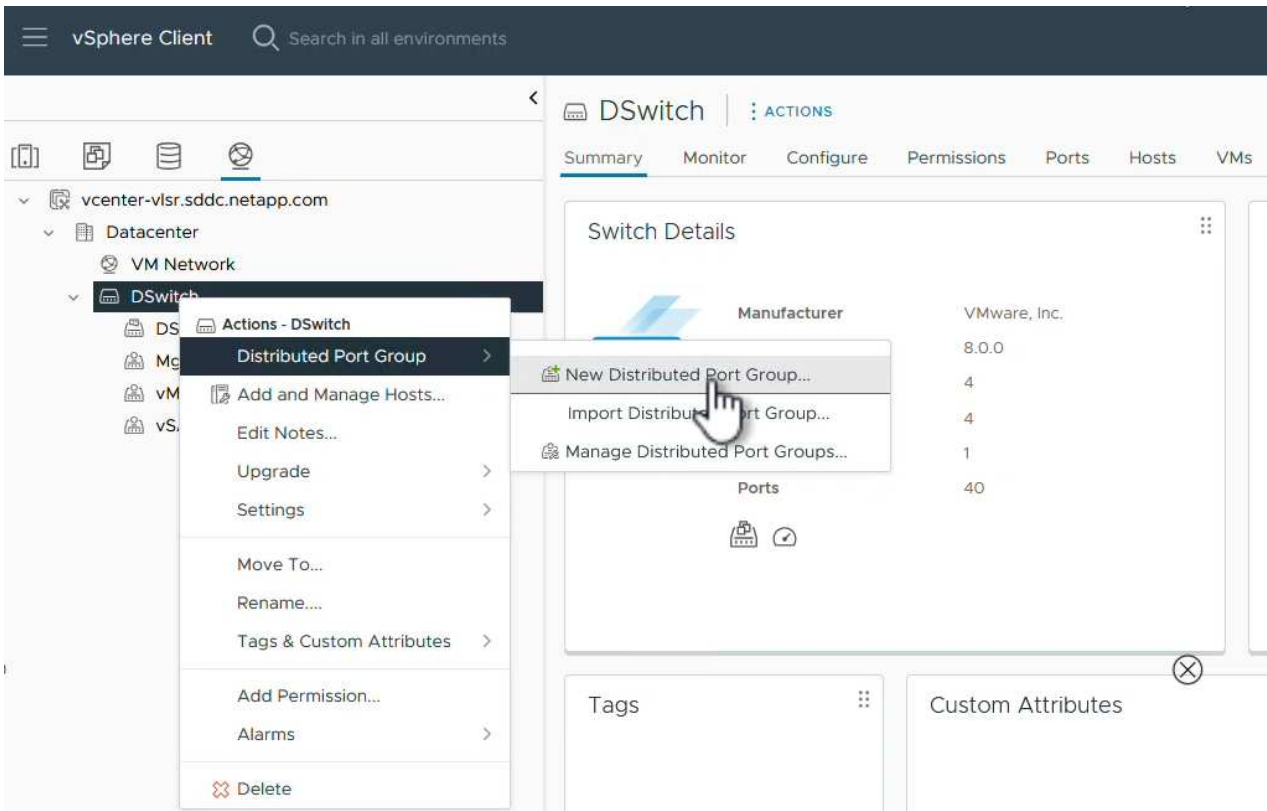
Configuration de la mise en réseau pour NFS sur les hôtes ESXi

Les étapes suivantes sont effectuées sur le cluster VI Workload Domain à l'aide du client vSphere. Dans ce cas, l'authentification unique vCenter est utilisée, de sorte que le client vSphere est commun aux domaines de gestion et de charge de travail.

Créez un Port Group distribué pour le trafic NFS

Pour créer un nouveau groupe de ports distribués pour le réseau qui transporte le trafic NFS, procédez comme suit :

1. Dans le client vSphere , accédez à **Inventory > Networking** pour le domaine de charge de travail. Naviguez jusqu'au commutateur distribué existant et choisissez l'action pour créer **Nouveau groupe de ports distribués....**



2. Dans l'assistant **Nouveau groupe de ports distribués**, entrez un nom pour le nouveau groupe de ports et cliquez sur **Suivant** pour continuer.
3. Sur la page **configurer les paramètres**, remplissez tous les paramètres. Si des VLAN sont utilisés, assurez-vous de fournir l'ID de VLAN correct. Cliquez sur **Suivant** pour continuer.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

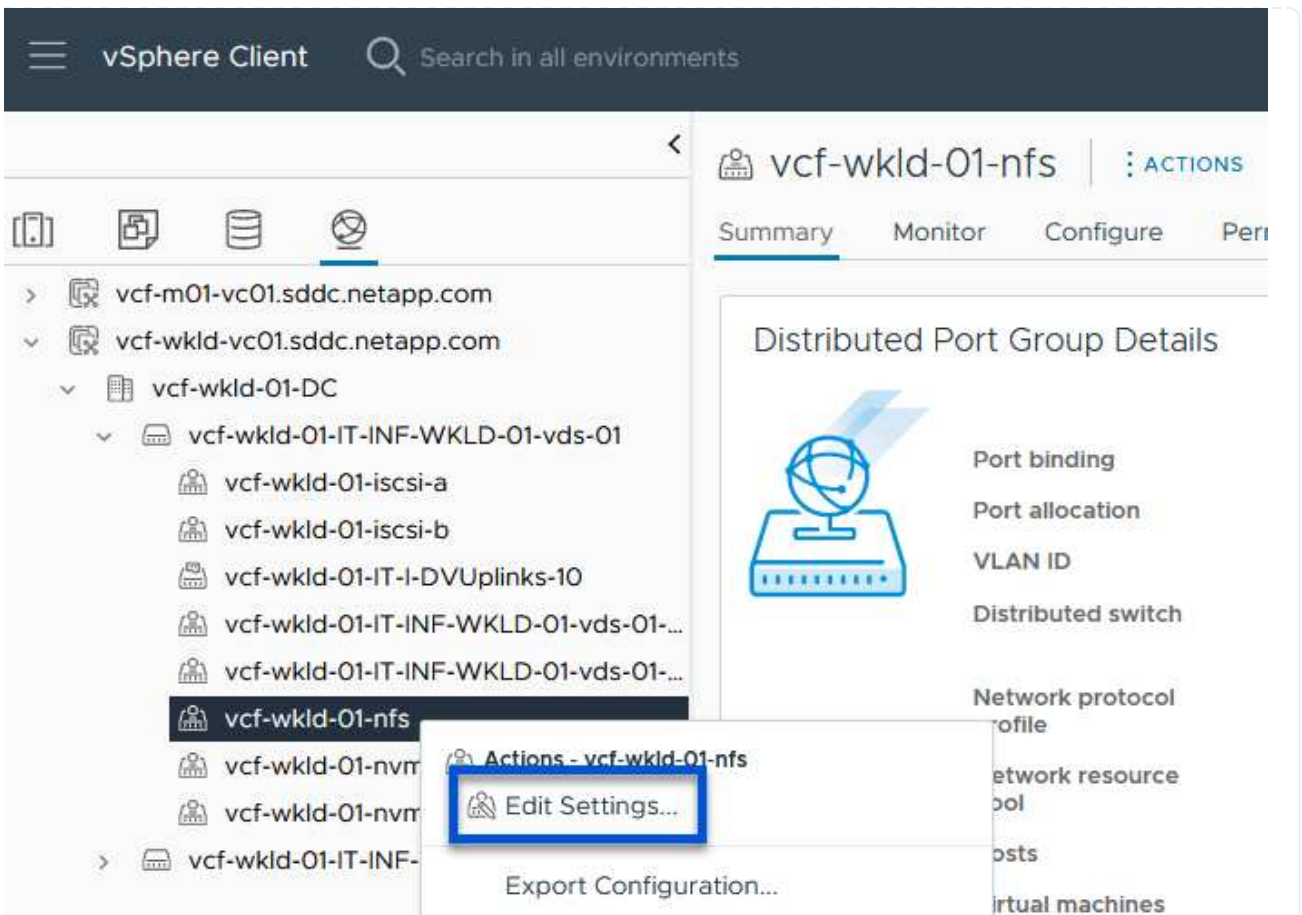
| | |
|---|------------------------|
| Port binding | Static binding |
| Port allocation | Elastic ? |
| Number of ports | 8 |
| Network resource pool | (default) |
| VLAN | |
| VLAN type | VLAN |
| VLAN ID | 3374 |
| Advanced | |
| <input type="checkbox"/> Customize default policies configuration | |

CANCEL

BACK

NEXT

4. Sur la page **prêt à terminer**, passez en revue les modifications et cliquez sur **Terminer** pour créer le nouveau groupe de ports distribués.
5. Une fois le groupe de ports créé, naviguez jusqu'au groupe de ports et sélectionnez l'action **Modifier les paramètres....**



6. Sur la page **Distributed Port Group - Edit Settings**, accédez à **Teaming and failover** dans le menu de gauche. Activez l'agrégation pour les liaisons montantes à utiliser pour le trafic NFS en vous assurant qu'elles sont regroupées dans la zone **Active uplinks**. Déplacez toutes les liaisons ascendantes inutilisées vers le bas jusqu'à **uplinks non utilisés**.

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Uplink 1

Uplink 2

Standby uplinks

Unused uplinks

CANCEL

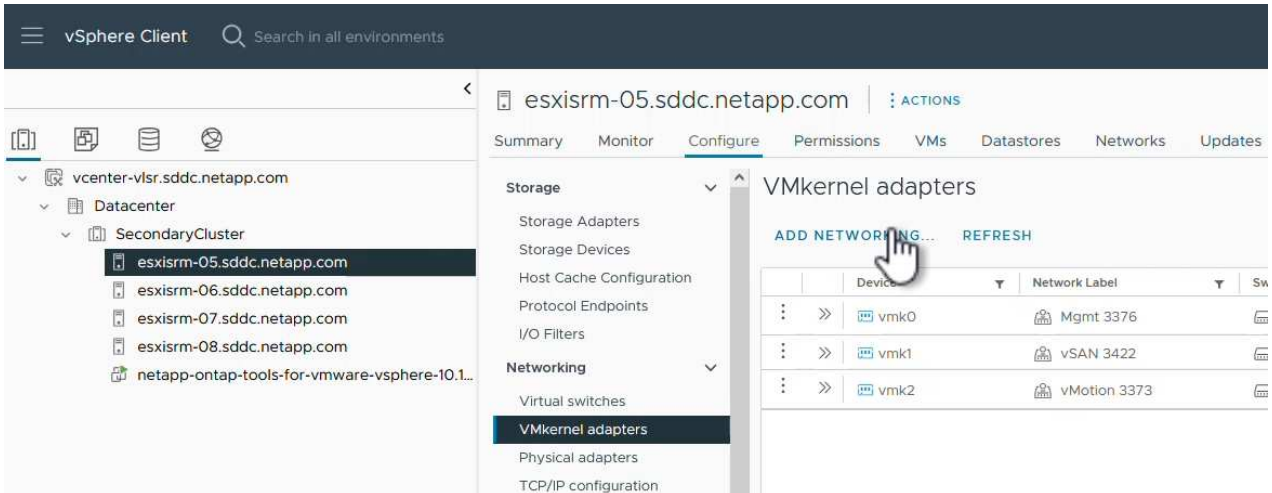
OK

7. Répétez ce processus pour chaque hôte ESXi du cluster.

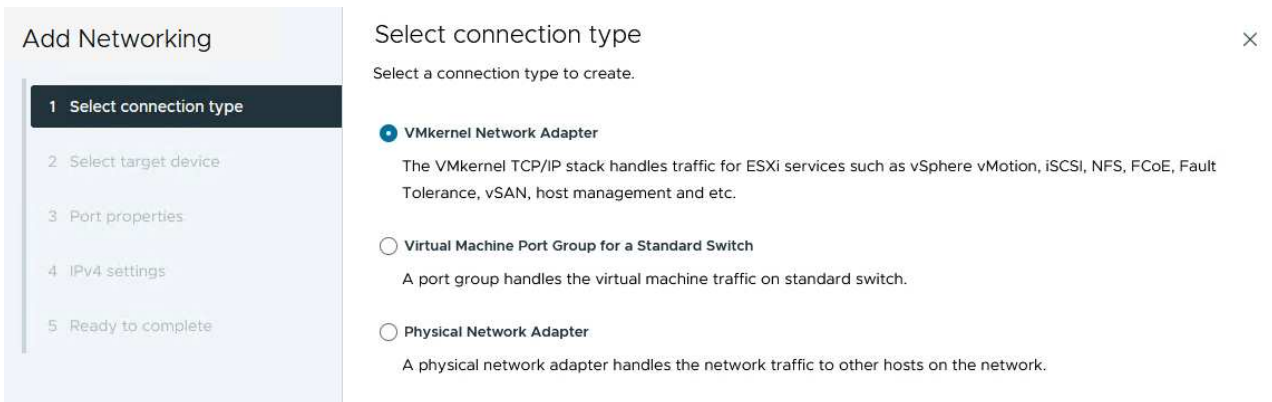
Créez un adaptateur VMkernel sur chaque hôte ESXi

Répétez ce processus sur chaque hôte ESXi du domaine de charge de travail.

1. À partir du client vSphere, accédez à l'un des hôtes ESXi de l'inventaire du domaine de charge de travail. Dans l'onglet **configurer**, sélectionnez **adaptateurs VMkernel** et cliquez sur **Ajouter réseau...** pour démarrer.



2. Dans la fenêtre **Select connection type**, choisissez **VMkernel Network adapter** et cliquez sur **Next** pour continuer.



3. Sur la page **Sélectionner le périphérique cible**, choisissez l'un des groupes de ports distribués pour NFS créés précédemment.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

| | Name | NSX Port Group ID | Distributed Switch |
|----------------------------------|--------------|-------------------|--------------------|
| <input type="radio"/> | Mgmt 3376 | -- | DSwitch |
| <input checked="" type="radio"/> | NFS 3374 | -- | DSwitch |
| <input type="radio"/> | vMotion 3373 | -- | DSwitch |
| <input type="radio"/> | vSAN 3422 | -- | DSwitch |

Manage Columns 4 items

CANCEL

BACK

NEXT

4. Sur la page **Port properties**, conservez les valeurs par défaut (aucun service activé) et cliquez sur **Next** pour continuer.
5. Sur la page **IPv4 settings**, remplissez **adresse IP**, **masque de sous-réseau** et fournissez une nouvelle adresse IP de passerelle (uniquement si nécessaire). Cliquez sur **Suivant** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings**
- 5 Ready to complete

IPv4 settings



Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

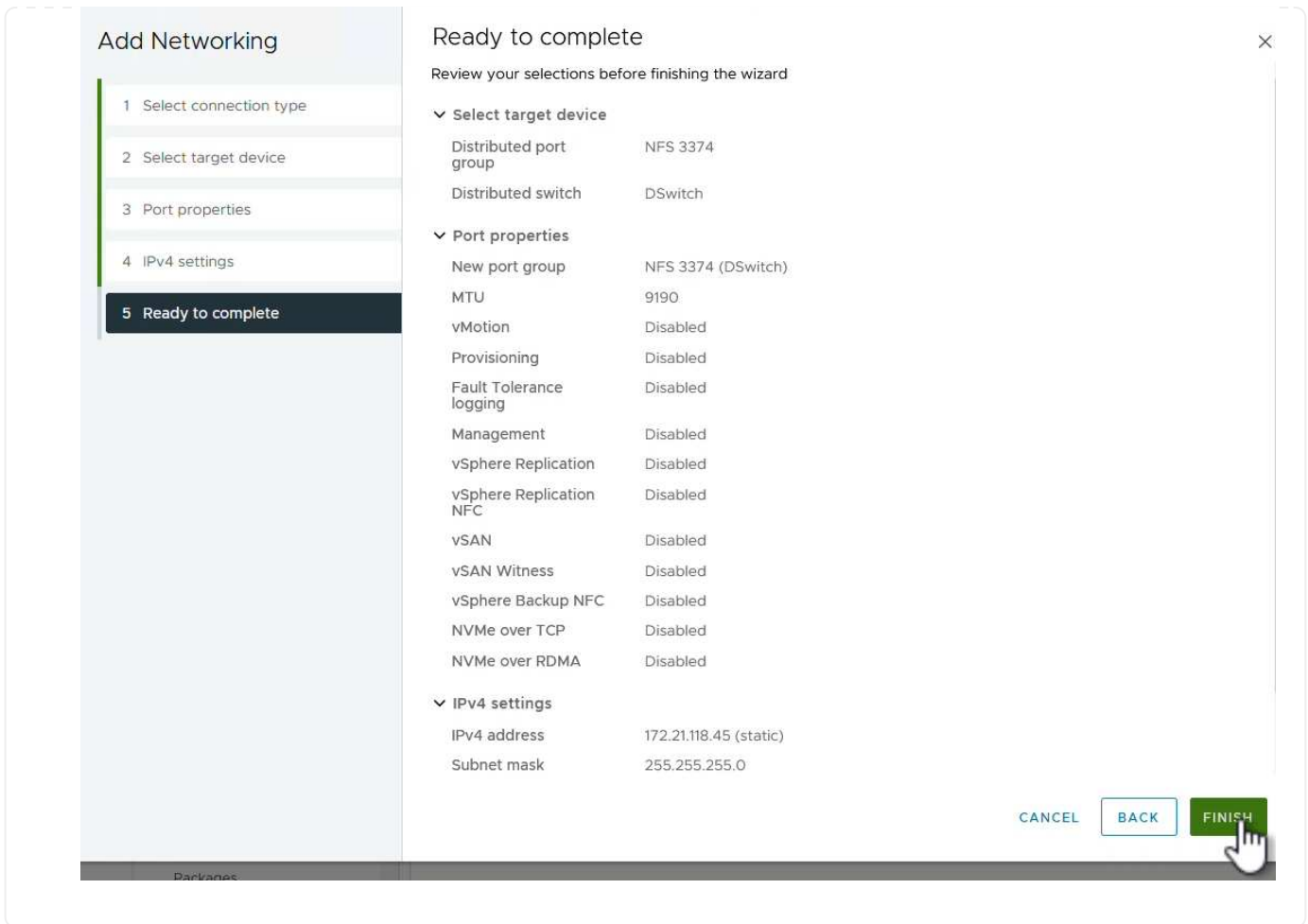
DNS server addresses

CANCEL

BACK

NEXT

6. Consultez vos sélections sur la page **prêt à terminer** et cliquez sur **Terminer** pour créer l'adaptateur VMkernel.



Déployer et utiliser les outils ONTAP 10 pour configurer le stockage

Les étapes suivantes sont effectuées sur un cluster vSphere 8 à l'aide du client vSphere et impliquent le déploiement d'OTV, la configuration du gestionnaire d'outils ONTAP et la création d'un datastore NFS vVols.

Pour obtenir la documentation complète sur le déploiement et l'utilisation des outils ONTAP pour VMware vSphere 10, reportez-vous "[Préparez-vous à déployer les outils ONTAP pour VMware vSphere](#)" à la .

Déployez les outils ONTAP pour VMware vSphere 10

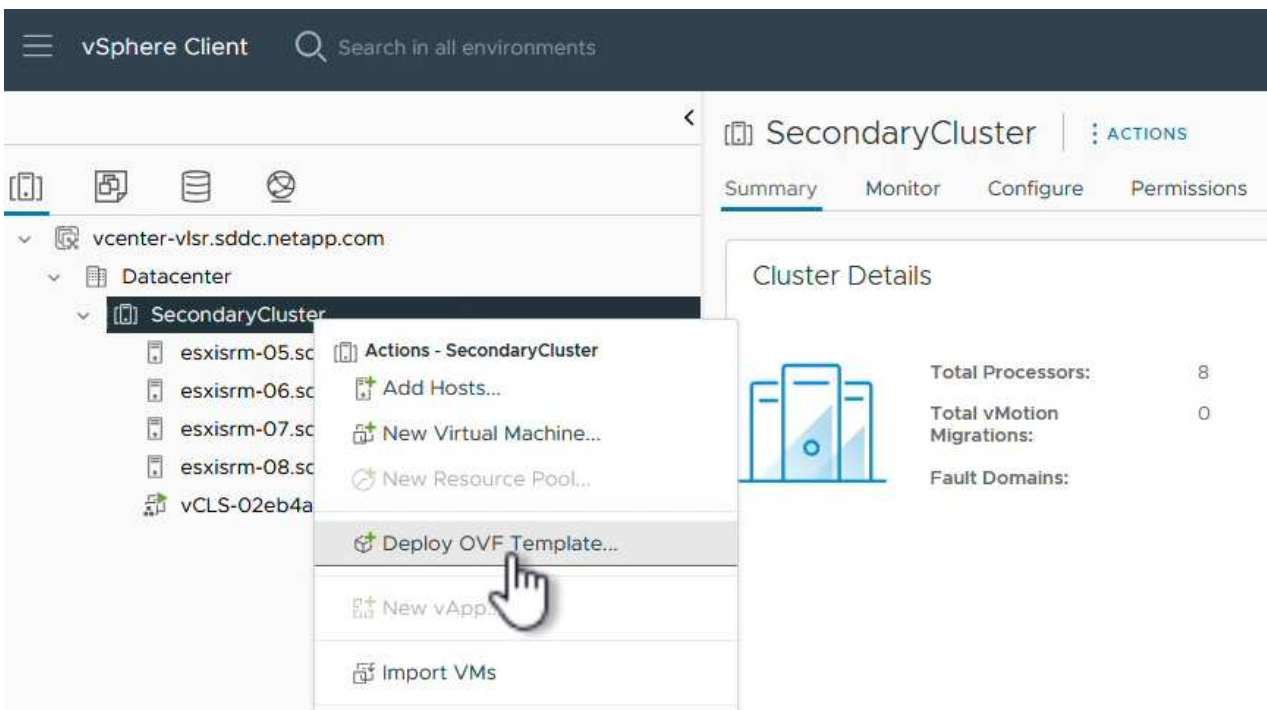
Les outils ONTAP pour VMware vSphere 10 sont déployés en tant qu'appliance de machine virtuelle et fournissent une interface utilisateur vCenter intégrée pour la gestion du stockage ONTAP. ONTAP Tools 10 inclut un nouveau portail de gestion global pour la gestion des connexions à plusieurs serveurs vCenter et systèmes back-end de stockage ONTAP.



Dans le cas d'un déploiement non HA, trois adresses IP disponibles sont requises. Une adresse IP est allouée à l'équilibreur de charge, une autre au plan de contrôle Kubernetes et l'autre au nœud. Dans un déploiement haute disponibilité, deux adresses IP supplémentaires sont nécessaires pour les deuxième et troisième nœuds, en plus des trois nœuds initiaux. Avant l'affectation, les noms d'hôte doivent être associés aux adresses IP dans DNS. Il est important que les cinq adresses IP se trouvent sur le même VLAN, qui est choisi pour le déploiement.

Procédez comme suit pour déployer les outils ONTAP pour VMware vSphere :

1. Obtenez l'image OVA des outils ONTAP à partir du "[Site de support NetApp](#)" et téléchargez-la dans un dossier local.
2. Connectez-vous à l'appliance vCenter pour le cluster vSphere 8.
3. Dans l'interface de l'appliance vCenter, cliquez avec le bouton droit de la souris sur le cluster de gestion et sélectionnez **déployer le modèle OVF...**



4. Dans l'assistant **déployer modèle OVF**, cliquez sur le bouton radio **fichier local** et sélectionnez le fichier OVA des outils ONTAP téléchargé à l'étape précédente.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Pour les étapes 2 à 5 de l'assistant, sélectionnez un nom et un dossier pour la machine virtuelle, sélectionnez la ressource de calcul, vérifiez les détails et acceptez le contrat de licence.
6. Pour l'emplacement de stockage des fichiers de configuration et de disque, sélectionnez un datastore local ou VSAN.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage**
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

VM Storage Policy

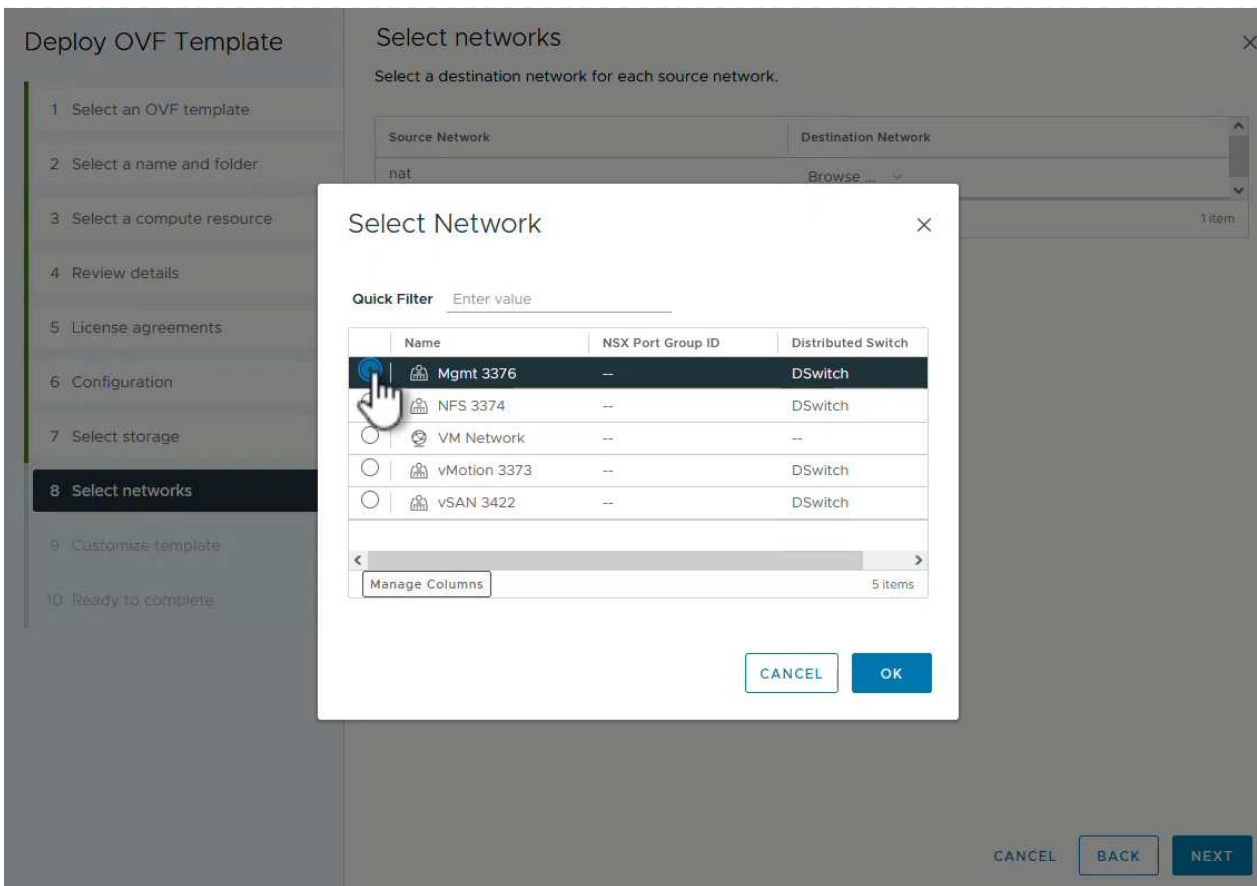
Disable Storage DRS for this virtual machine

| Name | Storage Compatibility | Capacity | Provisioned | Free | |
|---------------|-----------------------|-----------|-------------|-----------|--|
| vsanDatastore | -- | 799.97 GB | 26.05 GB | 783.98 GB | |

Items per page 10 1 Item

Compatibility

7. Sur la page Sélectionner le réseau, sélectionnez le réseau utilisé pour le trafic de gestion.



8. Sur la page Configuration, sélectionnez la configuration de déploiement à utiliser. Dans ce scénario, la méthode de déploiement facile est utilisée.



Les outils ONTAP 10 comprennent plusieurs configurations de déploiement, notamment des déploiements haute disponibilité à l'aide de plusieurs nœuds. Pour obtenir de la documentation sur toutes les configurations de déploiement, reportez-vous à "[Préparez-vous à déployer les outils ONTAP pour VMware vSphere](#)" la section.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration**
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Configuration

Select a deployment configuration

| | | |
|--|---|--|
| <input checked="" type="radio"/> Easy deployment (S) | Description Deploy local provisioner Non-HA Small single node instance of ONTAP tools | |
| <input type="radio"/> Easy deployment (M) | | |
| <input type="radio"/> Advanced deployment (S) | | |
| <input type="radio"/> Advanced deployment (M) | | |
| <input type="radio"/> High-Availability deployment (S) | | |
| <input type="radio"/> High-Availability deployment (M) | | |
| <input type="radio"/> High-Availability deployment (L) | | |
| <input type="radio"/> Recovery | | |
| 8 Items | | |

CANCEL

BACK

NEXT

9. Sur la page Personnaliser le modèle, remplissez toutes les informations requises :

- Nom d'utilisateur de l'application à utiliser pour enregistrer le fournisseur VASA et SRA dans vCenter Server.
- Activez ASUP pour le support automatisé.
- URL du proxy ASUP, si nécessaire.
- Nom d'utilisateur et mot de passe administrateur.
- Serveurs NTP.
- Mot de passe utilisateur de maintenance pour accéder aux fonctions de gestion à partir de la console.
- Adresse IP de l'équilibreur de charge.
- IP virtuelle pour le plan de contrôle K8s.
- Machine virtuelle primaire pour sélectionner la machine virtuelle actuelle comme principale (pour les configurations haute disponibilité).
- Nom d'hôte de la machine virtuelle
- Renseignez les champs de propriétés réseau requis.

Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Customize the deployment properties of this software solution.

! 10 properties have invalid values X

| System Configuration | | 8 settings |
|----------------------------------|---|---|
| Application username(*) | Username to assign to the Application | <input type="text" value="vsphere-services"/> |
| Application password(*) | Password to assign to the Application | <input type="password" value="....."/> |
| | Confirm Password | <input type="password" value="....."/> |
| Enable ASUP | Select this checkbox to enable ASUP | <input checked="" type="checkbox"/> |
| ASUP Proxy URL | Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle. | <input type="text"/> |
| Administrator username(*) | Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '.', ':', '-' special characters are supported | <input style="border: 1px solid red;" type="text"/> |
| Administrator password(*) | Password to assign to the Administrator | <input type="password"/> |

CANCEL BACK NEXT

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

| Maintenance user password(*) | Password to assign to maint user account | <input type="password" value="....."/> |
|--|---|---|
| | Confirm Password | <input type="password" value="....."/> |
| Deployment Configuration | | 3 settings |
| Load balancer IP(*) | Load balancer IP (*) | <input type="text" value="172.21.120.57"/> |
| Virtual IP for K8s control plane(*) | Provide the virtual IP address for K8s control plane | <input type="text" value="172.21.120.58"/> |
| Primary VM | Maintain this field as selected to set the current VM as primary and install the ONTAP tools. | <input checked="" type="checkbox"/> |
| Node Configuration | | 10 settings |
| HostName(*) | Specify the hostname for the VM | <input style="border: 1px solid red;" type="text"/> |
| IP Address(*) | Specify the IP address for the appliance | <input style="border: 1px solid red;" type="text"/> |
| IPv6 Address | Specify the IPv6 address on the deployed network only when you need dual stack. | <input type="text"/> |

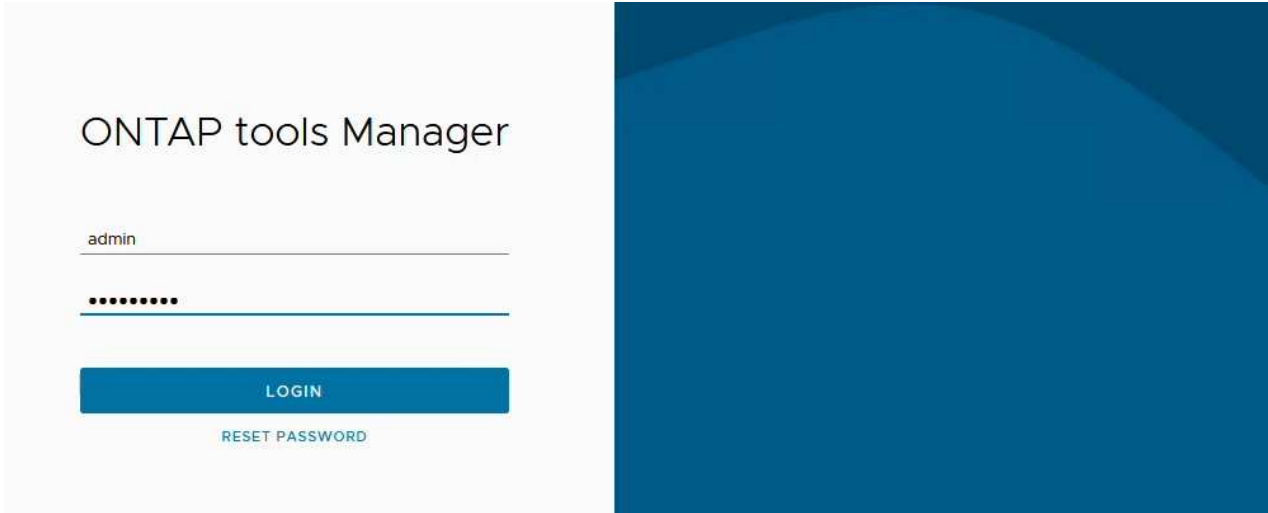
CANCEL BACK NEXT

10. Passez en revue toutes les informations de la page prêt à terminer et cliquez sur Terminer pour commencer à déployer l'appliance ONTAP Tools.

Connectez le système de stockage interne et vCenter Server aux outils ONTAP 10.

Le gestionnaire d'outils ONTAP permet de configurer les paramètres globaux des outils ONTAP 10.

1. Accédez au Gestionnaire des outils ONTAP en accédant à <https://loadBalanceIP:8443/virtualization/ui/> dans un navigateur Web et en vous connectant à l'aide des informations d'identification administratives fournies lors du déploiement.



2. Sur la page **mise en route**, cliquez sur **aller à stockage backend**.

Getting Started



ONTAP tools Manager allows you to manage ONTAP Storage Backends and associate them with vCenters. You can also download support log bundles.



Storage Backends

Add, modify, and remove storage backends.

[Go to Storage Backends](#)



vCenters

Add, modify, and remove vCenters and associate storage backends with them.

[Go to vCenters](#)



Log Bundles

Generate and download log bundles for support purposes.

[Go to Log Bundles](#)

Don't show again

3. Sur la page **systèmes backend de stockage**, cliquez sur **AJOUTER** pour saisir les informations d'identification d'un système de stockage ONTAP à enregistrer avec les outils ONTAP 10.

ONTAP tools Manager

Storage Backends

The ESXi hosts use Storage Backends for data storage.

| Name | Type | IP Address or FQDN |
|------|------|--------------------|
|------|------|--------------------|


This list is empty!

4. Dans la zone **Ajouter un système de stockage interne**, renseignez les informations d'identification du système de stockage ONTAP.

Add Storage Backend

Hostname: * 172.16.9.25

Username: * admin

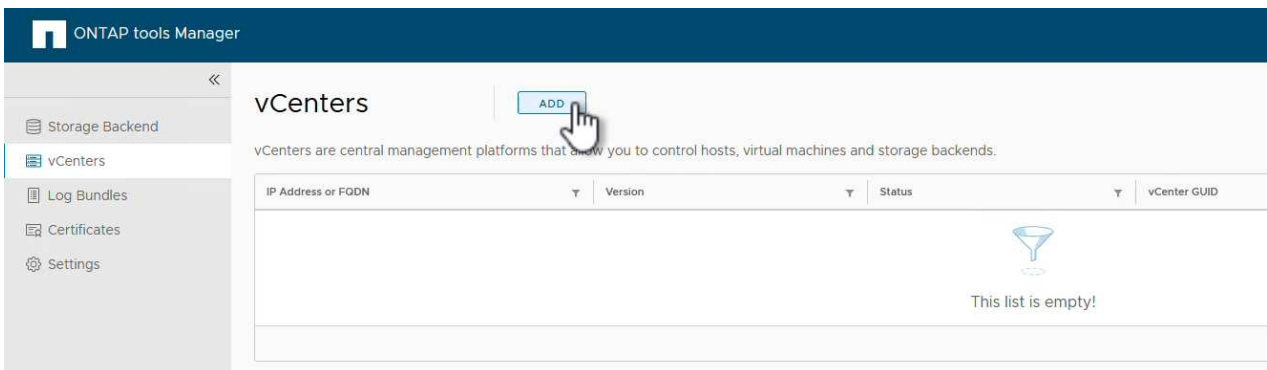
Password: * ●●●●●●●● 

Port: * 443

CANCEL

ADD 

5. Dans le menu de gauche, cliquez sur **vCenters**, puis sur **ADD** pour saisir les informations d'identification d'un serveur vCenter à enregistrer avec les outils ONTAP 10.




ONTAP tools Manager

vCenters

ADD

vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends.

| IP Address or FQDN | Version | Status | vCenter GUID |
|--|---------|--------|--------------|
|  This list is empty! | | | |

6. Dans la zone **Ajouter vCenter**, remplissez les informations d'identification du système de stockage ONTAP.

Add vCenter

Server IP Address or FQDN: *

Username: *

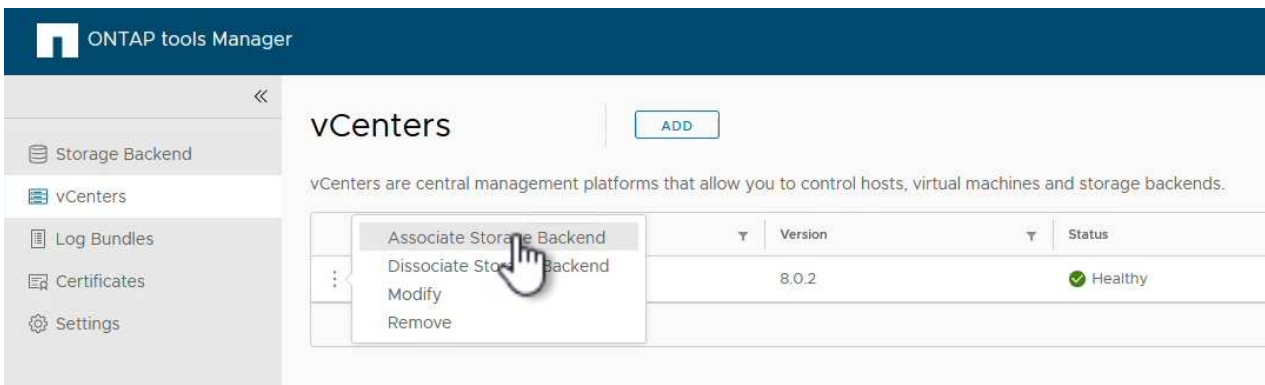
Password: * 

Port: *

CANCEL

ADD 

7. Dans le menu vertical à trois points du serveur vCenter récemment découvert, sélectionnez **associer le stockage interne**.



The screenshot shows the ONTAP tools Manager interface. On the left is a navigation menu with options: Storage Backend, vCenters, Log Bundles, Certificates, and Settings. The main area is titled 'vCenters' and contains a table of vCenter servers. A context menu is open over the first row, with 'Associate Storage Backend' selected. The table has columns for Version and Status.

| | Version | Status |
|-------|---------|--------|
| 8.0.2 | Healthy | |

8. Dans la zone **associer le stockage interne**, sélectionnez le système de stockage ONTAP à associer au serveur vCenter et cliquez sur **associer** pour terminer l'action.

Associate Storage Backend

vcenter-vlsr.sddc.netapp.com



Storage Backend

ntaphci-a300e9u25

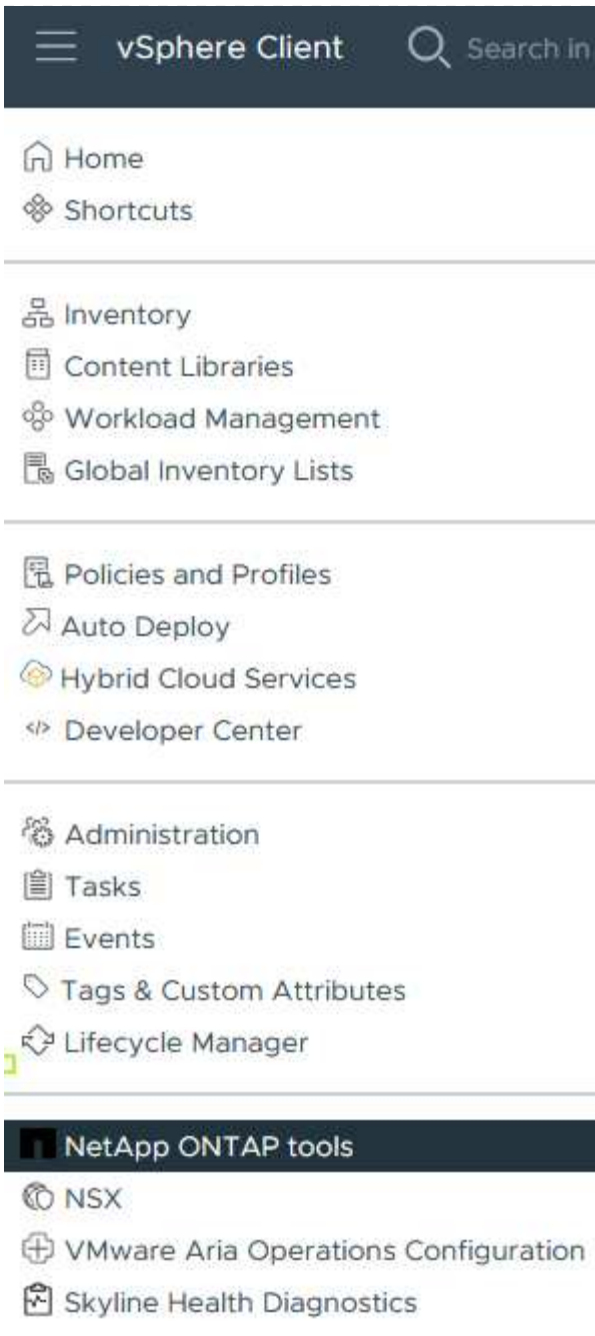


CANCEL

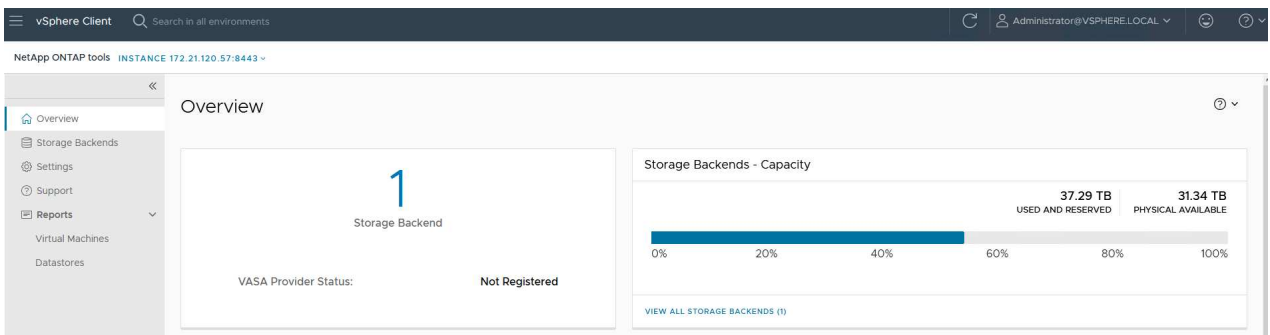
ASSOCIATE



9. Pour vérifier l'installation, connectez-vous au client vSphere et sélectionnez **NetApp ONTAP Tools** dans le menu de gauche.



10. Dans le tableau de bord des outils ONTAP, vous devriez voir qu'un système back-end de stockage a été associé au serveur vCenter.

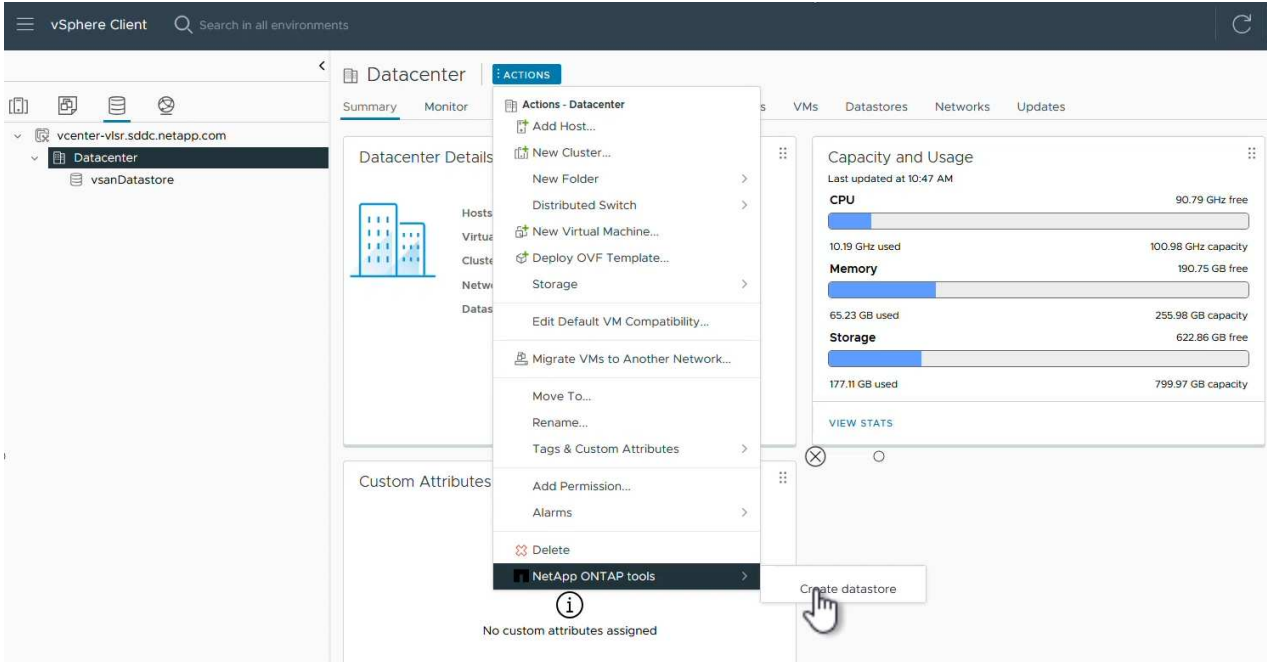




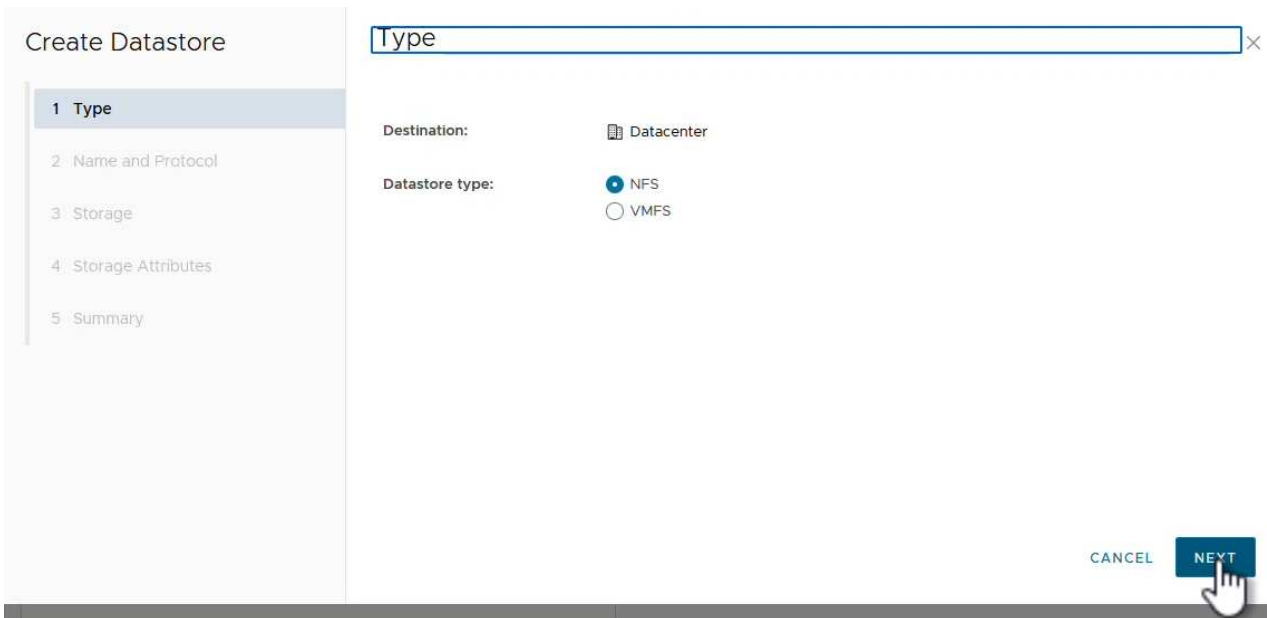
Créer un datastore NFS à l'aide des outils ONTAP 10

Procédez comme suit pour déployer un datastore ONTAP, exécuté sur NFS, à l'aide des outils ONTAP 10.

1. Dans le client vSphere, accédez à l'inventaire du stockage. Dans le menu **ACTIONS**, sélectionnez **Outils NetApp ONTAP > Créer un datastore**.



2. Sur la page **Type** de l'assistant Créer un datastore, cliquez sur le bouton radio NFS, puis sur **Suivant** pour continuer.



3. Sur la page **Nom et protocole**, indiquez le nom, la taille et le protocole du datastore. Cliquez sur **Suivant** pour continuer.

The screenshot shows the 'Create Datastore' wizard in the 'Name and Protocol' step. On the left, a sidebar lists five steps: 1 Type, 2 Name and Protocol (highlighted), 3 Storage, 4 Storage Attributes, and 5 Summary. The main area is titled 'Name and Protocol' and contains the following fields:

- Datastore name:** NFS_DS1
- Size:** 2 TB (with a note: 'Minimum supported size is 1 GB.')
- Protocol:** NFS 3
- Advanced Options:** expanded, showing **Datastore Cluster:** (empty dropdown).

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

4. Sur la page **Storage**, sélectionnez une plate-forme (filtre le système de stockage par type) et une machine virtuelle de stockage pour le volume. Si vous le souhaitez, sélectionnez une export policy personnalisée. Cliquez sur **Suivant** pour continuer.

The screenshot shows the 'Create Datastore' wizard in the 'Storage' step. On the left, the sidebar lists five steps: 1 Type, 2 Name and Protocol, 3 Storage (highlighted), 4 Storage Attributes, and 5 Summary. The main area is titled 'Storage' and contains the following fields:

- Platform: *** Performance (A)
- Storage VM: *** VCF_NFS (with IP: ntaphci-a300e9u25 (172.16.9.25))
- Advanced Options:** expanded, showing **Custom Export Policy:** Search or specify policy name (with a note: 'Choose an existing policy or give a new name to the default policy.')

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

5. Sur la page **attributs de stockage**, sélectionnez l'agrégat de stockage à utiliser et éventuellement des options avancées telles que la réservation d'espace et la qualité de service. Cliquez sur **Suivant** pour continuer.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 Summary

Storage Attributes

Specify the storage details for provisioning the datastore.

Aggregate: * EHCaggr02 (16.61 TB Free) ▾

Volume: A new volume will be created automatically.

^ Advanced Options

Space Reserve: * Thin ▾

Enable QoS

CANCEL

BACK

NEXT

6. Enfin, passez en revue le **Résumé** et cliquez sur Terminer pour commencer à créer le datastore NFS.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 Summary

Summary

A new datastore will be created with these settings.

Type

Destination: Datacenter
Datastore type: NFS

Name and Protocol

Datastore name: NFS_DS1
Size: 2 TB
Protocol: NFS 3

Storage

Platform: Performance (A)
Storage VM: VCF_NFS

CANCEL

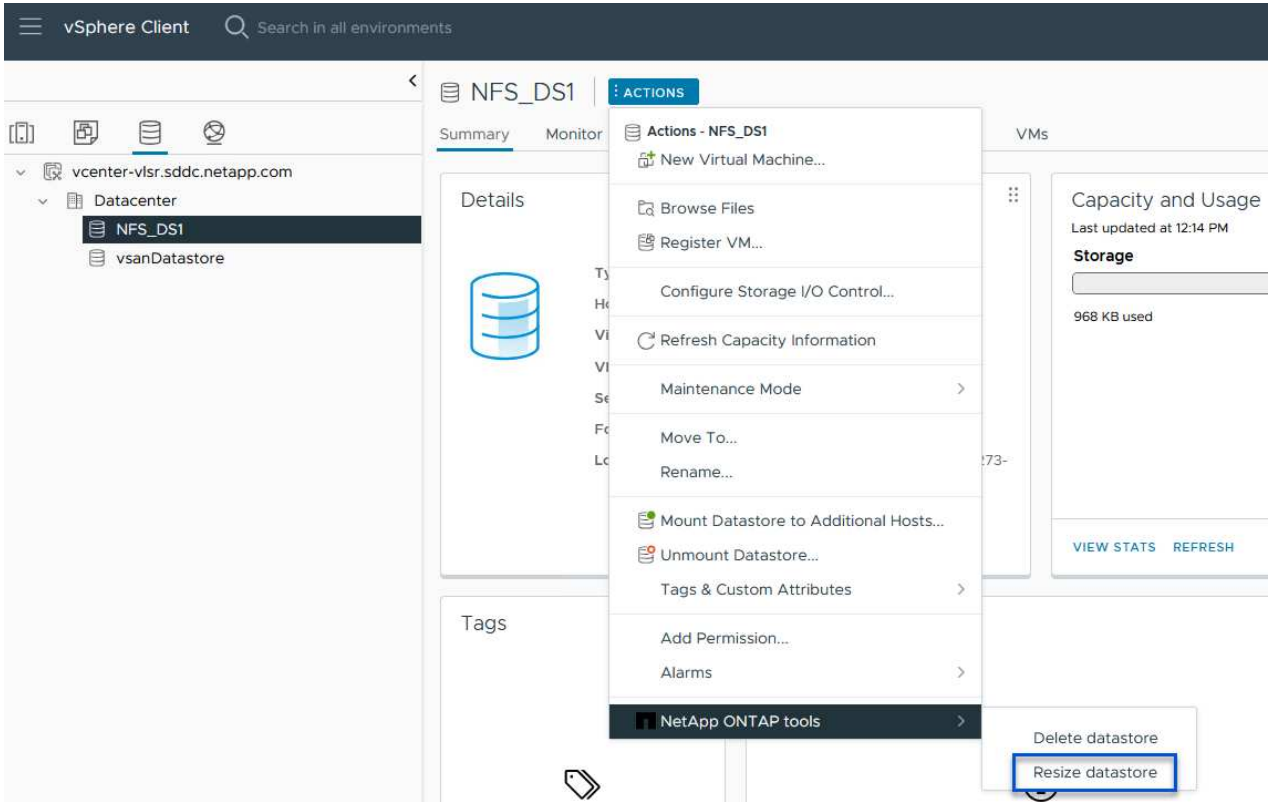
BACK

FINISH

Redimensionner un datastore NFS à l'aide des outils ONTAP 10

Procédez comme suit pour redimensionner un datastore NFS existant à l'aide des outils ONTAP 10.

1. Dans le client vSphere, accédez à l'inventaire du stockage. Dans le menu **ACTIONS**, sélectionnez **Outils NetApp ONTAP > Redimensionner le datastore**.



2. Dans l'assistant **Redimensionner datastore**, indiquez la nouvelle taille du datastore en Go et cliquez sur **Redimensionner** pour continuer.

Resize Datastore | NFS_DS1


Volume Details

| | |
|-----------------------|---------|
| Volume Name: | NFS_DS1 |
| Total Size: | 2.1 TB |
| Used Size: | 968 KB |
| Snapshot Reserve (%): | 5 |
| Thin Provisioned: | Yes |

Size

| | |
|----------------------------|------|
| Current Datastore Size: | 2 TB |
| New Datastore Size (GB): * | 3000 |

3. Surveillez la progression du travail de redimensionnement dans le volet **tâches récentes**.

| Task Name | Target | Status | Details |
|------------------|---|--|---|
| Expand Datastore | vcenter-vlsr.sddc.net app.com | 100%  | Expand datastore initiated with job id 2807 |

Informations supplémentaires

Pour obtenir la liste complète des outils ONTAP pour les ressources VMware vSphere 10, reportez-vous à "[Ressources de documentation des outils ONTAP pour VMware vSphere](#)" la .

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP "[Documentation ONTAP 10](#)", reportez-vous au centre.

Utilisez VMware site Recovery Manager pour la reprise après incident des datastores NFS

L'utilisation des outils ONTAP pour VMware vSphere 10 et de site Replication adapter (SRA) conjointement avec VMware site Recovery Manager (SRM) apporte une valeur ajoutée considérable aux efforts de reprise après incident. Les outils ONTAP 10 fournissent des fonctionnalités de stockage fiables, notamment la haute disponibilité native et l'évolutivité pour le fournisseur VASA, prenant en charge les vVols iSCSI et NFS. Les données sont ainsi disponibles et la gestion des clusters ONTAP et des serveurs VMware vCenter est simplifiée. Grâce à SRA et VMware site Recovery

Manager, vous pouvez répliquer et basculer des machines virtuelles et des données entre des sites de manière fluide, ce qui permet des processus de reprise après incident efficaces. L'association des outils ONTAP et de SRA permet aux entreprises de protéger leurs workloads stratégiques, de minimiser les temps d'indisponibilité et de maintenir la continuité de l'activité en cas d'événements ou d'incidents imprévus.

Les outils ONTAP 10 simplifient la gestion du stockage et les fonctionnalités d'efficacité, améliorent la disponibilité, et réduisent les coûts de stockage et la surcharge opérationnelle, que vous utilisiez SAN ou NAS. Il s'appuie sur les bonnes pratiques pour le provisionnement des datastores et optimise les paramètres d'hôte ESXi pour les environnements de stockage NFS et bloc. Pour tous ces avantages, NetApp recommande ce plug-in lorsque vous utilisez vSphere avec les systèmes exécutant le logiciel ONTAP.

SRA est utilisée en association avec SRM pour gérer la réplication des données des machines virtuelles entre les sites de production et de reprise après incident pour les datastores VMFS et NFS traditionnels, et pour les tests non disruptives des répliques de DR. Il permet d'automatiser les tâches de détection, de restauration et de reprotection.

Dans ce scénario, nous montrerons comment déployer et utiliser VMware site Recovery Manager pour protéger les datastores et exécuter à la fois un test et un basculement final vers un site secondaire. Il est également question de la reprotection et de la restauration.

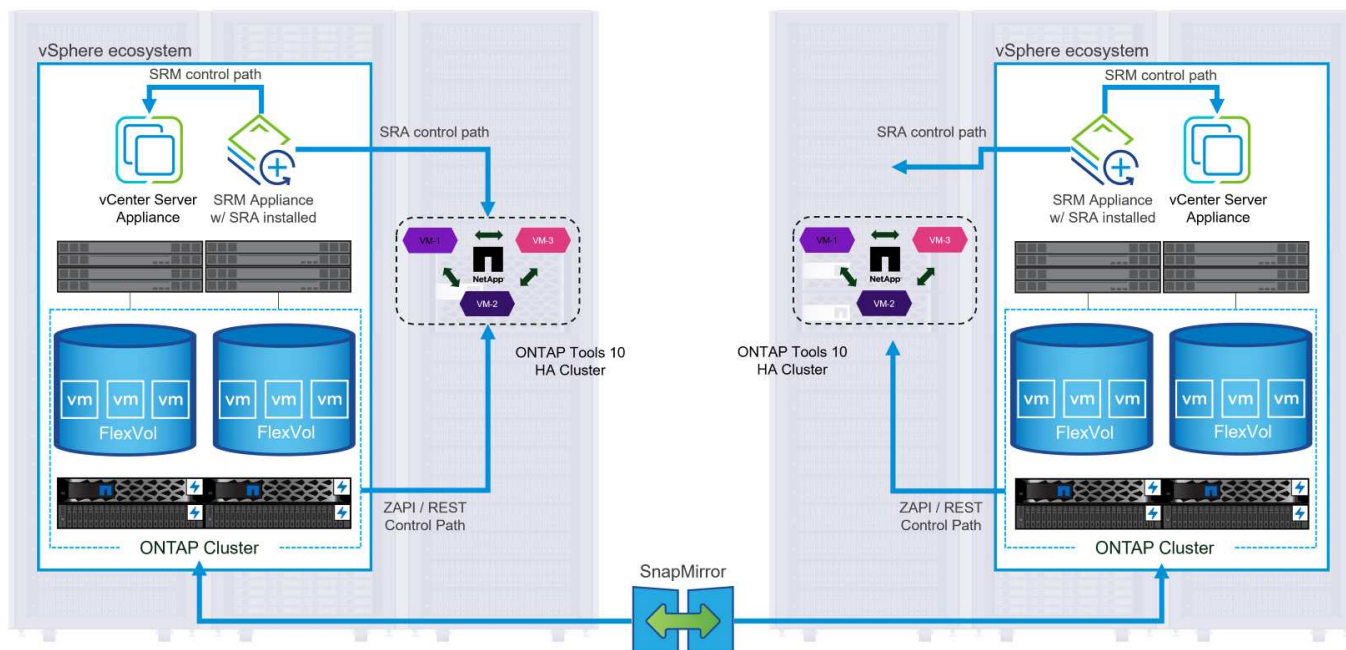
Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

- Configurer SRM avec les serveurs vCenter sur les sites principal et secondaire
- Installez l'adaptateur SRA pour les outils ONTAP pour VMware vSphere 10 et enregistrez-vous auprès de vCenters.
- Création de relations SnapMirror entre les systèmes de stockage ONTAP source et destination
- Configurer site Recovery pour SRM.
- Effectuer le test et le basculement final.
- Discutez de la reprotection et de la restauration.

Architecture

Le schéma suivant présente une architecture VMware site Recovery type avec les outils ONTAP pour VMware vSphere 10 configurés dans une configuration haute disponibilité à 3 nœuds.



Prérequis

Ce scénario nécessite les composants et configurations suivants :

- Clusters vSphere 8 installés sur les sites principal et secondaire avec une mise en réseau adaptée aux communications entre les environnements.
- Systèmes de stockage ONTAP sur les sites principal et secondaire, avec des ports de données physiques sur les switches ethernet dédiés au trafic de stockage NFS.
- Les outils ONTAP pour VMware vSphere 10 sont installés et les deux serveurs vCenter sont enregistrés.
- Les appliances VMware site Recovery Manager ont été installées pour les sites principal et secondaire.
 - Les mappages d'inventaire (réseau, dossier, ressource, stratégie de stockage) ont été configurés pour SRM.

NetApp recommande un réseau redondant pour NFS, offrant une tolérance aux pannes pour les systèmes de stockage, les switches, les adaptateurs réseau et les systèmes hôtes. Il est courant de déployer NFS avec un ou plusieurs sous-réseaux, selon les exigences architecturales.

Reportez-vous à la section ["Meilleures pratiques pour l'exécution de NFS avec VMware vSphere"](#) Pour obtenir des informations détaillées spécifiques à VMware vSphere.

Pour obtenir des conseils réseau sur l'utilisation de ONTAP avec VMware vSphere, reportez-vous au ["Configuration réseau - NFS"](#) De la documentation des applications d'entreprise NetApp.

Pour obtenir la documentation NetApp sur l'utilisation du stockage ONTAP avec VMware SRM, reportez-vous à la section ["VMware site Recovery Manager et ONTAP"](#)

Étapes de déploiement

Les sections suivantes présentent les étapes de déploiement à suivre pour implémenter et tester une configuration VMware site Recovery Manager avec un système de stockage ONTAP.

Création d'une relation SnapMirror entre les systèmes de stockage ONTAP

Pour que les volumes de datastore soient protégés, une relation SnapMirror doit être établie entre les systèmes de stockage ONTAP source et destination.

Pour plus d' ["ICI"](#) informations sur la création de relations SnapMirror pour les volumes ONTAP, consultez la documentation ONTAP à partir de.

Les instructions détaillées sont présentées dans le document suivant, situé à l'adresse ["ICI"](#). Cette procédure décrit comment créer des relations entre clusters et pairs de SVM, puis des relations SnapMirror pour chaque volume. Ces étapes peuvent être effectuées dans ONTAP System Manager ou via l'interface de ligne de commandes ONTAP.

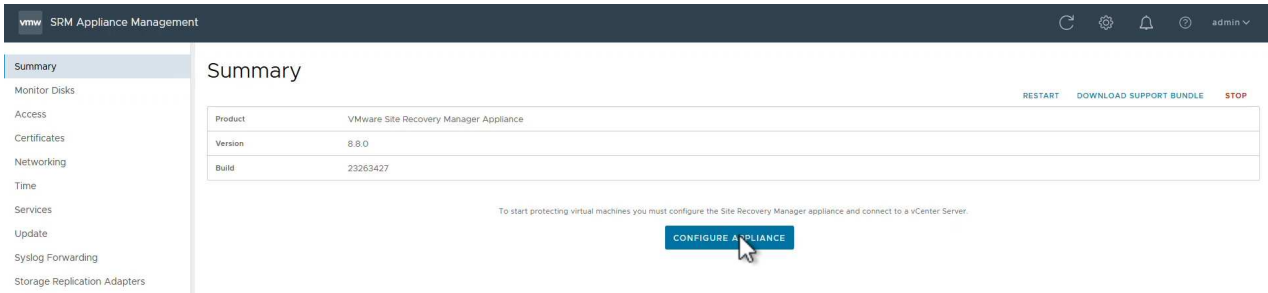
Configurez l'appliance SRM

Procédez comme suit pour configurer l'appliance SRM et l'adaptateur SRA.

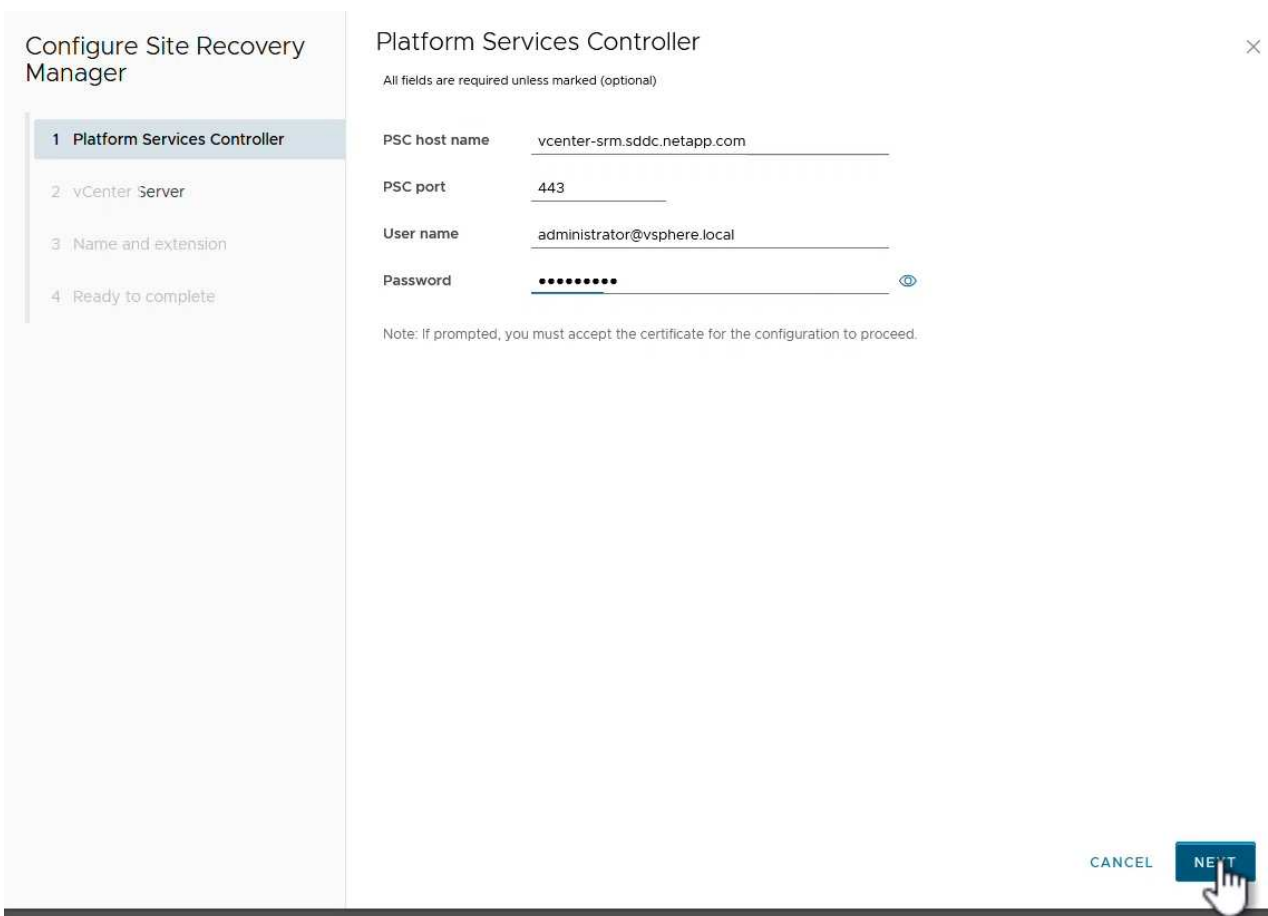
Connectez l'appliance SRM aux sites principaux et secondaires

Les étapes suivantes doivent être effectuées pour les sites principal et secondaire.

1. Dans un navigateur Web, accédez à https://<SRM_appliance_IP>:5480 et connectez-vous. Cliquez sur **configurer l'appareil** pour commencer.



2. Sur la page **Platform Services Controller** de l'assistant Configure site Recovery Manager, entrez les informations d'identification du serveur vCenter sur lequel SRM sera enregistré. Cliquez sur **Suivant** pour continuer.



3. Sur la page **vCenter Server**, affichez le vServer connecté et cliquez sur **Suivant** pour continuer.

4. Sur la page **Nom et extension**, saisissez un nom pour le site SRM, une adresse e-mail d'administrateur et l'hôte local à utiliser par SRM. Cliquez sur **Suivant** pour continuer.

Configure Site Recovery Manager

- 1 Platform Services Controller
- 2 vCenter Server
- 3 Name and extension**
- 4 Ready to complete

Name and extension ✕

All fields are required unless marked (optional)

Enter name and extension for Site Recovery Manager

Site name
A unique display name for this Site Recovery Manager site.

Administrator email
An email address to use for system notifications.

Local host ▼
The address on the local host to be used by Site Recovery Manager.

Extension ID

Default extension ID (com.vmware.vcDr)
 Custom extension ID

The default extension ID is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom extension ID for each SRM pair.

Extension ID

Organization

Description

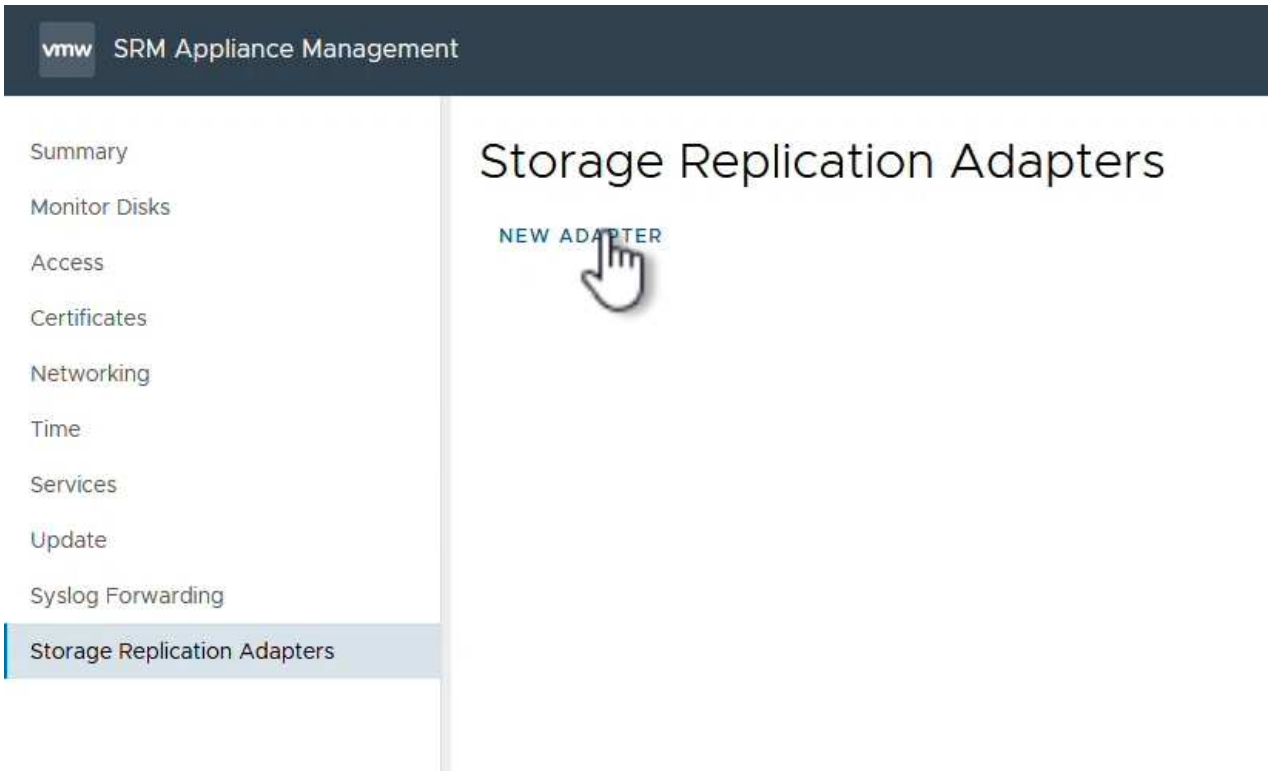
[CANCEL](#) [BACK](#) [NEXT](#)

5. Sur la page **prêt à terminer**, passez en revue le résumé des modifications

Configurez SRA sur l'appliance SRM

Pour configurer SRA sur l'appliance SRM, procédez comme suit :

1. Téléchargez SRA pour ONTAP Tools 10 sur le "[Site de support NetApp](#)" et enregistrez le fichier tar.gz dans un dossier local.
2. Dans l'appliance de gestion SRM, cliquez sur **Storage Replication Adapters** dans le menu de gauche, puis sur **New adapter**.



3. Suivez les étapes décrites sur le site de documentation des outils ONTAP 10 à l'adresse "[Configurez SRA sur l'appliance SRM](#)". Une fois l'opération terminée, SRA peut communiquer avec SRA à l'aide de l'adresse IP et des informations d'identification fournies par le serveur vCenter.

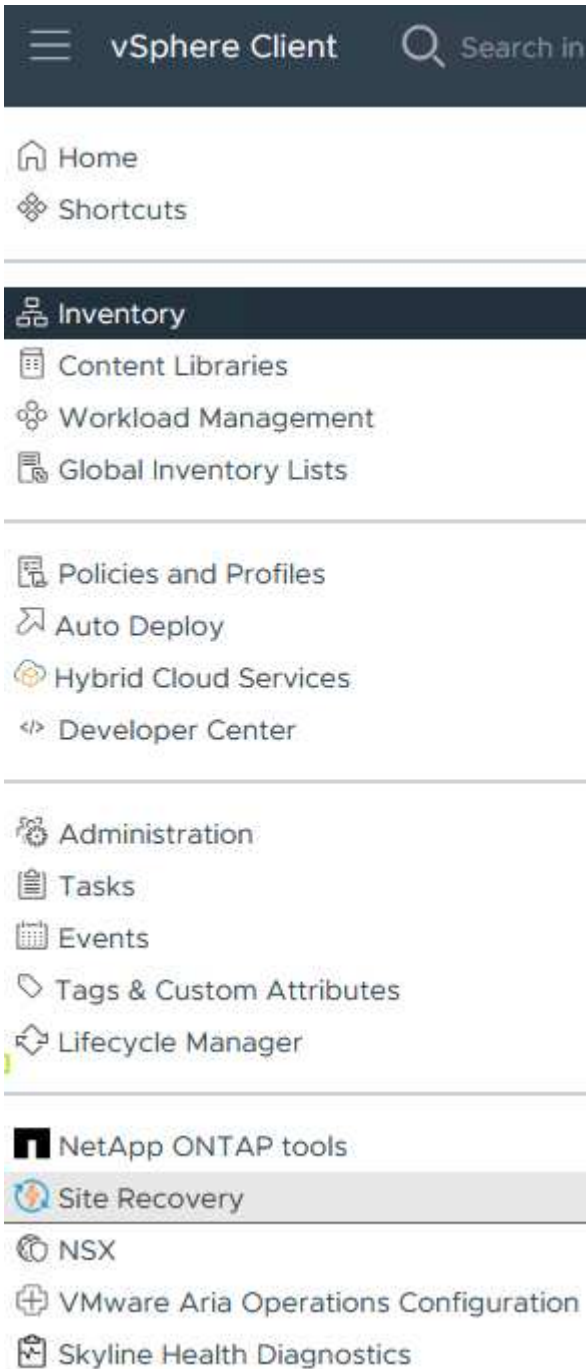
Configurer site Recovery pour SRM

Procédez comme suit pour configurer le couplage de site, créer des groupes de protection,

Configurer le couplage de site pour SRM

L'étape suivante s'effectue dans le client vCenter du site principal.

1. Dans le client vSphere, cliquez sur **site Recovery** dans le menu de gauche. Une nouvelle fenêtre de navigateur s'ouvre dans l'interface utilisateur de gestion SRM sur le site principal.



2. Sur la page **site Recovery**, cliquez sur **NOUVEAU SITE PAIR**.

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

[NEW SITE PAIR](#)[Learn More](#)

3. Sur la page **Type de paire** de l'assistant **Nouvelle paire**, vérifiez que le serveur vCenter local est sélectionné et sélectionnez **Type de paire**. Cliquez sur **Suivant** pour continuer.

The screenshot shows the 'New Pair' wizard in the Site Recovery Manager interface. The left sidebar contains a navigation pane with four steps: 1. Pair type (selected), 2. Peer vCenter Server, 3. Services, and 4. Ready to complete. The main content area is titled 'Pair type' and includes a close button (X). Below the title, it says 'Select a local vCenter Server.' and displays a dropdown menu with one option: 'vcenter-vlsr.sddc.netapp.com'. Underneath, there are two radio button options for 'Pair type': 'Pair with a peer vCenter Server located in a different SSO domain' (which is selected) and 'Pair with a peer vCenter Server located in the same SSO domain'. At the bottom right, there are 'CANCEL' and 'NEXT' buttons, with a mouse cursor clicking on the 'NEXT' button.

4. Sur la page **Peer vCenter**, remplissez les informations d'identification du vCenter sur le site secondaire et cliquez sur **Find vCenter instances**. Vérifiez que l'instance vCenter a été découverte et cliquez sur **Suivant** pour continuer.

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

Peer vCenter Server



All fields are required unless marked (optional)

Enter the Platform Services Controller details for the peer vCenter Server.

PSC host name
PSC port
User name
Password

FIND VCENTER SERVER INSTANCES

Select a vCenter Server you want to pair.

vCenter Server

- vcenter-srm.sddc.netapp.com

CANCEL

BACK

NEXT

5. Sur la page **Services**, cochez la case en regard du couplage de site proposé. Cliquez sur **Suivant** pour continuer.

New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

Services

The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

| Service | vcenter-vlsr.sddc.netapp.com | vcenter-srm.sddc.netapp.com |
|---|------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> Site Recovery Manager (com.vmware.vc... | Site 1 | Site 2 |

CANCEL

BACK

NEXT

6. Sur la page **prêt à terminer**, passez en revue la configuration proposée, puis cliquez sur le bouton **Terminer** pour créer le couplage de site
7. La nouvelle paire de sites et son résumé peuvent être affichés sur la page Résumé.

Summary

RECONNECT

BREAK SITE PAIR



vCenter Server: [vcenter-vlsr.sddc.netapp.com](#) [vcenter-srm.sddc.netapp.com](#)
vCenter Version: 8.0.2, 22385739 8.0.2, 22385739
vCenter Host Name: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443
Platform Services Controller: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443

Site Recovery Manager

EXPORT/IMPORT SRM CONFIGURATION

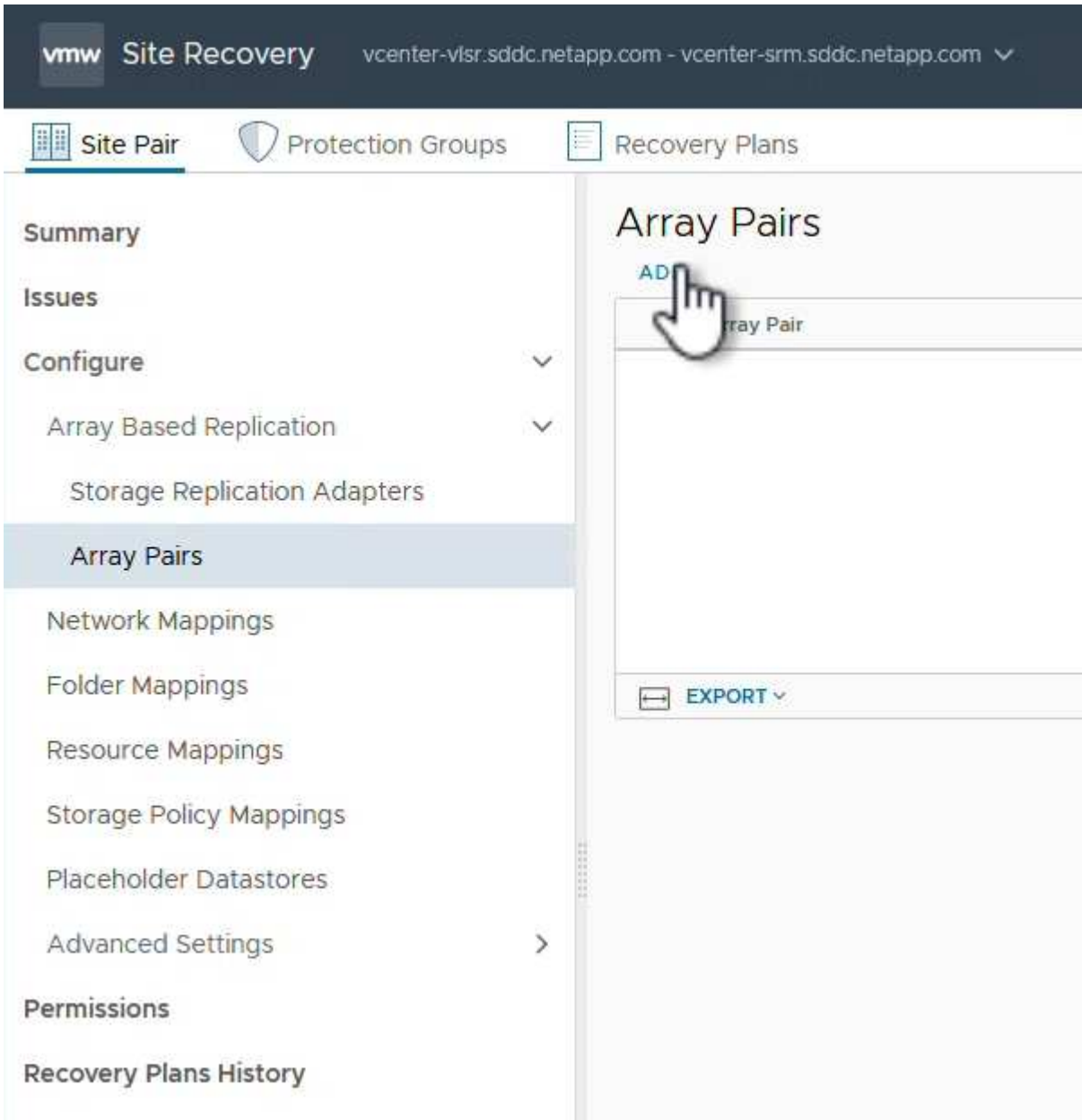
Protection Groups:0 Recovery Plans:0

| Name | Site 1 RENAME | Site 2 RENAME |
|-----------------------|---|---|
| Server | srm-site1.sddc.netapp.com:443 ACTIONS | srm-site2.sddc.netapp.com:443 ACTIONS |
| Version | 8.8.0, 23263429 | 8.8.0, 23263429 |
| ID | com.vmware.vcDr | com.vmware.vcDr |
| Logged in as | VSPHERE.LOCAL\Administrator | VSPHERE.LOCAL\Administrator |
| Remote SRM connection | ✓ Connected | ✓ Connected |

Ajoutez une paire de matrices pour SRM

L'étape suivante est effectuée dans l'interface de récupération de site du site principal.

1. Dans l'interface site Recovery, accédez à **Configure > Array Based Replication > Array pairs** dans le menu de gauche. Cliquez sur **AJOUTER** pour commencer.



2. Sur la page **Storage Replication adapter** de l'assistant **Add Array pair**, vérifiez que l'adaptateur SRA est présent pour le site principal et cliquez sur **Next** pour continuer.

Add Array Pair

1 Storage replication adapter

2 Local array manager

3 Remote array manager

4 Array pairs

5 Ready to complete

Storage replication adapter

Select a storage replication adapter (SRA):

| | Storage Replication Adapter | Status | Vendor | Version | Stretched Storage |
|---|-----------------------------------|--------|--------|---------|-------------------|
| > | NetApp Storage Replication Ada... | ✓ OK | NetApp | 10.1 | Not Support... |

Items per page: AUTO 1 items

CANCEL

NEXT

3. Sur la page **local array Manager**, entrez le nom de la baie sur le site principal, le nom de domaine complet du système de stockage, les adresses IP du SVM servant NFS et éventuellement les noms de volumes spécifiques à découvrir. Cliquez sur **Suivant** pour continuer.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcenter-vlsr.sddc.netapp.com":

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname
Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses
Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name
Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list
Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list
Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

4. Sur le **Remote array Manager**, remplissez les mêmes informations que la dernière étape pour le système de stockage ONTAP sur le site secondaire.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Remote array manager

Do not create a remote array manager now.

Enter a name for the array manager on "vcenter-srm.sddc.netapp.com":

Array_2

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname ontap-destination.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses 172.21.118.51

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name SRM_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list |

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list |

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT

5. Sur la page **paires de matrices**, sélectionnez les paires de matrices à activer et cliquez sur **Suivant** pour continuer.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs**
- 5 Ready to complete

Array pairs

Select the array pairs to enable:

| <input checked="" type="checkbox"/> | vcenter-vlsr.sddc.netapp.com | vcenter-srm.sddc.netapp.com | Status |
|-------------------------------------|--------------------------------|-------------------------------------|---------------------|
| <input checked="" type="checkbox"/> | ontap-source:SQL_NFS (Array_1) | ontap-destination:SRM_NFS (Array_2) | Ready to be enabled |

1 1 items

CANCEL

BACK

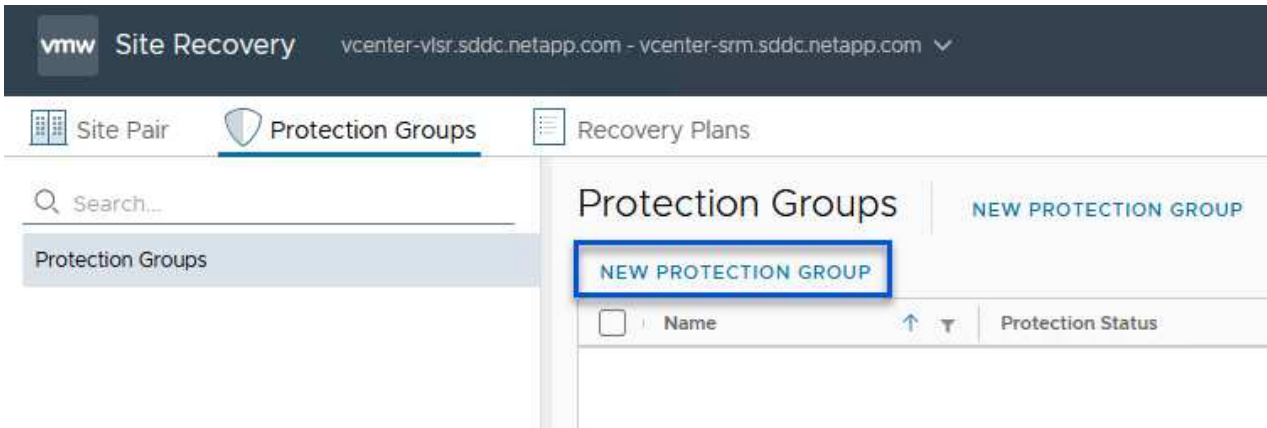
NEXT

6. Consultez les informations de la page **prêt à terminer** et cliquez sur **Terminer** pour créer la paire de matrices.

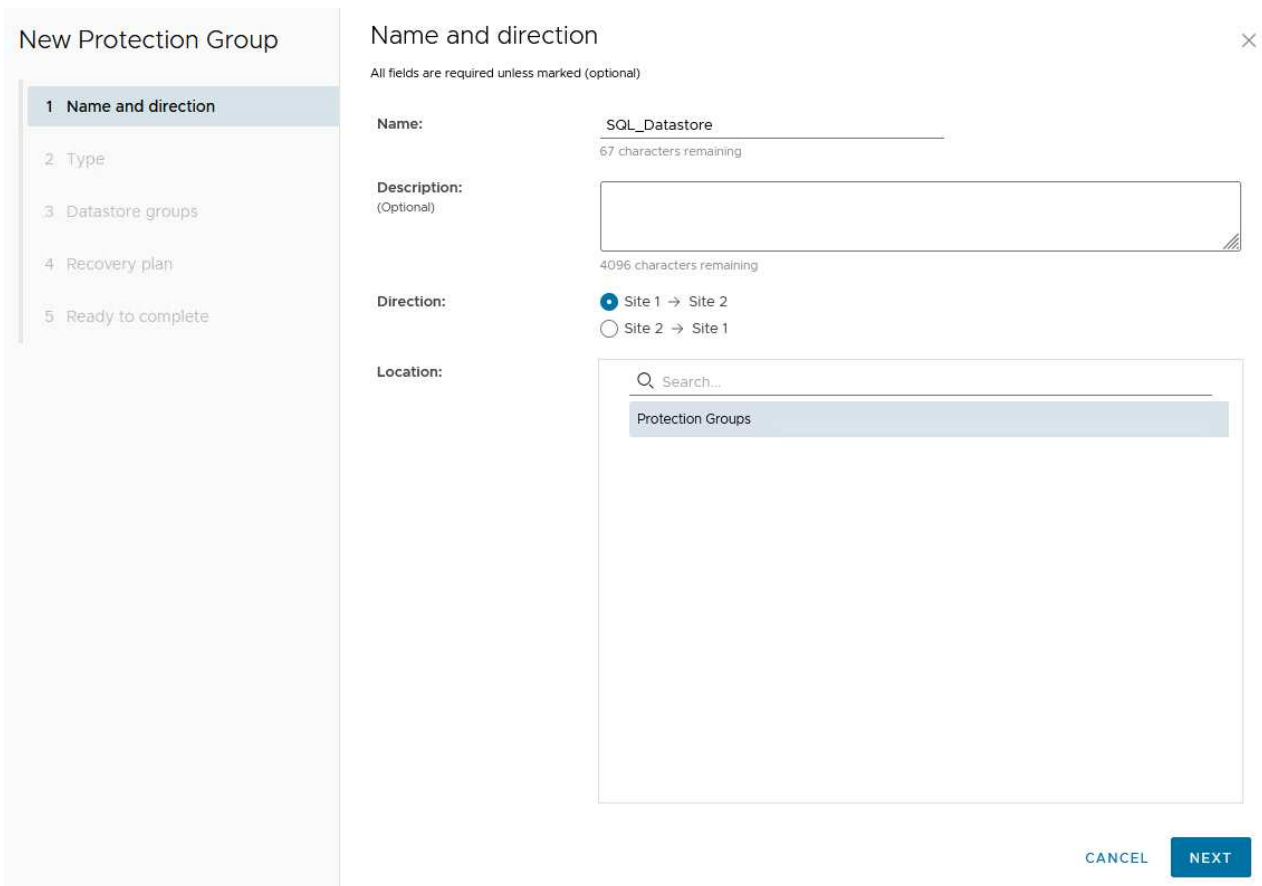
Configurer les groupes de protection pour SRM

L'étape suivante est effectuée dans l'interface de récupération de site du site principal.

1. Dans l'interface site Recovery, cliquez sur l'onglet **groupes de protection**, puis sur **Nouveau groupe de protection** pour commencer.



2. Sur la page **Nom et direction** de l'assistant **Nouveau groupe de protection**, indiquez un nom pour le groupe et choisissez la direction du site pour la protection des données.

The screenshot shows the 'New Protection Group' wizard. On the left, there's a sidebar with five steps: '1 Name and direction', '2 Type', '3 Datastore groups', '4 Recovery plan', and '5 Ready to complete'. The 'Name and direction' step is selected. The main area is titled 'Name and direction' and has a close button (X). Below the title, it says 'All fields are required unless marked (optional)'. There are four fields: 'Name' with the value 'SQL_Datastore' and '67 characters remaining'; 'Description' (Optional) with a text area and '4096 characters remaining'; 'Direction' with two radio buttons: 'Site 1 -> Site 2' (selected) and 'Site 2 -> Site 1'; and 'Location' with a search bar and a dropdown menu showing 'Protection Groups'. At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

3. Sur la page **Type**, sélectionnez le type de groupe de protection (datastore, VM ou vVol) et sélectionnez la paire de baies. Cliquez sur **Suivant** pour continuer.

New Protection Group

- 1 Name and direction
- 2 Type**
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Type

Select the type of protection group you want to create:

- Datastore groups (array-based replication)**
Protect all virtual machines which are on specific datastores.
- Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.
- Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

Select array pair

| Array Pair | Array Manager Pair |
|---|-------------------------|
| <input checked="" type="radio"/> <input checked="" type="checkbox"/> ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 | nfs_array1 ↔ nfs_Array2 |
| <input type="radio"/> <input checked="" type="checkbox"/> ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS | Array_1 ↔ Array_2 |

Items per page: AUTO 2 array pairs

[CANCEL](#) [BACK](#) [NEXT](#)

4. Sur la page **datastore Groups**, sélectionnez les datastores à inclure dans le groupe de protection. Les machines virtuelles qui résident actuellement sur le datastore s'affichent pour chaque datastore sélectionné. Cliquez sur **Suivant** pour continuer.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together.

[SELECT ALL](#) [CLEAR SELECTION](#)

| <input checked="" type="checkbox"/> | Datastore Group | Status |
|-------------------------------------|-----------------|------------------------------|
| <input checked="" type="checkbox"/> | NFS_DS1 | Add to this protection group |

1 Items per page: [AUTO](#) 1 datastore groups

The following virtual machines are in the selected datastore groups:

| Virtual Machine | Datastore | Status |
|-----------------|-----------|------------------------------|
| SQLSRV-01 | NFS_DS1 | Add to this protection group |
| SQLSRV-03 | NFS_DS1 | Add to this protection group |
| SQLSRV-02 | NFS_DS1 | Add to this protection group |

[CANCEL](#)

[BACK](#)

[NEXT](#)

5. Sur la page **Plan de récupération**, vous pouvez éventuellement ajouter le groupe de protection à un plan de récupération. Dans ce cas, le plan de récupération n'est pas encore créé, donc **ne pas ajouter au plan de récupération** est sélectionné. Cliquez sur **Suivant** pour continuer.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan**
- 5 Ready to complete

Recovery plan



You can optionally add this protection group to a recovery plan.

- Add to existing recovery plan
- Add to new recovery plan
- Do not add to recovery plan now

 The protection group cannot be recovered unless it is added to a recovery plan.

CANCEL

BACK

NEXT

6. Sur la page **prêt à terminer**, passez en revue les nouveaux paramètres du groupe de protection et cliquez sur **Terminer** pour créer le groupe.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete**

Ready to complete



Review your selected settings.

| | |
|-------------------------------|--|
| Name | SQL_Datastore |
| Description | |
| Protected site | Site 1 |
| Recovery site | Site 2 |
| Location | Protection Groups |
| Protection group type | Datastore groups (array-based replication) |
| Array pair | ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_array2) |
| Datastore groups | NFS_DS1 |
| Total virtual machines | 3 |
| Recovery plan | none |

CANCEL

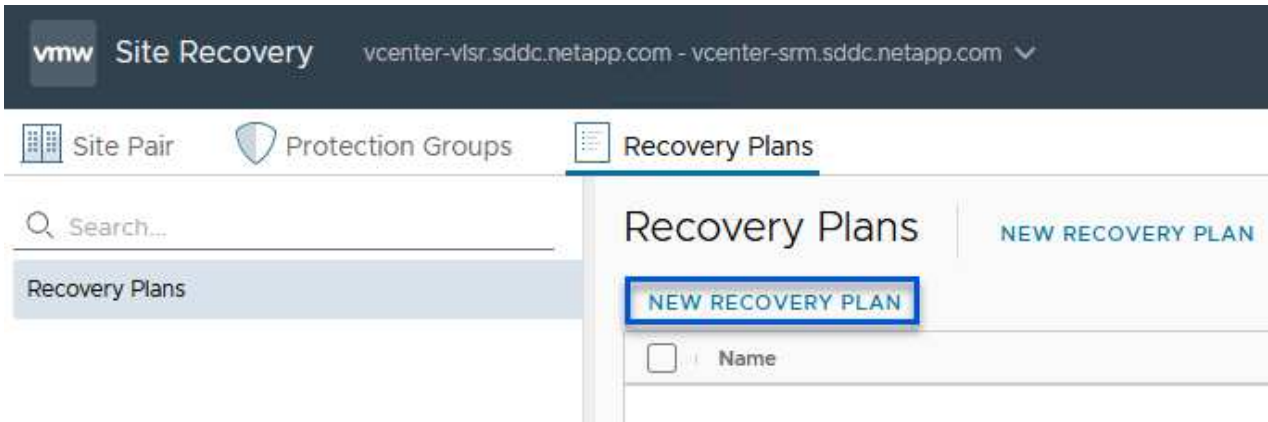
BACK

FINISH

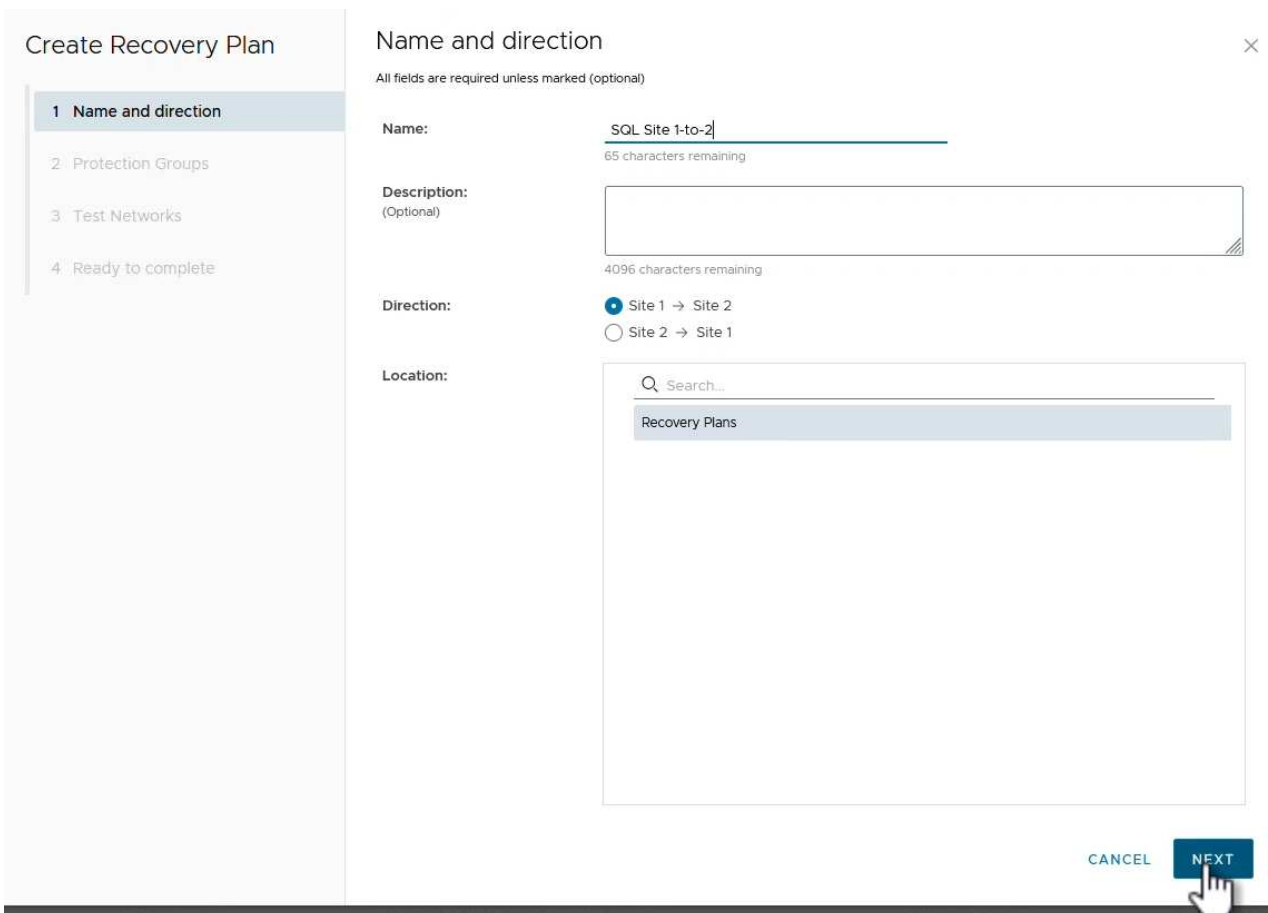
Configurer le plan de reprise pour SRM

L'étape suivante est effectuée dans l'interface de récupération de site du site principal.

1. Dans l'interface de récupération de site, cliquez sur l'onglet **Plan de récupération**, puis sur **Nouveau Plan de récupération** pour commencer.



2. Sur la page **Nom et direction** de l'assistant **Créer un plan de récupération**, indiquez un nom pour le plan de récupération et choisissez la direction entre les sites source et de destination. Cliquez sur **Suivant** pour continuer.



3. Sur la page **groupes de protection**, sélectionnez les groupes de protection précédemment créés à inclure dans le plan de reprise. Cliquez sur **Suivant** pour continuer.

The screenshot shows the 'Create Recovery Plan' wizard in step 2, 'Protection Groups'. The wizard is titled 'Create Recovery Plan' and has four steps: 1. Name and direction, 2. Protection Groups (current), 3. Test Networks, and 4. Ready to complete. The 'Protection Groups' window shows a table with columns 'Name' and 'Description'. One group, 'SQL_Datastore', is selected. At the bottom right, there are buttons for 'CANCEL', 'BACK', and 'NEXT', with a mouse cursor clicking on 'NEXT'.

4. Sur les **réseaux de test**, configurez des réseaux spécifiques qui seront utilisés pendant le test du plan. Si aucun mappage n'existe ou si aucun réseau n'est sélectionné, un réseau de test isolé est créé. Cliquez sur **Suivant** pour continuer.

Create Recovery Plan

- 1 Name and direction
- 2 Protection Groups
- 3 Test Networks
- 4 Ready to complete

Test Networks

Select the networks to use while running tests of this plan.

i If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

| Recovery Network | ↑ ↓ | Test Network | |
|---------------------------|-----|------------------------|--------------------------|
| Datacenter > DPortGroup | ☰ | Use site-level mapping | CHANGE |
| Datacenter > Mgmt 3376 | ☰ | Mgmt 3376 | ☰ CHANGE |
| Datacenter > NFS 3374 | ☰ | NFS 3374 | ☰ CHANGE |
| Datacenter > VLAN 181 | ☰ | Use site-level mapping | CHANGE |
| Datacenter > VM Network | ☰ | Use site-level mapping | CHANGE |
| Datacenter > vMotion 3373 | ☰ | Use site-level mapping | CHANGE |
| Datacenter > vSAN 3422 | ☰ | Use site-level mapping | CHANGE |

7 network(s)

CANCEL
BACK
NEXT

5. Sur la page **prêt à terminer**, passez en revue les paramètres choisis, puis cliquez sur **Terminer** pour créer le plan de récupération.

Opérations de reprise après incident avec SRM

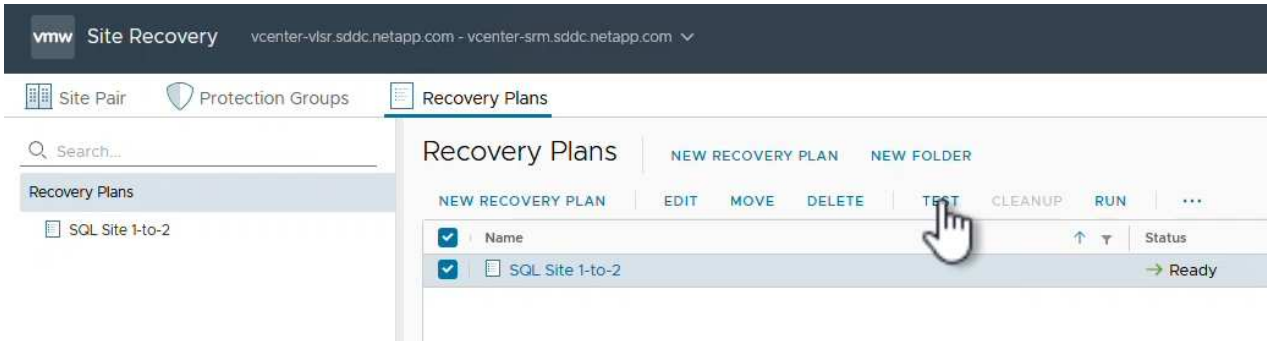
Cette section traite des différentes fonctions d'utilisation de la reprise sur incident avec SRM, notamment le test du basculement, l'exécution du basculement, la reprotection et la restauration.

Pour "[Meilleures pratiques opérationnelles](#)" plus d'informations sur l'utilisation du stockage ONTAP avec les opérations de reprise après incident SRM, reportez-vous à la section.

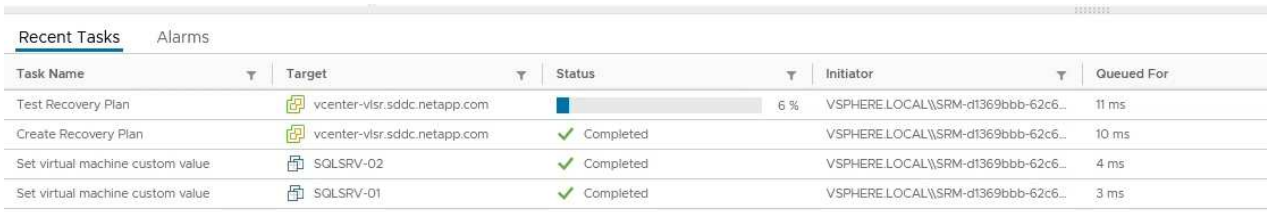
Test du basculement avec SRM

L'étape suivante est effectuée dans l'interface site Recovery.

1. Dans l'interface de récupération de site, cliquez sur l'onglet **Plan de récupération**, puis sélectionnez un plan de récupération. Cliquez sur le bouton **Test** pour commencer le test du basculement vers le site secondaire.



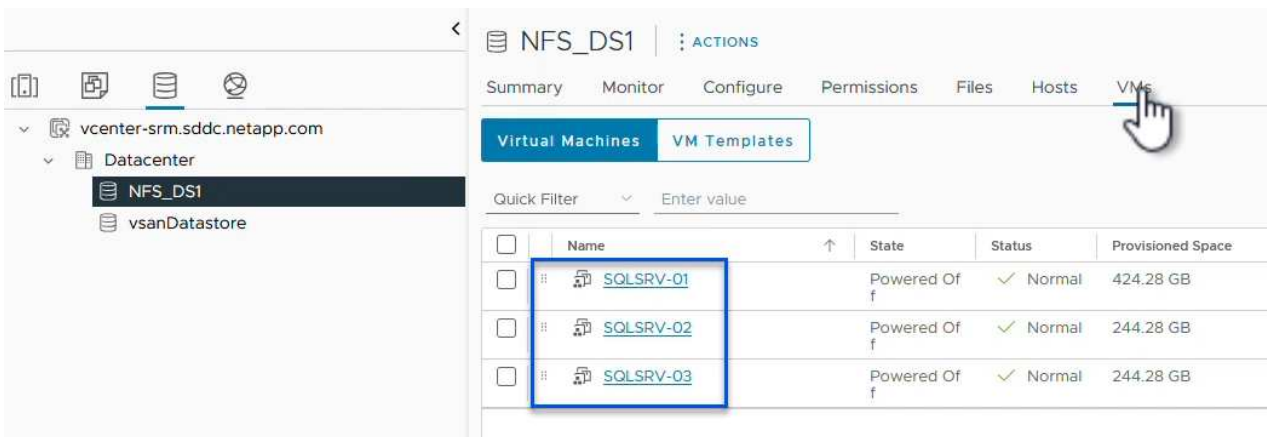
2. Vous pouvez afficher la progression du test à partir du volet des tâches site Recovery ainsi que du volet des tâches vCenter.



The screenshot shows the 'Recent Tasks' section. A table lists tasks with their status and progress. The 'Test Recovery Plan' task is highlighted, showing a progress bar at 6%.

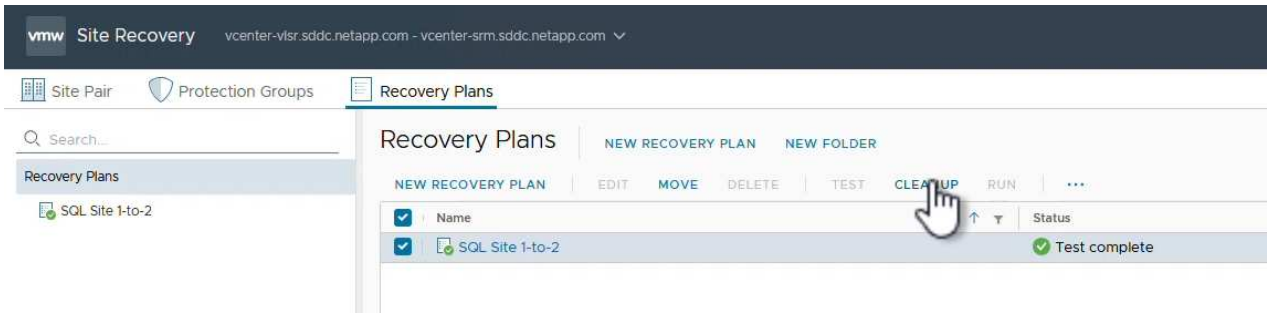
| Task Name | Target | Status | Initiator | Queued For |
|----------------------------------|------------------------------|-------------|------------------------------------|------------|
| Test Recovery Plan | vcenter-vlsr.sddc.netapp.com | 6 % | VSPHERE.LOCAL\SRM-d1369bbb-62c6... | 11 ms |
| Create Recovery Plan | vcenter-vlsr.sddc.netapp.com | ✓ Completed | VSPHERE.LOCAL\SRM-d1369bbb-62c6... | 10 ms |
| Set virtual machine custom value | SQLSRV-02 | ✓ Completed | VSPHERE.LOCAL\SRM-d1369bbb-62c6... | 4 ms |
| Set virtual machine custom value | SQLSRV-01 | ✓ Completed | VSPHERE.LOCAL\SRM-d1369bbb-62c6... | 3 ms |

3. SRM envoie les commandes via SRA au système de stockage ONTAP secondaire. Une FlexClone du snapshot le plus récent est créée et montée sur le cluster vSphere secondaire. Le nouveau datastore monté peut être consulté dans l'inventaire du stockage.



4. Une fois le test terminé, cliquez sur **Cleanup** pour démonter le datastore et revenir à l'environnement

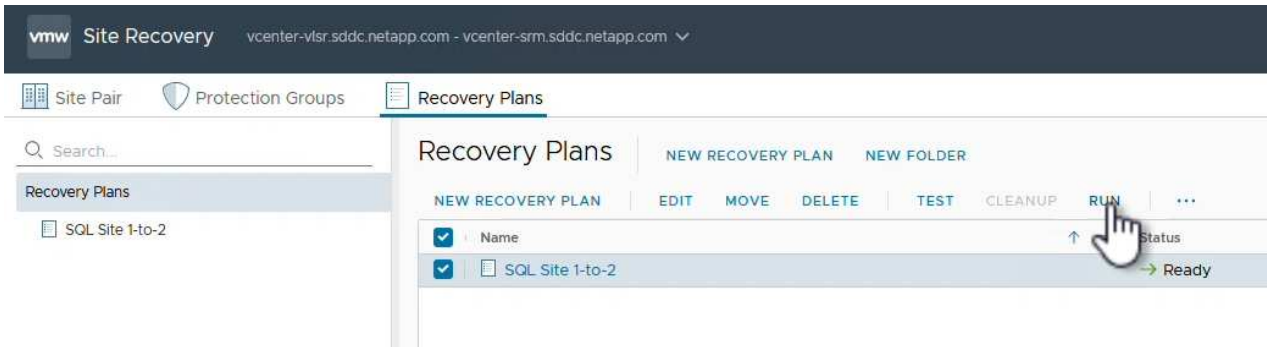
d'origine.



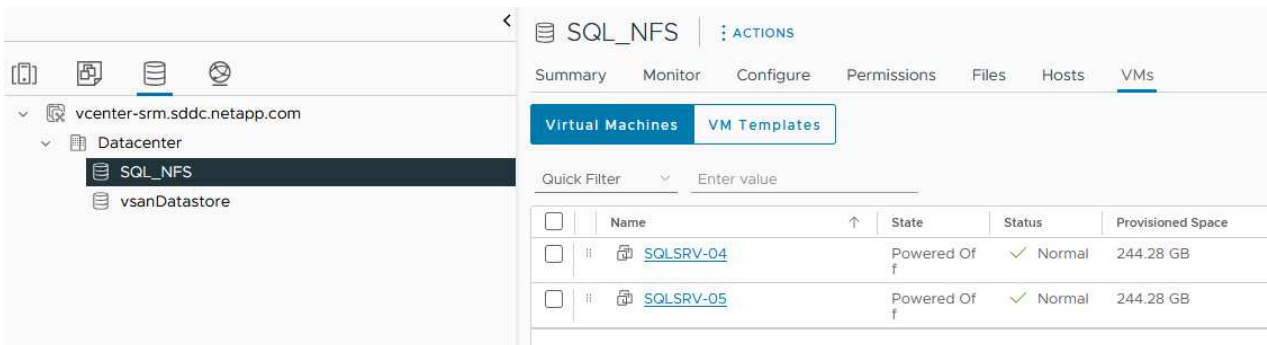
Exécuter un plan de reprise avec SRM

Effectuez une restauration complète et un basculement vers le site secondaire.

1. Dans l'interface de récupération de site, cliquez sur l'onglet **Plan de récupération**, puis sélectionnez un plan de récupération. Cliquez sur le bouton **Exécuter** pour commencer le basculement vers le site secondaire.



2. Une fois le basculement terminé, vous pouvez voir le datastore monté et les machines virtuelles enregistrées sur le site secondaire.



Des fonctions supplémentaires sont disponibles dans SRM une fois le basculement terminé.

Reprotection : une fois le processus de récupération terminé, le site de récupération précédemment désigné assume le rôle du nouveau site de production. Cependant, il est important de noter que la réplication SnapMirror est interrompue pendant l'opération de reprise, ce qui expose le nouveau site de production à des

incidents futurs. Pour assurer une protection continue, il est recommandé d'établir une nouvelle protection pour le nouveau site de production en le répliquant sur un autre site. Lorsque le site de production d'origine reste opérationnel, l'administrateur VMware peut le réutiliser en tant que nouveau site de reprise, inversant ainsi le sens de la protection. Il est essentiel de souligner que la reprotection n'est possible qu'en cas de défaillance non catastrophique, ce qui nécessite la restauration éventuelle des serveurs vCenter d'origine, des serveurs ESXi, des serveurs SRM et de leurs bases de données respectives. Si ces composants ne sont pas disponibles, la création d'un nouveau groupe de protection et d'un nouveau plan de reprise devient nécessaire.

Retour arrière : une opération de retour arrière est un basculement arrière, qui renvoie les opérations au site d'origine. Il est essentiel de s'assurer que le site d'origine a retrouvé ses fonctionnalités avant de lancer le processus de restauration. Pour garantir un retour arrière fluide, il est recommandé d'effectuer un basculement de test après avoir terminé le processus de reprotection et avant d'exécuter le retour arrière final. Cette pratique sert d'étape de vérification, confirmant que les systèmes du site d'origine sont entièrement capables de gérer l'opération. En suivant cette approche, vous pouvez minimiser les risques et assurer une transition plus fiable vers l'environnement de production d'origine.

Informations supplémentaires

Pour obtenir la documentation NetApp sur l'utilisation du stockage ONTAP avec VMware SRM, reportez-vous à la section "[VMware site Recovery Manager et ONTAP](#)"

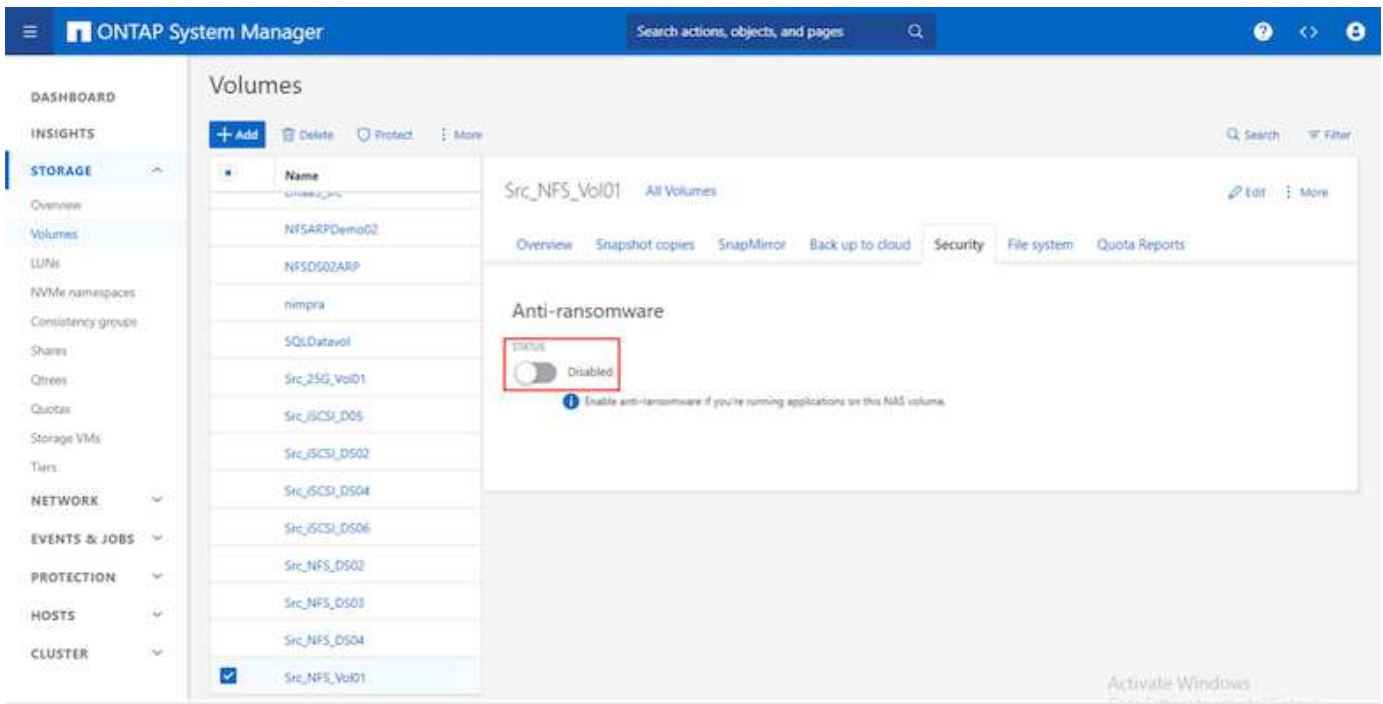
Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au "[Documentation ONTAP 9](#)" centre.

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section "[Documentation de VMware Cloud Foundation](#)".

Protection anti-ransomware autonome pour le stockage NFS

Il est essentiel de détecter les ransomware dès que possible pour prévenir la propagation de ces attaques et éviter les temps d'indisponibilité coûteux. Une stratégie de détection des ransomwares efficace doit intégrer plusieurs couches de protection au niveau des machines virtuelles hôtes et hôtes ESXi. Même si plusieurs mesures de sécurité sont implémentées pour créer une défense complète contre les attaques par ransomware, ONTAP permet d'ajouter des couches de protection supplémentaires à l'approche de la défense globale. Pour n'en citer que quelques-unes, l'opération commence par les snapshots, la protection anti-ransomware autonome, les snapshots inviolables, etc.

Voyons comment les fonctionnalités mentionnées ci-dessus fonctionnent avec VMware pour protéger et restaurer les données contre les ransomwares. Pour protéger vSphere et les ordinateurs virtuels invités contre les attaques, il est essentiel de prendre plusieurs mesures, notamment la segmentation, l'utilisation d'EDR/XDR/SIEM pour les terminaux, l'installation de mises à jour de sécurité et le respect des directives de renforcement appropriées. Chaque machine virtuelle résidant sur un datastore héberge également un système d'exploitation standard. Assurez-vous que des suites de produits contre les programmes malveillants sont installées sur vos serveurs d'entreprise et régulièrement mises à jour, ce qui constitue un composant essentiel de la stratégie de protection multicouche contre les ransomwares. Par ailleurs, activez la protection anti-ransomware autonome (ARP) sur le volume NFS qui alimente le datastore. ARP exploite le ML intégré DE LA MACHINE à ML qui analyse l'activité des workloads de volume et l'entropie des données pour détecter automatiquement les ransomware. Le protocole ARP est configurable via l'interface de gestion intégrée ONTAP ou le gestionnaire système. Il est activé par volume.

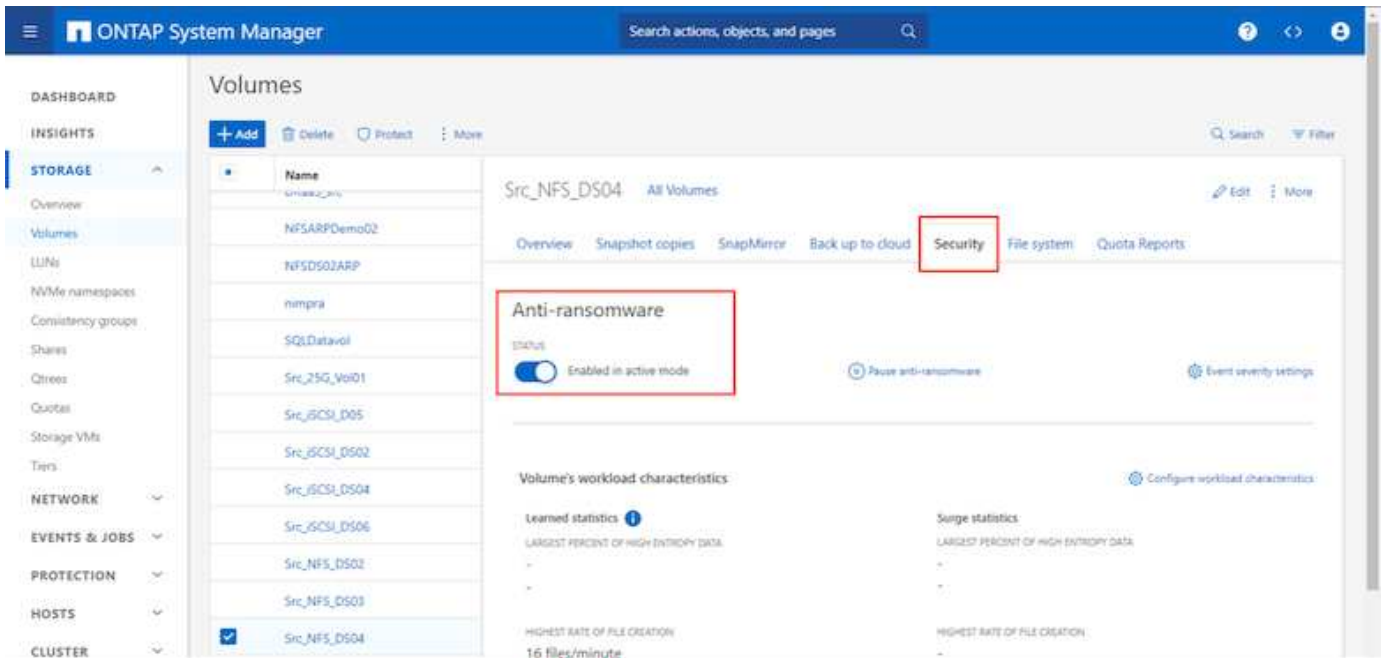


Avec le nouveau NetApp ARP/ai, actuellement en préversion technique, il n'est pas nécessaire de disposer d'un mode d'apprentissage. Il peut plutôt passer directement en mode actif grâce à sa fonctionnalité de détection des ransomwares optimisée par l'IA.



Avec ONTAP One, tous ces ensembles de fonctionnalités sont entièrement gratuits. Accédez à la suite robuste NetApp de protection des données, de sécurité et à toutes les fonctionnalités d'ONTAP sans vous soucier des obstacles liés aux licences.

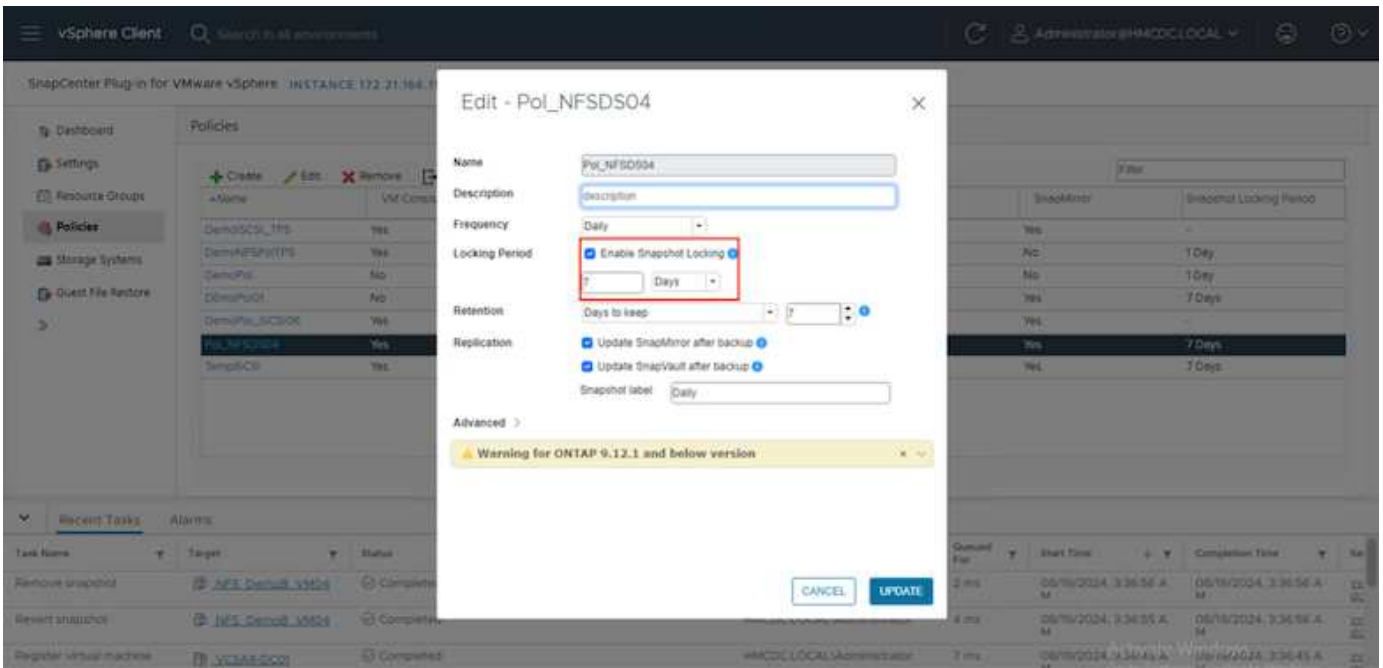
Une fois en mode actif, il commence à rechercher l'activité de volume anormale qui pourrait être une attaque par ransomware. En cas d'activité anormale, une copie Snapshot automatique est immédiatement effectuée, ce qui fournit un point de restauration aussi proche que possible de l'infection par le fichier. ARP peut détecter les modifications des extensions de fichiers spécifiques à la machine virtuelle sur un volume NFS situé en dehors de la machine virtuelle lorsqu'une nouvelle extension est ajoutée au volume chiffré ou qu'une extension de fichier est modifiée.



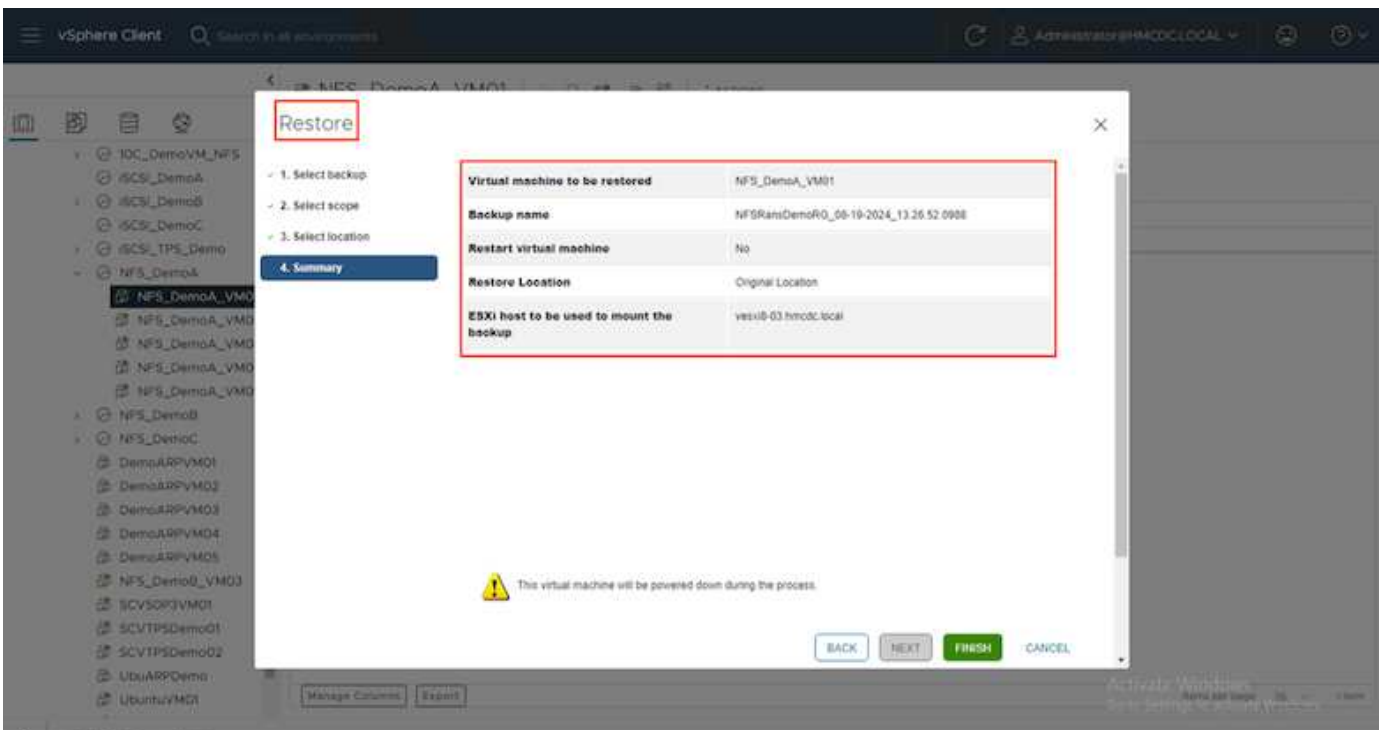
Si une attaque par ransomware cible la machine virtuelle et altère les fichiers au sein de la machine virtuelle sans effectuer de modifications hors de la machine virtuelle, la protection avancée contre les ransomware (ARP) continue de détecter la menace si l'entropie par défaut de la machine virtuelle est faible, par exemple pour des fichiers de type .txt, .docx ou .mp4. Même si ARP crée un snapshot de protection dans ce scénario, il ne génère pas d'alerte de menace car les extensions de fichier en dehors de la machine virtuelle n'ont pas été falsifiées. Dans de tels scénarios, les couches de défense initiales identifieraient l'anomalie, mais ARP aide à créer un instantané basé sur l'entropie.

Pour plus d'informations, reportez-vous à la section "ARP et machines virtuelles" dans ["ARP usecas et considérations"](#).

En passant des fichiers aux données de sauvegarde, les attaques par ransomware ciblent de plus en plus les sauvegardes et les points de restauration Snapshot en essayant de les supprimer avant de commencer à chiffrer des fichiers. Cependant, avec ONTAP, cela peut être empêché en créant des snapshots inviolables sur les systèmes primaires ou secondaires avec ["Verrouillage des copies NetApp Snapshot™"](#).



Ces copies Snapshot ne peuvent pas être supprimées ou modifiées par des attaquants de ransomware ou des administrateurs peu scrupuleux, et elles sont disponibles même après une attaque. Si le datastore ou des machines virtuelles spécifiques sont affectés, SnapCenter peut restaurer les données des serveurs virtuels en quelques secondes, ce qui réduit au minimum le temps d'indisponibilité de l'entreprise.



La démonstration ci-dessus montre comment le stockage ONTAP ajoute une couche supplémentaire aux techniques existantes pour améliorer la pérennisation de l'environnement.

Pour plus d'informations, consultez le guide pour ["Solutions NetApp pour ransomware"](#).

Si toutes ces questions doivent être orchestrées et intégrées avec des outils SIEM, il est possible d'utiliser le service OFFTAP tel que la protection contre les ransomware BlueXP . Il s'agit d'un service conçu pour protéger

les données contre les ransomwares. Ce service protège les charges de travail basées sur les applications, comme Oracle, MySQL, les datastores de machines virtuelles et les partages de fichiers sur un stockage NFS sur site.

Dans cet exemple, le datastore NFS « SRC_NFS_DS04 » est protégé grâce à la protection contre les ransomwares de BlueXP .

| Workload | Type | Connector | Importance | Protection st... | Detection sta... | Detection pol... | Snapshot an... | Backup destina... | |
|---------------------|---------------|-------------|------------|------------------|------------------|--------------------|-----------------------|----------------------|-----------------|
| Src_nfs_ds02 | VM datastore | GISABXPConn | Critical | Protected | Learning mode | rps-policy-primary | SnapCenter for VMw... | netapp-backup-add... | Edit protection |
| Draas_src_test_3130 | VM file share | GISABXPConn | Standard | At risk | None | None | None | n/a | Protect |
| Nfsds02zrp_804 | VM file share | GISABXPConn | Standard | Protected | Active | rps-policy-primary | None | netapp-backup-add... | Edit protection |
| Draas_src_7027 | VM file share | GISABXPConn | Standard | At risk | None | None | None | netapp-backup-add... | Protect |
| Src_nfs_vol01_7948 | VM file share | GISABXPConn | Standard | At risk | None | None | None | netapp-backup-add... | Protect |
| Src_nfs_ds03 | VM datastore | GISABXPConn | Standard | At risk | None | None | SnapCenter for VMw... | netapp-backup-add... | Protect |
| Src_nfs_ds04 | VM datastore | GISABXPConn | Standard | Protected | Active | rps-policy-primary | SnapCenter for VMw... | netapp-backup-add... | Edit protection |
| Src_nfs_ds04 | File share | GISABXPConn | Critical | Protected | Active | rps-policy-primary | BlueXP backup and ... | netapp-backup-ba3... | Edit protection |
| Testvol_1787 | File share | GISABXPConn | Standard | Protected | Learning mode | rps-policy-primary | None | netapp-backup-ba3... | Edit protection |
| Nfsarpdemo02_3419 | File share | GISABXPConn | Standard | Protected | Active | rps-policy-primary | None | netapp-backup-add... | Edit protection |

Datastore protected and No Alerts reported

Protected
 Protection health
[Edit protection](#)

Protection

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

- P Pol_NFSDS04 Snapshot policy
- P 1 Year Daily LTR Backup policy

VM datastore

| | |
|----------------|-------------------------|
| Location | urn:acv:scvmUI:Resou... |
| vCenter server | vcsa01-01.hmclic.local |
| Connector | GISABXPConn |

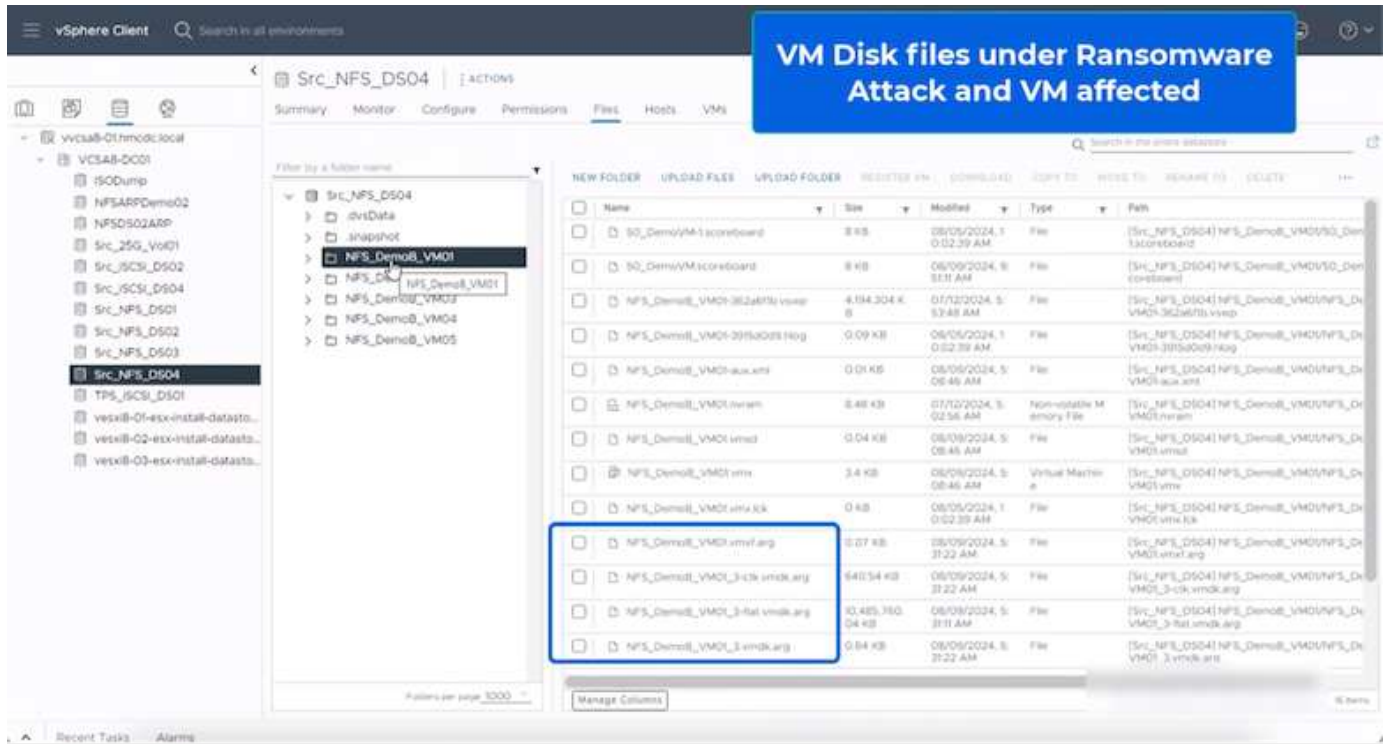
Storage

| | |
|------------------|-------------------------|
| Cluster id | add38d26-348c-11ef-8... |
| Working Env name | NTAP915_Src |
| Storage VM name | svm_NFS |
| Volume name | Src_NFS_DS04 |
| Used size | 29 GiB |

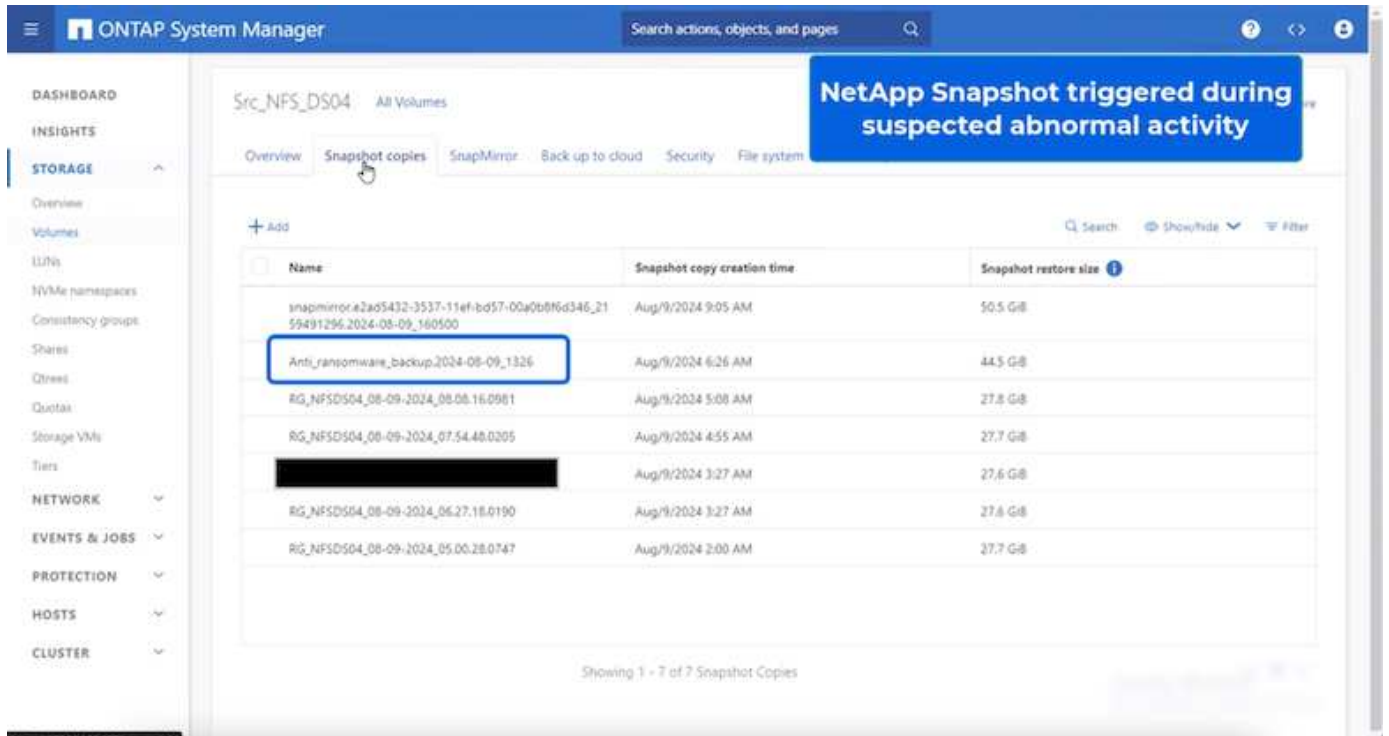
Pour plus d'informations sur la configuration de la protection contre les ransomwares BlueXP , reportez-vous aux sections "[Configurez la protection BlueXP contre les ransomware](#)" et "[Configurez les paramètres de](#)

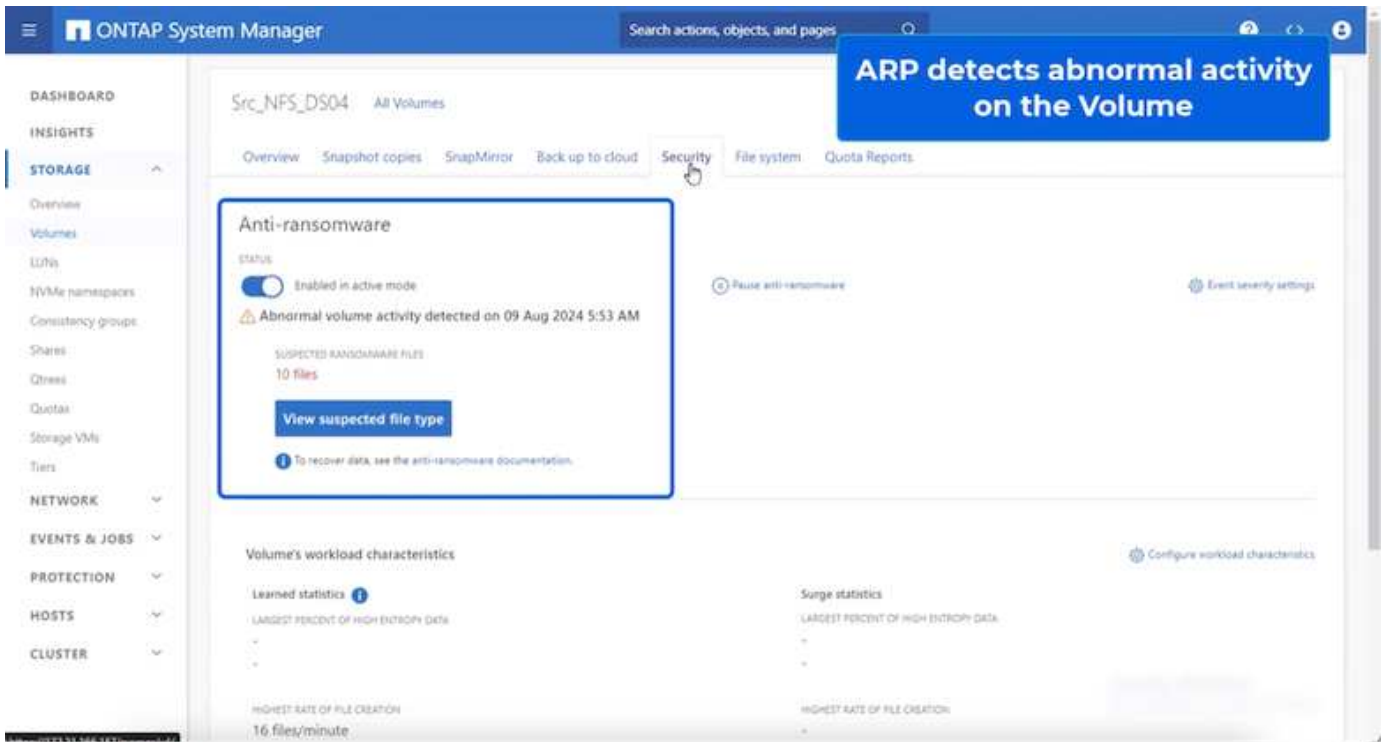
protection contre les ransomwares BlueXP".

Il est temps de citer un exemple. Dans cette procédure, le datastore "SRC_NFS_DS04" est affecté.

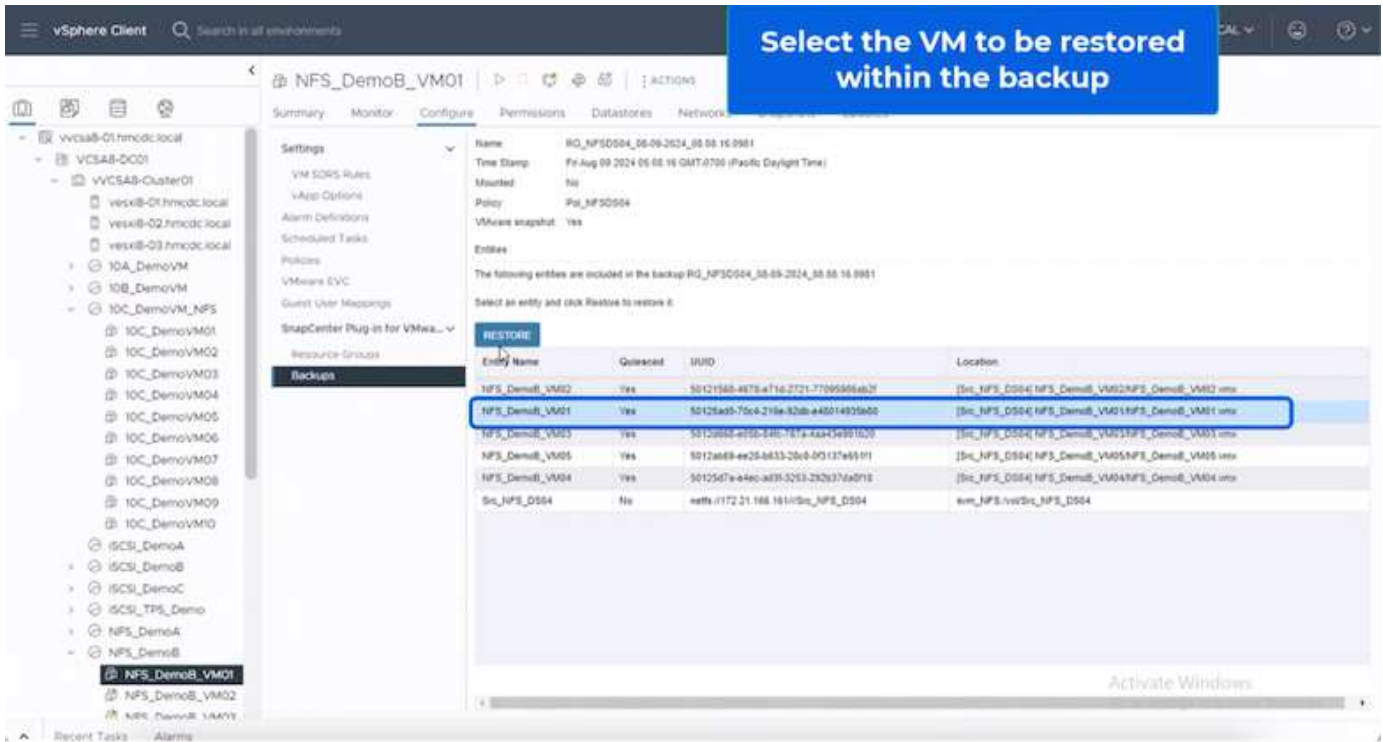


ARP a immédiatement déclenché un snapshot sur le volume lors de la détection.





Une fois l'analyse approfondie terminée, les restaurations peuvent être effectuées rapidement et de manière transparente à l'aide de la protection contre les ransomware de SnapCenter ou de BlueXP . Avec SnapCenter, accédez aux machines virtuelles concernées et sélectionnez l'instantané approprié à restaurer.

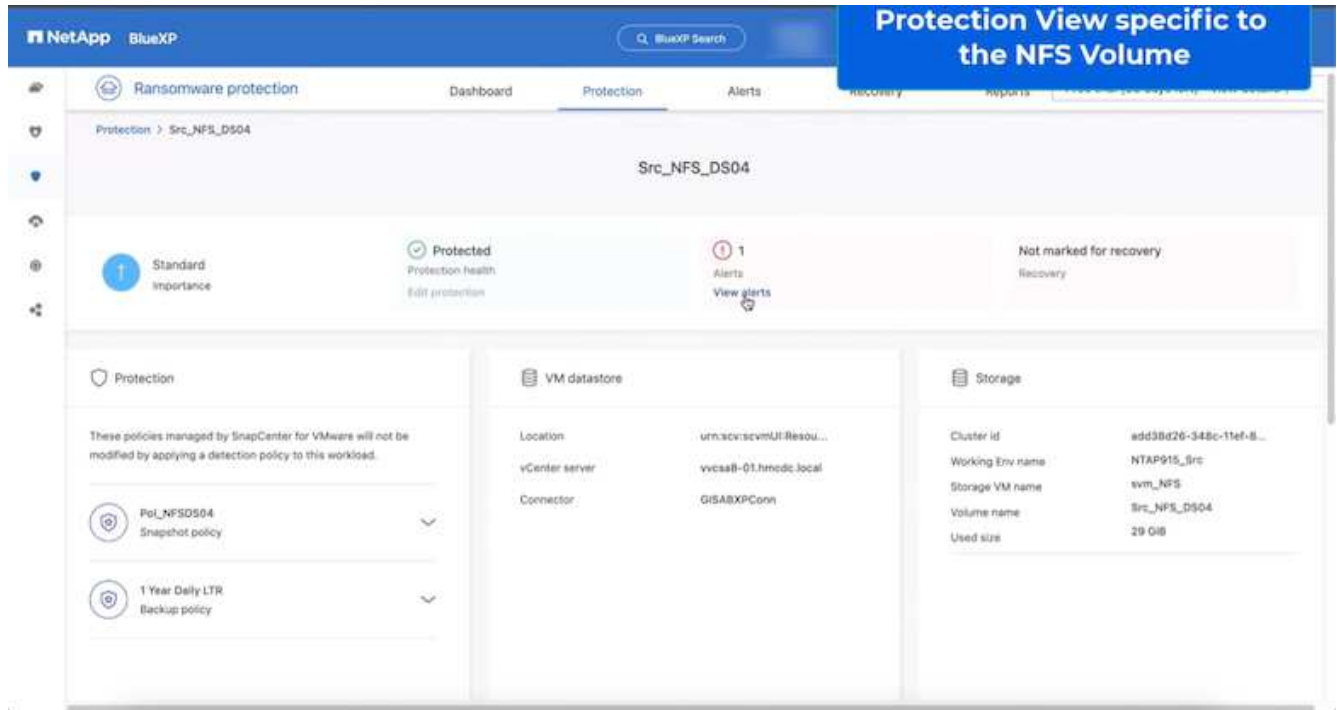


Dans cette section, nous vous expliquera comment BlueXP orchestre la protection contre les ransomwares en cas d'incident avec lequel les fichiers de la VM sont chiffrés.

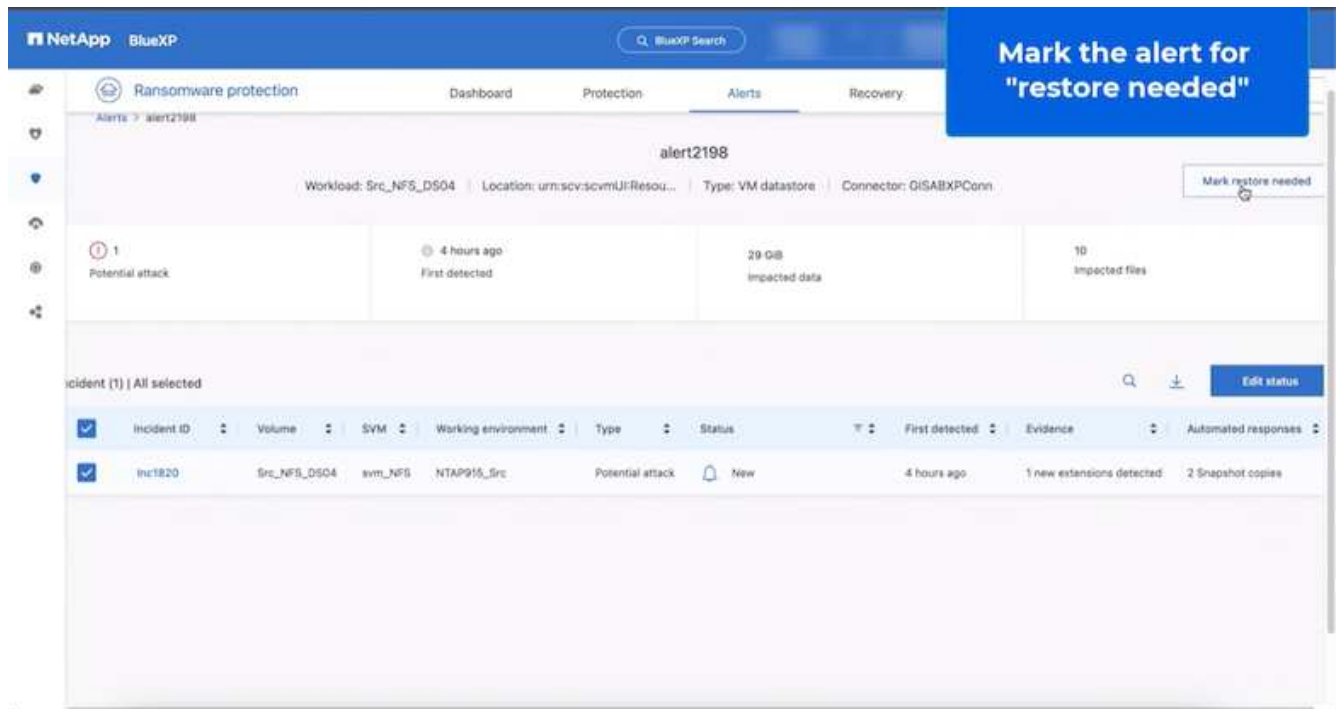


Si la machine virtuelle est gérée par SnapCenter, la protection contre les ransomwares BlueXP restaure la machine virtuelle à son état précédent en utilisant le processus cohérent avec les machines virtuelles.

1. Accédez à la protection contre les ransomware BlueXP et une alerte s'affiche sur le tableau de bord de protection contre les ransomware de BlueXP .
2. Cliquez sur l'alerte pour consulter les incidents sur ce volume spécifique pour l'alerte générée



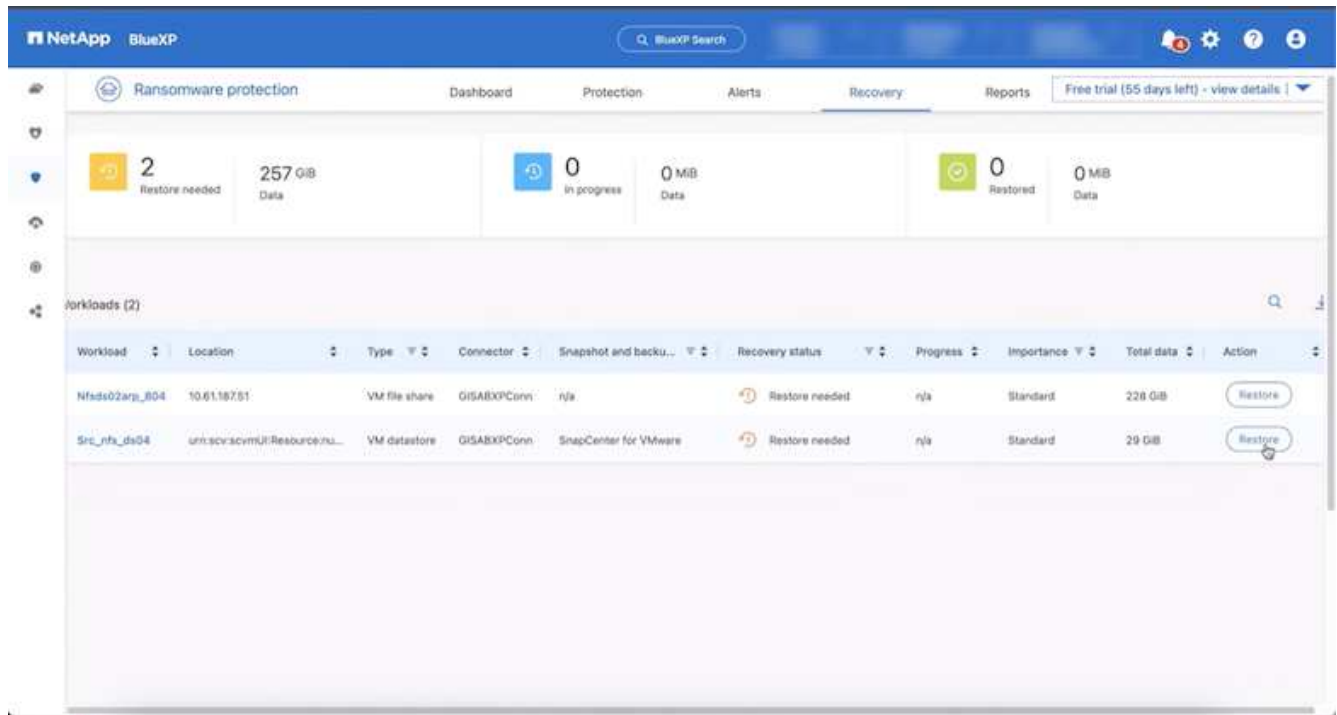
3. Marquer l'incident de ransomware comme étant prêt pour la restauration (après neutralisation des incidents) en sélectionnant « Mark restore READY » (Marquer la restauration nécessaire)



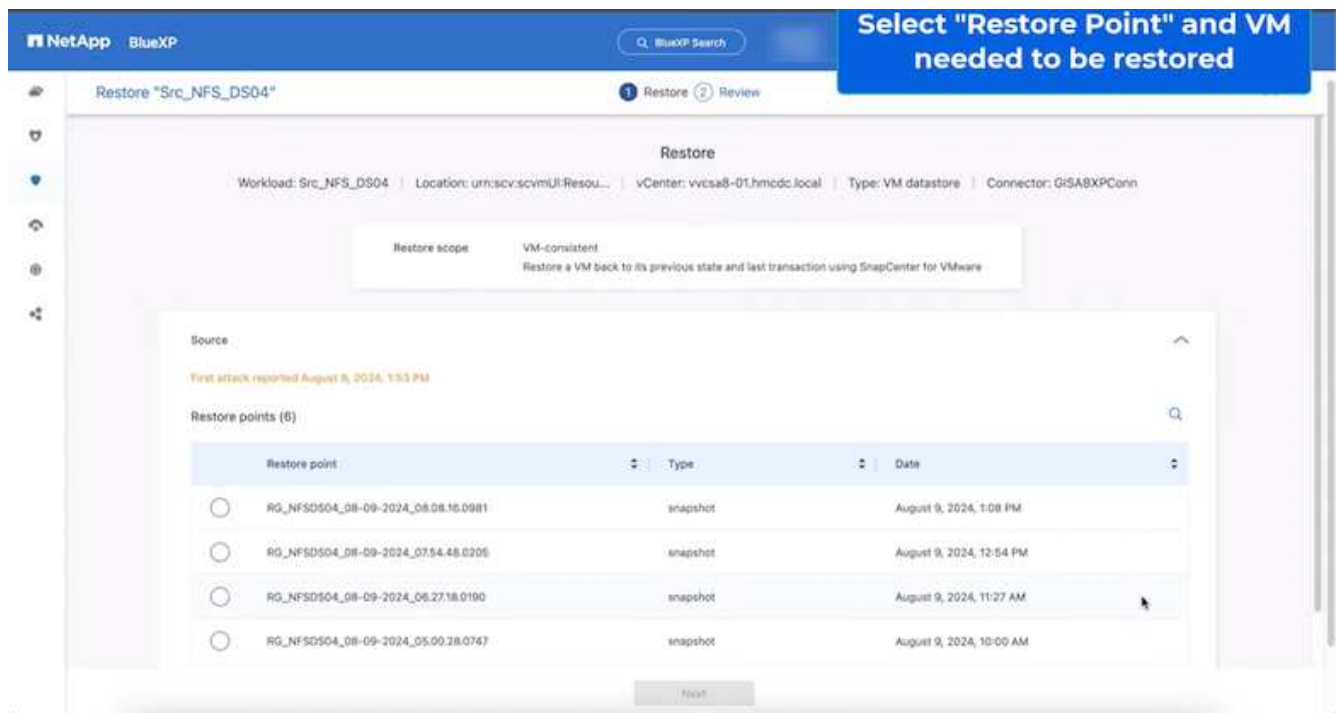


L'alerte peut être rejetée si l'incident s'avère être faux positif.

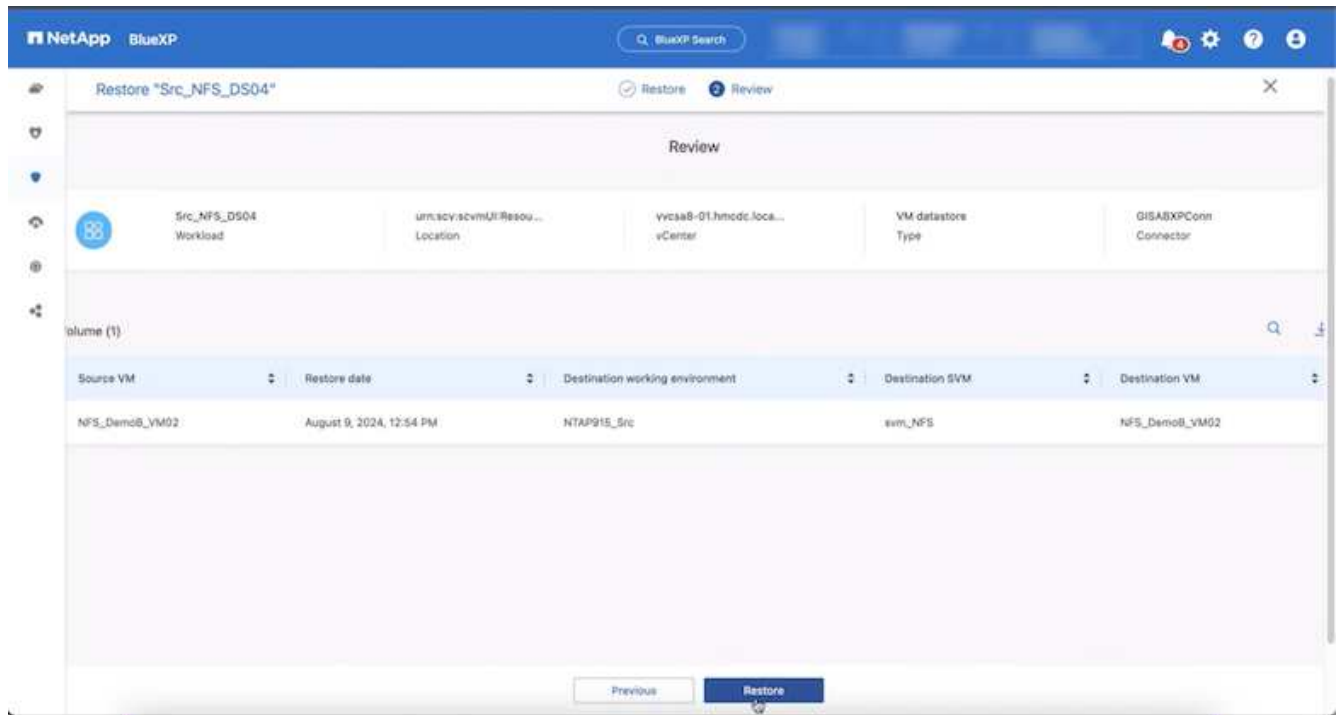
4. Accédez à l'onglet Recovery, consultez les informations de charge de travail sur la page Recovery, sélectionnez le volume de datastore à l'état Restore tionned et sélectionnez Restore.



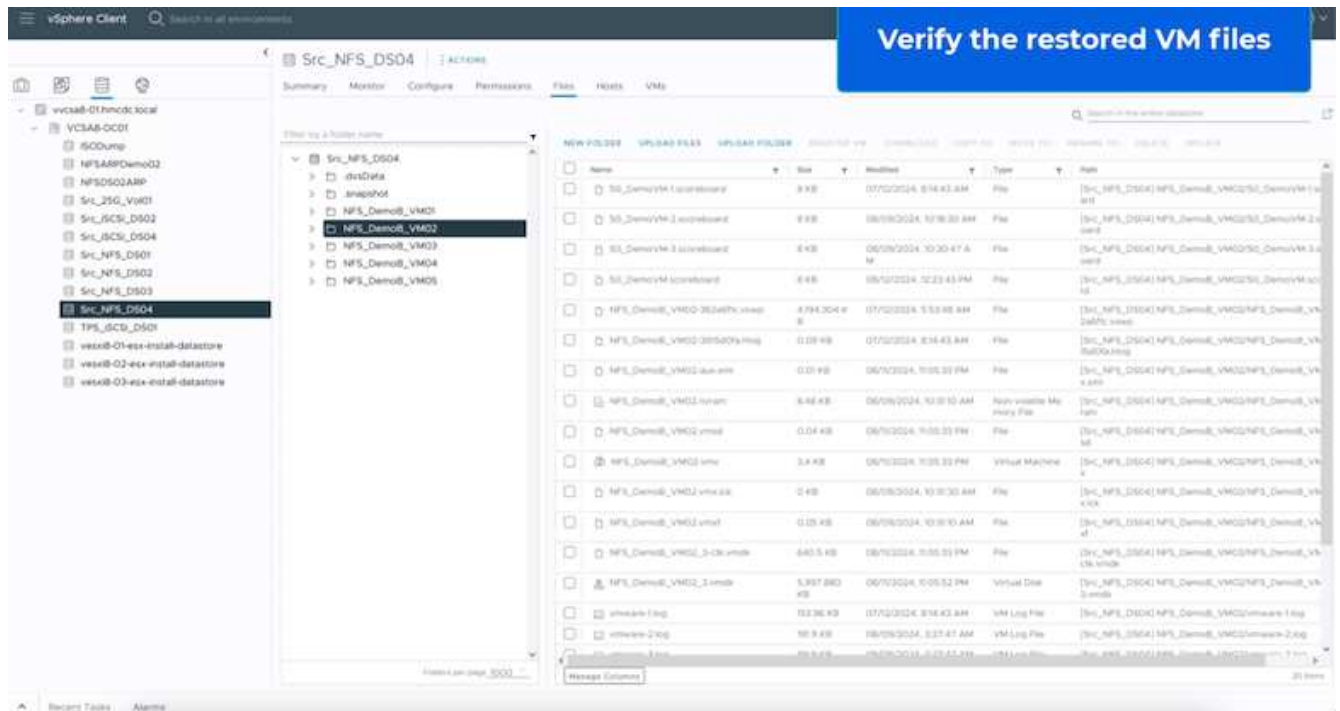
5. Dans ce cas, la portée de la restauration est « par machine virtuelle » (pour SnapCenter pour les machines virtuelles, la portée de la restauration est « par machine virtuelle »)



6. Choisissez le point de restauration à utiliser pour restaurer les données, sélectionnez destination et cliquez sur Restaurer.



7. Dans le menu supérieur, sélectionnez récupération pour examiner la charge de travail sur la page récupération, où l'état de l'opération se déplace dans les États. Une fois la restauration terminée, les fichiers VM sont restaurés comme indiqué ci-dessous.



La restauration peut être effectuée à partir de SnapCenter pour VMware ou du plug-in SnapCenter, selon l'application.

La solution NetApp fournit divers outils efficaces pour la visibilité, la détection et la résolution des problèmes, ce qui vous aide à détecter rapidement les ransomware, à prévenir cette propagation et à restaurer rapidement, si nécessaire, pour éviter les interruptions coûteuses. Les solutions de défense à plusieurs

couches classiques restent répandues, tout comme les solutions tierces et partenaires pour la visibilité et la détection. Une solution efficace reste une partie essentielle de la réponse à toute menace.

VMware Virtual volumes avec ONTAP

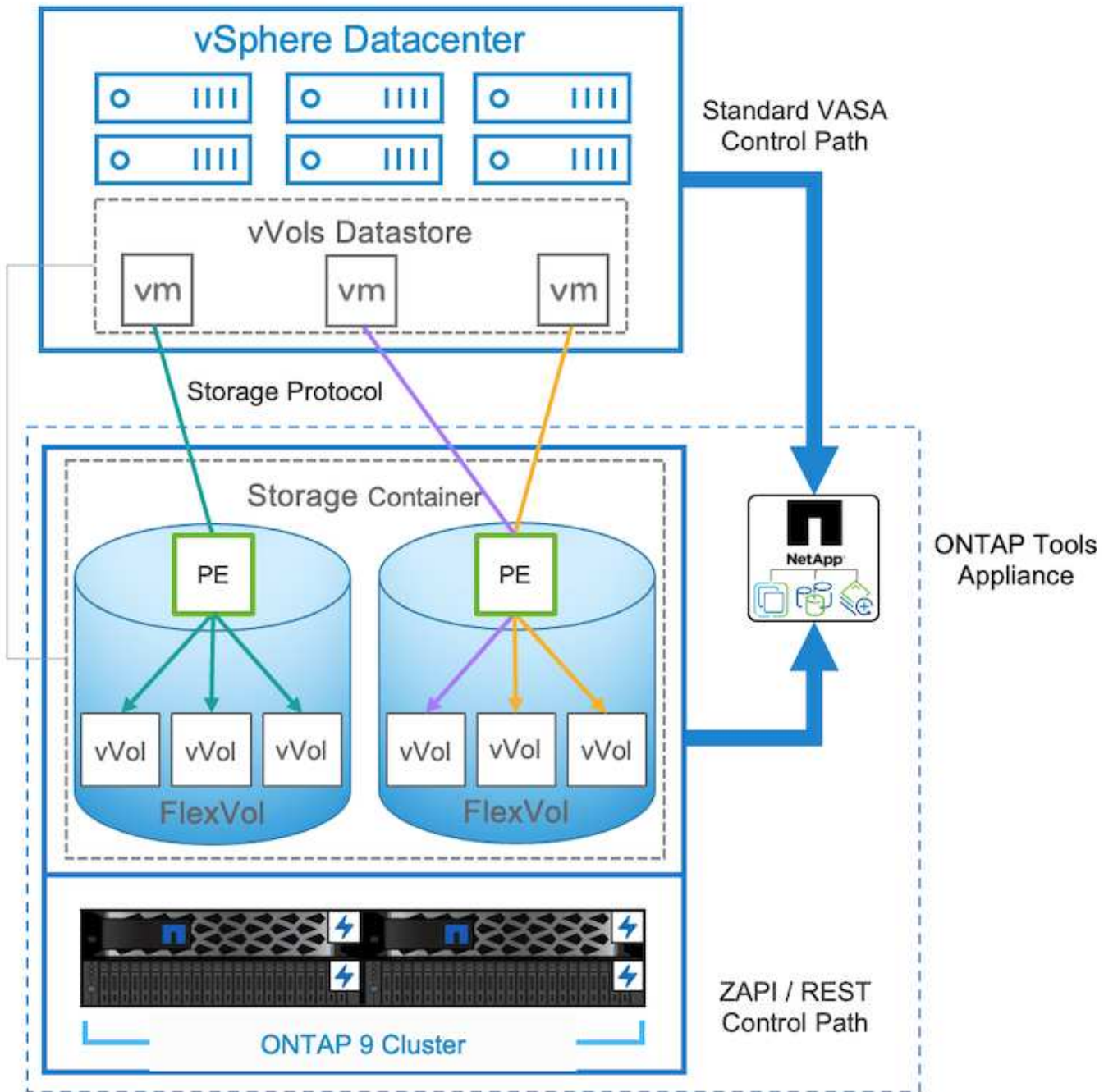
VMware Virtual volumes (vVols) permet aux exigences spécifiques des applications de prendre des décisions en matière de provisionnement du stockage tout en exploitant le riche ensemble de fonctionnalités des baies de stockage. Avec vSphere API for Storage Awareness (VASA), un administrateur de serveurs virtuels peut facilement utiliser les fonctionnalités de stockage nécessaires pour provisionner des serveurs virtuels sans avoir à interagir avec son équipe de stockage. Avant VASA, les administrateurs de VM pouvaient définir des règles de stockage de VM, mais devaient travailler avec leurs administrateurs de stockage pour identifier les datastores appropriés, souvent à l'aide de la documentation ou des conventions de nommage. Dans VASA, les administrateurs de vCenter disposant des autorisations appropriées peuvent définir une gamme de fonctionnalités de stockage que les utilisateurs de vCenter peuvent ensuite utiliser pour provisionner des VM. Le mappage entre la règle de stockage de machine virtuelle et le profil de capacité de stockage de datastore permet à vCenter d'afficher une liste de datastores compatibles à sélectionner, ainsi que d'activer d'autres technologies telles que Aria (anciennement vRealize) Automation ou Tanzu Kubernetes Grid pour sélectionner automatiquement le stockage dans une règle attribuée. Cette approche est appelée gestion basée sur des règles de stockage. Si les profils et les politiques de capacité de stockage peuvent également être utilisés avec les datastores classiques, nous nous concentrons ici sur les datastores vVols. Le fournisseur VASA pour ONTAP est inclus dans les outils ONTAP pour VMware vSphere.

Vasa Provider en dehors de la baie de stockage présente plusieurs avantages :

- Une seule instance peut gérer plusieurs baies de stockage.
- Le cycle de lancement ne dépend pas de la version du système d'exploitation du stockage.
- Les ressources de la baie de stockage sont bien onéreuses.

Chaque datastore vVol est pris en charge par un conteneur de stockage, qui constitue une entrée logique dans le fournisseur VASA pour définir la capacité de stockage. Le conteneur de stockage avec les outils ONTAP est construit avec des volumes ONTAP. Le conteneur de stockage peut être étendu en ajoutant des volumes ONTAP au sein d'une même SVM.

Le terminal PE (Protocol Endpoint) est principalement géré par les outils ONTAP. Dans le cas des vVols basés sur iSCSI, un PE est créé pour chaque volume ONTAP qui fait partie de ce conteneur de stockage ou de ce datastore vVol. Le PE pour iSCSI est une LUN de petite taille (4 Mio pour 9.x et 2 Gio pour 10.x) présentée à l'hôte vSphere et les règles de chemins d'accès multiples sont appliquées au PE.



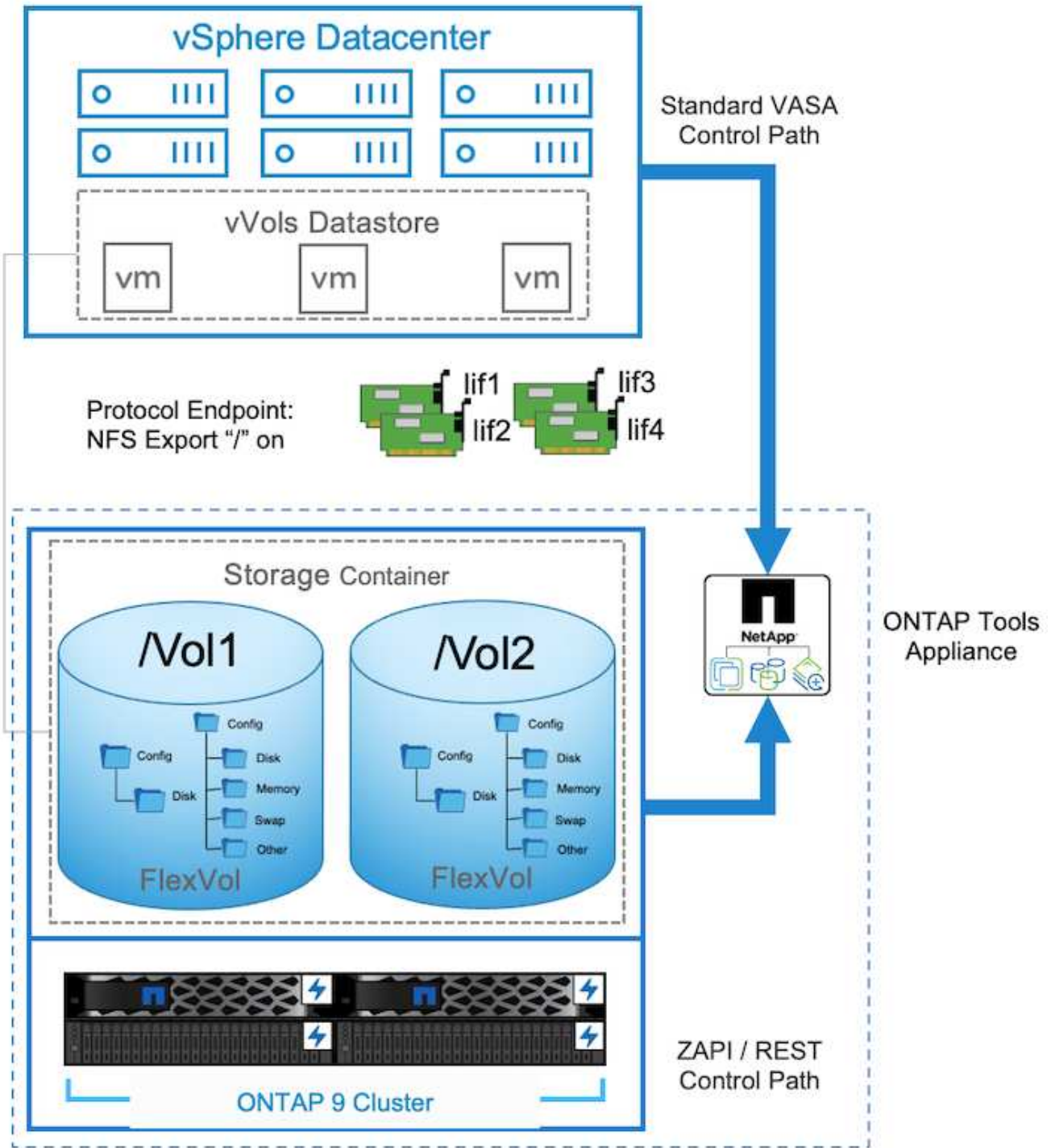
```

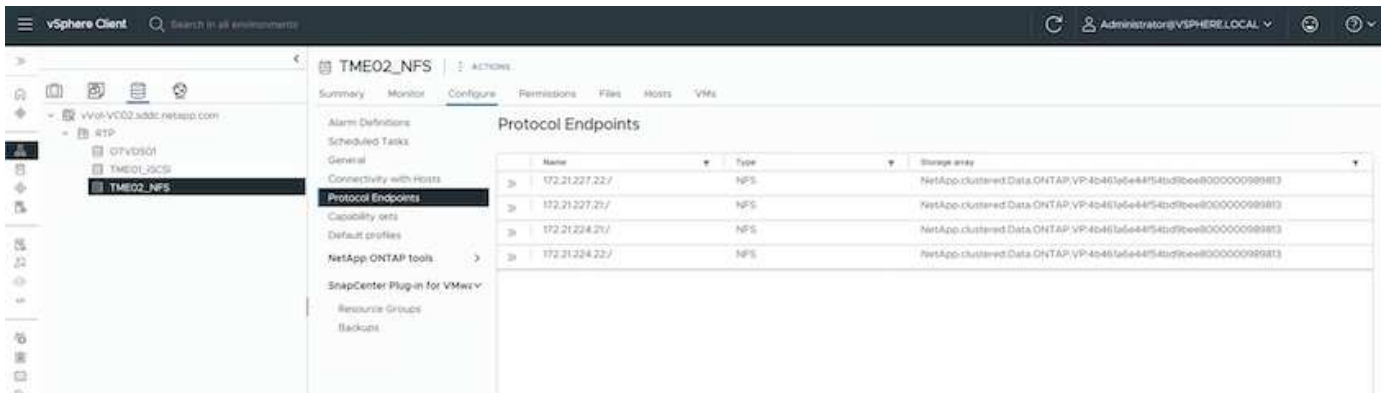
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint -fields size
vserver path size
-----
zoneb /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 2GB
zoneb /vol/TME01_iSCSI_01/vvolPE-1723727751956 4MB
zoneb /vol/TME01_iSCSI_02/vvolPE-1723727751970 4MB
4 entries were displayed.

```

Pour NFS, un PE est créé pour l'exportation du système de fichiers racine avec chaque lif de données NFS sur

un SVM sur lequel réside le conteneur de stockage ou le datastore vVol.





Les outils ONTAP gèrent le cycle de vie du terminal PE, ainsi que la communication des hôtes vSphere avec l'extension et la réduction des clusters vSphere. L'API des outils ONTAP est disponible pour s'intégrer avec l'outil d'automatisation existant.

Deux versions des outils ONTAP pour VMware vSphere sont actuellement disponibles.

Outils ONTAP 9.x

- Lorsque la prise en charge de vVol pour NVMe/FC est requise
- Exigences réglementaires fédérales ou européennes des ÉTATS-UNIS
- Davantage de cas d'utilisation intégrés au plug-in SnapCenter pour VMware vSphere

Outils ONTAP 10.x

- Haute disponibilité
- Colocation
- Grande échelle
- Prise en charge de la synchronisation active SnapMirror pour le datastore VMFS
- Intégration prochaine pour certaines utilisations avec le plug-in SnapCenter pour VMware vSphere

Pourquoi choisir les vVols ?

VMware Virtual volumes (vVols) offre les avantages suivants :

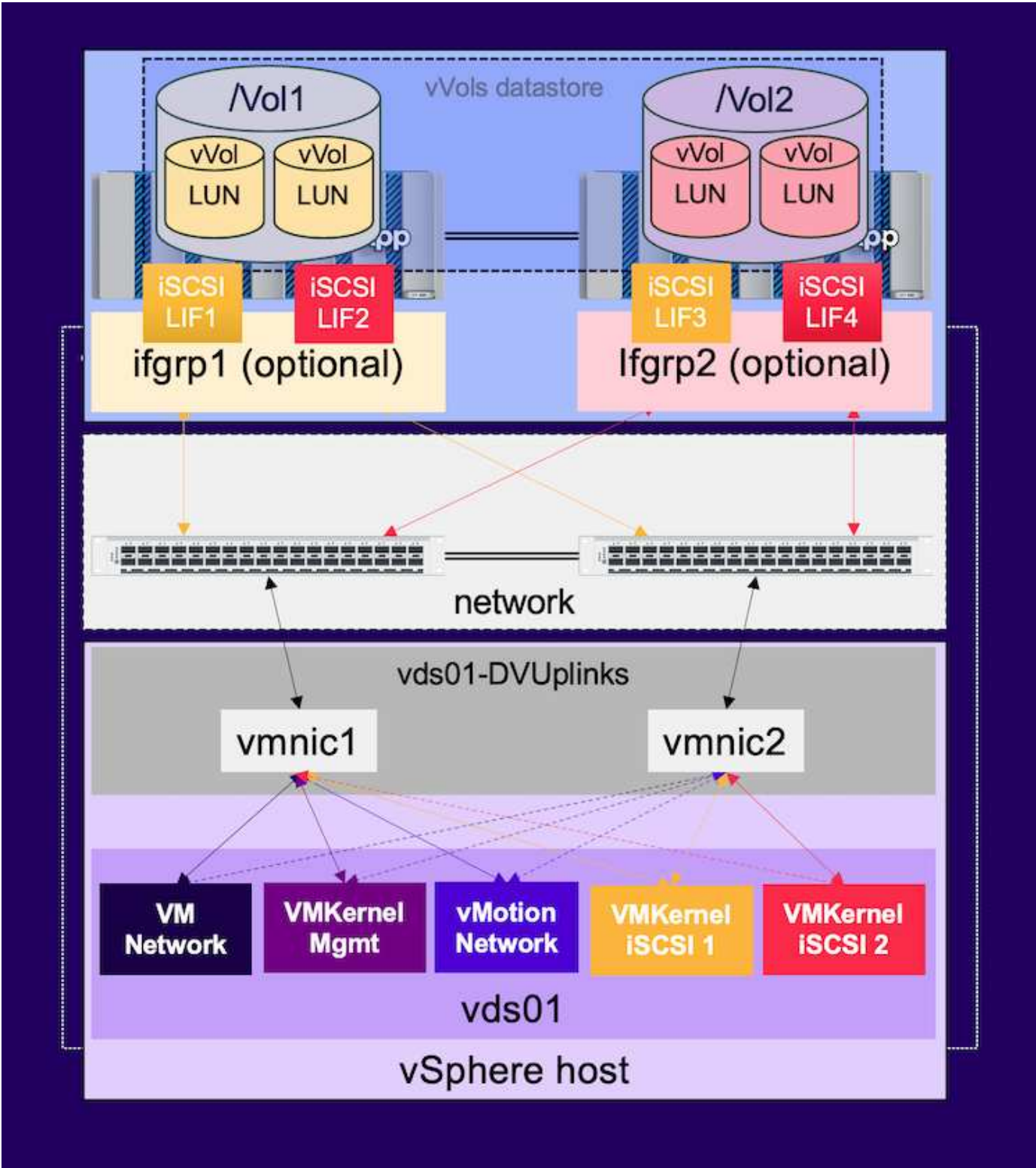
- Provisionnement simplifié (pas besoin de se soucier du nombre maximal de LUN par hôte vSphere ou de créer des exportations NFS pour chaque volume)
- Réduction du nombre de chemins iSCSI/FC (pour les vVol basés sur SCSI bloc)
- Les copies Snapshot, les clones et autres opérations de stockage sont généralement déchargés sur la baie de stockage et sont beaucoup plus rapides.
- Migrations de données simplifiées pour les VM (aucune coordination nécessaire avec les autres propriétaires de VM dans le même LUN)
- Règles de QoS appliquées au niveau des disques des machines virtuelles plutôt qu'au niveau des volumes.
- Simplicité opérationnelle (les fournisseurs de stockage proposent leurs fonctionnalités différentes dans VASA Provider)
- Prise en charge d'une grande échelle de machines virtuelles.

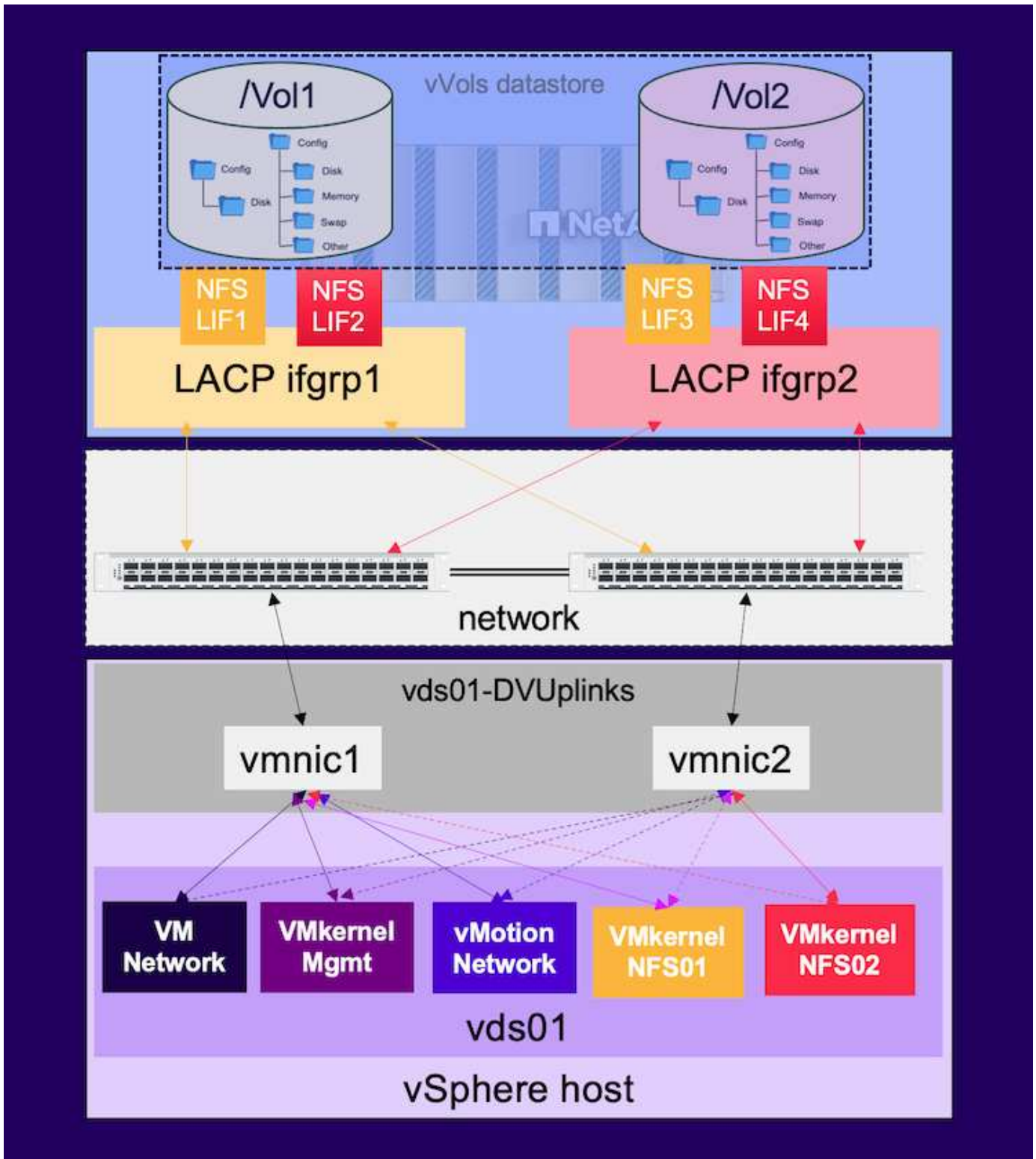
- La prise en charge de la réplication vVol pour la migration entre les instances vCenter.
- Les administrateurs du stockage ont la possibilité de surveiller au niveau du disque de la machine virtuelle.

Options de connectivité

Il est généralement recommandé d'utiliser un environnement à structure double pour les réseaux de stockage afin d'assurer la haute disponibilité, la performance et la tolérance aux pannes. Les vVols sont pris en charge avec iSCSI, FC, NFSv3 et NVMe/FC. REMARQUE : reportez-vous "[Matrice d'interopérabilité \(IMT\)](#)" à la section pour connaître la version de l'outil ONTAP prise en charge

L'option de connectivité reste cohérente avec les options de datastore VMFS ou NFS. Vous trouverez ci-dessous un exemple de réseau vSphere de référence pour iSCSI et NFS.





Provisionnement avec les outils ONTAP pour VMware vSphere

Le datastore vVol peut être provisionné de la même manière que le datastore VMFS ou NFS à l'aide des outils ONTAP. Si le plug-in des outils ONTAP n'est pas disponible dans l'interface utilisateur du client vSphere, reportez-vous à la section mise en route ci-dessous.

Avec les outils ONTAP 9.13

1. Cliquez avec le bouton droit de la souris sur le cluster ou l'hôte vSphere et sélectionnez provisionner un datastore sous Outils NetApp ONTAP.
2. Conservez le type en tant que vVols, indiquez le nom du datastore et sélectionnez le protocole souhaité

The image displays two screenshots of the 'New Datastore' configuration wizard in ONTAP 9.13. Both screenshots show the 'General' tab with the following fields:

- Provisioning destination:** Cluster01 (with a BROWSE button)
- Type:** NFS, VMFS, vVols (selected)
- Name:** TME01_ISCSI
- Description:** (empty text box)
- Protocol:** NFS, ISCSI (selected), FC / FCoE, NVMe/FC

The bottom screenshot shows the 'Protocol' field with NFS selected instead of ISCSI, and the Name field containing TME02_NFS.

3. Sélectionnez le profil de capacité de stockage souhaité, choisissez le système de stockage et le SVM.

New Datastore

- 1 General
- 2 Storage system**
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles: **Default profiles**

- Platinum_AFF_A
- Platinum_AFF_C
- Platinum_ASA_A
- Platinum_ASA_C

[Create storage capability profile](#)

Storage system:

Storage VM:

4. Créez de nouveaux volumes ONTAP ou sélectionnez un volume existant pour le datastore vVol.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes**
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

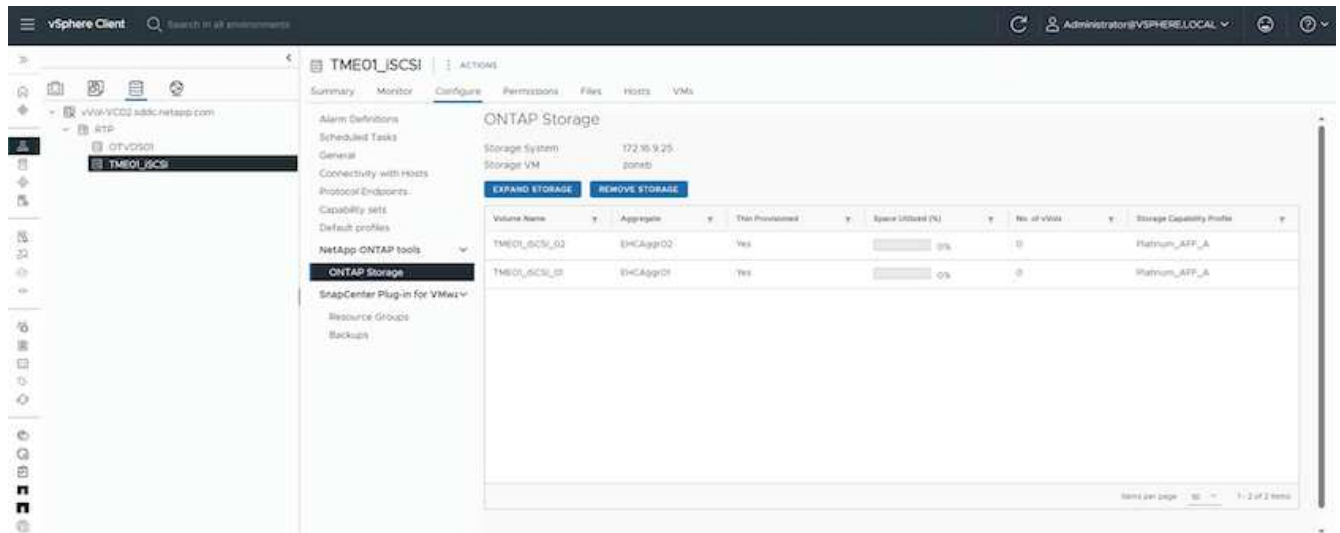
Create new volumes

| Name | Size | Storage Capability Profile | Aggregate |
|----------------|--------|----------------------------|-----------|
| TME01_ISCSI_01 | 250 GB | Platinum_AFF_A | EHCAGgr01 |
| TME01_ISCSI_02 | 250 GB | Platinum_AFF_A | EHCAGgr02 |

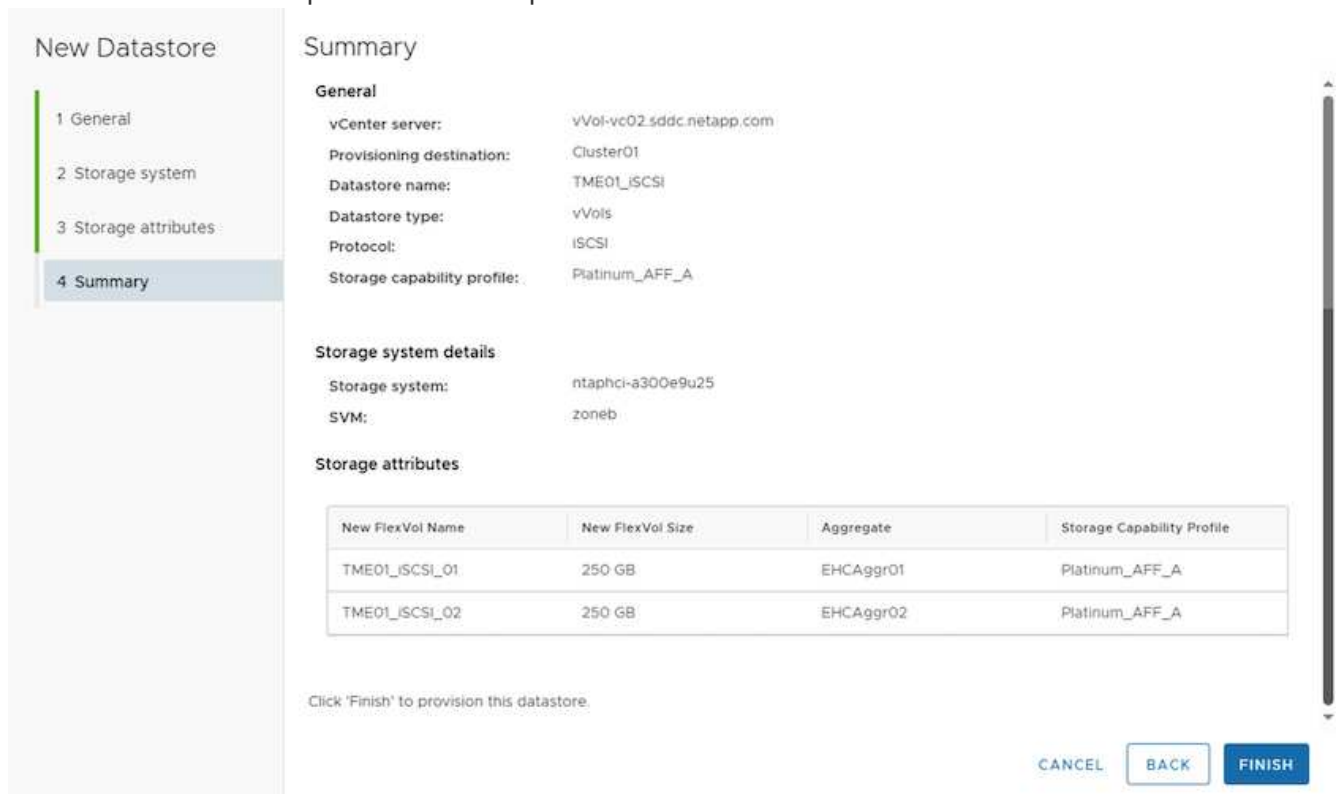
1 - 2 of 2 items

| Name | Size(GB) | Storage capability profile | Aggregates | Space reserve |
|----------------------|----------------------|---|--|-----------------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text" value="Platinum_AFF_A"/> | <input type="text" value="EHCAGgr02 - (17109.63 Gi)"/> | <input type="text" value="Thin"/> |

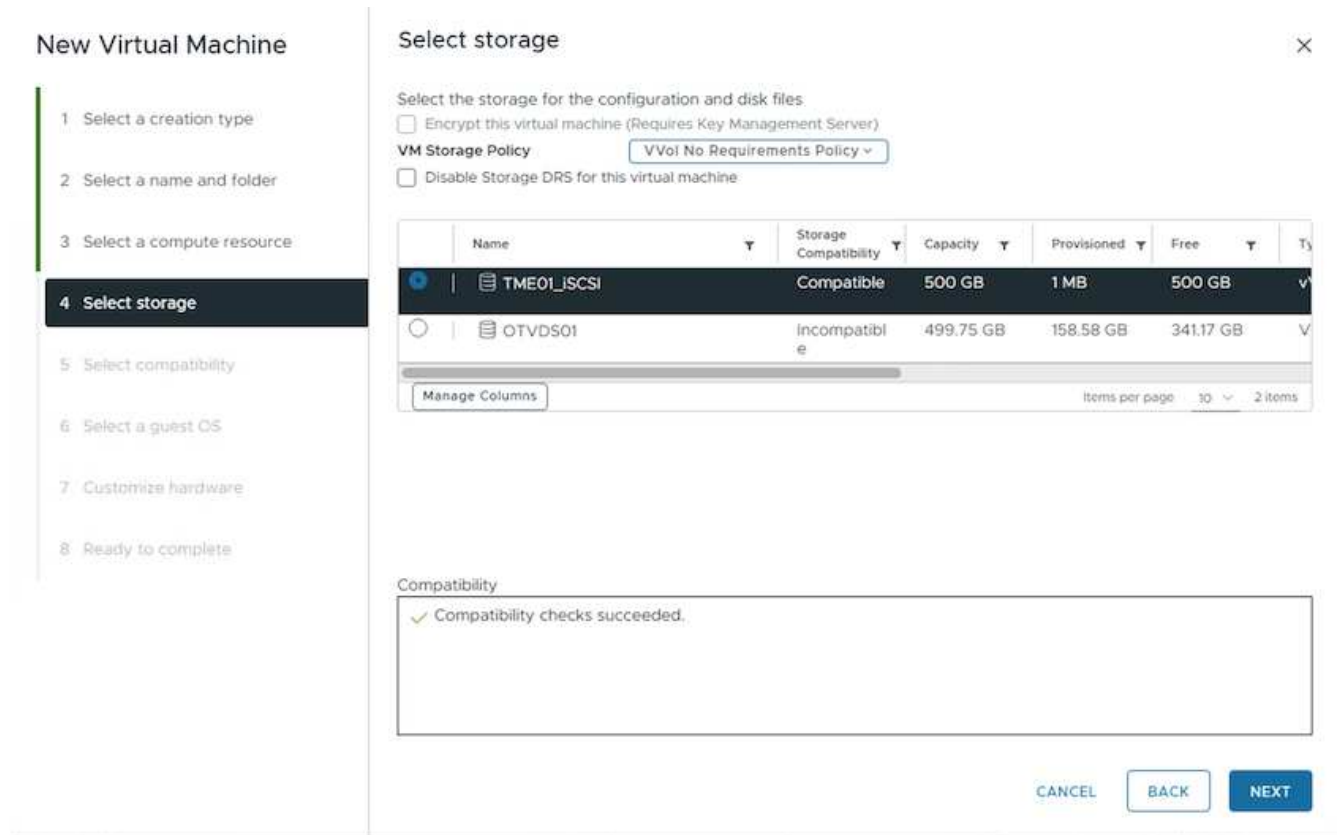
Les volumes ONTAP peuvent être affichés ou modifiés ultérieurement à partir de l'option datastore.



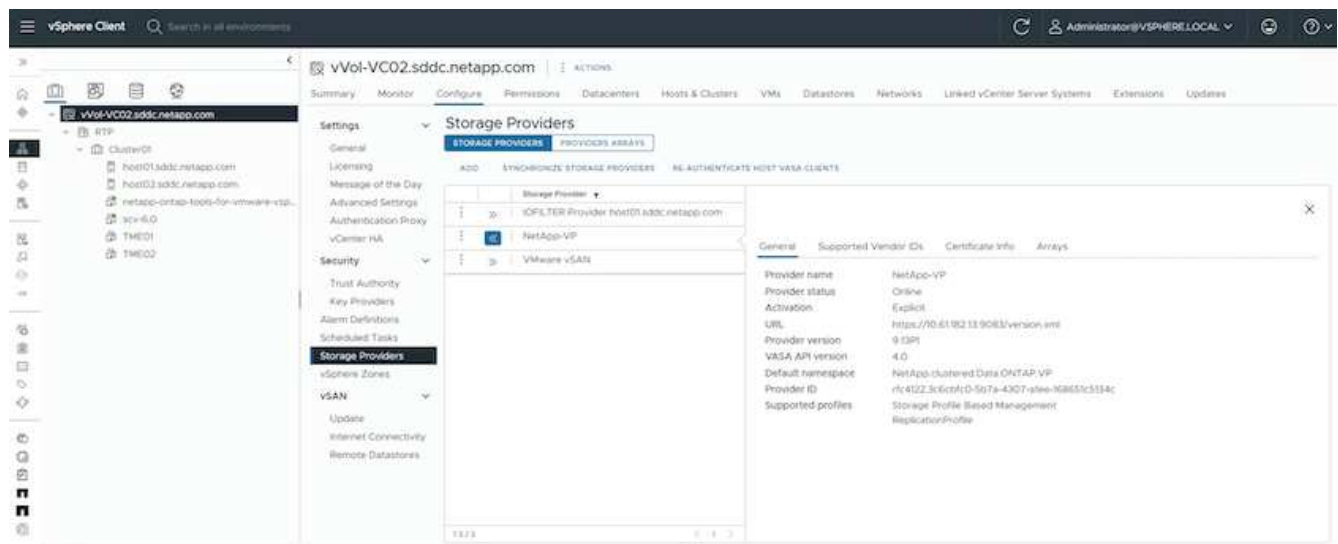
5. Vérifiez le résumé et cliquez sur Terminer pour créer le datastore vVol.



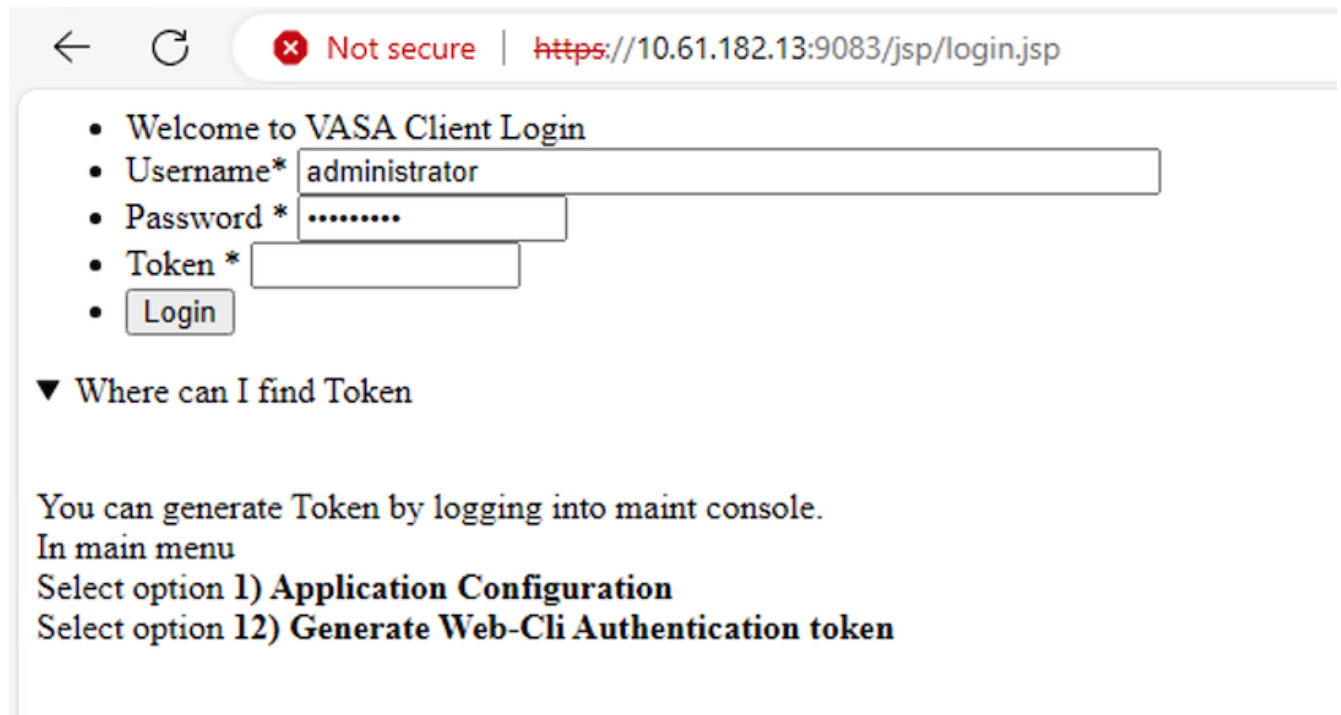
6. Une fois le datastore vVol créé, il peut être utilisé comme n'importe quel autre datastore. Voici un exemple d'affectation d'un datastore basé sur une stratégie de stockage de VM à une VM en cours de création.



7. Les détails de vVol peuvent être récupérés à l'aide de l'interface CLI Web. L'URL du portail est identique à celle du fournisseur VASA sans le nom de fichier version.xml.



Les informations d'identification doivent correspondre aux informations utilisées lors de la mise à disposition des outils ONTAP



Ou utilisez le mot de passe mis à jour avec la console de maintenance des outils ONTAP.

Application Configuration Menu:

- 1) Display server status summary
 - 2) Start Virtual Storage Console service
 - 3) Stop Virtual Storage Console service
 - 4) Start VASA Provider and SRA service
 - 5) Stop VASA Provider and SRA service
 - 6) Change 'administrator' user password
 - 7) Re-generate certificates
 - 8) Hard reset database
 - 9) Change LOG level for Virtual Storage Console service
 - 10) Change LOG level for VASA Provider and SRA service
 - 11) Display TLS configuration
 - 12) Generate Web-Cli Authentication token
 - 13) Start ONTAP tools plug-in service
 - 14) Stop ONTAP tools plug-in service
 - 15) Start Log Integrity service
 - 16) Stop Log Integrity service
 - 17) Change database password
-
- b) Back
 - x) Exit

Enter your choice: 12

Starting token creation
Your webcli auth token is :668826

This token is for one time use only. Its valid for 20 minutes.

Press ENTER to continue.

Sélectionnez interface CLI Web.

NetApp ONTAP tools for VMware vSphere - Control Panel:

| Operation | Description |
|---|--|
| Web based CLI interface | Web based access to the command line interface for administrative tasks |
| Inventory | Listing of all objects and information currently known in Unified Virtual Appliance database |
| Statistics | Listing of all counters and information regarding internal state |
| Right Now | See what operations are in flight right now |
| Logout | Logout |

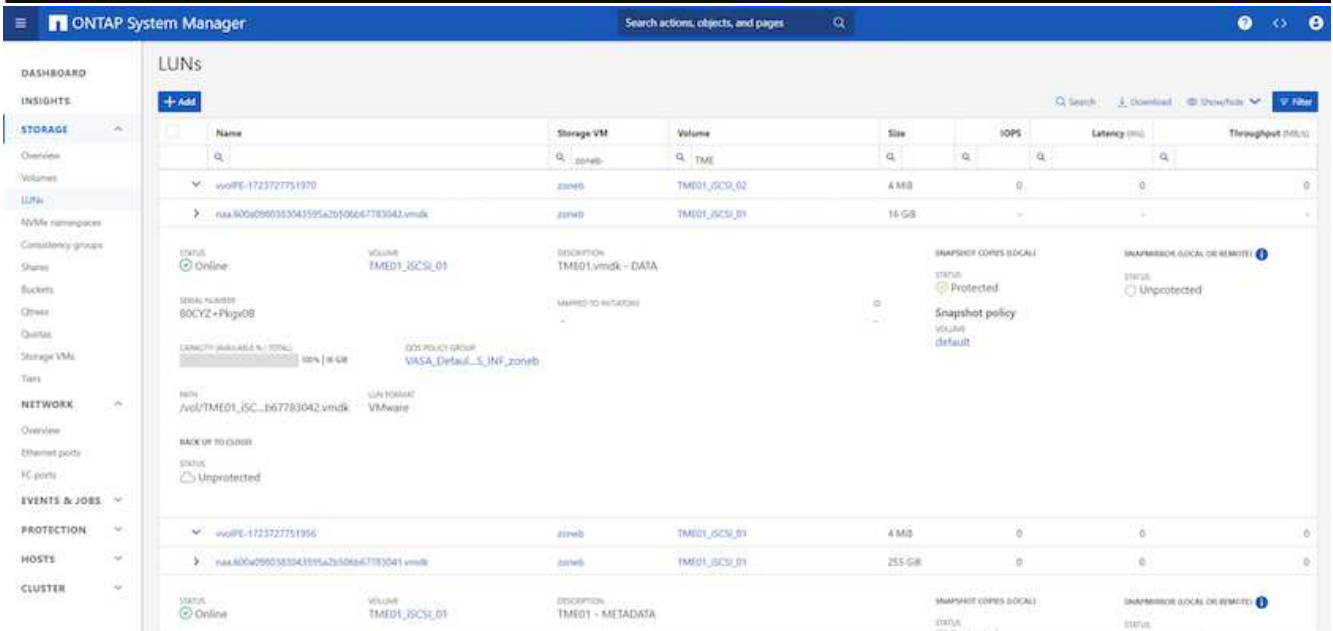
Build Release 9.13P1
Build Timestamp 03/08/2024 11:11:42 AM
System up since Thu Aug 15 02:23:18 UTC 2024
Current time Thu Aug 15 17:59:26 UTC 2024

Saisissez la commande souhaitée dans la liste des commandes disponibles. Pour afficher la liste des détails de vVol ainsi que les informations de stockage sous-jacentes, essayez `vvol list -verbose=true`

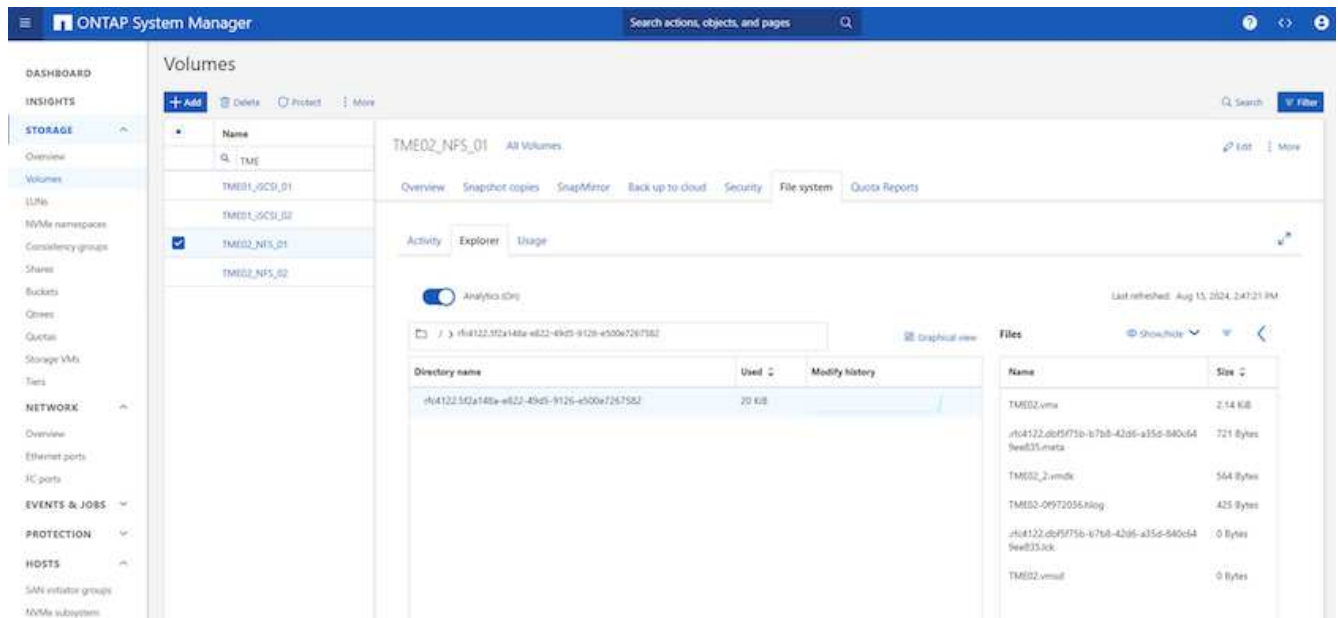


afin d'obtenir une liste basée sur les LUN, l'interface de ligne de commande de ONTAP ou System Manager peuvent également être utilisés.

```
ntapcli-a300e9u25:~> lun show -vserver zoneb -class vvol -fields comment,size
vserver path                                size comment
-----
zoneb /vol/Demo01_fv01/naa.600a0980383043595a2b506b67783038.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683735.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683736.vmdk 16GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683737.vmdk 16GB
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk 255GB TME01 - METADATA
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk 16GB TME01.vmdk - DATA
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk 16GB TME01.vmdk - DATA
```

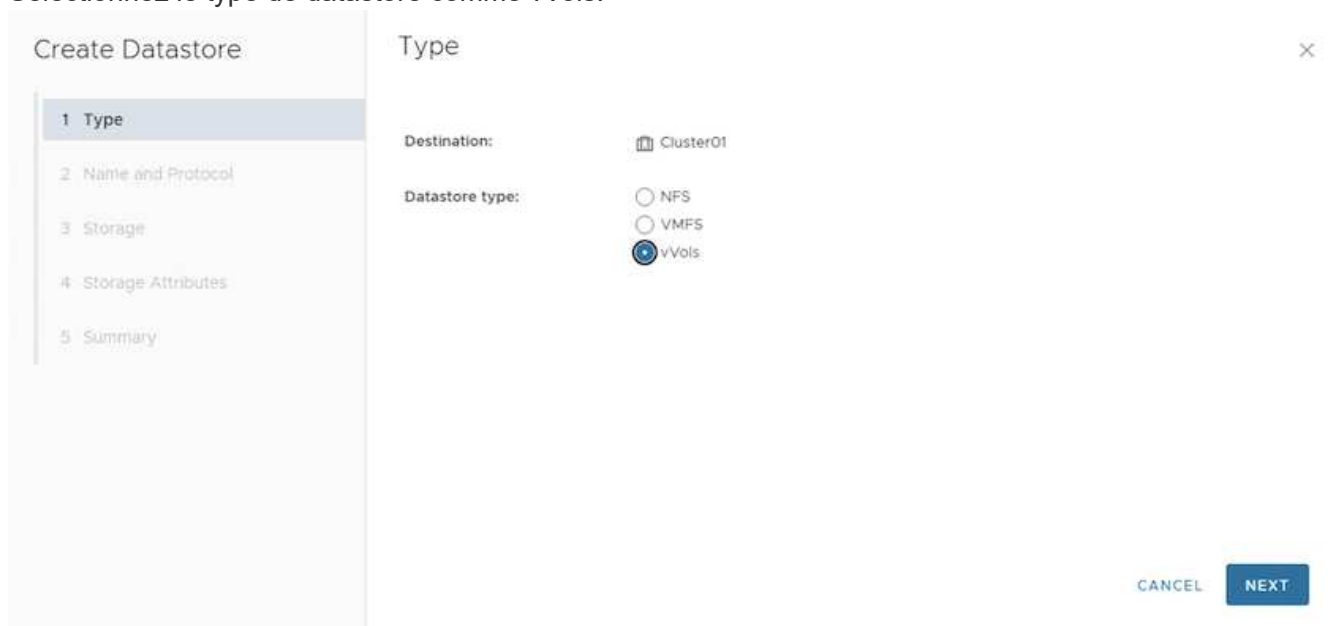


Pour les systèmes NFS, System Manager peut être utilisé pour parcourir le datastore.

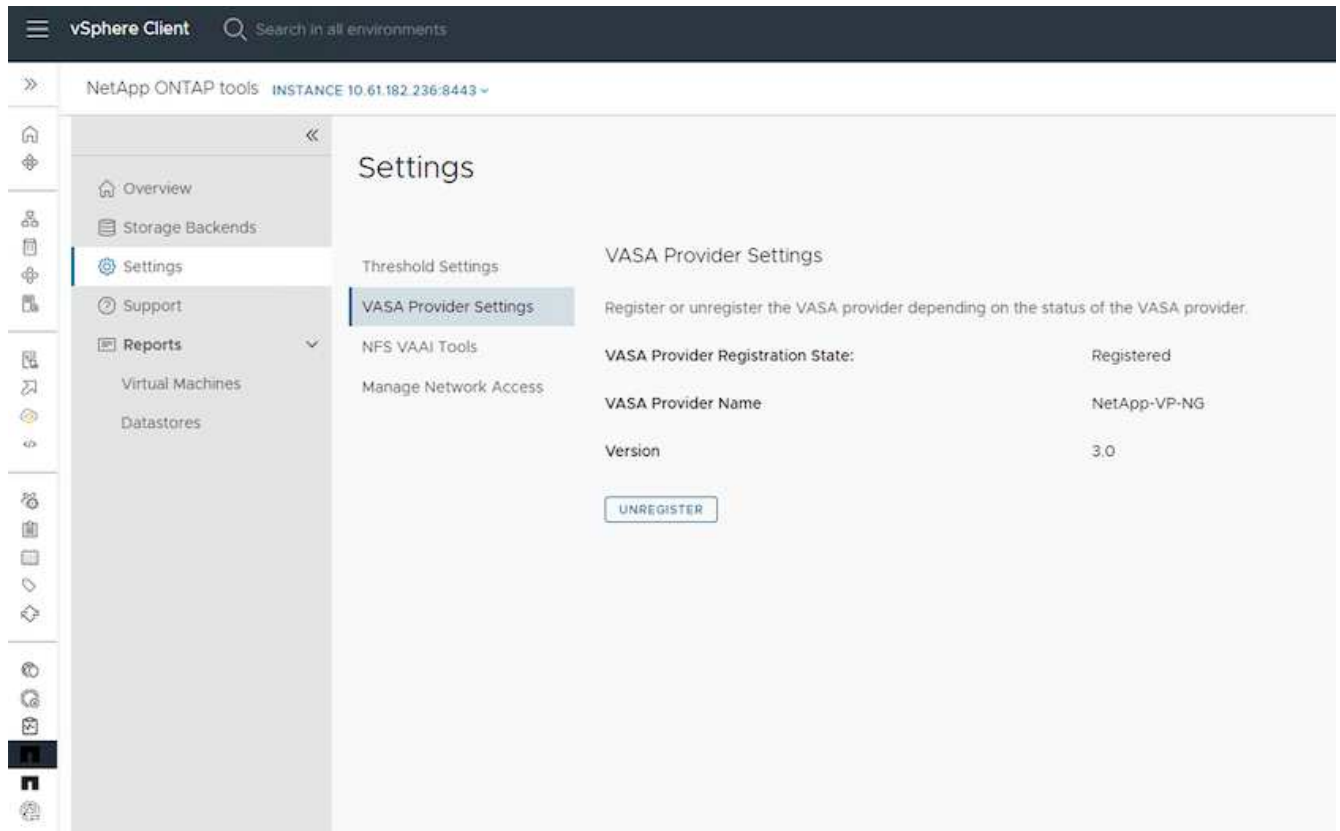


Avec les outils ONTAP 10.1

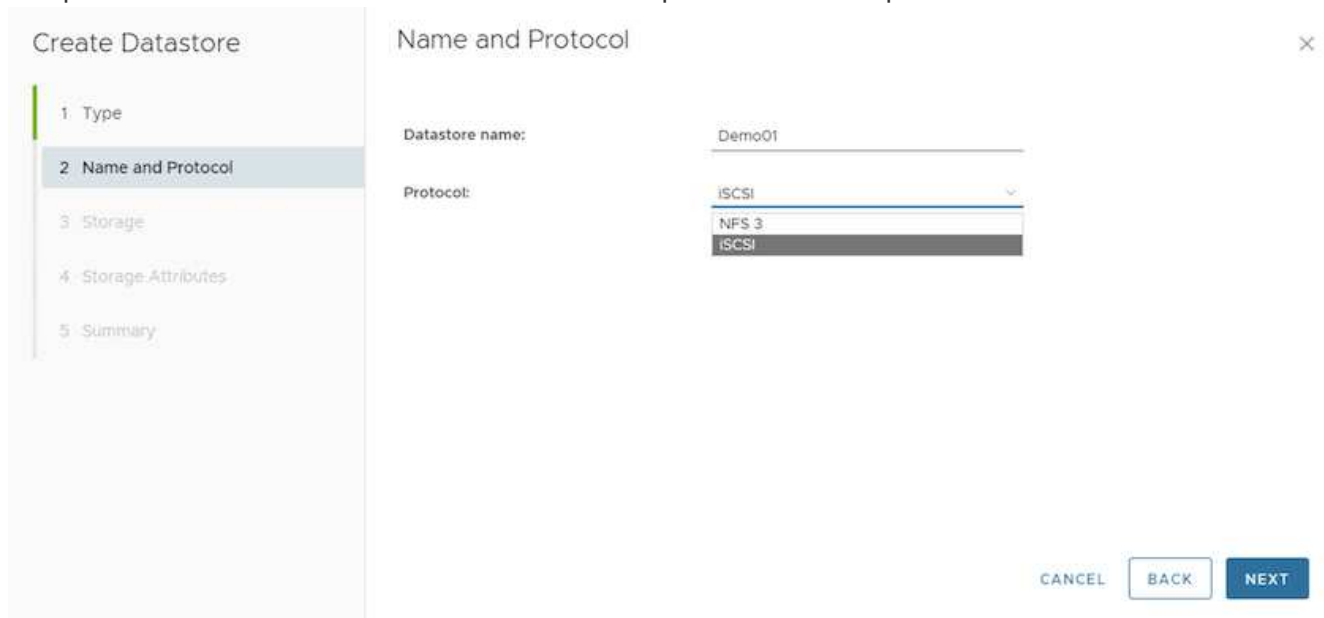
1. Cliquez avec le bouton droit de la souris sur le cluster ou l'hôte vSphere et sélectionnez Créer un datastore (10.1) sous Outils NetApp ONTAP.
2. Sélectionnez le type de datastore comme vVols.



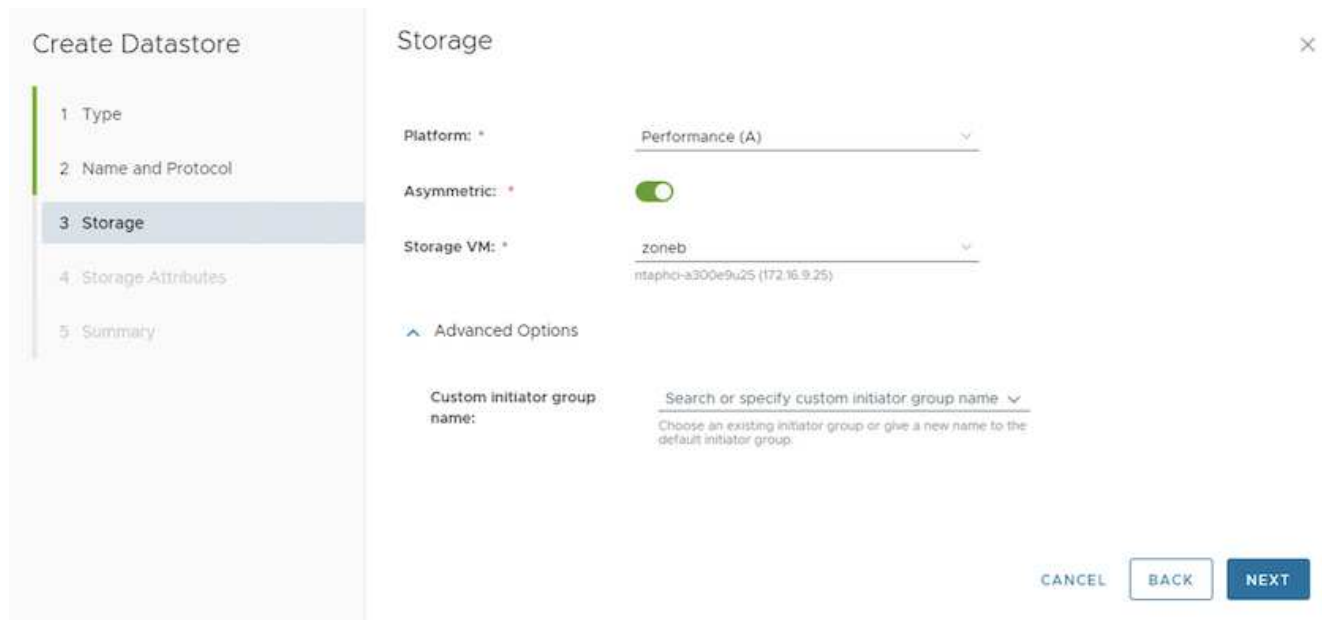
Si l'option vVols n'est pas disponible, assurez-vous que le fournisseur VASA est enregistré.



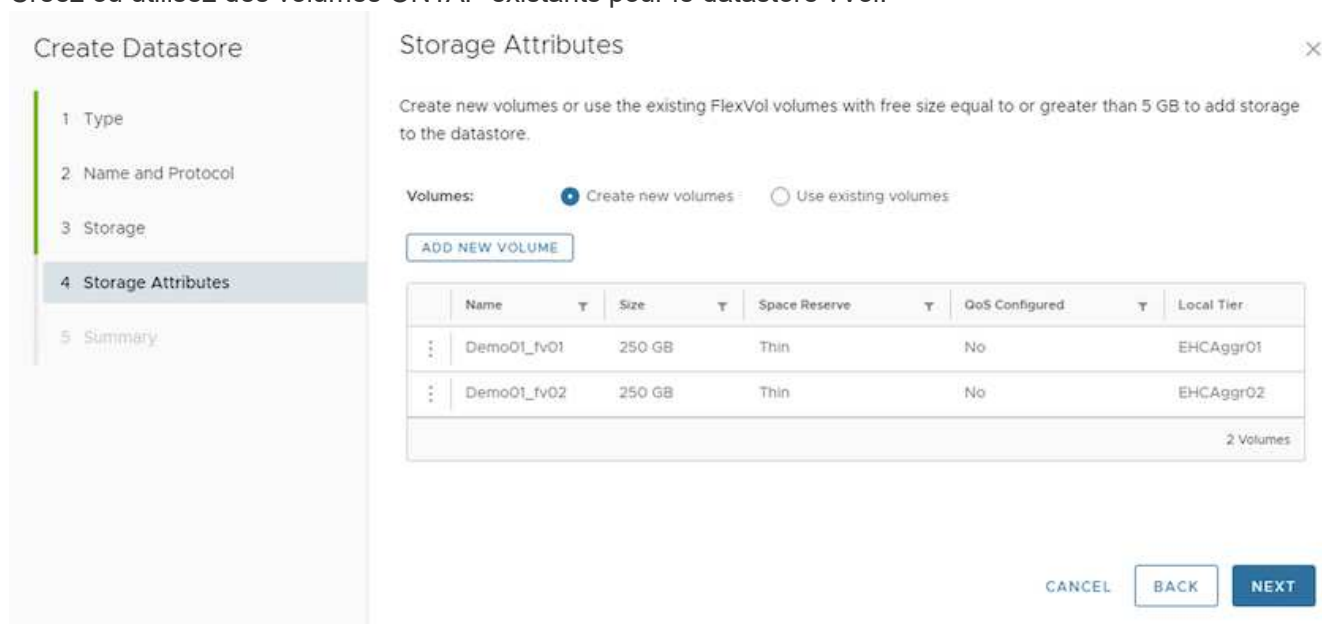
3. Indiquez le nom du datastore vVol et sélectionnez le protocole de transport.



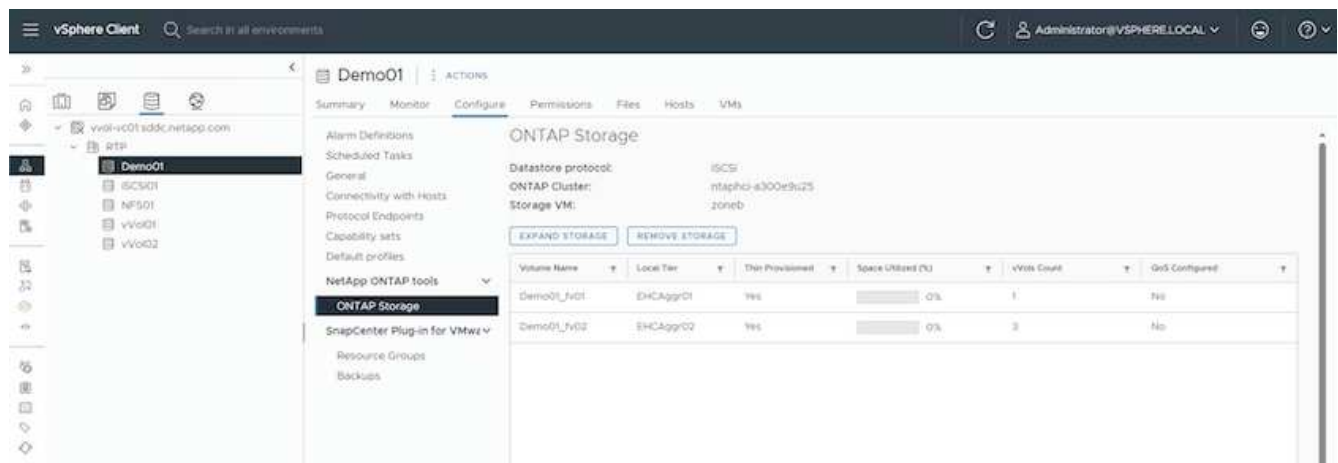
4. Sélectionnez la plateforme et la VM de stockage.



5. Créez ou utilisez des volumes ONTAP existants pour le datastore vVol.



Les volumes ONTAP peuvent être affichés ou mis à jour ultérieurement à partir de la configuration du datastore.



6. Une fois le datastore vVol provisionné, sa consommation peut être similaire à celle de n'importe quel autre

datastore.

7. Les outils ONTAP fournissent le rapport sur les ordinateurs virtuels et les datastores.

The top screenshot shows the 'Virtual Machines' section in the vSphere Client. It features a table with the following data:

| VM Name | Primary Datastore Type | Primary Datastore Name | vCenter VM Latency | Max Datastore Latency | Total Datastore IOPS | Average Datastore Throughput | Total Datastore Capacity | Uptime | Power State | vCenter VM Committed Capacity |
|---------|------------------------|------------------------|--------------------|-----------------------|----------------------|------------------------------|--------------------------|----------|-------------|-------------------------------|
| scv | VMFS | DCSD01 | 0 ms | 100 µs | 3 | 10.89 KB/s | 37.27% | 16 hours | On | 96.08 GB |
| Demo01 | vVol | Demo01 | - | 53 µs | 1 | 86 Bytes/s | 0.03% | - | Off | 287 GB |
| Demo02 | vVol | VVOL02 | - | 0 µs | 0 | 0 Bytes/s | 0.01% | - | Off | 271 GB |

The bottom screenshot shows the 'Datastores' section in the vSphere Client. It features a table with the following data:

| Name | Space Utilized (D%) | Type | IOPS | Latency | Throughput | Storage VM | Storage Controller |
|--------|---------------------|------|------|---------|------------|------------|--------------------|
| DCSD01 | 37.27% | VMFS | 3 | 100 µs | 10.89 KB/s | Demo | ntaprci-4300w9u25 |
| NP001 | 0.01% | NFS | 0 | 297 µs | 21 Bytes/s | Demo | ntaprci-4300w9u25 |
| VVOL01 | 0.02% | vVol | 2 | 48 µs | 81 Bytes/s | Demo | ntaprci-4300w9u25 |
| VVOL02 | 5.01% | vVol | 0 | 0 µs | 0 Bytes/s | Demo | ntaprci-4300w9u25 |
| Demo01 | 5.03% | vVol | 1 | 53 µs | 86 Bytes/s | Demo | ntaprci-4300w9u25 |

Protection des données des VM sur le datastore vVol

Vous trouverez une vue d'ensemble de la protection des données des machines virtuelles sur "[Protection des vVols](#)" un datastore vVol à l'adresse .

1. Enregistrez le système de stockage hébergeant le datastore vVol et tout partenaire de réplication.

vSphere Client Search in all environments Administrator@VSPHERE.LOCAL

SnapCenter Plug-in for VMware vSphere INSTANCE 10.10.102.12-8144

Dashboard Settings Resource Groups Policies Storage Systems Guest File Restore

Storage Systems

Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAP as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods. Click here to know more.

| Name | Display Name | Type | Protocol | Port | Username | SVM | TimeOutSec | Cache |
|--------------------------------|-------------------|---------------|----------|------|----------|-----|------------|-------|
| B:RTH-C503-5403-orig.e... | nasadm-4300e9a25 | ONTAP Cluster | HTTPS | 443 | admin | 0 | 60 | No |
| VCF_SCSI | VCF_SCSI | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| isur0 | isur0 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 02.21.228.20 | isur0 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| HMC_SCSI_3510 | HMC_SCSI_3510 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| JL_SHC_SCSI | JL_SHC_SCSI | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 0301102.217 | psdadm-symb-SCSI | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| HMC_3E7 | HMC_3E7 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| VCF_3422 | VCF_3422 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| VCF_NVMe | VCF_NVMe | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| demo | demo | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 02.21.254.120 | Temp_3510_N1 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 02.21.35.10 | HYPERV-SCSI | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| EHC_NFS | EHC_NFS | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 02.21.18.203 | EHC_SCSI | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 02.21.18.10 | VCF_NFS | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| HMC_3510 | HMC_3510 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| 00fa_symb_4300 | 00fa_symb_4300 | ONTAP SVM | HTTPS | 443 | - | - | 60 | No |
| B:ontap-destination-s403-ne... | ontap-destination | ONTAP Cluster | HTTPS | 443 | admin | 1 | 90 | No |
| 0301102.147 | symb2 | ONTAP SVM | HTTPS | 443 | - | - | 90 | No |

2. Créez une règle avec les attributs requis.

New Backup Policy



Name

Description

Frequency

Locking Period Enable Snapshot Locking

Retention

Replication Update SnapMirror after backup
 Update SnapVault after backup

Snapshot label

Advanced

VM consistency

Include datastores with independent disks

Scripts

CANCEL

ADD

3. Créer un groupe de ressources et l'associer à une stratégie (ou règles).

Create Resource Group



1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope:

Virtual Machines

Parent entity:

Datstores

Virtual Machines

Tags

Folders

Enter available entity name

Available entities

TME01

Selected entities

BACK

NEXT

FINISH

CANCEL

REMARQUE : pour le datastore vVol, la protection est nécessaire avec une machine virtuelle, une balise ou un dossier. Le datastore vVol ne peut pas être inclus dans le groupe de ressources.

4. L'état de sauvegarde spécifique de la machine virtuelle peut être affiché dans son onglet configurer.

| Name | Status | Locations | Snapshot Lock Expression | Created Time | Mounted | Policy | VMware Snapshot |
|---------------------|-----------|---------------------|--------------------------|-----------------------|---------|--------|-----------------|
| TME_00-05-2024_10.4 | Completed | Primary & Secondary | - | 8/15/2024 10:44:10 AM | No | hourly | No |
| TME_00-05-2024_10.2 | Completed | Primary & Secondary | - | 8/15/2024 10:24:52 AM | No | hourly | No |
| TME_00-05-2024_06.5 | Completed | Primary | - | 8/15/2024 9:53:15 AM | No | hourly | No |
| TME_00-05-2024_09.4 | Completed | Primary | - | 8/15/2024 9:47:24 AM | No | hourly | No |
| TME_00-05-2024_09.4 | Completed | Primary | - | 8/15/2024 9:44:50 AM | No | hourly | No |
| TME_00-05-2024_09.4 | Completed | Primary | - | 8/15/2024 9:44:08 AM | No | hourly | No |
| TME_00-05-2024_09.3 | Completed | Primary | - | 8/15/2024 9:40:04 AM | No | hourly | No |

5. La machine virtuelle peut être restaurée à partir de son emplacement principal ou secondaire.

Reportez-vous "[Documentation du plug-in SnapCenter](#)" à pour des utilisations supplémentaires.

Migration des machines virtuelles depuis les datastores classiques vers un datastore vVol

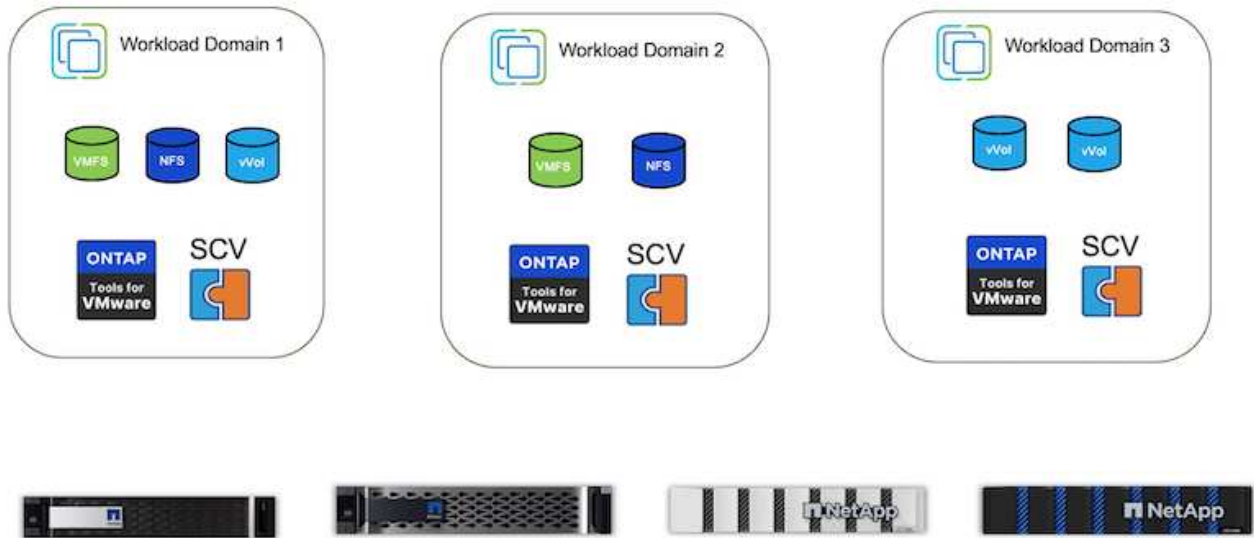
Pour migrer des machines virtuelles d'autres datastores vers un datastore vVol, plusieurs options sont disponibles en fonction du scénario. Elle peut varier d'une simple opération Storage vMotion à une migration à l'aide de HCX. Voir "[Migrer des machines virtuelles vers un datastore ONTAP](#)" pour plus de détails.

Migration des VM entre les datastores vVol

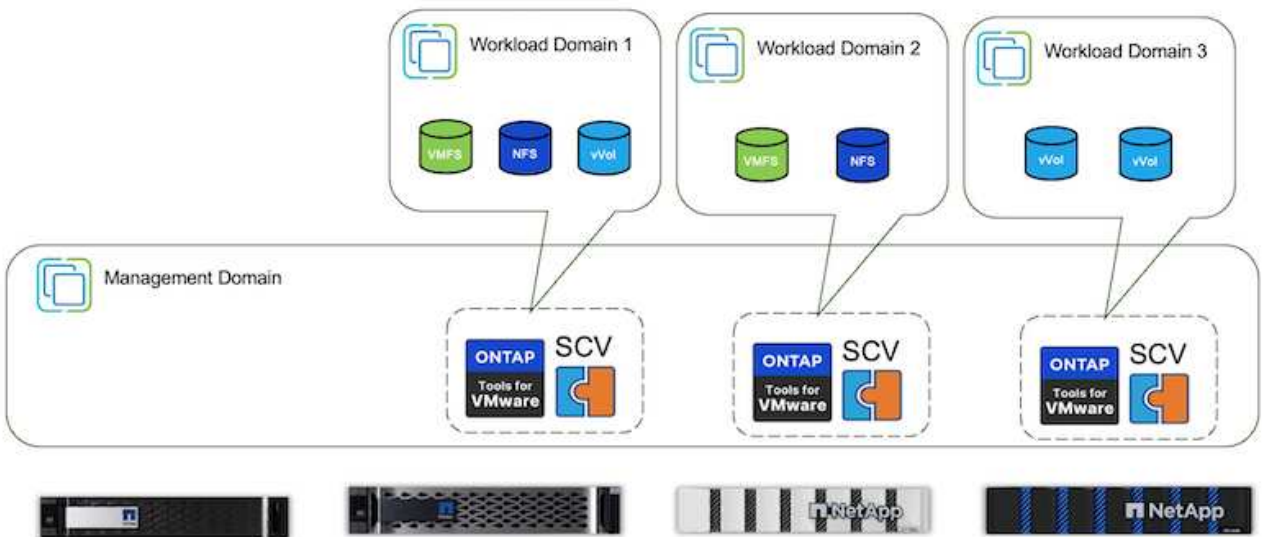
Pour la migration en bloc de machines virtuelles entre les datastores vVol, vérifiez "[Migrer des machines virtuelles vers un datastore ONTAP](#)".

Exemple d'architecture de référence

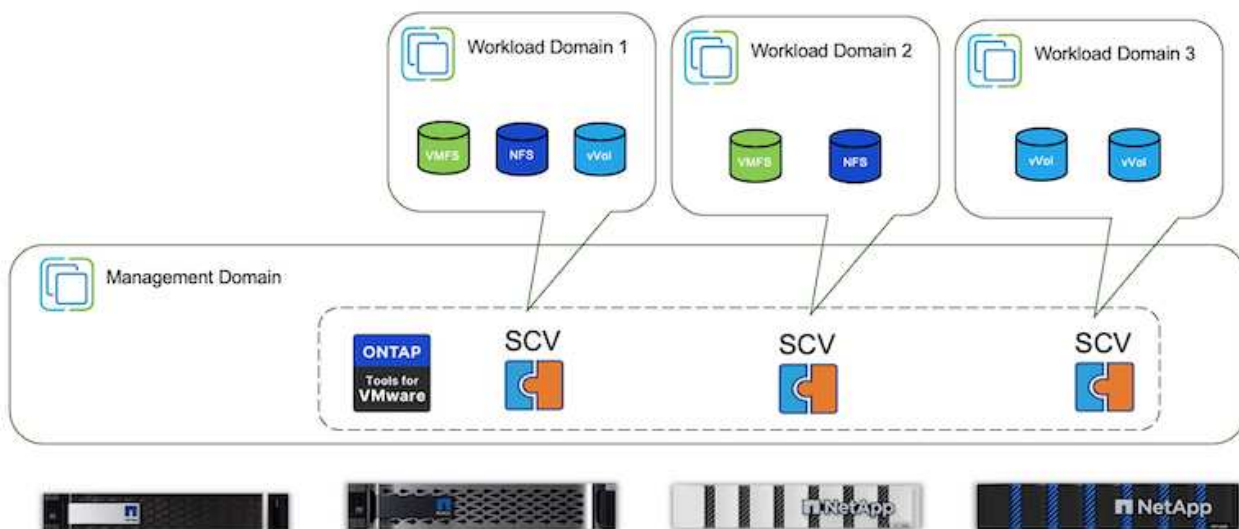
Les outils ONTAP pour VMware vSphere et SCV peuvent être installés sur le même serveur vCenter qu'il gère ou sur un autre serveur vCenter. Il est préférable d'éviter d'héberger les données sur un datastore vVol géré.



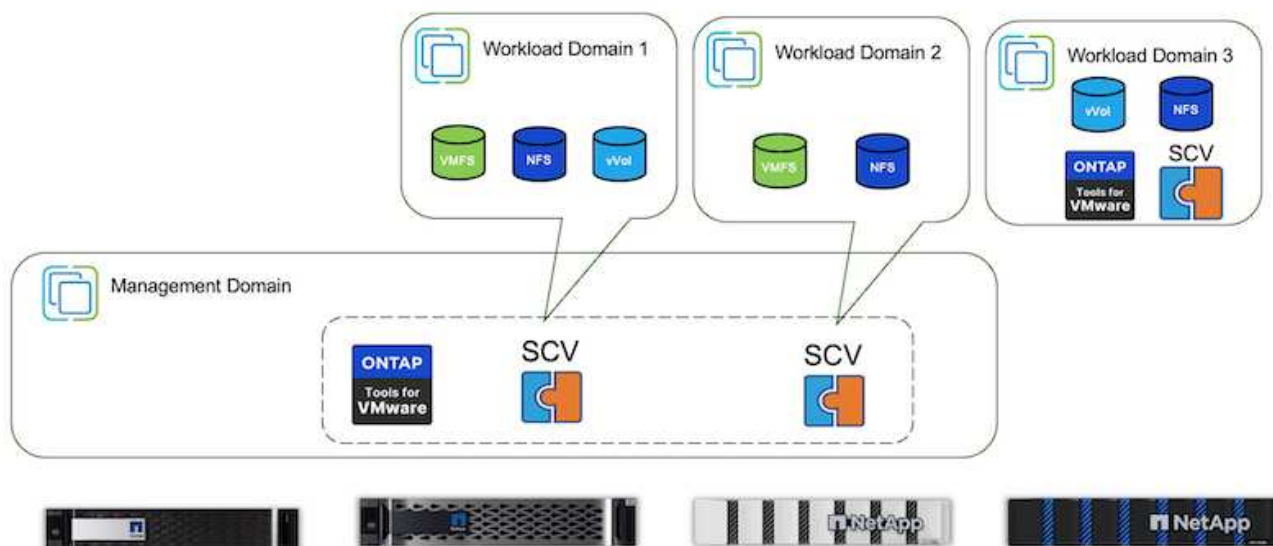
Comme de nombreux clients hébergent leurs serveurs vCenter sur un serveur différent plutôt que de le gérer, une approche similaire est également conseillée pour les outils ONTAP et SCV.



Avec les outils ONTAP 10.x, une seule instance peut gérer plusieurs environnements vCenter. Les systèmes de stockage sont enregistrés globalement avec des informations d'identification du cluster et les SVM sont attribués à chaque serveur vCenter localitaire.



La combinaison de modèles dédiés et partagés est également prise en charge.



Comment démarrer

Si les outils ONTAP ne sont pas installés sur votre environnement, téléchargez-les "[Site de support NetApp](#)" à partir de et suivez les instructions disponibles à l'adresse "[Utilisation de vVols avec ONTAP](#)".

Guide de déploiement pour VMFS

Les solutions et offres de stockage de NetApp permettent aux clients de tirer pleinement parti des avantages d'une infrastructure virtualisée. Grâce aux solutions NetApp, les clients peuvent implémenter efficacement un logiciel complet de gestion des données qui garantit l'automatisation, l'efficacité, la protection des données et la sécurité pour répondre efficacement aux exigences élevées en termes de performances. L'association du logiciel ONTAP à VMware vSphere permet de réduire les frais de licence VMware et le

matériel hôte, de protéger les données à moindre coût et d'offrir des performances élevées et prévisibles.

Introduction

Les charges de travail virtualisées sont mobiles. Par conséquent, les administrateurs utilisent VMware Storage vMotion pour déplacer des machines virtuelles entre des datastores VMware Virtual machine File System (VMFS), NFS ou vVols, tous résidant sur le même système de stockage et explorer ainsi différentes approches de stockage si un système 100 % Flash est utilisé ou si les derniers modèles ASA avec innovation SAN sont utilisés pour une meilleure rentabilité.

Le message clé ici est que la migration vers ONTAP améliore l'expérience client et les performances applicatives tout en offrant la flexibilité nécessaire pour migrer les données et les applications entre FCP, iSCSI, NVMe/FC et NVMe/TCP. Pour les entreprises fortement investies dans VMware vSphere, le stockage ONTAP constitue une option rentable compte tenu des conditions actuelles du marché, qui représente une opportunité unique. Les entreprises doivent répondre à de nouveaux impératifs, simples et rapides, auxquels les approches SAN modernes peuvent répondre. Voici quelques-unes des façons dont les clients NetApp, nouveaux et existants, ajoutent de la valeur à ONTAP.

- Maîtrise des coûts - l'efficacité du stockage intégrée permet à ONTAP de réduire considérablement les coûts de stockage. Les systèmes NetApp ASA peuvent exécuter toutes les fonctionnalités d'efficacité du stockage en production sans affecter les performances. NetApp simplifie la planification de ces avantages avec la meilleure garantie d'efficacité disponible.
- Protection des données : le logiciel SnapCenter qui utilise des snapshots offre une protection avancée des données au niveau des applications et des machines virtuelles pour diverses applications d'entreprise déployées dans une configuration de machines virtuelles.
- Sécurité : utilisez les copies Snapshot pour vous protéger contre les malwares et les ransomwares. Améliorez la protection en rendant les copies Snapshot immuables à l'aide du verrouillage Snapshot et du logiciel NetApp SnapLock®.
- Cloud : ONTAP propose un large éventail d'options de cloud hybride qui permettent aux entreprises de combiner des clouds publics et privés, afin d'offrir plus de flexibilité et de réduire la surcharge administrative liée à l'infrastructure. La prise en charge supplémentaire du datastore basée sur les offres ONTAP permet d'utiliser VMware Cloud sur Azure, AWS et Google pour un déploiement optimisé du coût total de possession, la protection des données et la continuité de l'activité, tout en évitant la dépendance vis-à-vis d'un seul fournisseur.
- Flexibilité - ONTAP est bien équipé pour répondre à l'évolution rapide des besoins des entreprises modernes. Avec ONTAP One, toutes ces fonctionnalités sont fournies en standard avec un système ONTAP sans frais supplémentaires.

Redimensionnez et optimisez

Avec les changements imminents de licence, les entreprises s'attaquent de manière proactive à l'augmentation potentielle du coût total de possession (TCO). Ils optimisent leur infrastructure VMware de manière stratégique grâce à une gestion agressive des ressources et à un dimensionnement adapté afin d'améliorer l'utilisation des ressources et de rationaliser la planification de la capacité. Grâce à une utilisation efficace d'outils spécialisés, les entreprises peuvent identifier et récupérer efficacement les ressources gaspillées, ce qui réduit le nombre de cœurs et les dépenses globales de licence. Il est important de souligner que de nombreuses entreprises intègrent déjà ces pratiques dans leur évaluation du cloud, en démontrant ainsi comment ces processus et outils réduisent efficacement les problèmes de coûts dans les environnements sur site et éliminent les dépenses de migration inutiles vers d'autres hyperviseurs.

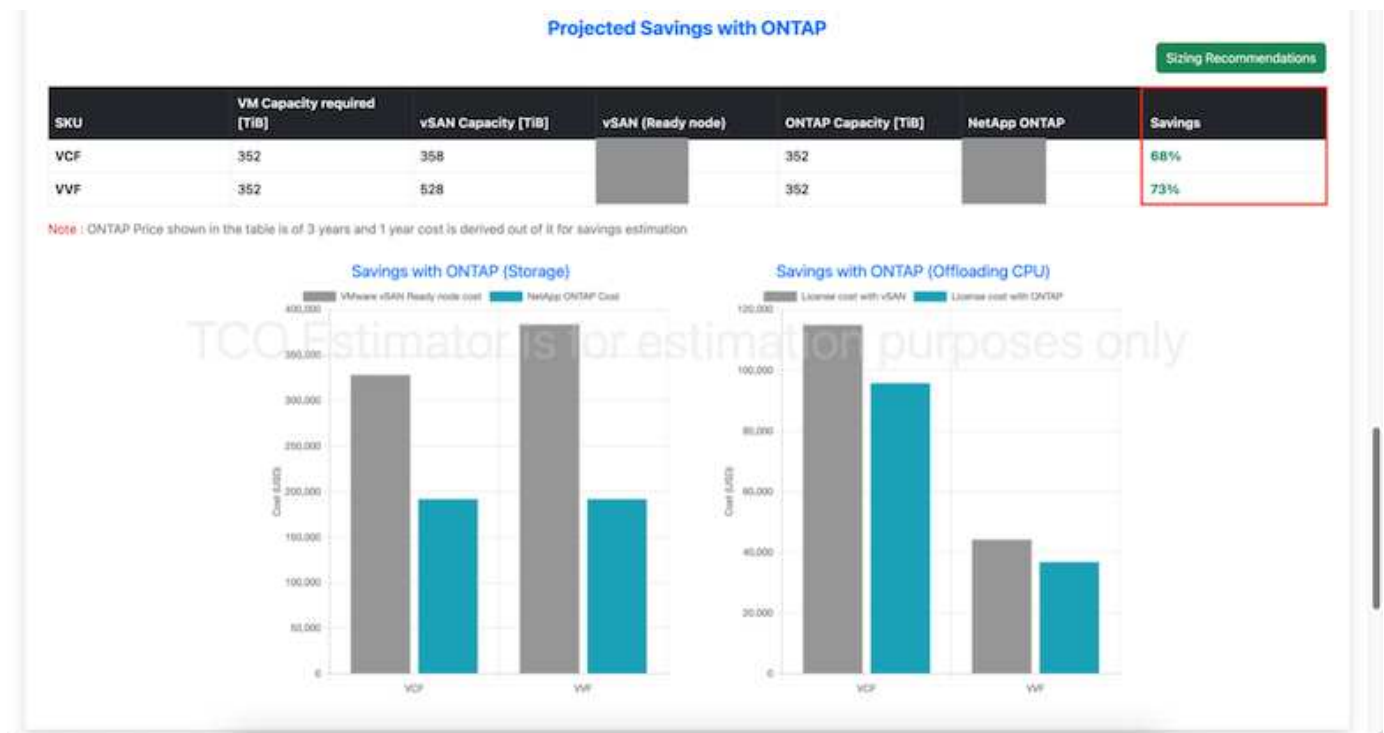
Estimateur du coût total de possession

NetApp a créé un outil simple d'estimation du coût total de possession qui serait le premier pas vers cette optimisation. L'estimateur du coût total de possession utilise des outils RVou des méthodes de saisie manuelles pour déterminer facilement le nombre d'hôtes requis pour le déploiement donné et calculer les économies réalisées afin d'optimiser le déploiement à l'aide des systèmes de stockage NetApp ONTAP. Gardez à l'esprit qu'il s'agit de la marche à suivre.



L'estimateur du coût total de possession n'est accessible qu'aux équipes de terrain et aux partenaires de NetApp. Évaluez votre environnement existant avec les équipes de gestion de compte NetApp.

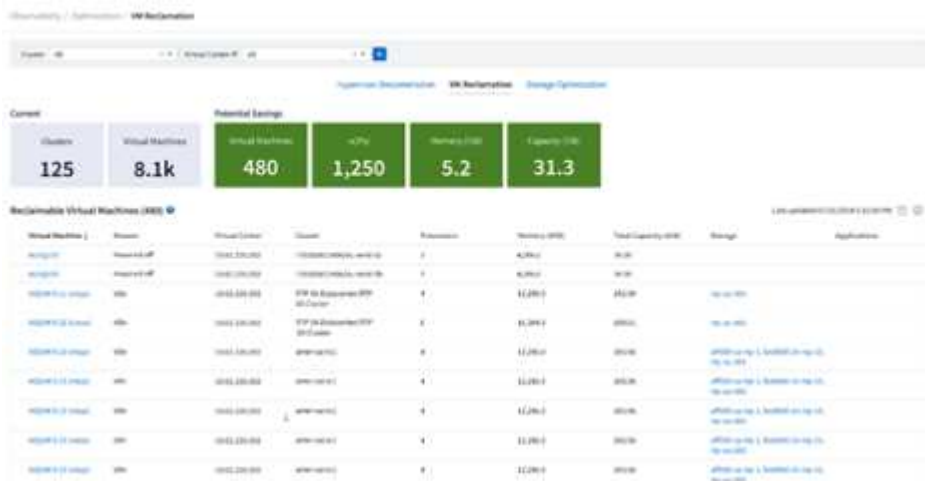
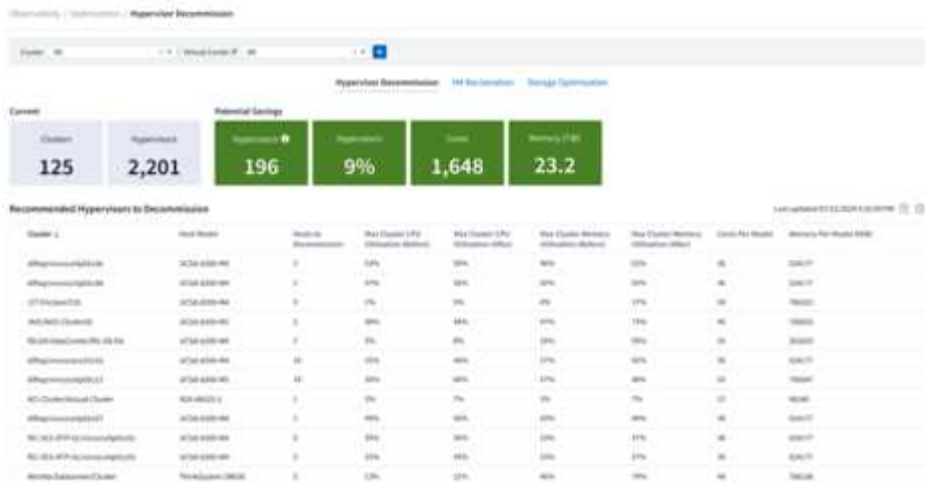
Voici une capture d'écran de l'estimateur du coût total de possession.



Cloud Insights

Une fois que l'estimateur montre les économies possibles (qui seront le cas pour une entreprise donnée), il est temps d'étudier en profondeur les profils d'E/S de workload sur des machines virtuelles à l'aide de metrics en temps réel. Pour cela, NetApp fournit Cloud Insights. En fournissant des analyses détaillées et des recommandations pour la récupération de machines virtuelles, Cloud Insights aide les entreprises à prendre des décisions éclairées concernant l'optimisation de leur environnement de machines virtuelles. Il permet d'identifier les emplacements où les ressources peuvent être récupérées ou désaffectées des hôtes avec un impact minimal sur la production, ce qui aide les entreprises à gérer les changements apportés par l'acquisition de VMware par Broadcom, de manière réfléchie et stratégique. En d'autres termes, Cloud Insight aide les entreprises à se sortir des émotions de la décision. Au lieu de réagir avec panique ou frustration aux changements, ils peuvent utiliser les informations fournies par l'outil Cloud Insights pour prendre des décisions stratégiques rationnelles qui équilibrent l'optimisation des coûts avec l'efficacité opérationnelle et la productivité.

Vous trouverez ci-dessous les captures d'écran de Cloud Insights.



Réalisez des évaluations régulières afin d'identifier les ressources sous-utilisées, d'augmenter la densité des machines virtuelles et d'optimiser l'utilisation au sein des clusters VMware, afin de contrôler la hausse des coûts associés aux nouvelles licences d'abonnement. Pensez à réduire le nombre de cœurs par processeur à 16 pour l'achat de nouveaux serveurs, en adéquation avec les modifications des modèles de licence VMware.

Avec NetApp, dimensionnez correctement vos environnements virtualisés et bénéficiez de performances de stockage Flash économiques, ainsi que de solutions simplifiées de gestion des données et de protection contre les ransomwares. Les entreprises sont ainsi prêtes à adopter un nouveau modèle par abonnement tout en optimisant les ressources INFORMATIQUES existantes.

Outils NetApp ONTAP pour VMware vSphere

Pour améliorer et simplifier davantage l'intégration avec VMware, NetApp propose plusieurs outils OFFTAP qui peuvent être utilisés avec NetApp ONTAP et VMware vSphere pour gérer efficacement les environnements virtualisés. Cette section se concentre sur les outils ONTAP pour VMware. Les outils ONTAP pour VMware vSphere 10 offrent un ensemble complet d'outils pour la gestion du cycle de vie des machines virtuelles, ce qui simplifie la gestion du stockage, améliore les fonctionnalités d'efficacité, améliore la disponibilité et réduit les coûts de stockage et les charges opérationnelles. Ces outils s'intègrent en toute transparence à l'écosystème VMware, ce qui facilite le provisionnement des datastores et offre une protection de base pour les machines virtuelles. La version 10.x des outils ONTAP pour VMware vSphere comprend des microservices évolutifs horizontalement, pilotés par les événements déployés en tant qu'appliance virtuelle ouverte (OVA). Elle suit les bonnes pratiques de provisionnement des datastores et d'optimisation des paramètres d'hôte ESXi pour les

environnements de stockage en mode bloc et NFS. Compte tenu de ces avantages, OTV est recommandé comme meilleure pratique à utiliser avec les systèmes exécutant le logiciel ONTAP.

Mise en route

Avant de déployer et de configurer les outils ONTAP pour VMware, assurez-vous que les conditions préalables sont remplies. Ensuite, déployez une configuration à un seul nœud.



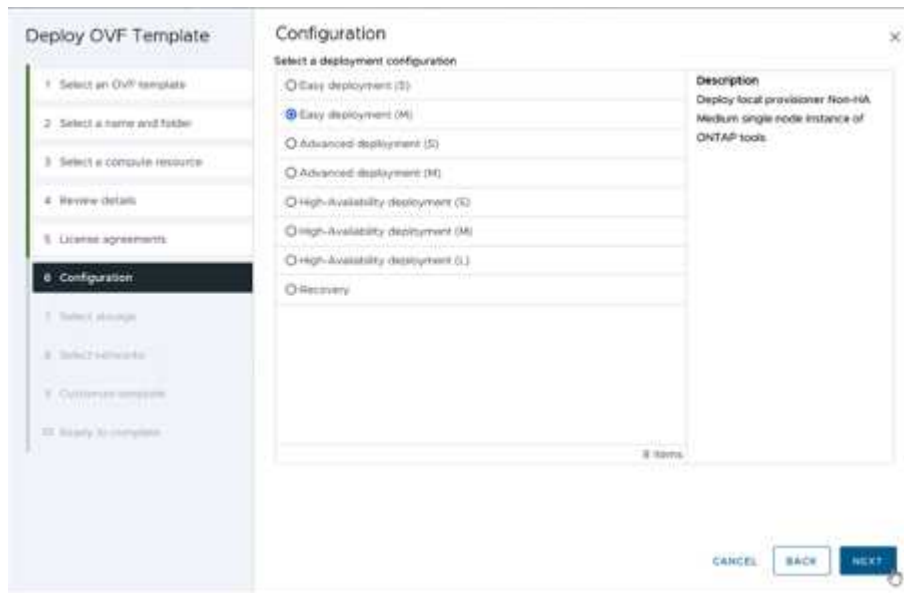
Trois adresses IP sont requises pour le déploiement : une adresse IP pour l'équilibreur de charge, une adresse IP pour le plan de contrôle Kubernetes et une autre pour le nœud.

Étapes

1. Connectez-vous au serveur vSphere.
2. Accédez au cluster ou à l'hôte sur lequel vous souhaitez déployer l'OVA.
3. Cliquez avec le bouton droit de la souris sur l'emplacement requis et sélectionnez déployer le modèle OVF.
 - a. Entrez l'URL du fichier .ova ou naviguez jusqu'au dossier dans lequel le fichier .ova est enregistré, puis sélectionnez Suivant.
4. Sélectionnez un nom, un dossier, un cluster ou un hôte pour la machine virtuelle et sélectionnez Suivant.
5. Dans la fenêtre Configuration, sélectionnez Easy deployment(S), Easy deployment(M), Advanced deployment(S) ou Advanced deployment(M).



L'option de déploiement facile est utilisée dans cette présentation.



6. Choisissez le datastore pour déployer l'OVA ainsi que le réseau source et de destination. Une fois l'opération terminée, sélectionnez Suivant.
7. Il est temps de personnaliser le modèle > fenêtre de configuration du système.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Customize template

| | | | | | | | |
|-------------------------------------|---|----------|-------|---|------------------|-------|---|
| Administrator username(*) | Username to assign to the Administrator. Please use only a letter as the beginning. And only [a-z, 0-9, -, _] special characters are supported. <input type="text" value="admin"/> | | | | | | |
| Administrator password(*) | Password to assign to the Administrator | | | | | | |
| | <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Password</td> <td style="border: 1px solid #ccc; padding: 2px;">*****</td> <td style="text-align: right; width: 10px;">👁</td> </tr> <tr> <td>Confirm Password</td> <td style="border: 1px solid #ccc; padding: 2px;">*****</td> <td style="text-align: right;">👁</td> </tr> </table> | Password | ***** | 👁 | Confirm Password | ***** | 👁 |
| Password | ***** | 👁 | | | | | |
| Confirm Password | ***** | 👁 | | | | | |
| NTP servers | A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware Tools based time synchronization will be used. <input type="text" value="172.21.166.1"/> | | | | | | |
| Maintenance user password(*) | Password to assign to maint user account | | | | | | |
| | <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">Password</td> <td style="border: 1px solid #ccc; padding: 2px;">*****</td> <td style="text-align: right; width: 10px;">👁</td> </tr> <tr> <td>Confirm Password</td> <td style="border: 1px solid #ccc; padding: 2px;">*****</td> <td style="text-align: right;">👁</td> </tr> </table> | Password | ***** | 👁 | Confirm Password | ***** | 👁 |
| Password | ***** | 👁 | | | | | |
| Confirm Password | ***** | 👁 | | | | | |

CANCEL
BACK
NEXT

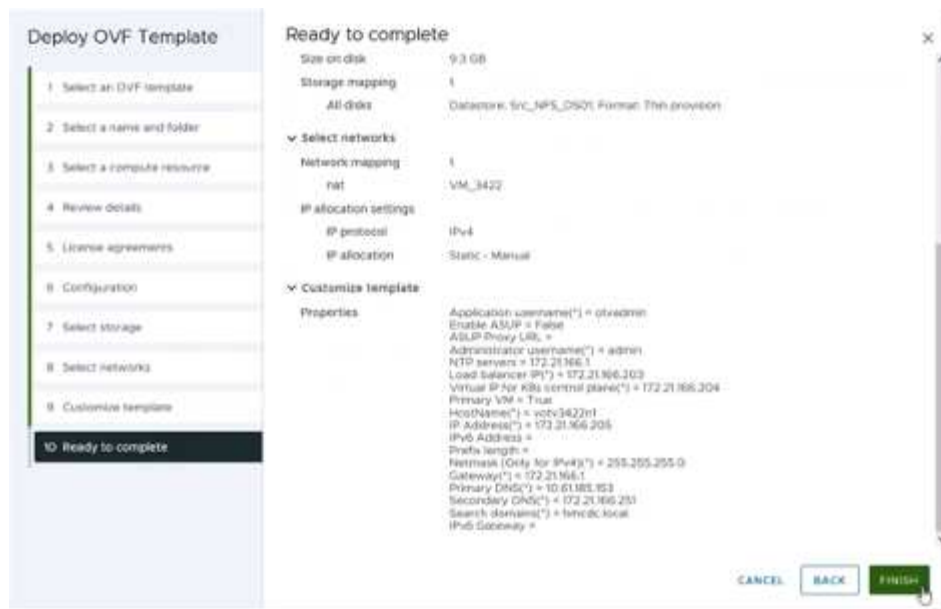
Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

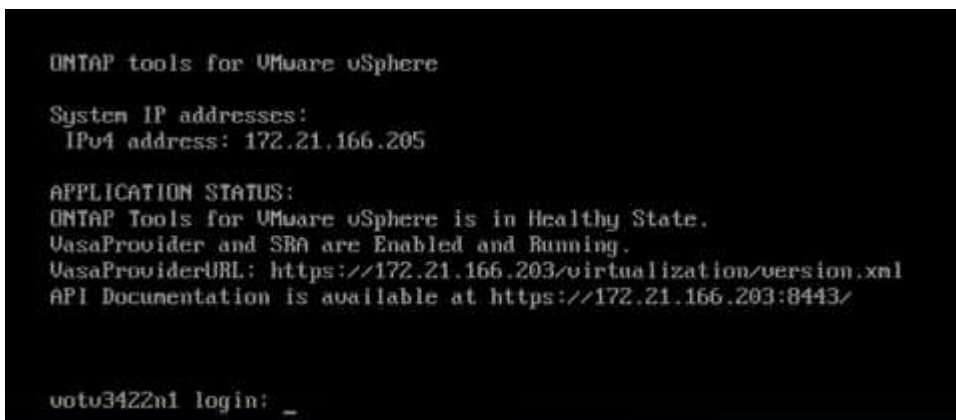
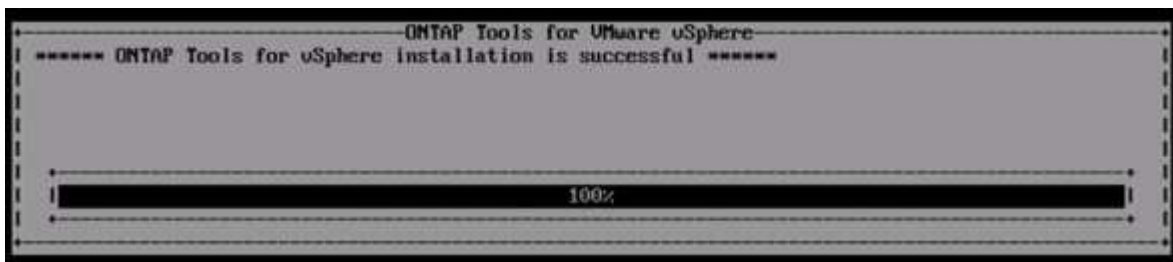
Customize template

| | |
|--|--|
| Deployment Configuration 3 settings | |
| Load balancer IP(*) | Load balancer IP (*) <input type="text" value="172.21.166.203"/> |
| Virtual IP for K8s control plane(*) | Provides the virtual IP address for K8s control plane. <input type="text" value="172.21.166.204"/> |
| Primary VM | Maintain this field as selected to set the current VM as primary and install the ONTAP tools. <input checked="" type="checkbox"/> |
| Node Configuration 10 settings | |
| HostName(*) | Specify the hostname for the VM. <input type="text" value="vst-0422r1"/> |
| IP Address(*) | Specify the IP address for the appliance. <input type="text" value="172.21.166.205"/> |
| IPv6 Address | Specify the IPv6 address on the deployed network only when you need dual stack. <input type="text"/> |
| Prefix length | Specify the prefix length. <input type="text"/> |

CANCEL
BACK
NEXT



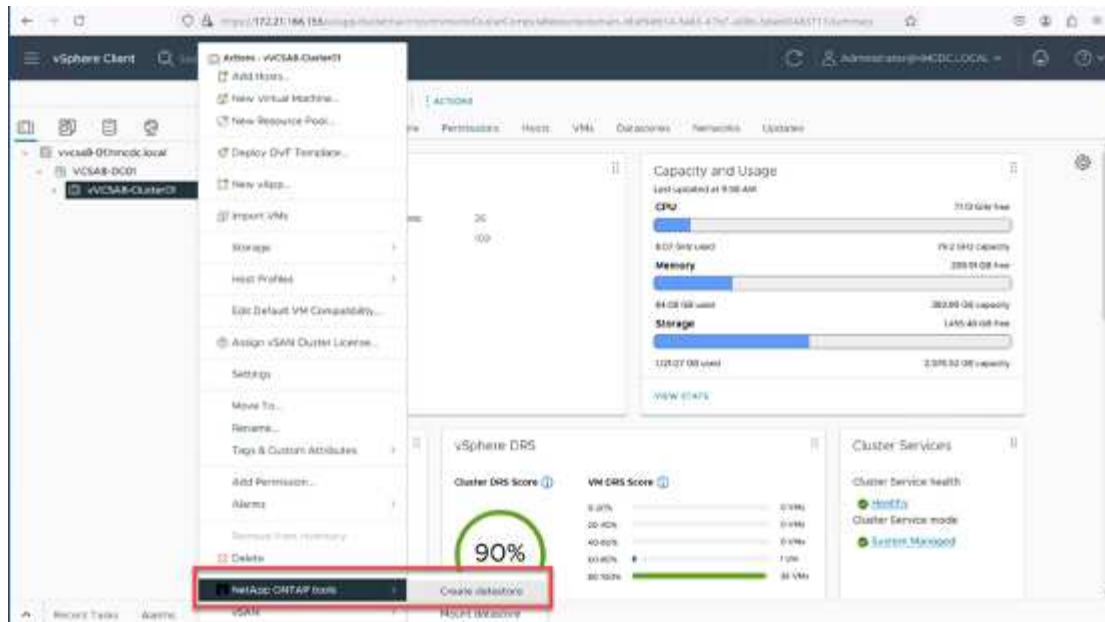
Une fois l'installation terminée, la console Web affiche l'état des outils ONTAP pour VMware vSphere.



L'assistant de création de datastores prend en charge le provisionnement des datastores VMFS, NFS et vVols.

Il est temps de provisionner des datastores VMFS basés sur iSCSI pour cette présentation.

1. Connectez-vous au client vSphere à l'aide de <https://vcenterip/ui>
2. Cliquez avec le bouton droit de la souris sur un hôte, un cluster hôte ou un datastore, puis sélectionnez Outils NetApp ONTAP > Créer un datastore.



3. Dans le volet Type, sélectionnez VMFS dans Type de datastore.



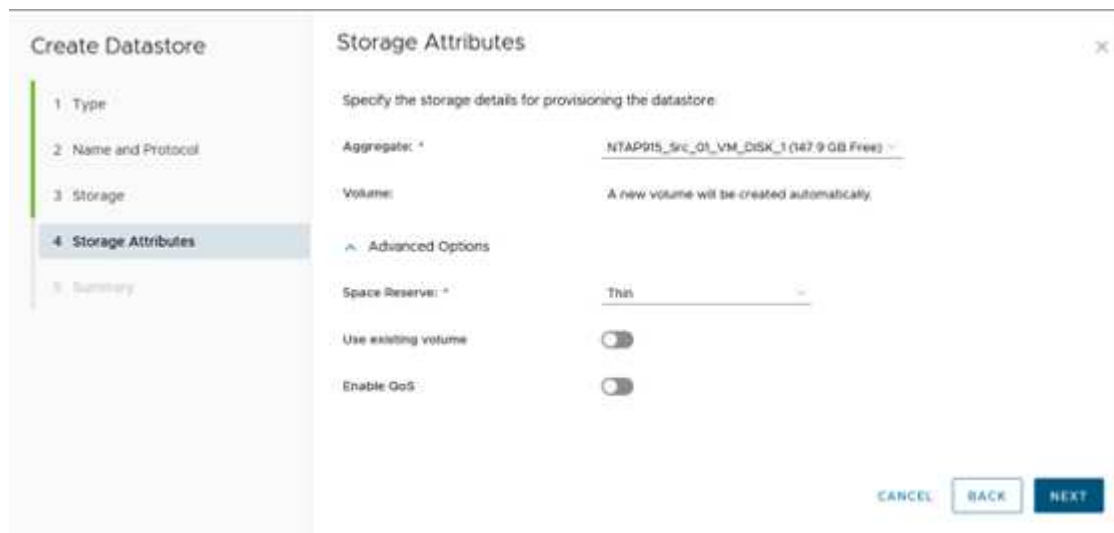
4. Dans le volet Nom et Protocole, entrez le nom, la taille et les informations de protocole du datastore. Dans la section Options avancées du volet, sélectionnez le cluster datastore si vous souhaitez ajouter ce datastore à.



5. Sélectionnez plate-forme et VM de stockage dans le volet stockage. Indiquez le nom du groupe initiateur personnalisé dans la section Options avancées du volet (facultatif). Vous pouvez choisir un groupe initiateur existant pour le datastore ou créer un nouveau groupe initiateur avec un nom personnalisé.



6. Dans le volet Storage Attributes, sélectionnez Aggregate dans le menu déroulant. Sélectionnez les options de réserve d'espace, de volume et d'activation de la qualité de service, selon les besoins, dans la section Options avancées.



7. Vérifiez les détails du datastore dans le volet Résumé et cliquez sur Terminer. Le datastore VMFS est créé et monté sur tous les hôtes.



Reportez-vous à ces liens pour le provisionnement des datastores vVol, FC, NVMe/TCP.

Déchargement VAAI

Les primitives VAAI sont utilisées dans les opérations vSphere de routine, telles que la création, le clonage, la migration, le démarrage et l'arrêt des machines virtuelles. Ces opérations peuvent être exécutées via le client vSphere pour plus de simplicité, ou à partir de la ligne de commande pour la création de scripts ou pour une synchronisation plus précise. VAAI pour SAN est pris en charge de manière native par ESX. VAAI est toujours activé sur les systèmes de stockage NetApp pris en charge et fournit un support natif pour les opérations VAAI suivantes sur des systèmes de stockage SAN :

- Copie auxiliaire
- Verrouillage de l'essai atomique et du réglage (ATS)
- Écrire de même
- Gestion des conditions de manque d'espace
- Réclamations d'espace

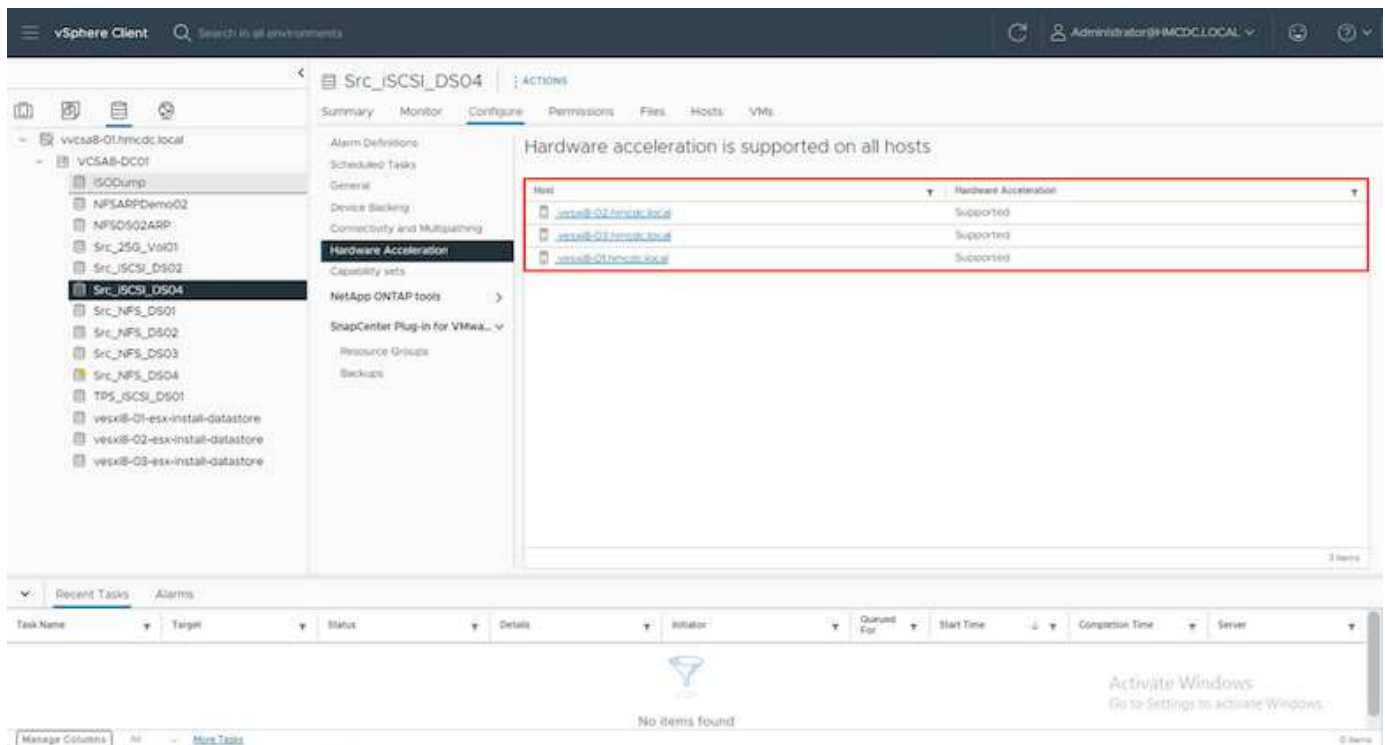
```
[root@vesxi8-02:~] esxcli storage core device vaa1 status get -d=naa.600a09805a506576495d576a57553455
naa.600a09805a506576495d576a57553455
VAAI Plugin Name: VMW_VAAIP_NETAPP
ATS Status: supported
Clone Status: supported
Zero Status: supported
Delete Status: supported
```



Vérifiez que HardwareAcceleratedMove est activé via les options de configuration avancée ESX.



Vérifiez que l'allocation d'espace est activée sur la LUN. Si cette option n'est pas activée, activez-la et relancez la recherche de tous les HBA.





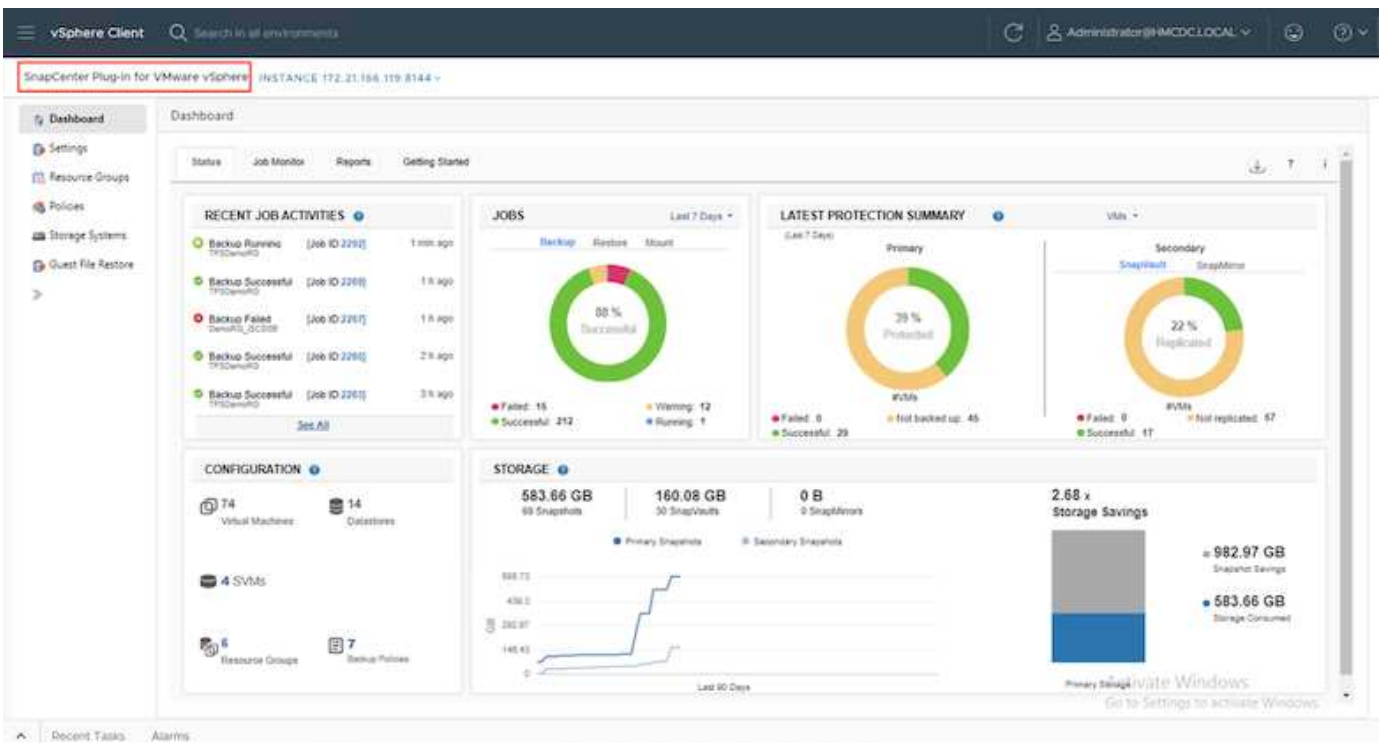
Ces valeurs sont aisément définies avec les outils ONTAP pour VMware vSphere. Dans le tableau de bord Présentation, accédez à la carte de conformité de l'hôte ESXi et sélectionnez l'option appliquer les paramètres recommandés. Dans la fenêtre appliquer les paramètres d'hôte recommandés, sélectionnez les hôtes et cliquez sur Suivant pour appliquer les paramètres d'hôte recommandés par NetApp.



Afficher des conseils détaillés pour "[Hôte ESXi recommandé et autres paramètres ONTAP recommandés](#)".

La protection des données

ONTAP pour vSphere présente des avantages clés : sauvegarde efficace des machines virtuelles sur un datastore VMFS et restauration rapide de ces machines. En s'intégrant à vCenter, le logiciel NetApp SnapCenter® offre un large éventail de fonctionnalités de sauvegarde et de restauration pour les machines virtuelles. Cette solution permet des opérations de sauvegarde et de restauration rapides, compactes, cohérentes après panne et cohérentes avec les machines virtuelles pour les machines virtuelles, les datastores et les VMDK. Il fonctionne également avec SnapCenter Server pour prendre en charge les opérations de sauvegarde et de restauration basées sur les applications dans les environnements VMware à l'aide de plug-ins spécifiques aux applications SnapCenter. L'exploitation des copies Snapshot permet de réaliser des copies rapides de la machine virtuelle ou du datastore sans aucun impact sur les performances et d'utiliser la technologie NetApp SnapMirror® ou NetApp SnapVault® pour la protection des données hors site à long terme.



Le flux de travail est simple. Ajout de systèmes de stockage primaire et de SVM (et secondaire si SnapMirror/SnapVault est requis)

Étapes générales de déploiement et de configuration :

1. Téléchargez le plug-in OVA SnapCenter pour VMware
2. Connectez-vous avec les informations d'identification du client vSphere
3. Déployez le modèle OVF pour démarrer l'assistant de déploiement VMware et terminer l'installation
4. Pour accéder au plug-in, sélectionnez SnapCenter Plug-in for VMware vSphere dans le menu
5. Ajouter un stockage
6. Création de règles de sauvegarde
7. Créer des groupes de ressources
8. Groupes de ressources de sauvegarde
9. Restaurer une machine virtuelle entière ou un disque virtuel particulier

Configuration du plug-in SnapCenter pour VMware pour les machines virtuelles

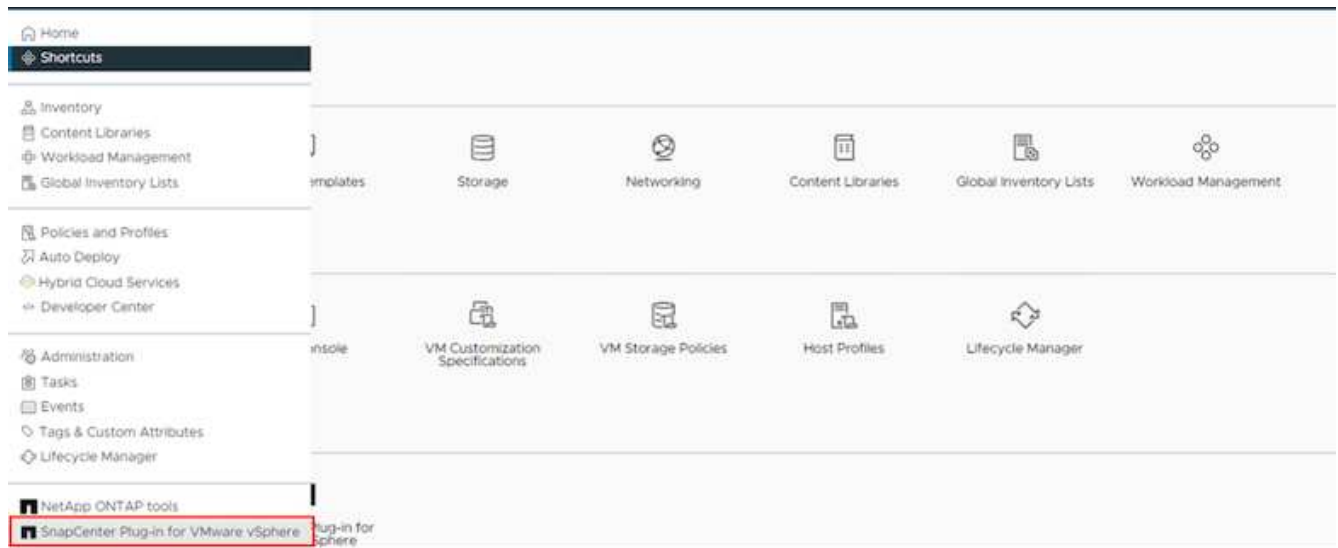
Pour protéger les machines virtuelles et les datastores iSCSI qui les hébergent, le plug-in SnapCenter pour VMware doit être déployé. Il s'agit d'une simple importation OVF.

La procédure de déploiement est la suivante :

1. Téléchargez l'appliance virtuelle ouverte (OVA) sur le site du support NetApp.
2. Connectez-vous au vCenter.
3. Dans vCenter, cliquez avec le bouton droit de la souris sur un objet d'inventaire tel qu'un data Center, un dossier, un cluster ou un hôte, puis sélectionnez déployer le modèle OVF.
4. Sélectionnez les paramètres appropriés, y compris le stockage et le réseau, et personnalisez le modèle pour mettre à jour vCenter et ses informations d'identification. Une fois la révision effectuée, cliquez sur Terminer.
5. Attendez que les tâches d'importation et de déploiement OVF soient terminées.
6. Une fois le déploiement du plug-in SnapCenter pour VMware réussi, il sera enregistré dans vCenter. Il est possible de vérifier la même chose en accédant à Administration > Plugins client



7. Pour accéder au plug-in, accédez au panneau latéral gauche de la page du client Web vCenter, puis sélectionnez SnapCenter Plug-in for VMware.



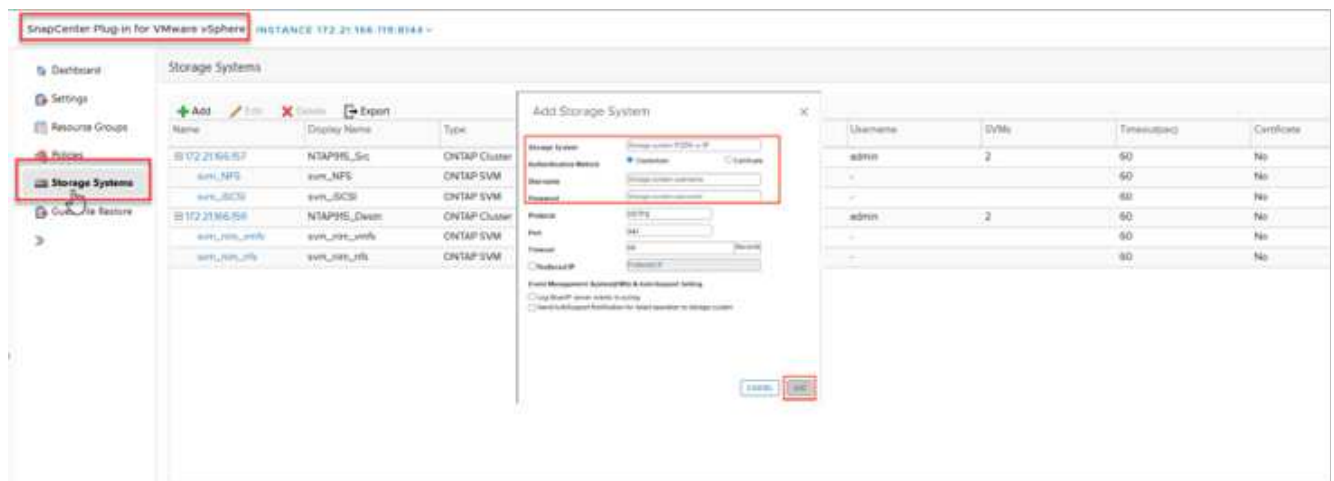
Ajoutez du stockage, créez des règles et un groupe de ressources

Ajout d'un système de stockage

L'étape suivante consiste à ajouter le système de stockage. Le terminal de gestion du cluster ou l'IP du terminal d'administration des machines virtuelles de stockage (SVM) doit être ajouté en tant que système de stockage pour sauvegarder ou restaurer des VM. L'ajout de stockage permet au plug-in SnapCenter pour VMware de reconnaître et de gérer les opérations de sauvegarde et de restauration dans vCenter.

Le processus est tout droit.

1. Dans le menu de navigation de gauche, sélectionnez SnapCenter Plug-in for VMware.
2. Sélectionnez Storage Systems.
3. Sélectionnez Add pour ajouter les détails du « stockage ».
4. Utilisez les informations d'identification comme méthode d'authentification, saisissez le nom d'utilisateur et son mot de passe, puis cliquez sur Ajouter pour enregistrer les paramètres.





Création d'une règle de sauvegarde

Une stratégie de sauvegarde complète comprend des facteurs tels que le moment, le type de sauvegarde et la durée de conservation des sauvegardes. Vous pouvez tenir les snapshots toutes les heures ou tous les jours pour sauvegarder des datastores entiers. Cette approche capture non seulement les datastores, mais permet également de sauvegarder et de restaurer les machines virtuelles et les VMDK dans ces magasins de données.

Avant de sauvegarder les machines virtuelles et les datastores, une stratégie de sauvegarde et un groupe de ressources doivent être créés. Une règle de sauvegarde inclut des paramètres tels que la planification et la stratégie de conservation. Pour créer une stratégie de sauvegarde, procédez comme suit :

1. Dans le volet gauche du navigateur du plug-in SnapCenter pour VMware, cliquez sur stratégies.
2. Sur la page stratégies, cliquez sur Créer pour démarrer l'assistant.



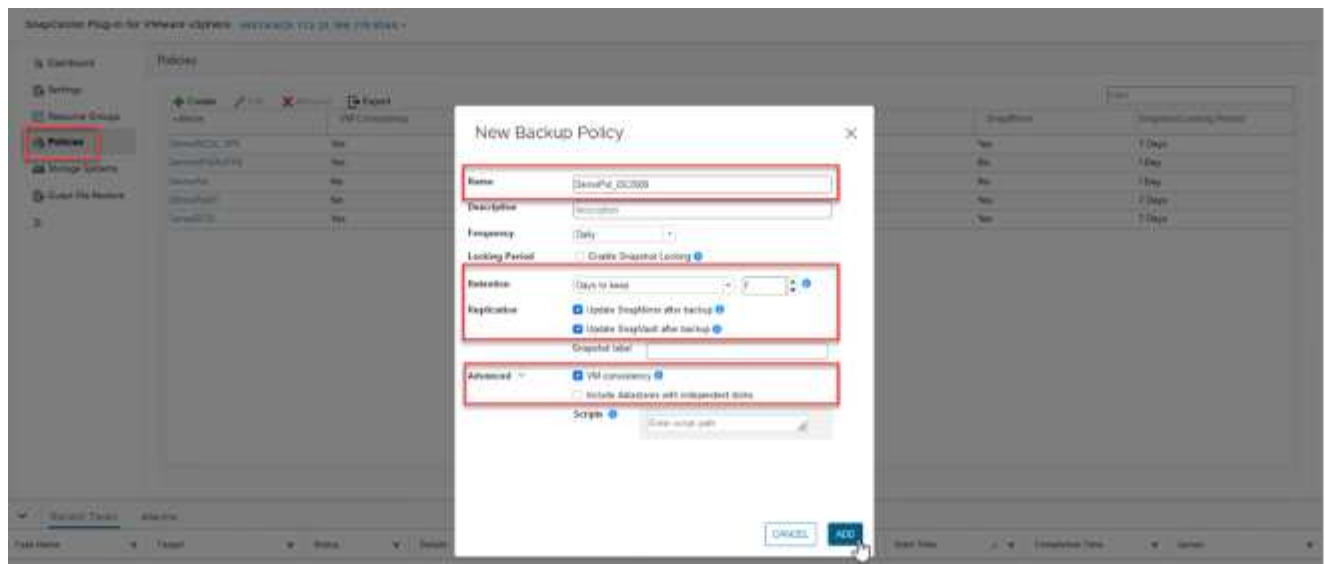
3. Sur la page Nouvelle stratégie de sauvegarde, entrez le nom de la stratégie.
4. Spécifiez la rétention, les paramètres de fréquence et la réplication.



Pour répliquer des copies Snapshot sur un système de stockage secondaire mis en miroir ou vault, les relations doivent être configurées au préalable.



Pour permettre des sauvegardes cohérentes avec les machines virtuelles, les outils VMware doivent être installés et exécutés. Lorsque la case de cohérence des machines virtuelles est cochée, les machines virtuelles sont d'abord suspendues. VMware effectue alors un snapshot cohérent des machines virtuelles (à l'exception de la mémoire), puis le plug-in SnapCenter pour VMware effectue son opération de sauvegarde, puis les opérations des machines virtuelles sont reprises.



Une fois la règle créée, l'étape suivante consiste à créer le groupe de ressources qui définira les datastores iSCSI et les machines virtuelles appropriés à sauvegarder. Une fois le groupe de ressources créé, il est temps d déclencher des sauvegardes.

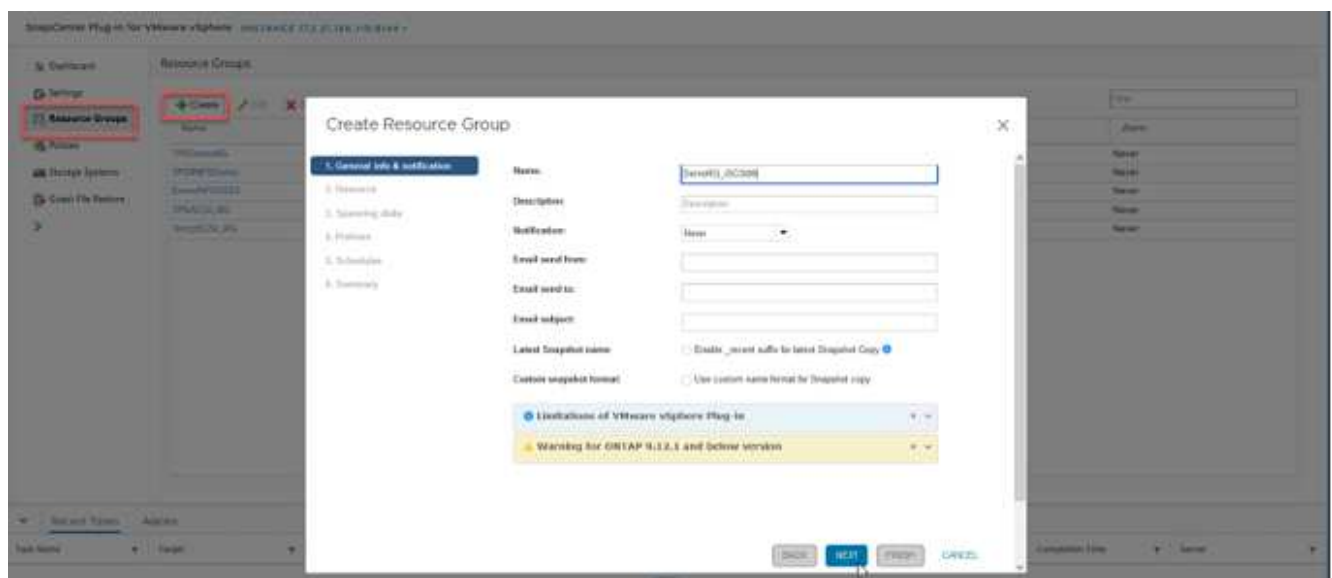
Créer un groupe de ressources

Un groupe de ressources est le conteneur pour les VM et les datastores qui doivent être protégés. Les ressources peuvent être ajoutées ou supprimées aux groupes de ressources à tout moment.

Suivez les étapes ci-dessous pour créer un groupe de ressources.

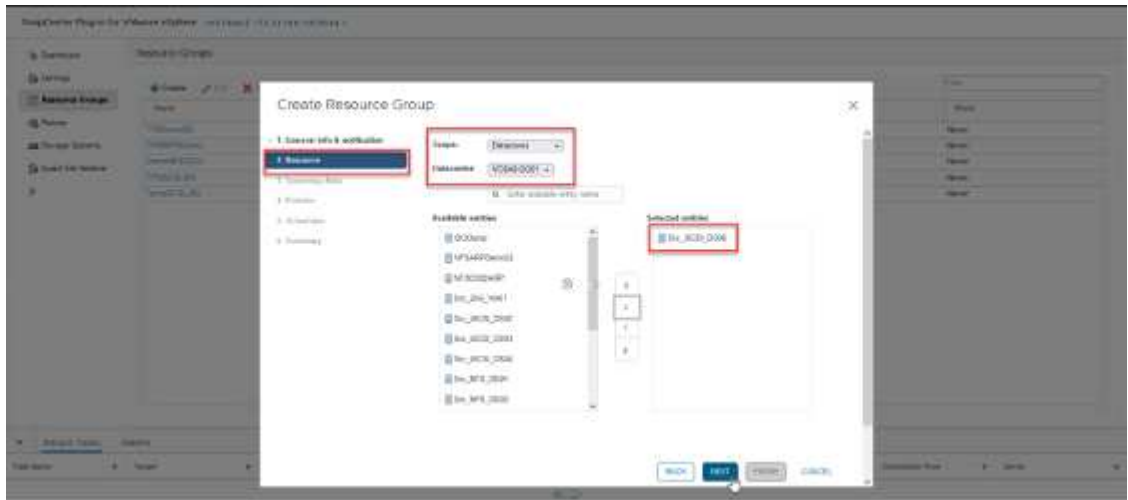
1. Dans le volet gauche du navigateur du plug-in SnapCenter pour VMware, cliquez sur groupes de ressources.
2. Sur la page groupes de ressources, cliquez sur Créer pour démarrer l'assistant.

Une autre option pour créer un groupe de ressources consiste à sélectionner la machine virtuelle ou le datastore individuel et à créer un groupe de ressources respectivement.

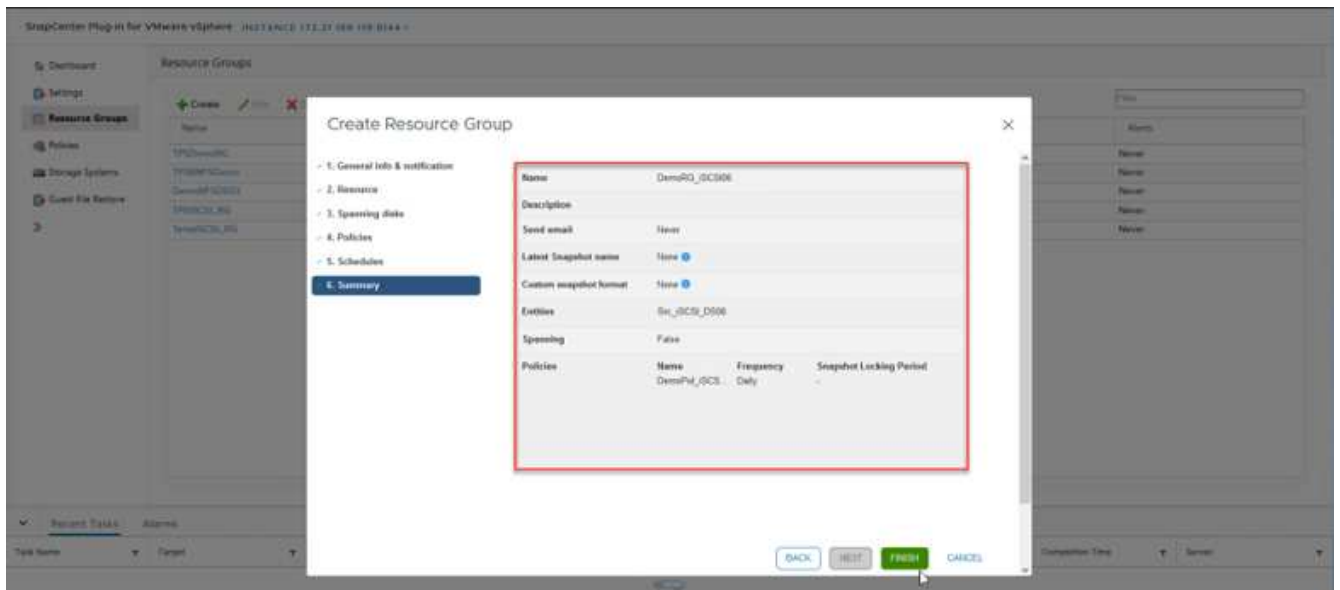


3. Sur la page Resources (Ressources), sélectionnez la portée (machines virtuelles ou datastores) et le

datacenter.

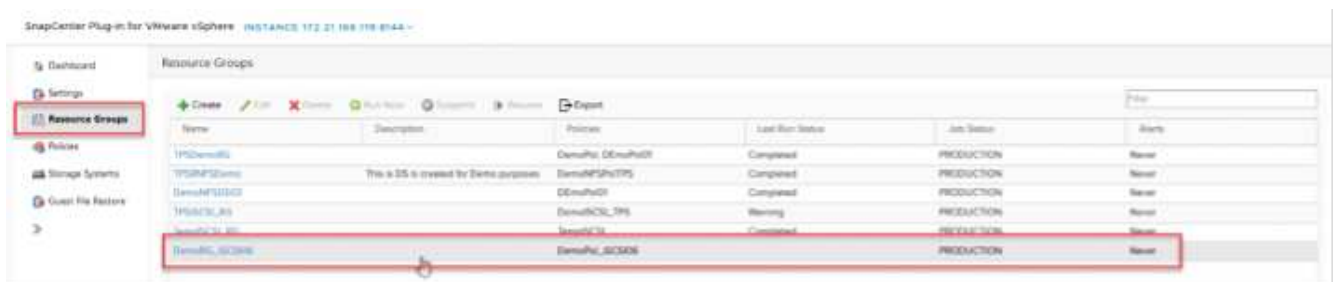


4. Sur la page Spanning Disks (Spanning Disks), sélectionnez une option pour les machines virtuelles avec plusieurs VMDK sur plusieurs datastores
5. L'étape suivante consiste à associer une stratégie de sauvegarde. Sélectionnez une règle existante ou créez une nouvelle règle de sauvegarde.
6. Sur la page plannings, configurez le planning de sauvegarde pour chaque stratégie sélectionnée.



7. Une fois les sélections appropriées effectuées, cliquez sur Terminer.

Cela va créer un nouveau groupe de ressources et l'ajouter à la liste des groupes de ressources.



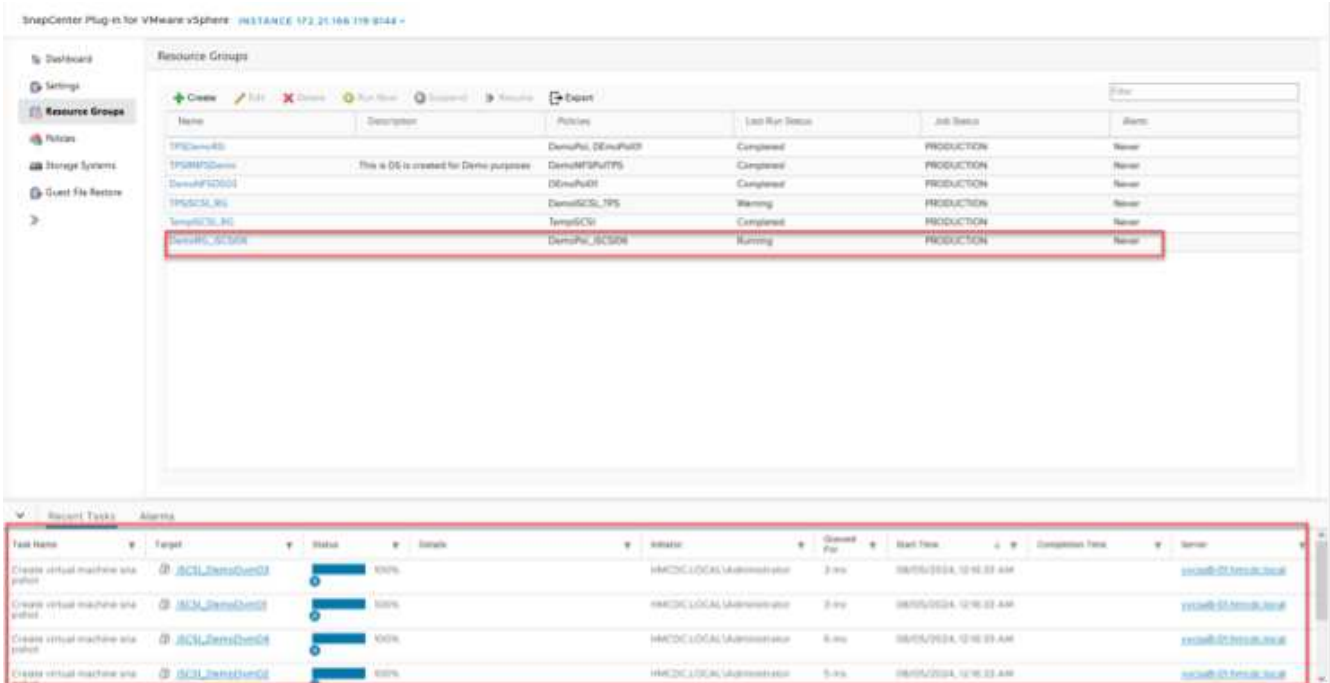
Sauvegarder les groupes de ressources

Il est maintenant temps de déclencher une sauvegarde. Les opérations de sauvegarde sont effectuées sur toutes les ressources définies dans un groupe de ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont effectuées automatiquement en fonction de la planification.

1. Dans le menu de navigation de gauche de la page du client Web vCenter, sélectionnez SnapCenter Plug-in pour VMware > groupes de ressources, puis sélectionnez le groupe de ressources désigné. Sélectionnez Exécuter maintenant pour lancer la sauvegarde ad hoc.



2. Si plusieurs stratégies sont configurées pour le groupe de ressources, sélectionnez la stratégie pour l'opération de sauvegarde dans la boîte de dialogue Sauvegarder maintenant.
3. Sélectionnez OK pour lancer la sauvegarde.



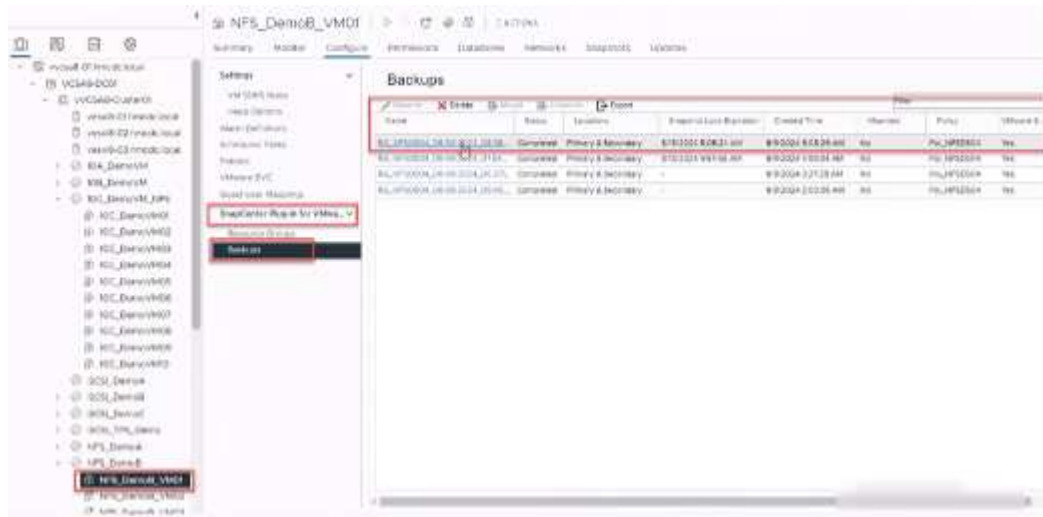
Surveillez la progression de l'opération en sélectionnant tâches récentes en bas de la fenêtre ou sur le moniteur des tâches du tableau de bord pour plus de détails.

Restaurer les machines virtuelles à partir de la sauvegarde

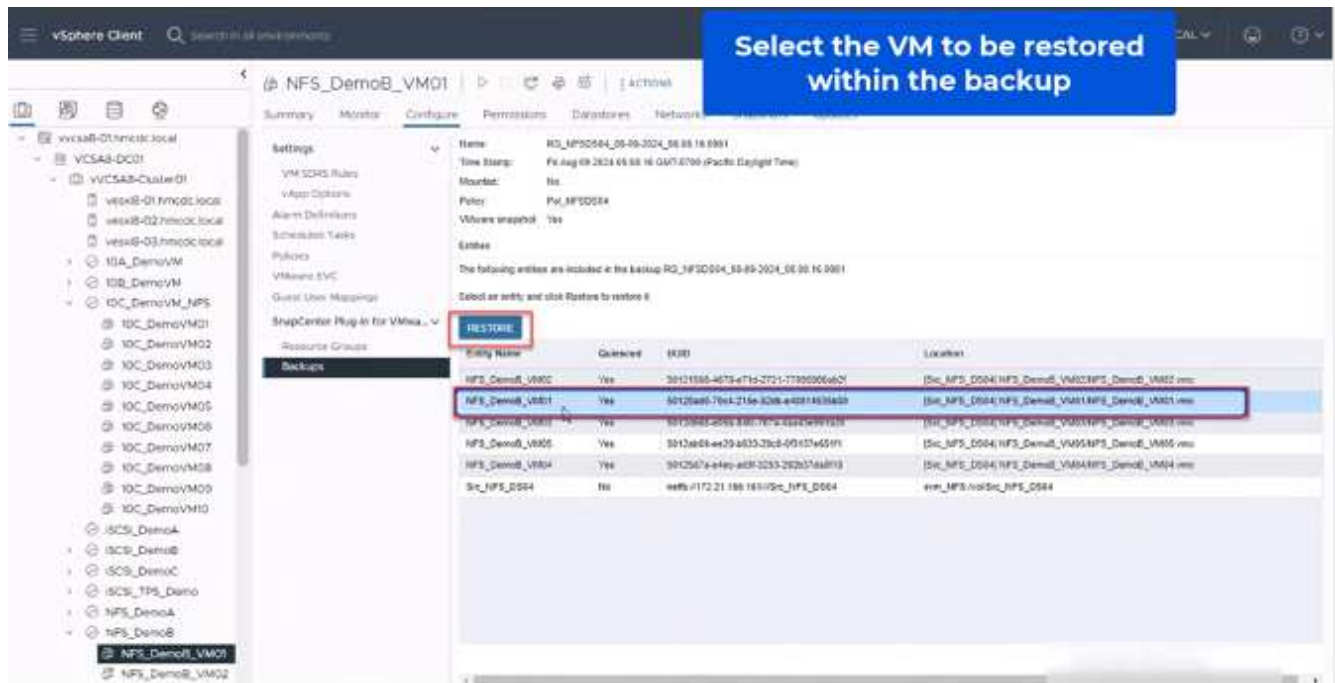
Le plug-in SnapCenter pour VMware permet de restaurer des machines virtuelles dans vCenter. Lors de la restauration d'une machine virtuelle, elle peut être restaurée sur le datastore d'origine monté sur l'hôte ESXi d'origine. Le contenu existant sera remplacé par la copie de sauvegarde sélectionnée ou une machine virtuelle supprimée/renommée peut être restaurée à partir d'une copie de sauvegarde (l'opération écrase les données).

dans les disques virtuels d'origine). Pour effectuer une restauration, procédez comme suit :

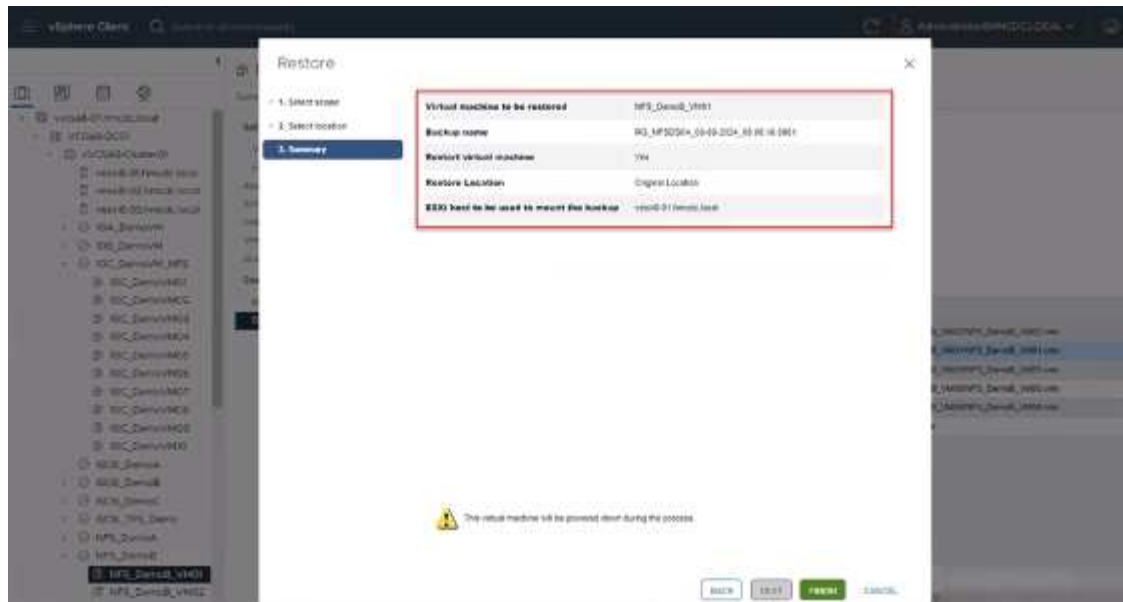
1. Dans l'interface graphique du client Web VMware vSphere, sélectionnez Menu dans la barre d'outils. Sélectionnez Inventaire, puis machines virtuelles et modèles.
2. Dans le menu de navigation de gauche, sélectionnez la machine virtuelle, puis l'onglet configurer, sélectionnez sauvegardes sous SnapCenter Plug-in for VMware. Cliquez sur la procédure de sauvegarde à partir de laquelle la machine virtuelle doit être restaurée.



3. Sélectionnez la machine virtuelle à restaurer à partir de la sauvegarde.



4. Sur la page Select Scope, sélectionnez l'intégralité de l'ordinateur virtuel dans le champ Restore Scope, sélectionnez Restore location, puis entrez les informations ESXi de destination sur lesquelles la sauvegarde doit être montée. Cochez la case redémarrer VM si la machine virtuelle doit être mise sous tension après l'opération de restauration.

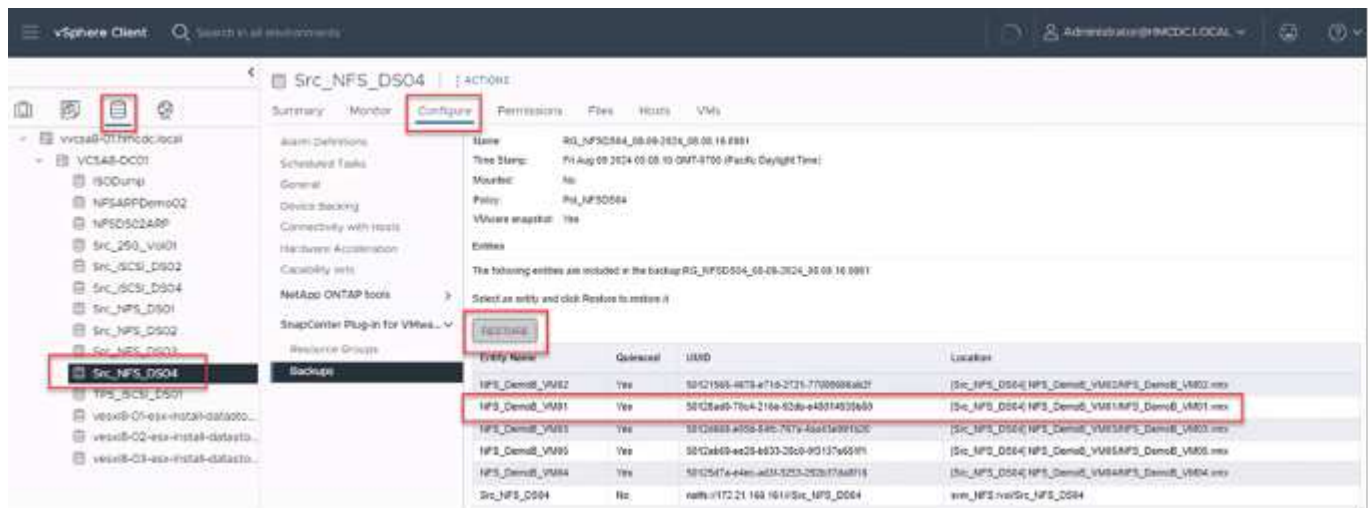


Surveillez la progression de l'opération en sélectionnant tâches récentes au bas de l'écran.



Bien que les machines virtuelles soient restaurées, elles ne sont pas automatiquement ajoutées à leurs anciens groupes de ressources. Par conséquent, ajoutez manuellement les machines virtuelles restaurées aux groupes de ressources appropriés si la protection de ces machines virtuelles est requise.

Que se passe-t-il si la machine virtuelle d'origine a été supprimée ? La tâche est simple grâce au plug-in SnapCenter pour VMware. L'opération de restauration d'une machine virtuelle supprimée peut être effectuée au niveau du datastore respectif > configurer > sauvegardes, sélectionnez la machine virtuelle supprimée et sélectionnez Restaurer.

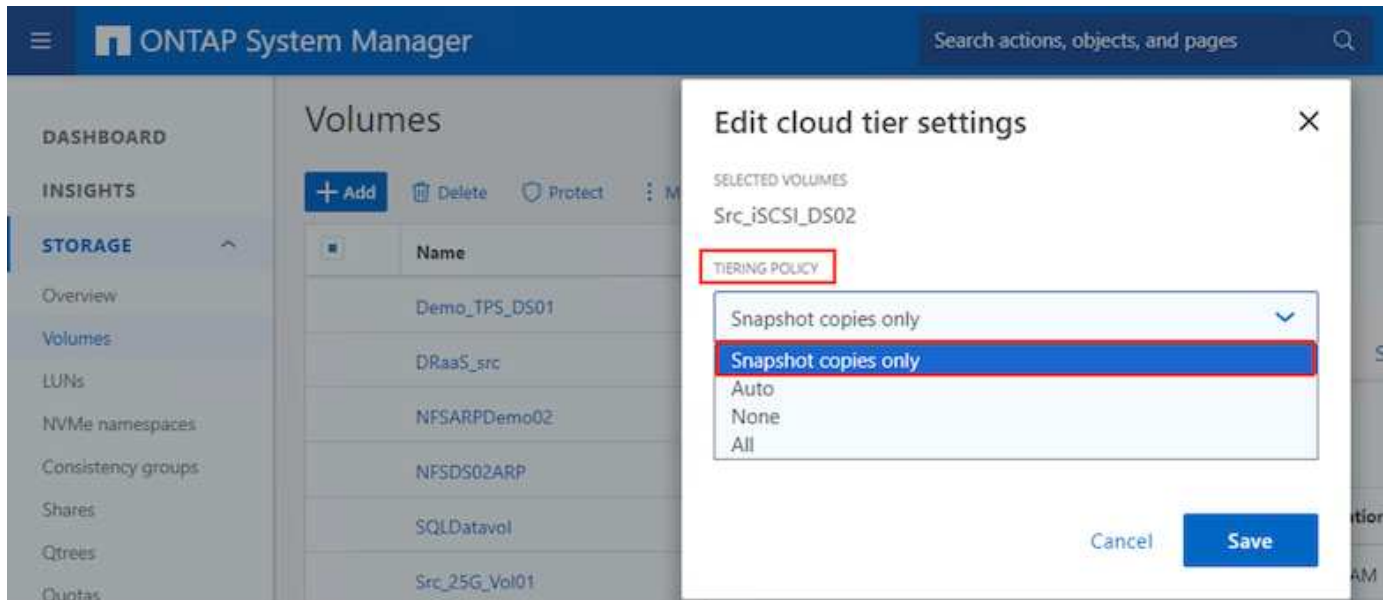


En résumé, lorsque vous utilisez le stockage ONTAP ASA pour optimiser le coût total de possession d'un déploiement VMware, utilisez le plug-in SnapCenter pour VMware comme méthode simple et efficace de sauvegarde des machines virtuelles. Il permet de sauvegarder et de restaurer des machines virtuelles de manière transparente et rapide, car les sauvegardes Snapshot prennent littéralement des secondes.

Vous y "guide de la solution" "documentation produit" trouverez des informations sur la configuration, la sauvegarde, la restauration SnapCenter à partir d'un système de stockage primaire ou secondaire, voire à

partir de sauvegardes stockées sur un stockage objet, pour une conservation à long terme.

Afin de réduire les coûts de stockage, le Tiering des volumes FabricPool peut être activé pour déplacer automatiquement les données pour les copies Snapshot vers un Tier de stockage moins coûteux. Les copies Snapshot utilisent en général plus de 10 % du stockage alloué. Bien qu'elles soient importantes pour la protection des données et la reprise sur incident, ces copies instantanées sont rarement utilisées et ne permettent pas une utilisation efficace du stockage haute performance. Grâce aux règles « Snapshot uniquement » pour FabricPool, vous pouvez facilement libérer de l'espace sur un stockage haute performance. Lorsque cette règle est activée, les blocs de copie Snapshot inactifs du volume qui ne sont pas utilisés par le système de fichiers actif sont déplacés vers le niveau objet. Une fois lus, la copie Snapshot est déplacée vers le niveau local pour restaurer une machine virtuelle ou un datastore complet. Ce Tier d'objet peut se présenter sous la forme d'un cloud privé (tel qu'NetApp StorageGRID) ou public (tel qu'AWS ou Azure).

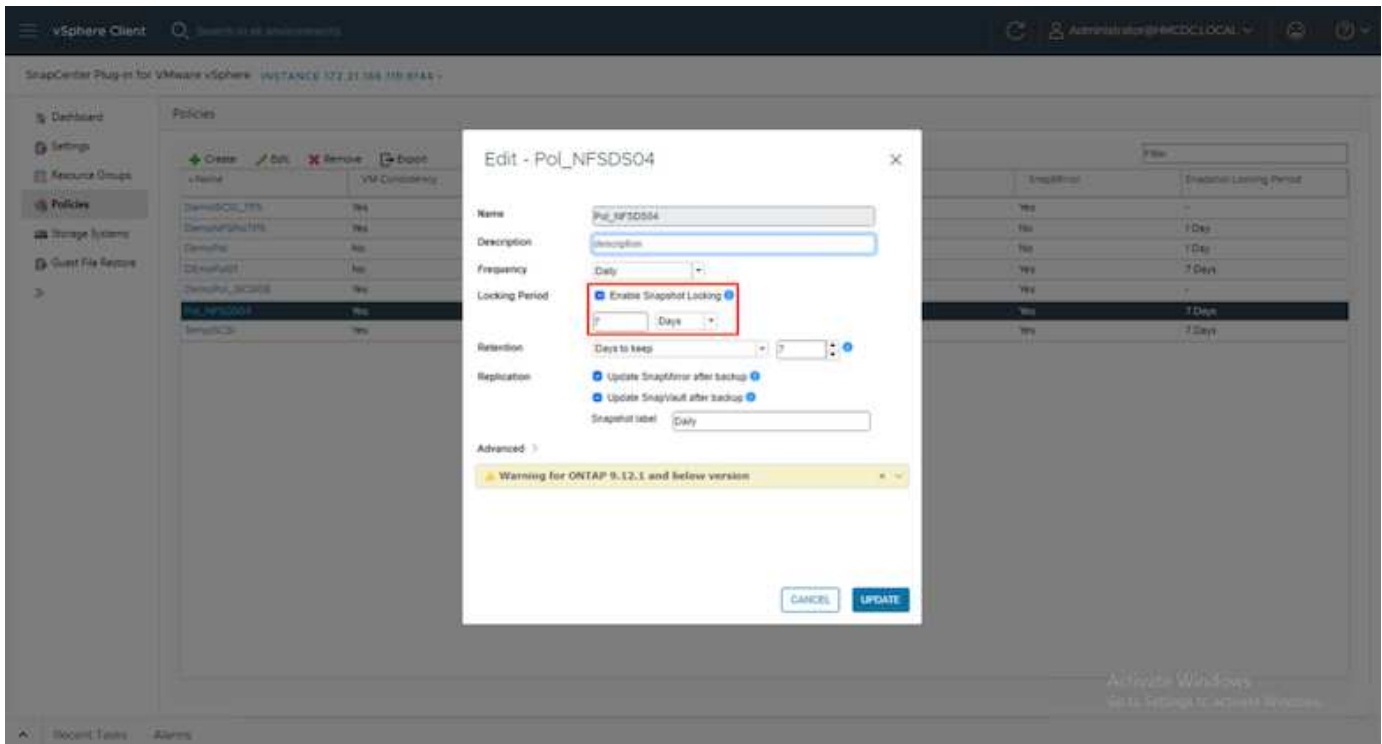


Afficher des conseils détaillés pour ["VMware vSphere avec ONTAP"](#).

Protection contre les ransomwares

L'un des moyens les plus efficaces de se protéger contre les attaques par ransomware est d'implémenter des mesures de sécurité multicouches. Chaque machine virtuelle résidant sur un datastore héberge un système d'exploitation standard. Assurez-vous que des suites de produits contre les programmes malveillants sont installées sur vos serveurs d'entreprise et régulièrement mises à jour, ce qui constitue un composant essentiel de la stratégie de protection multicouche contre les ransomwares. Renforcez également la protection des données à l'aide de la technologie NetApp Snapshot afin de garantir une restauration rapide et fiable en cas d'attaque par ransomware.

Les attaques par ransomware ciblent de plus en plus les sauvegardes et les points de restauration Snapshot en essayant de les supprimer avant de commencer à chiffrer les fichiers. Cependant, avec ONTAP, cela peut être empêché en créant des snapshots inviolables sur les systèmes primaires ou secondaires avec ["Verrouillage des copies NetApp Snapshot™"](#) dans ONTAP. Ces copies Snapshot ne peuvent pas être supprimées ou modifiées par des attaquants de ransomware ou des administrateurs peu scrupuleux, et elles sont disponibles même après une attaque. Vous pouvez restaurer les données des machines virtuelles en quelques secondes, minimisant ainsi les interruptions d'activité. De plus, vous avez la possibilité de choisir la planification et la durée de verrouillage des snapshots adaptées à votre organisation.



Dans le cadre de l'ajout de plusieurs couches, une solution ONTAP intégrée native protège les suppressions non autorisées des copies Snapshot de sauvegarde. Il est connu sous le nom de vérification multiadministrateur ou MAV qui est disponible dans ONTAP 9.11.1 et versions ultérieures. L'approche idéale sera d'utiliser des requêtes pour des opérations spécifiques de MAV.

Pour en savoir plus sur MAV et sur la configuration de ses fonctions de protection, consultez le "[Présentation de la vérification multi-administrateur](#)".

Migration

De nombreux services IT adoptent une approche axée sur le cloud hybride lorsqu'ils effectuent une phase de transformation. Les clients évaluent leur infrastructure IT actuelle et déplacent leurs workloads vers le cloud en fonction de cette évaluation et de cette découverte. Les raisons de la migration vers le cloud varient et peuvent inclure des facteurs tels que l'élasticité et les rafales, la sortie d'un data Center, la consolidation d'un data Center, des scénarios de fin de vie, des fusions, des acquisitions, etc. Le raisonnement de migration de chaque entreprise dépend de ses priorités commerciales spécifiques, l'optimisation des coûts étant la priorité absolue. Pour exploiter toute la puissance du déploiement cloud et de l'élasticité, il est essentiel de choisir le stockage cloud adapté au moment de migrer vers le cloud hybride.

En intégrant des services 1P optimisés par NetApp sur chaque hyperscaler, les entreprises peuvent mettre en place une solution cloud vSphere avec une approche de migration simple, sans changer de plateforme ni modifier leurs adresses IP, ni modifier leur architecture. De plus, cette optimisation vous permet de faire évoluer l'empreinte du stockage tout en réduisant le nombre d'hôtes à un volume minimal dans vSphere, sans modification de la hiérarchie de stockage, de la sécurité ou des fichiers disponibles.

- Afficher des conseils détaillés pour "[Migrez vos workloads vers le datastore FSX for ONTAP](#)".
- Afficher des conseils détaillés pour "[Migrez vos charges de travail vers le datastore Azure NetApp Files](#)".
- Afficher des conseils détaillés pour "[Migrez vos workloads vers le datastore Google Cloud NetApp volumes](#)".

Reprise sur incident

Reprise après incident entre les sites sur site

Pour plus d'informations, rendez-vous sur "[Reprise après incident à l'aide de la DRaaS BlueXP pour les datastores VMFS](#)"

Reprise après incident entre l'infrastructure sur site et VMware Cloud chez n'importe quel hyperscaler

Les clients qui cherchent à utiliser VMware Cloud sur n'importe quel hyperscaler en tant que cible de reprise d'activité peuvent utiliser les datastores ONTAP optimisés pour le stockage (Azure NetApp Files, FSX pour ONTAP, Google Cloud NetApp volumes) pour répliquer les données à partir d'environnements sur site à l'aide de n'importe quelle solution tierce validée qui fournit des fonctionnalités de réplication de serveur virtuel. En ajoutant des datastores basés sur le stockage ONTAP, il optimise les coûts de la reprise après incident sur la destination avec moins d'hôtes ESXi. Cela permet également de désaffecter le site secondaire dans l'environnement sur site pour réaliser des économies considérables.

- Afficher des conseils détaillés pour "[Reprise d'activité dans FSX pour le datastore ONTAP](#)".
- Afficher des conseils détaillés pour "[Reprise après incident vers le datastore Azure NetApp Files](#)".
- Afficher des conseils détaillés pour "[Reprise d'activité dans le datastore Google Cloud NetApp volumes](#)".

Conclusion

Cette solution démontre l'approche optimale de l'utilisation des technologies SAN et des outils OFFTAP de ONTAP pour fournir des services INFORMATIQUES essentiels aux entreprises, aujourd'hui et demain. Ces avantages sont particulièrement avantageux pour les environnements virtualisés exécutant VMware vSphere dans une configuration SAN. Grâce à la flexibilité et à l'évolutivité des systèmes de stockage NetApp, les entreprises peuvent poser les bases nécessaires pour mettre à jour et ajuster leur infrastructure. Elles pourront ainsi répondre à l'évolution des besoins de l'entreprise au fil du temps. Ce système est en mesure de gérer les charges de travail actuelles et d'améliorer l'efficacité de l'infrastructure, réduisant ainsi les coûts d'exploitation et préparant les charges de travail futures.

Baie SAN 100 % Flash NetApp avec VMware vSphere 8

Baie SAN 100 % Flash NetApp avec VMware vSphere 8

Depuis près de vingt ans, le logiciel NetApp ONTAP s'est imposé comme une solution de stockage de premier plan pour les environnements VMware vSphere, grâce à des fonctionnalités innovantes qui simplifient la gestion et réduisent les coûts. NetApp est un leader établi dans le développement de plateformes NAS et de stockage unifié qui offrent un large éventail de protocoles et de protocoles de prise en charge de la connectivité. Parallèlement à ce segment de marché, de nombreux clients préfèrent la simplicité et les avantages financiers des plateformes de stockage SAN en mode bloc qui visent à réaliser un seul travail. La baie SAN 100 % Flash (ASA) de NetApp concrétise cette promesse avec une évolutivité simple, ainsi que des fonctionnalités cohérentes de gestion et d'automatisation pour toutes les applications et les fournisseurs cloud.

Auteur : Josh Powell - Ingénierie de solutions NetApp

Présentation de la solution

Objectif de ce document

Dans ce document, nous allons parler des avantages uniques de l'utilisation de systèmes de stockage NetApp ASA avec VMware vSphere et fournir une présentation technologique de la baie SAN 100 % Flash NetApp. Nous allons également examiner des outils supplémentaires pour simplifier le provisionnement du stockage, la protection des données et la surveillance de votre data Center VMware et ONTAP.

Les sections déploiement de ce document couvrent la création de datastores vVol avec les outils ONTAP pour VMware vSphere et l'observabilité pour le data Center moderne avec NetApp Cloud Insights.

Présentation de la technologie

Cette solution intègre des technologies innovantes de VMware et NetApp.

VMware vSphere 8.0

VMware vSphere est une plateforme de virtualisation qui transforme les ressources physiques en pools de calcul, de réseau et de stockage pouvant être utilisés pour répondre aux exigences des clients en matière de charge de travail et d'applications. Les principaux composants de VMware vSphere sont les suivants :

- **ESXi** - hyperviseur VMware qui permet l'abstraction des processeurs de calcul, de la mémoire, du réseau et d'autres ressources et les met à disposition des machines virtuelles et des charges de travail de conteneur.
- **VCenter** - VMware vCenter est une plate-forme de gestion centralisée permettant d'interagir avec les ressources de calcul, le réseau et le stockage dans le cadre d'une infrastructure virtuelle. VCenter joue un rôle crucial dans la simplification de l'administration de l'infrastructure virtualisée.

Nouvelles améliorations dans vSphere 8.0

vSphere 8.0 apporte de nouvelles améliorations, notamment :

Évolutivité - vSphere 8.0 prend en charge les derniers processeurs Intel et AMD et a des limites étendues pour les périphériques vGPU, les hôtes ESXi, les machines virtuelles par cluster et les périphériques d'E/S VM DirectPath.

Distributed Services Engine - déchargement réseau avec NSX vers des unités de traitement de données (DPU).

Amélioration de l'efficacité des périphériques - vSphere 8.0 renforce les capacités de gestion des périphériques grâce à des fonctions telles que les groupes de périphériques et les extensions de virtualisation des périphériques (DVX).

Sécurité améliorée - l'inclusion d'un délai SSH et d'une politique de fourniture de TPM renforce le cadre de sécurité.

Intégration avec les services de cloud hybride - cette fonctionnalité facilite la transition transparente entre les charges de travail sur site et dans le cloud.

Integrated Kubernetes Runtime - avec l'inclusion de Tanzu, vSphere 8.0 simplifie l'orchestration des conteneurs.

Pour plus d'informations, consultez le blog, "[Nouveautés de vSphere 8](#)".

Volumes virtuels VMware (vVols)

Les vVols sont une nouvelle approche révolutionnaire de la gestion du stockage dans les clusters vSphere, offrant ainsi une gestion simplifiée et un contrôle plus granulaire des ressources de stockage. Dans un datastore vVols, chaque disque virtuel est un vVol et devient un objet LUN natif sur le système de stockage. L'intégration du système de stockage et de vSphere s'effectue via le fournisseur * VASA (VMware API for Storage Awareness)* et permet au système de stockage d'être conscient des données des machines virtuelles et de les gérer en conséquence. Les stratégies de stockage, définies dans le client vCenter, sont utilisées pour allouer et gérer les ressources de stockage.

Les vVols sont une approche simplifiée de la gestion du stockage et sont préférables dans certains cas d'usage.

Pour plus d'informations sur les vVols, reportez-vous au "[Guide de démarrage de vVols](#)".

NVMe over Fabrics

Avec le lancement de vSphere 8.0, NVMe est désormais pris en charge de bout en bout, avec la prise en charge complète des vVols avec NVMe-TCP et NVMe-FC.

Pour plus d'informations sur l'utilisation de NVMe avec vSphere, reportez-vous à la section "[À propos du stockage VMware NVMe](#)" Dans la documentation vSphere Storage.

NetApp ONTAP

Depuis près de vingt ans, le logiciel NetApp ONTAP est une solution de stockage leader pour les environnements VMware vSphere. Il continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion, tout en réduisant les coûts. L'association de ONTAP et de vSphere permet de réduire les dépenses liées au matériel hôte et aux logiciels VMware. Vous pouvez également protéger vos données à moindre coût grâce à des performances élevées prévisibles tout en profitant des fonctionnalités natives d'efficacité du stockage.

Fonctionnalités de base de ONTAP

Copies Snapshot NetApp : copies Snapshot d'une machine virtuelle ou d'un datastore, pour garantir qu'elles n'affectent pas les performances lors de la création ou de l'utilisation d'une copie Snapshot. Ces répliques peuvent servir de points de restauration pour les machines virtuelles ou servir de simple sauvegarde des données. Ces snapshots basés sur la baie sont différents des snapshots VMware (cohérence). La méthode la plus simple pour générer une copie Snapshot ONTAP s'effectue via le plug-in SnapCenter pour VMware vSphere, en sauvegardant les machines virtuelles et les datastores.

- **Efficacité du stockage** - ONTAP assure la déduplication et la compression en arrière-plan et en temps réel, la déduplication de blocs « zéro » et la compaction des données.
- **Déplacement de volumes et de LUN** - permet le déplacement sans interruption de volumes et de LUN prenant en charge les datastores vSphere et les vVols au sein du cluster ONTAP afin d'équilibrer les performances et les capacités ou de prendre en charge les opérations de maintenance et de mise à niveau sans interruption.
- **Transfert de volume et de LUN** - ONTAP permet le déplacement sans interruption des volumes et des LUN qui hébergent les datastores vSphere et les vVols au sein du cluster ONTAP. Cette fonctionnalité facilite l'équilibrage des performances et de la capacité, et permet des mises à niveau sans interruption.
- **Qualité de service** - QoS est une fonctionnalité qui permet la gestion des performances sur un LUN, un volume ou un fichier individuel. Elle peut servir à limiter un VM agressif ou à s'assurer qu'un VM

stratégique reçoit des ressources de performance suffisantes.

- **Chiffrement** - chiffrement de volume NetApp et chiffrement d'agrégat NetApp. Ces options proposent une approche logicielle simple pour chiffrer les données au repos et assurer leur protection.
- **FabricPool** : cette fonctionnalité transfère les données moins fréquemment utilisées vers un magasin d'objets distinct, libérant ainsi un stockage Flash précieux. Fonctionnant au niveau des blocs, il identifie et hiérarchise efficacement les données moins utilisées, ce qui contribue à optimiser les ressources de stockage et à réduire les coûts.
- **Automatisation** - simplifie les tâches de gestion du stockage et des données en utilisant les API REST ONTAP pour l'automatisation et en exploitant les modules Ansible pour une gestion transparente de la configuration des systèmes ONTAP. Les modules Ansible constituent une solution pratique pour gérer efficacement les configurations des systèmes ONTAP. L'association de ces puissants outils permet de rationaliser les flux de travail et d'améliorer la gestion globale de l'infrastructure de stockage.

Fonctionnalités de reprise d'activité de ONTAP

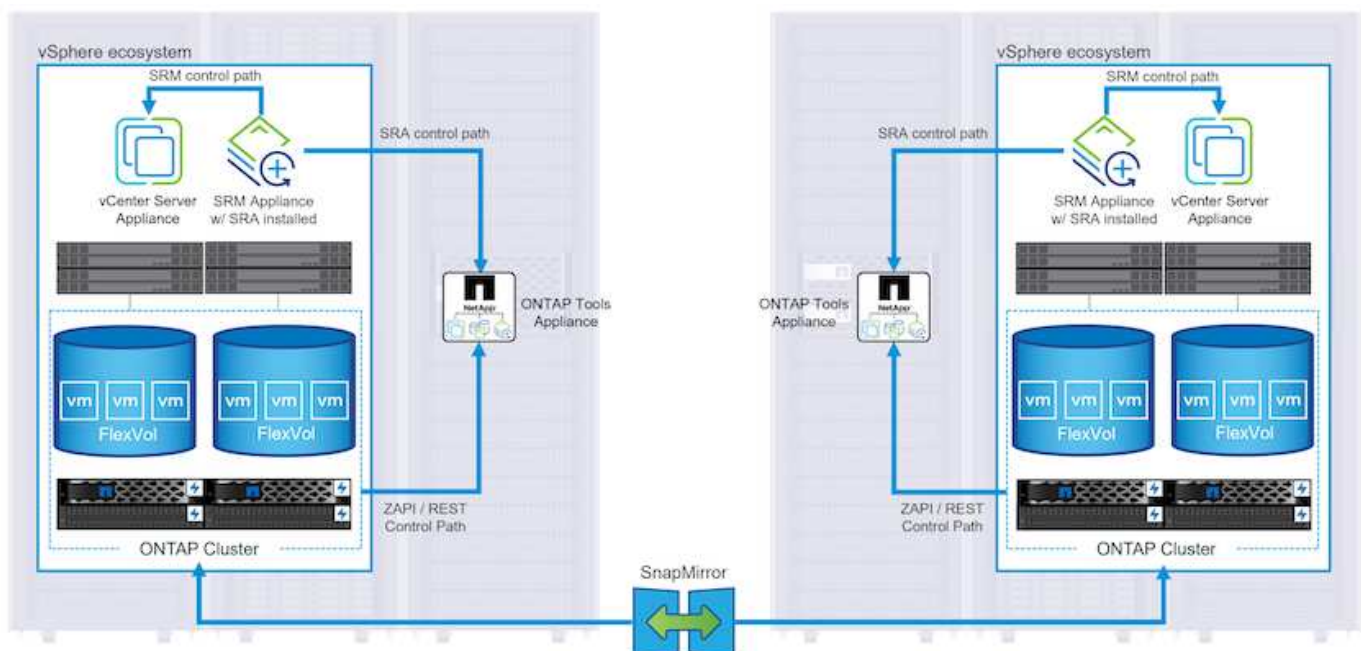
NetApp ONTAP propose des solutions fiables de reprise après incident pour les environnements VMware. Ces solutions s'appuient sur les technologies de réplication SnapMirror entre les systèmes de stockage primaire et secondaire pour permettre le basculement et une restauration rapide en cas de défaillance.

Storage Replication adapter:

L'adaptateur de réplication du stockage NetApp (SRA) est un composant logiciel permettant l'intégration entre les systèmes de stockage NetApp et VMware site Recovery Manager (SRM). Elle facilite la réplication des données des machines virtuelles sur l'ensemble des baies de stockage NetApp, offrant ainsi une protection renforcée des données et des fonctionnalités de reprise après incident. SRA utilise SnapMirror et SnapVault pour répliquer les données des VM sur des systèmes de stockage disparates ou plusieurs sites géographiques.

L'adaptateur assure une réplication asynchrone au niveau des machines virtuelles de stockage (SVM) à l'aide de la technologie SnapMirror et étend la prise en charge de VMFS dans les environnements de stockage SAN (iSCSI et FC) et NFS dans les environnements de stockage NAS.

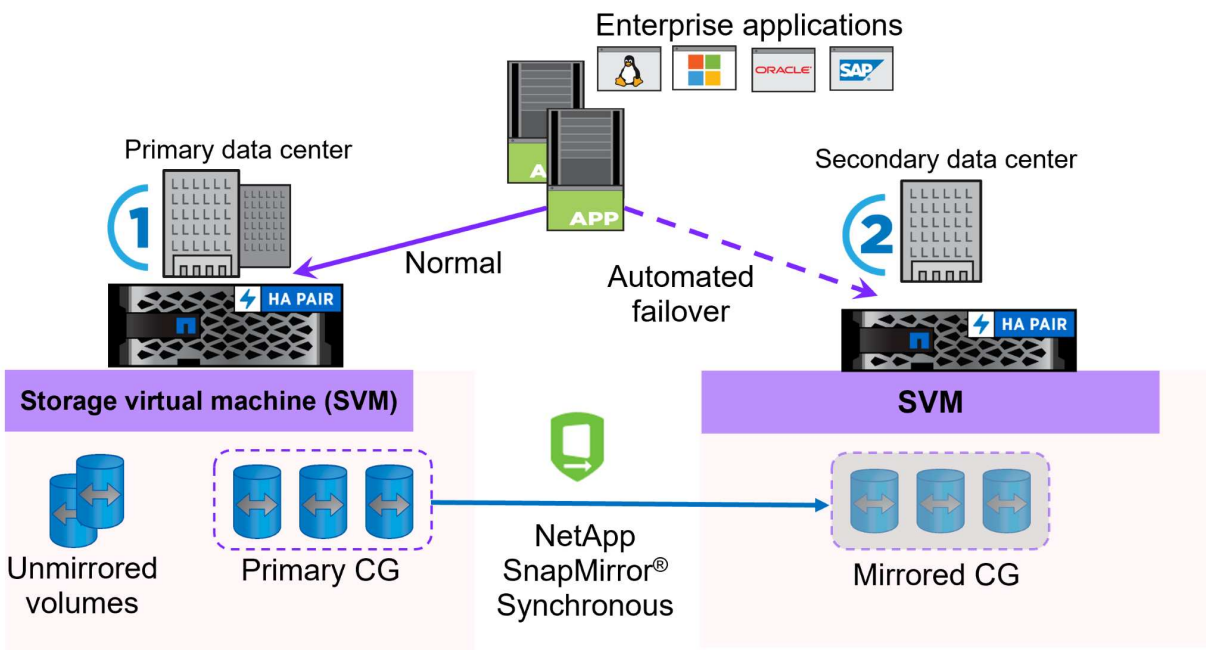
NetApp SRA est installée dans le cadre des outils ONTAP pour VMware vSphere.



Pour plus d'informations sur l'adaptateur de réplication de stockage NetApp pour SRM, reportez-vous à la section "[VMware site Recovery Manager et NetApp ONTAP](#)".

SnapMirror continuité de l'activité :

SnapMirror est une technologie de réplication des données NetApp qui assure une réplication synchrone des données entre les systèmes de stockage. Et permet de créer plusieurs copies de données à différents emplacements afin de pouvoir restaurer les données en cas d'incident ou de perte de données. SnapMirror offre une fréquence de réplication flexible et permet de créer des copies instantanées de données à des fins de sauvegarde et de restauration. SM-BC réplique les données au niveau du groupe de cohérence.



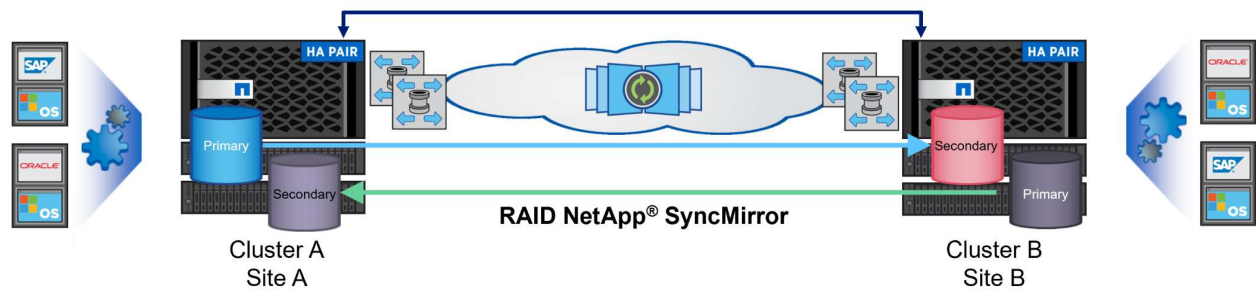
Pour en savoir plus, reportez-vous à SnapMirror "[Présentation de la continuité de l'activité](#)".

NetApp MetroCluster:

NetApp MetroCluster est une solution haute disponibilité de reprise après incident qui assure la réplication synchrone des données entre deux systèmes de stockage NetApp dispersés géographiquement. Elle est conçue pour assurer la disponibilité et la protection continues des données en cas de défaillance à l'échelle du site.

MetroCluster utilise SyncMirror pour répliquer de manière synchrone les données au-dessus du niveau RAID. SyncMirror est conçu pour une transition efficace entre les modes synchrone et asynchrone. Cela permet au cluster de stockage primaire de continuer à fonctionner dans un état non répliqué lorsque le site secondaire devient temporairement inaccessible. SyncMirror effectue également une nouvelle réplication vers un état RPO = 0 une fois la connectivité restaurée.

MetroCluster peut fonctionner sur des réseaux IP ou Fibre Channel.



Pour plus d'informations sur l'architecture et la configuration de MetroCluster, reportez-vous au "[Site de documentation MetroCluster](#)".

Modèle de licence ONTAP One

ONTAP One est un modèle de licence complet qui permet d'accéder à toutes les fonctionnalités d'ONTAP sans nécessiter de licences supplémentaires. Notamment la protection des données, la reprise d'activité, la haute disponibilité, l'intégration au cloud, l'efficacité du stockage, les performances et la sécurité. Les clients disposant de systèmes de stockage NetApp sous licence Flash, Core plus Data protection ou Premium ont droit à une licence ONTAP One, leur permettant d'optimiser l'utilisation de leurs systèmes de stockage.

La licence ONTAP One inclut toutes les fonctionnalités suivantes :

NVMeoF – permet l'utilisation de NVMe over Fabrics pour les E/S du client front-end, NVMe/FC et NVMe/TCP.

FlexClone – permet la création rapide de clones de données compacts basés sur des snapshots.

S3 – active le protocole S3 pour les E/S client front-end.

SnapRestore – permet une récupération rapide des données à partir de snapshots.

Protection anti-ransomware autonome - permet la protection automatique des partages de fichiers NAS lorsqu'une activité anormale du système de fichiers est détectée.

Gestionnaire de clés multitenant - permet d'avoir plusieurs gestionnaires de clés pour différents locataires sur le système.

SnapLock – permet la protection des données contre la modification, la suppression ou la corruption sur le système.

SnapMirror Cloud – permet la réplication de volumes système vers des cibles d'objet.

SnapMirror S3 – permet la réplication d'objets ONTAP S3 vers d'autres cibles compatibles S3.

Baie SAN 100 % Flash NetApp

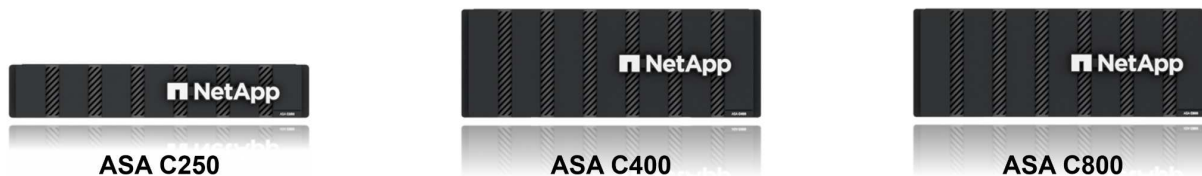
La baie SAN 100 % Flash (ASA) NetApp est une solution de stockage haute performance conçue pour répondre aux exigences élevées des data centers modernes. Il associe la vitesse et la fiabilité du stockage Flash aux fonctionnalités avancées de gestion des données de NetApp pour assurer des performances, une évolutivité et une protection des données exceptionnelles.

La gamme ASA comprend à la fois des modèles de la série A et des modèles de la série C.

Les baies Flash NetApp A-Series 100 % NVMe sont conçues pour les workloads haute performance. Elles offrent une latence ultra faible et une résilience élevée. Elles sont donc adaptées aux applications stratégiques.



Les baies Flash C-Series QLC sont destinées à des cas d'utilisation de capacité supérieure, offrant la vitesse de la technologie Flash et l'économie du Flash hybride.



Pour plus d'informations, reportez-vous au ["Page d'accueil NetApp ASA"](#).

Fonctionnalités NetApp ASA

La baie SAN 100 % Flash NetApp comprend les fonctionnalités suivantes :

Performances - la baie SAN 100 % Flash exploite des disques SSD avec une architecture NVMe de bout en bout pour fournir des performances fulgurantes, réduisant ainsi considérablement la latence et améliorant les temps de réponse des applications. Elle offre des IOPS élevées et prévisibles et une faible latence, ce qui la rend adaptée aux charges de travail sensibles à la latence, telles que les bases de données, la virtualisation et l'analytique.

Évolutivité - les baies SAN 100 % Flash NetApp sont conçues avec une architecture scale-out qui permet aux entreprises de faire évoluer leur infrastructure de stockage en toute transparence au fur et à mesure de l'évolution de leurs besoins. L'ajout de nœuds de stockage permet aux entreprises de développer la capacité et les performances sans interrompre l'activité, afin de s'adapter à l'augmentation des besoins en données.

Gestion des données - le système d'exploitation Data ONTAP de NetApp alimente la baie SAN 100 % Flash en fournissant une suite complète de fonctionnalités de gestion des données. Qui incluent l'allocation dynamique, la déduplication, la compression et la compaction des données, ce qui optimise l'utilisation du stockage et réduit les coûts. Des fonctionnalités avancées de protection des données telles que les snapshots, la réplication et le chiffrement assurent l'intégrité et la sécurité des données stockées.

Intégration et flexibilité - la baie SAN 100 % Flash s'intègre à l'écosystème plus vaste de NetApp, permettant une intégration transparente avec d'autres solutions de stockage NetApp, telles que les déploiements de clouds hybrides avec NetApp Cloud Volumes ONTAP. Il prend également en charge les protocoles standard comme Fibre Channel (FC) et iSCSI, facilitant ainsi l'intégration avec les infrastructures SAN existantes.

Analytique et automatisation - le logiciel de gestion de NetApp, dont NetApp Cloud Insights, offre des fonctionnalités complètes de surveillance, d'analyse et d'automatisation. Grâce à ces outils, les administrateurs peuvent obtenir des informations sur leur environnement de stockage, optimiser les performances et automatiser les tâches de routine, tout en simplifiant la gestion du stockage et en améliorant l'efficacité opérationnelle.

Protection des données et continuité de l'activité - la baie SAN 100 % Flash offre des fonctionnalités intégrées de protection des données telles que les snapshots à un point dans le temps, la réplication et la reprise après incident. Ces fonctionnalités assurent la disponibilité des données et facilitent une restauration rapide en cas de perte de données ou de défaillance du système.

Prise en charge de protocoles

La baie ASA prend en charge tous les protocoles SAN standard, notamment iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) et NVMe over Fabrics.

iSCSI - NetApp ASA fournit une prise en charge robuste pour iSCSI, permettant un accès au niveau des blocs aux périphériques de stockage sur les réseaux IP. Il offre une intégration transparente avec les initiateurs iSCSI pour un provisionnement et une gestion efficaces des LUN iSCSI. Fonctionnalités avancées d'ONTAP, telles que les chemins d'accès multiples, l'authentification CHAP et la prise en charge ALUA.

Pour obtenir des conseils de conception sur les configurations iSCSI, reportez-vous à la section .

Fibre Channel - NetApp ASA offre une prise en charge complète de Fibre Channel (FC), une technologie de réseau haut débit couramment utilisée dans les réseaux de stockage (SAN). ONTAP s'intègre en toute transparence à l'infrastructure FC, offrant ainsi un accès fiable et efficace au niveau des blocs aux systèmes de stockage. Elle offre des fonctionnalités telles que le zoning, les chemins d'accès multiples et la connexion à la fabric (FLOGI) pour optimiser les performances, améliorer la sécurité et assurer la connectivité transparente dans les environnements FC.

Pour obtenir des conseils de conception sur les configurations Fibre Channel, reportez-vous au ["Documentation de référence sur la configuration SAN"](#).

NVMe over Fabrics - NetApp ONTAP et ASA prennent en charge NVMe over Fabrics. NVMe/FC permet d'utiliser des périphériques de stockage NVMe sur l'infrastructure Fibre Channel et NVMe/TCP sur les réseaux de stockage IP.

Pour obtenir des conseils de conception sur NVMe, reportez-vous à la section ["Configuration, prise en charge et limitations de NVMe"](#).

Technologie active/active

Les baies SAN 100 % Flash de NetApp autorisent des chemins de données actif-actif à travers les deux contrôleurs, ce qui évite au système d'exploitation hôte d'attendre la panne d'un chemin actif avant d'activer le chemin alternatif. Cela signifie que l'hôte peut utiliser tous les chemins disponibles sur tous les contrôleurs, en veillant à ce que les chemins actifs soient toujours présents, que le système soit dans un état stable ou qu'il ait subi un basculement de contrôleur.

De plus, la fonctionnalité NetApp ASA améliore considérablement la vitesse de basculement du SAN. Chaque contrôleur réplique en continu les métadonnées de LUN essentielles à son partenaire. Par conséquent,

chaque contrôleur est prêt à reprendre les responsabilités liées à la transmission de données en cas de panne soudaine de son partenaire. Cette préparation est possible car le contrôleur possède déjà les informations nécessaires pour commencer à utiliser les lecteurs précédemment gérés par le contrôleur défectueux.

Avec les chemins d'accès actif-actif, les basculements planifiés et non planifiés bénéficient de délais de reprise des E/S de 2-3 secondes.

Pour plus d'informations, voir ["Tr-4968, Baie 100 % SAS NetApp – disponibilité et intégrité des données avec le NetApp ASA"](#).

Garanties de stockage

NetApp propose un ensemble unique de garanties de stockage grâce aux baies SAN 100 % Flash de NetApp. Ses avantages uniques incluent :

Garantie d'efficacité du stockage : atteignez une haute performance tout en réduisant les coûts de stockage grâce à la garantie d'efficacité du stockage. Ratio de 4:1 pour les workloads SAN

6 Nines (99.9999 %) garantie de disponibilité des données : garantit la correction des temps d'arrêt imprévus de plus de 31.56 secondes par an.

Garantie de restauration ransomware : garantie de récupération des données en cas d'attaque par ransomware.

Voir la ["Portail produit NetApp ASA"](#) pour en savoir plus.

Plug-ins NetApp pour VMware vSphere

Les services de stockage NetApp sont étroitement intégrés à VMware vSphere grâce aux plug-ins suivants :

Outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware permettent aux administrateurs de gérer le stockage NetApp directement à partir du client vSphere. Les outils ONTAP vous permettent de déployer et de gérer des datastores, ainsi que de provisionner des datastores VVol.

Les outils ONTAP permettent de mapper les datastores aux profils de capacité de stockage qui déterminent un ensemble d'attributs de système de stockage. Il est ainsi possible de créer des datastores dotés d'attributs spécifiques tels que les performances du stockage et la qualité de service.

Les outils ONTAP comprennent les composants suivants :

Virtual Storage Console (VSC) : VSC inclut l'interface intégrée au client vSphere, dans laquelle vous pouvez ajouter des contrôleurs de stockage, provisionner des datastores, surveiller les performances des datastores et afficher et mettre à jour les paramètres des hôtes ESXi.

VASA Provider : le fournisseur VMware vSphere APIs for Storage Awareness (VASA) pour ONTAP envoie des informations sur le stockage utilisé par VMware vSphere à vCenter Server, permettant le provisionnement de datastores VMware Virtual volumes (vVols), la création et l'utilisation de profils de fonctionnalités de stockage, la vérification de conformité et la surveillance des performances.

Storage Replication adapter (SRA): lorsqu'il est activé et utilisé avec VMware site Recovery Manager (SRM), SRA facilite la récupération des datastores et des machines virtuelles vCenter Server en cas de défaillance, permettant ainsi la configuration des sites protégés et des sites de reprise pour la reprise après incident.

Pour plus d'informations sur les outils NetApp ONTAP pour VMware, voir ["Documentation sur les outils ONTAP pour VMware vSphere"](#).

Plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter pour VMware vSphere (SCV) est une solution logicielle de NetApp qui protège intégralement les données dans les environnements VMware vSphere. Son objectif est de simplifier et de rationaliser le processus de protection et de gestion des machines virtuelles et des datastores.

Le plug-in SnapCenter pour VMware vSphere offre les fonctionnalités suivantes dans une interface unifiée, intégrée au client vSphere :

Snapshots basés sur des règles - SnapCenter vous permet de définir des règles pour la création et la gestion de snapshots cohérents au niveau des applications de machines virtuelles dans VMware vSphere.

Automatisation - la création et la gestion automatisées de snapshots basées sur des règles définies permettent d'assurer une protection cohérente et efficace des données.

Protection au niveau VM - la protection granulaire au niveau VM permet une gestion et une récupération efficaces des machines virtuelles individuelles.

Fonctionnalités d'efficacité du stockage - l'intégration aux technologies de stockage NetApp fournit des fonctionnalités d'efficacité du stockage telles que la déduplication et la compression pour les snapshots, ce qui réduit les besoins en stockage.

Le plug-in SnapCenter orchestre la mise en veille des machines virtuelles en association avec des snapshots matériels sur des baies de stockage NetApp. La technologie SnapMirror permet de répliquer des copies de sauvegarde sur les systèmes de stockage secondaires, y compris dans le cloud.

Pour plus d'informations, reportez-vous à la ["Documentation du plug-in SnapCenter pour VMware vSphere"](#).

L'intégration de BlueXP active 3-2-1 stratégies de sauvegarde qui étendent les copies de données au stockage objet dans le cloud.

Pour plus d'informations sur les stratégies de sauvegarde 3-2-1 avec BlueXP, rendez-vous sur ["3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration BlueXP pour les VM"](#).

NetApp Cloud Insights

NetApp Cloud Insights simplifie l'observation de l'infrastructure sur site et dans le cloud et propose des fonctionnalités d'analytique et de résolution des problèmes complexes. Cloud Insights collecte les données à partir d'un environnement de data Center et les envoie dans le cloud. Ceci s'effectue avec un logiciel installé localement appelé unité d'acquisition et avec des collecteurs spécifiques activés pour les actifs dans le centre de données.

Les ressources de Cloud Insights peuvent être balisées avec des annotations qui offrent une méthode d'organisation et de classification des données. Le tableau de bord peut être créé à l'aide de nombreux widgets pour l'affichage des données et des requêtes métriques peuvent être créées pour des vues tabulaires détaillées des données.

Cloud Insights est livré avec un grand nombre de tableaux de bord prêts à l'emploi qui permettent de cibler des types spécifiques de zones problématiques et de catégories de données.

Cloud Insights est un outil hétérogène conçu pour collecter des données à partir d'un large éventail d'appareils. Cependant, il existe une bibliothèque de modèles, appelée ONTAP Essentials, qui permet aux clients NetApp de se lancer rapidement et facilement.

Pour plus d'informations sur la mise en route de Cloud Insights, reportez-vous au ["Page d'accueil de NetApp BlueXP et Cloud Insights"](#).

Baie SAN 100 % Flash NetApp avec VMware vSphere 8

Les outils ONTAP pour VMware permettent aux administrateurs de gérer le stockage NetApp directement à partir du client vSphere. Les outils ONTAP vous permettent de déployer et de gérer des datastores, ainsi que de provisionner des datastores VVol. Les outils ONTAP permettent de mapper les datastores aux profils de capacité de stockage qui déterminent un ensemble d'attributs de système de stockage. Il est ainsi possible de créer des datastores dotés d'attributs spécifiques tels que les performances du stockage et la qualité de service.

Auteur : Josh Powell - Ingénierie de solutions NetApp

Gestion du stockage bloc avec les outils ONTAP pour VMware vSphere

Les outils ONTAP comprennent les composants suivants :

Virtual Storage Console (VSC) : VSC inclut l'interface intégrée au client vSphere, dans laquelle vous pouvez ajouter des contrôleurs de stockage, provisionner des datastores, surveiller les performances des datastores et afficher et mettre à jour les paramètres des hôtes ESXi.

VASA Provider : le fournisseur VMware vSphere APIs for Storage Awareness (VASA) pour ONTAP envoie des informations sur le stockage utilisé par VMware vSphere à vCenter Server, permettant le provisionnement de datastores VMware Virtual volumes (vVols), la création et l'utilisation de profils de fonctionnalités de stockage, la vérification de conformité et la surveillance des performances.

Storage Replication adapter (SRA): lorsqu'il est activé et utilisé avec VMware site Recovery Manager (SRM), SRA facilite la récupération des datastores et des machines virtuelles vCenter Server en cas de défaillance, permettant ainsi la configuration des sites protégés et des sites de reprise pour la reprise après incident.

Pour plus d'informations sur les outils NetApp ONTAP pour VMware, voir ["Documentation sur les outils ONTAP pour VMware vSphere"](#).

Présentation du déploiement de la solution

Dans cette solution, nous démontrerons l'utilisation des outils ONTAP pour VMware vSphere pour provisionner des datastores VMware Virtual volumes (vVol) et créer une machine virtuelle sur un datastore vVol.

Dans un datastore vVols, chaque disque virtuel est un vVol et devient un objet LUN natif sur le système de stockage. L'intégration du système de stockage et de vSphere s'effectue via le fournisseur VASA (VMware API for Storage Awareness) (installé avec les outils ONTAP). Il permet au système de stockage d'être conscient des données des machines virtuelles et de les gérer en conséquence. Les stratégies de stockage, définies dans le client vCenter, sont utilisées pour allouer et gérer les ressources de stockage.

Pour plus d'informations sur les vVols avec ONTAP, reportez-vous à ["Virtual volumes vVols\) avec ONTAP"](#).

Cette solution couvre les étapes générales suivantes :

1. Ajoutez un système de stockage dans les outils ONTAP.
2. Créez un profil de capacité de stockage dans les outils ONTAP.
3. Créez un datastore vVols dans les outils ONTAP.
4. Créer une règle de stockage de machine virtuelle dans le client vSphere.
5. Créez une nouvelle machine virtuelle sur le datastore vVol.

Prérequis

Cette solution a utilisé les composants suivants :

1. Baie SAN 100 % Flash NetApp A400 avec ONTAP 9.13.
2. SVM iSCSI créé sur le ASA avec connectivité réseau aux hôtes ESXi.
3. Outils ONTAP pour VMware vSphere 9.13 (VASA Provider activé par défaut).
4. Cluster vSphere 8.0 (appliance vCenter et hôtes ESXi).

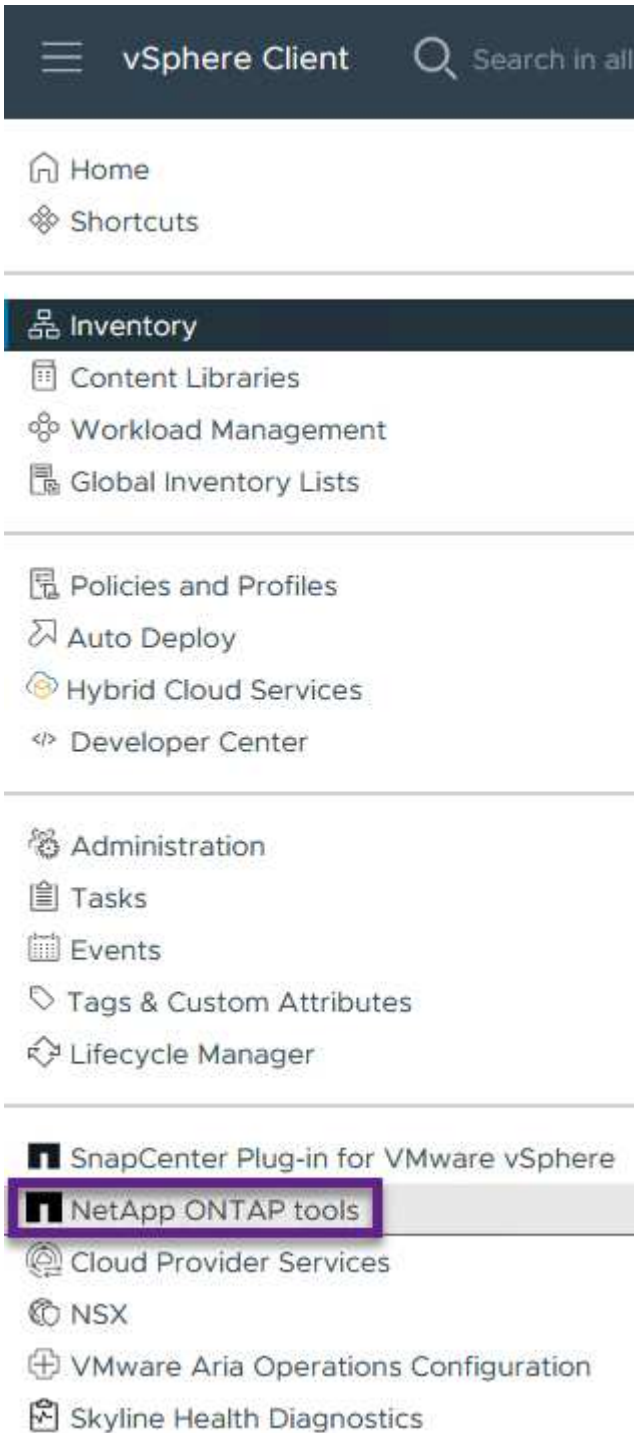
Déploiement de la solution

Créez un datastore vVols dans les outils ONTAP

Pour créer un datastore vVols dans les outils ONTAP, procédez comme suit :

Ajoutez un système de stockage aux outils ONTAP.

1. Accédez aux outils NetApp ONTAP en les sélectionnant dans le menu principal du client vSphere.



2. Dans Outils ONTAP, sélectionnez **systèmes de stockage** dans le menu de gauche, puis appuyez sur **Ajouter**.



NetApp ONTAP tools INSTANCE 10.61.181.154:8443 ▾

Overview

Storage Systems

Storage capability profile

Storage Systems

ADD **REDISCOVER ALL**

3. Indiquez l'adresse IP, les informations d'identification du système de stockage et le numéro de port. Cliquez sur **Ajouter** pour lancer le processus de découverte.

Add Storage System



Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.61.181.205 ▾

Name or IP address:

10.192.102.103

Username:

admin

Password:

●●●●●●●●

Port:

443

Advanced options ^

ONTAP Cluster Certificate:



Automatically fetch



Manually upload

CANCEL

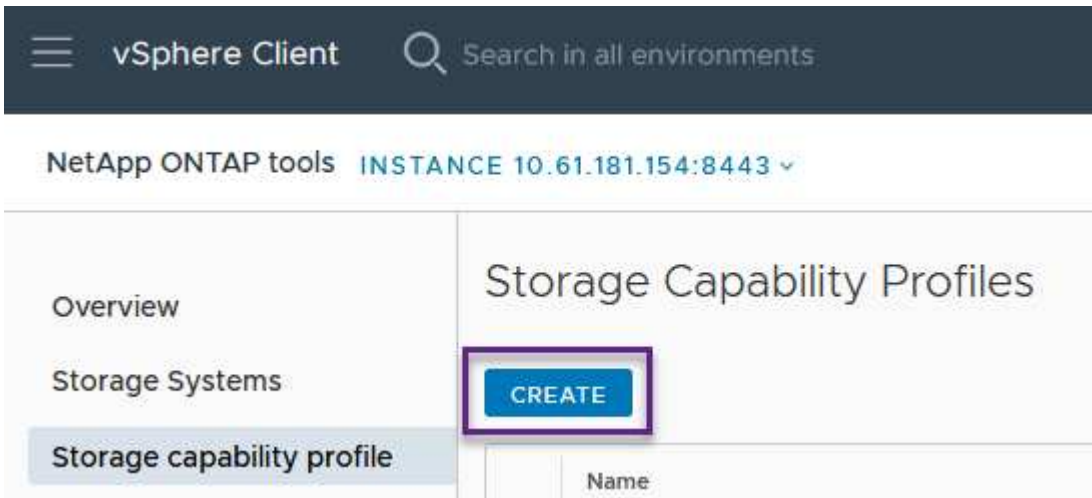
ADD

Créez un profil de capacité de stockage dans les outils ONTAP

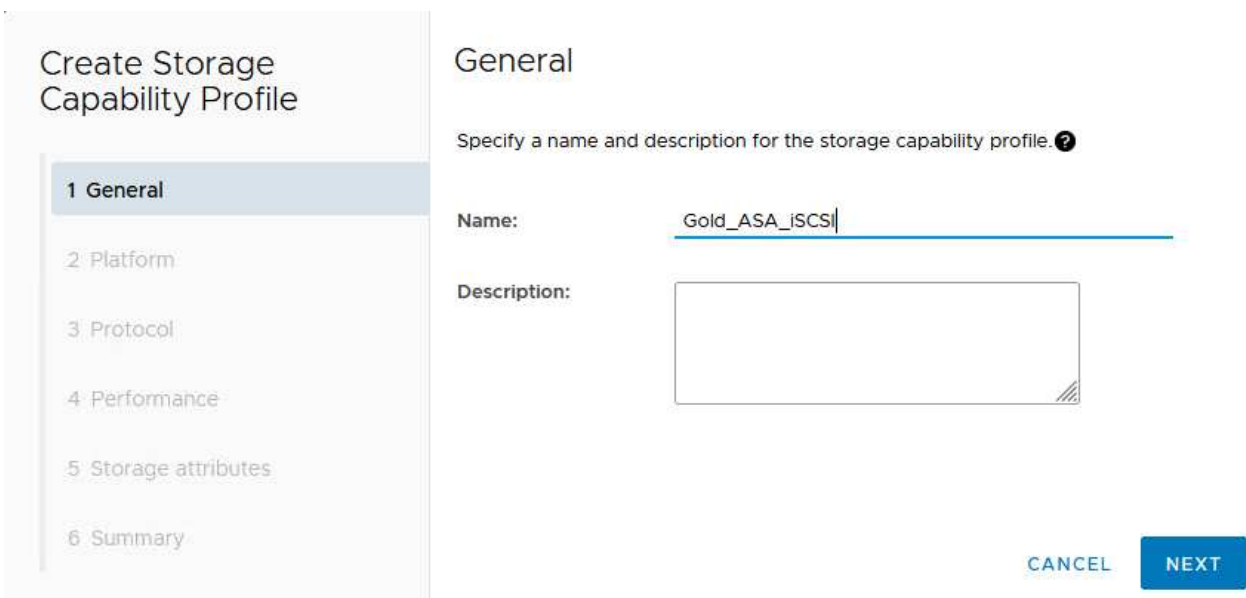
Les profils de capacité de stockage décrivent les fonctionnalités fournies par une baie de stockage ou un système de stockage. Ils incluent des définitions de qualité de service et sont utilisés pour sélectionner des systèmes de stockage qui répondent aux paramètres définis dans le profil.

Pour créer un profil de capacité de stockage dans les outils ONTAP, procédez comme suit :

1. Dans Outils ONTAP, sélectionnez **profil de capacité de stockage** dans le menu de gauche, puis appuyez sur **Créer**.



2. Dans l'assistant **Créer un profil de capacité de stockage**, indiquez un nom et une description du profil et cliquez sur **Suivant**.



3. Sélectionnez le type de plate-forme et pour spécifier que le système de stockage doit être un ensemble de baies SAN 100 % Flash **asymétrique** sur FALSE.

Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. Ensuite, sélectionnez le protocole ou **n'importe quel** pour autoriser tous les protocoles possibles. Cliquez sur **Suivant** pour continuer.

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. La page **performance** permet de définir la qualité de service sous la forme d'IOPS minimum et maximum autorisées.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

6. Complétez la page **Storage Attributes** en sélectionnant l'efficacité du stockage, la réservation d'espace, le cryptage et toute règle de hiérarchisation, le cas échéant.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Storage attributes

Deduplication:

Yes



Compression:

Yes



Space reserve:

Thin



Encryption:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

7. Enfin, passez en revue le résumé et cliquez sur Terminer pour créer le profil.

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

Summary

| | |
|------------------------------|-------------|
| Name: | ASA_Gold |
| Description: | N/A |
| Platform: | Performance |
| Asymmetric: | No |
| Protocol: | Any |
| Max IOPS: | 6000 IOPS |
| Space reserve: | Thin |
| Deduplication: | Yes |
| Compression: | Yes |
| Encryption: | No |
| Tiering policy (FabricPool): | None |

CANCEL

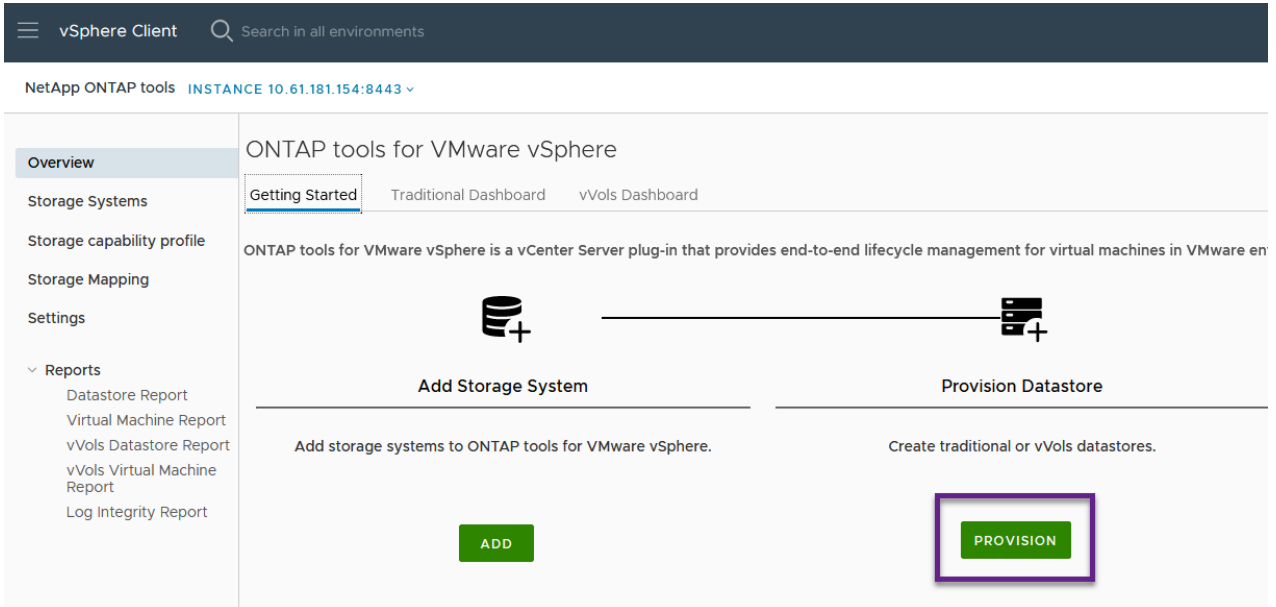
BACK

FINISH

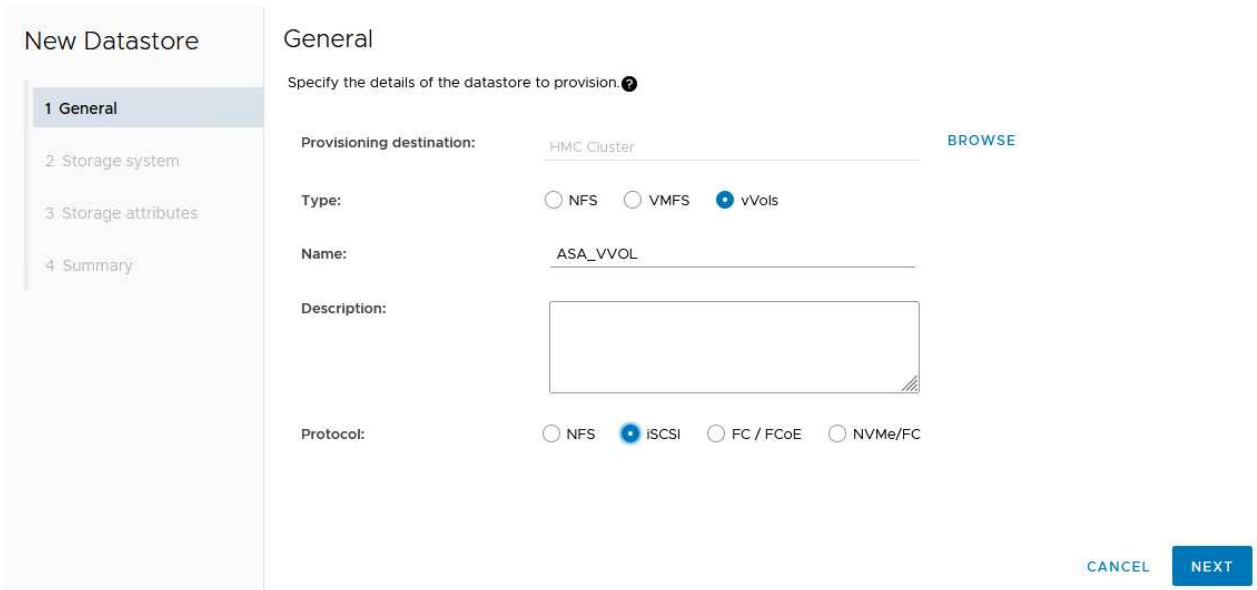
Créez un datastore vVols dans les outils ONTAP

Pour créer un datastore vVols dans les outils ONTAP, procédez comme suit :

1. Dans Outils ONTAP, sélectionnez **Présentation** et dans l'onglet **mise en route**, cliquez sur **Provision** pour démarrer l'assistant.



2. Sur la page **général** de l'assistant Nouveau datastore, sélectionnez le centre de données vSphere ou la destination du cluster. Sélectionnez **vVols** comme type de datastore, indiquez un nom pour le datastore et sélectionnez le protocole.



3. Sur la page **système de stockage**, sélectionner le profil de capacité de stockage, le système de stockage et le SVM. Cliquez sur **Suivant** pour continuer.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

FAS_Default
FAS_Max20
Custom profiles
Gold_ASA_JSCSI
Gold_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svml

CANCEL

BACK

NEXT

4. Sur la page **attributs de stockage**, sélectionnez pour créer un nouveau volume pour le datastore et remplissez les attributs de stockage du volume à créer. Cliquez sur **Ajouter** pour créer le volume, puis sur **Suivant** pour continuer.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

| Name | Size | Storage Capability Profile | Aggregate |
|---|------|----------------------------|-----------|
|  FlexVol volumes are not added. | | | |

| Name | Size(GB) ⓘ | Storage capability profile | Aggregates | Space reserve |
|----------|------------|----------------------------|---------------------|---------------|
| ASA_VVOL | 2000 | Gold_ASA | HCG_A400_E3u3b_NVMe | Thin |

ADD

CANCEL

BACK

NEXT

5. Enfin, passez en revue le résumé et cliquez sur **Finish** pour lancer le processus de création du datastore vVol.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

General

vCenter server: 10.61.181.205

Provisioning destination: HMC Cluster

Datastore name: ASA_VVOL

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: Gold_ASA

Storage system details

Storage system: HCG-NetApp-A400-E3U03

SVM: svm1

Storage attributes

| New FlexVol Name | New FlexVol Size | Aggregate | Storage Capability Profile |
|------------------|------------------|-----------|----------------------------|
| | | | |

CANCEL
BACK
FINISH

Créer une règle de stockage de machine virtuelle dans le client vSphere

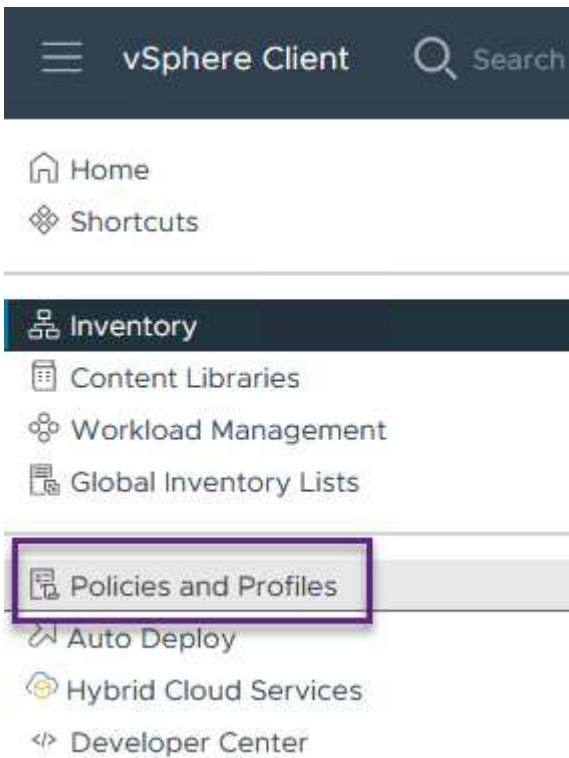
Une règle de stockage de machine virtuelle est un ensemble de règles et d'exigences qui définissent la façon dont les données des machines virtuelles doivent être stockées et gérées. Elle spécifie les caractéristiques de stockage souhaitées, telles que les performances, la disponibilité et les services de données, pour une machine virtuelle spécifique.

Dans ce cas, une stratégie de stockage de machine virtuelle doit être créée pour spécifier qu'une machine virtuelle sera générée sur les datastores vVol et pour établir un mappage un-à-un avec le profil de capacité de stockage généré précédemment.

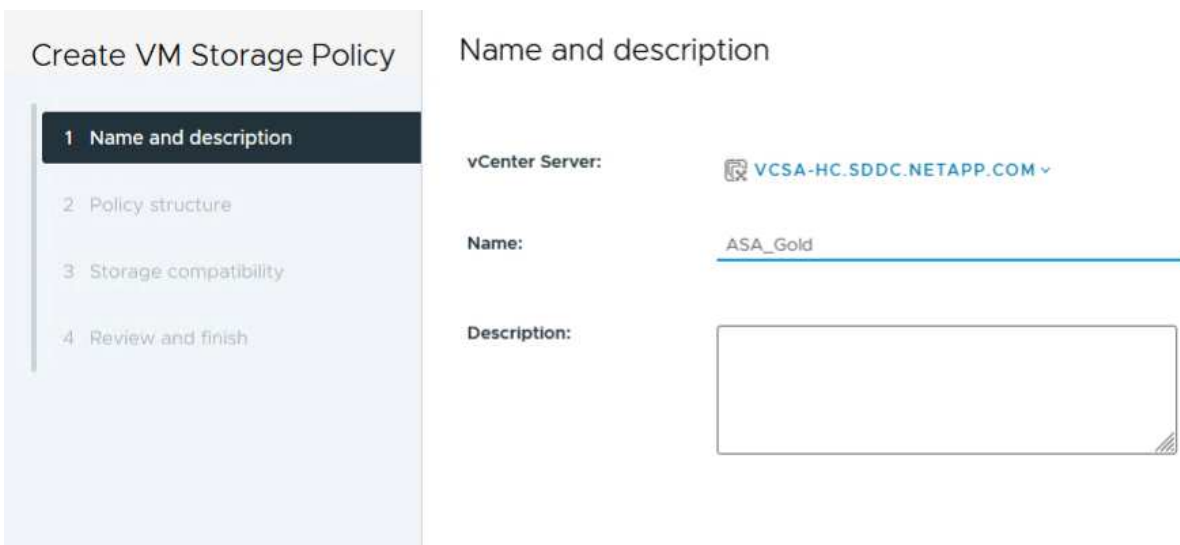
Créer une règle de stockage de machine virtuelle

Pour créer une stratégie de stockage de machine virtuelle, procédez comme suit :

1. Dans le menu principal des clients vSphere, sélectionnez **stratégies et profils**.



2. Dans l'assistant **Create VM Storage Policy**, indiquez d'abord un nom et une description pour la stratégie, puis cliquez sur **Next** pour continuer.

The image shows the 'Create VM Storage Policy' wizard. On the left, there is a sidebar with four steps: '1 Name and description' (highlighted), '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The main area is titled 'Name and description' and contains three fields: 'vCenter Server:' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name:' with a text input field containing 'ASA_Gold', and 'Description:' with a large empty text area.

3. Sur la page **Policy structure**, sélectionnez pour activer les règles pour le stockage vVol NetApp clustered Data ONTAP et cliquez sur **Suivant**.

4. Sur la page suivante, propre à la structure de règles choisie, sélectionnez le profil de capacité de stockage qui décrit le ou les systèmes de stockage à utiliser dans la stratégie de stockage de la machine virtuelle. Cliquez sur **Suivant** pour continuer.

5. Sur la page **compatibilité du stockage**, consultez la liste des datastores VSAN correspondant à cette stratégie et cliquez sur **Suivant**.
6. Enfin, passez en revue la politique à mettre en œuvre et cliquez sur **Terminer** pour créer la politique.

Créer une règle de stockage de machine virtuelle dans le client vSphere

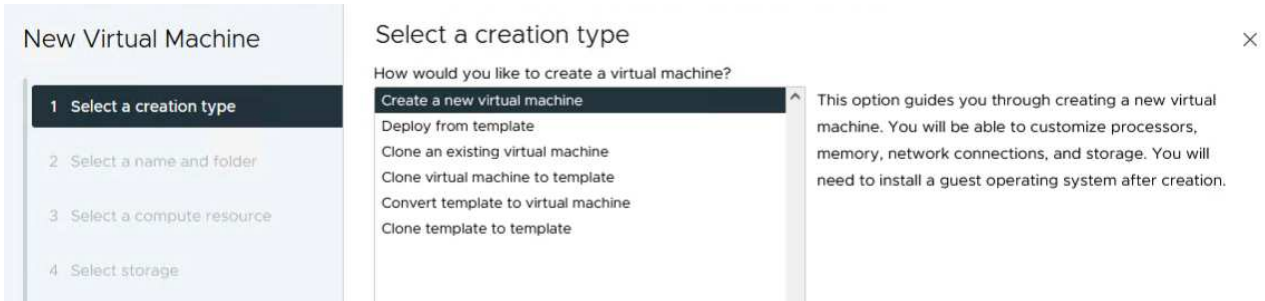
Une règle de stockage de machine virtuelle est un ensemble de règles et d'exigences qui définissent la façon dont les données des machines virtuelles doivent être stockées et gérées. Elle spécifie les caractéristiques de stockage souhaitées, telles que les performances, la disponibilité et les services de données, pour une machine virtuelle spécifique.

Dans ce cas, une stratégie de stockage de machine virtuelle doit être créée pour spécifier qu'une machine virtuelle sera générée sur les datastores vVol et pour établir un mappage un-à-un avec le profil de capacité de stockage généré précédemment.

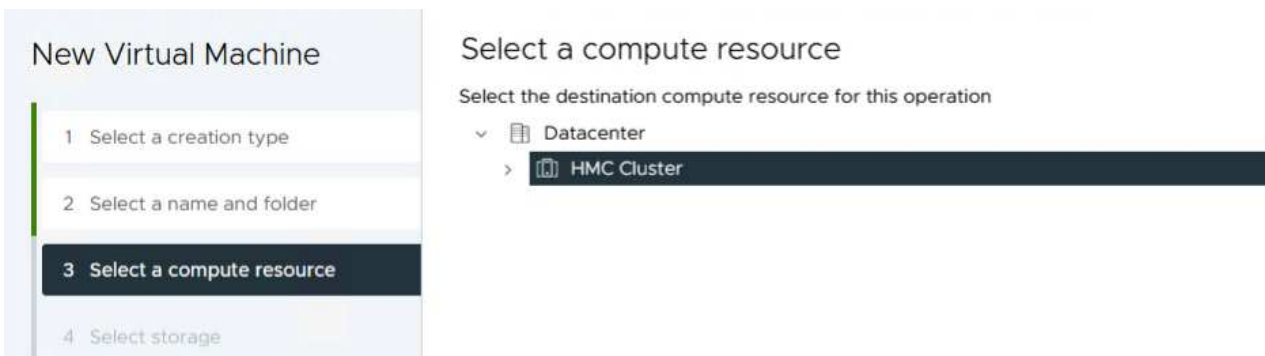
Créer une machine virtuelle sur un datastore vVol

La dernière étape consiste à créer une machine virtuelle à l'aide des règles de stockage de machine virtuelle créées précédemment :

1. Dans l'assistant **Nouvelle machine virtuelle**, sélectionnez **Créer une nouvelle machine virtuelle** et sélectionnez **Suivant** pour continuer.



2. Entrez un nom et sélectionnez un emplacement pour la machine virtuelle, puis cliquez sur **Suivant**.
3. Sur la page **Sélectionner une ressource de calcul**, sélectionnez une destination et cliquez sur **Suivant**.



4. Sur la page **Select Storage**, sélectionnez une stratégie de stockage de machine virtuelle et le datastore vVols qui sera la destination de la machine virtuelle. Cliquez sur **Suivant**.

New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

VM Storage Policy ASA_Gold ▾

Disable Storage DRS for this virtual machine

| | Name | Storage Compatibility | Capacity | Provisioned | Free | |
|----------------------------------|------------------|-----------------------|-----------|-------------|-----------|---|
| <input checked="" type="radio"/> | ASA_VVOLS_1 | Compatible | 1.95 TB | 9 MB | 1.95 TB | V |
| <input type="radio"/> | ASA400_ISCSI01 | Incompatible | 2 TB | 185.32 GB | 1.9 TB | V |
| <input type="radio"/> | DemoDS | Incompatible | 800 GB | 6.99 GB | 793.01 GB | N |
| <input type="radio"/> | destination | Incompatible | 250 GB | 32.66 MB | 249.97 GB | N |
| <input type="radio"/> | DRaaSTest | Incompatible | 1 TB | 133.27 GB | 956.83 GB | N |
| <input type="radio"/> | esxi-hc-01 local | Incompatible | 349.25 GB | 1.41 GB | 347.84 GB | V |
| <input type="radio"/> | esxi-hc-02 local | Incompatible | 349.25 GB | 1.41 GB | 347.84 GB | V |
| <input type="radio"/> | esxi-hc-03 local | Incompatible | 349.25 GB | 1.41 GB | 347.84 GB | V |

Manage Columns Items per page: 10 1 - 10 of 15 items 1 / 2

Compatibility

Validating...

CANCEL

BACK

NEXT

5. Sur la page **Select Compatibility**, choisissez la ou les versions de vSphere avec lesquelles la machine virtuelle sera compatible.
6. Sélectionnez la famille et la version du système d'exploitation invité pour la nouvelle machine virtuelle et cliquez sur **Suivant**.
7. Remplissez la page **Personnaliser le matériel**. Notez qu'il est possible de sélectionner une stratégie de stockage de machine virtuelle distincte pour chaque disque dur (fichier VMDK).

New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

ADD NEW DEVICE ▾

| | | |
|-------------------|-----|--------|
| > CPU * | 4 | ▼ ⓘ |
| > Memory * | 32 | ▼ GB ▼ |
| > New Hard disk * | 150 | ▼ GB ▼ |

Maximum Size 1.95 TB

VM storage policy ASA_Gold ▼

Location Store with the virtual machine ▼

Disk Provisioning Thin Provision ▼

Sharing Unspecified ▼

Disk Mode Dependent ▼

Virtual Device Node New SCSI controller ▼ SCSI(0:0) New Hard disk ▼

> New SCSI controller LSI Logic SAS

> New Network VM Network Connected

CANCEL
BACK
NEXT

En résumé, les outils NetApp ONTAP automatisent le processus de création de datastores vVol sur les systèmes de stockage ONTAP. Les profils de capacité de stockage définissent non seulement les systèmes de stockage à utiliser pour la création de datastores, mais également les règles de QoS qui peuvent être implémentées sur une base VMDK individuelle. Les vVols offrent un modèle de gestion du stockage simplifié et une intégration étroite entre NetApp et VMware en font une solution pratique permettant un contrôle rationalisé, efficace et granulaire des environnements virtualisés.

Baie SAN 100 % Flash NetApp avec VMware vSphere 8

NetApp Cloud Insights est une plateforme cloud d'analytique et de surveillance de l'infrastructure conçue pour fournir une visibilité complète sur les performances, l'intégrité et les coûts des infrastructures IT, à la fois sur site et dans le cloud. Les principales fonctionnalités de NetApp Cloud Insights comprennent la surveillance en temps réel, des tableaux de bord personnalisables, l'analytique prédictive et des outils d'optimisation des coûts qui permettent aux entreprises de gérer et d'optimiser efficacement leurs environnements sur site et dans le cloud.

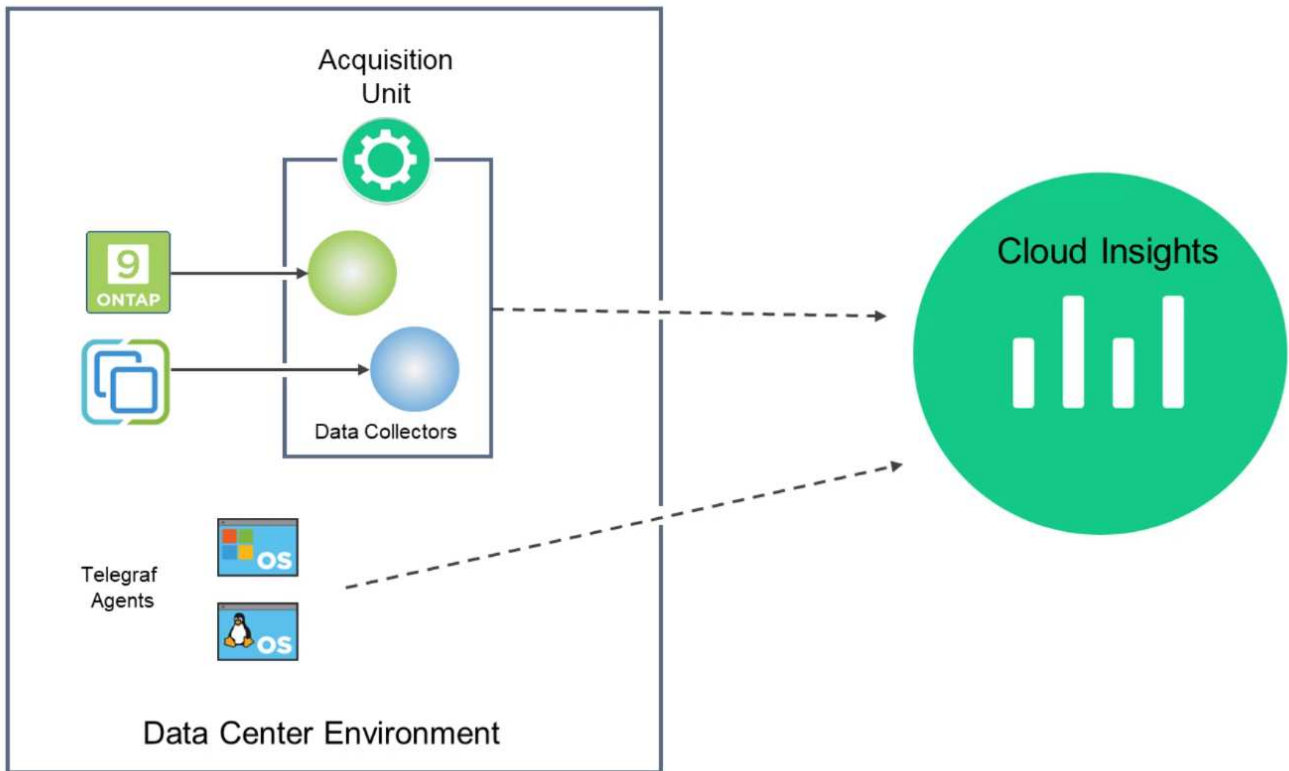
Auteur : Josh Powell - Ingénierie de solutions NetApp

Contrôler le stockage sur site avec NetApp Cloud Insights

NetApp Cloud Insights fonctionne via le logiciel acquisition Unit, qui est configuré avec des collecteurs de données pour les ressources telles que les systèmes de stockage VMware vSphere et NetApp ONTAP. Ces

collecteurs recueillent des données et les transmettent à Cloud Insights. La plateforme utilise ensuite divers tableaux de bord, widgets et requêtes métriques pour organiser les données en analyses pertinentes que les utilisateurs peuvent interpréter.

Schéma d'architecture Cloud Insights :



Présentation du déploiement de la solution

Cette solution fournit une introduction à la surveillance des systèmes de stockage VMware vSphere et ONTAP sur site à l'aide de NetApp Cloud Insights.

Cette liste répertorie les étapes générales décrites dans cette solution :

1. Configuration du Data Collector pour un cluster vSphere
2. Configurez le Data Collector pour un système de stockage ONTAP.
3. Utilisez les règles d'annotation pour marquer les actifs.
4. Explorez et mettez en corrélation les ressources.
5. Utilisez un tableau de bord Top VM Latency pour isoler les voisins bruyants.
6. Identifiez les opportunités d'ajustement des VM.
7. Utilisez des requêtes pour isoler et trier les mesures.

Prérequis

Cette solution utilise les composants suivants :

1. Baie SAN 100 % Flash NetApp A400 avec ONTAP 9.13.

2. Cluster VMware vSphere 8.0.
3. Compte NetApp Cloud Insights.
4. Logiciel NetApp Cloud Insights Acquisition Unit installé sur une machine virtuelle locale avec connectivité réseau aux ressources pour la collecte de données.

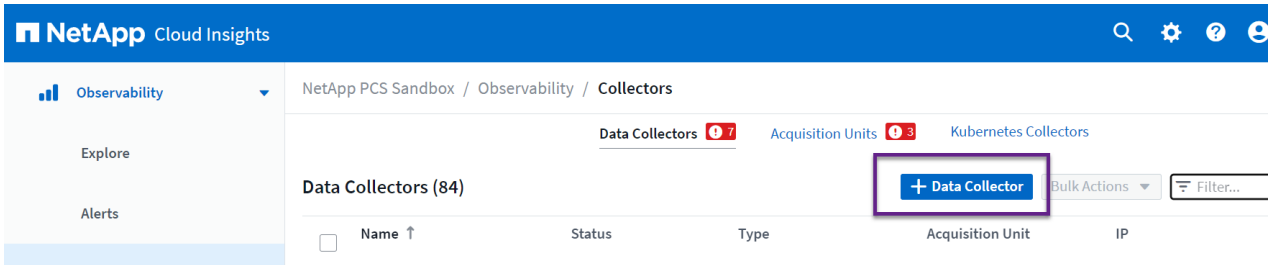
Déploiement de la solution

Configurer les collecteurs de données

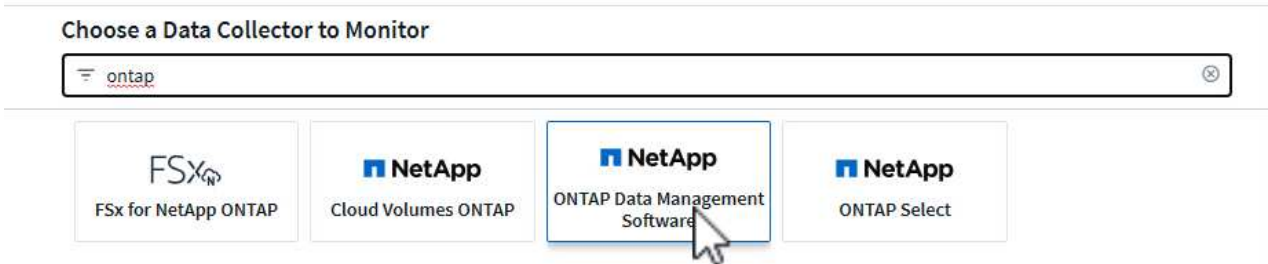
Pour configurer les collecteurs de données pour les systèmes de stockage VMware vSphere et ONTAP, effectuez les opérations suivantes :

Ajoutez un Data Collector pour un système de stockage ONTAP

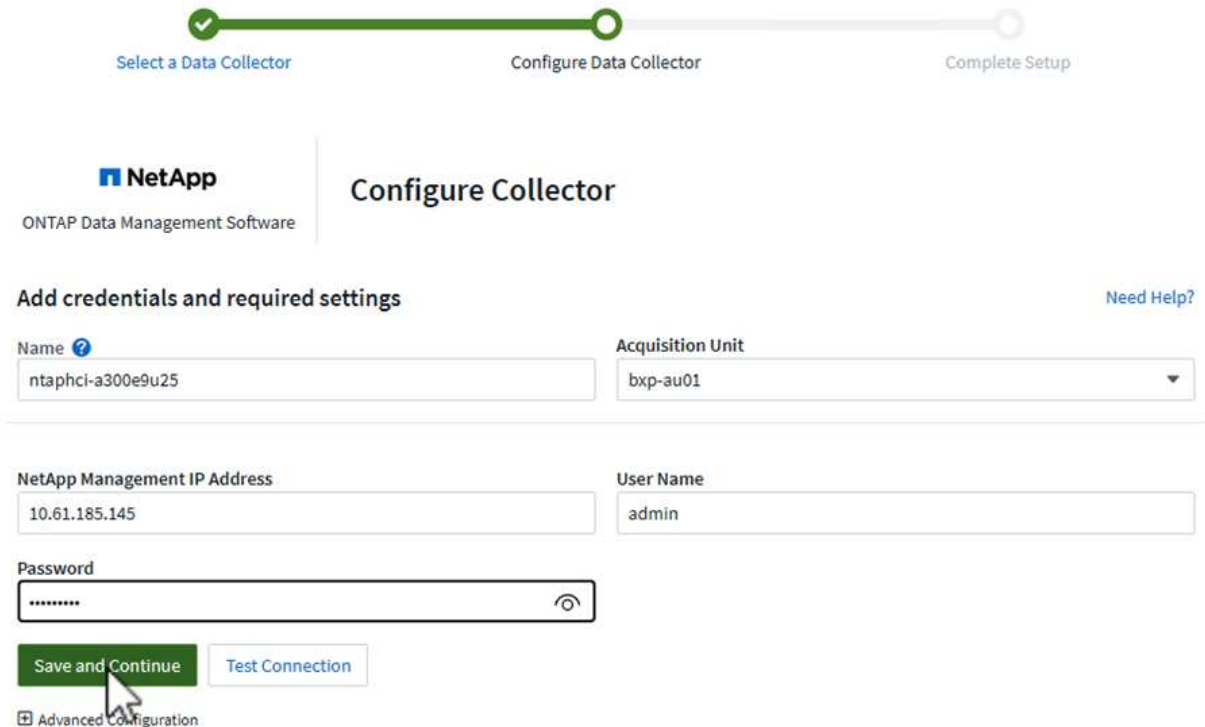
1. Une fois connecté à Cloud Insights, accédez à **observabilité > collecteurs > collecteurs de données** et appuyez sur le bouton pour installer un nouveau Data Collector.



2. À partir d'ici, recherchez **ONTAP** et cliquez sur **logiciel de gestion des données ONTAP**.

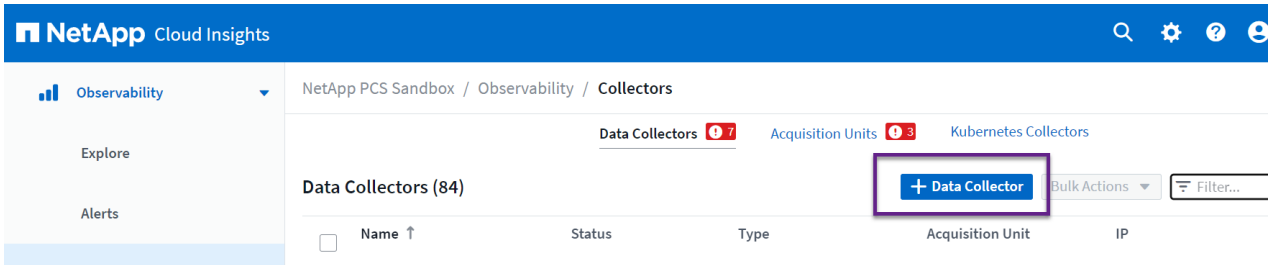


3. Sur la page **configurer le collecteur**, indiquez un nom pour le collecteur, indiquez l'unité **d'acquisition** correcte et fournissez les informations d'identification pour le système de stockage ONTAP. Cliquez sur **Enregistrer et continuer**, puis sur **Terminer la configuration** en bas de la page pour terminer la configuration.

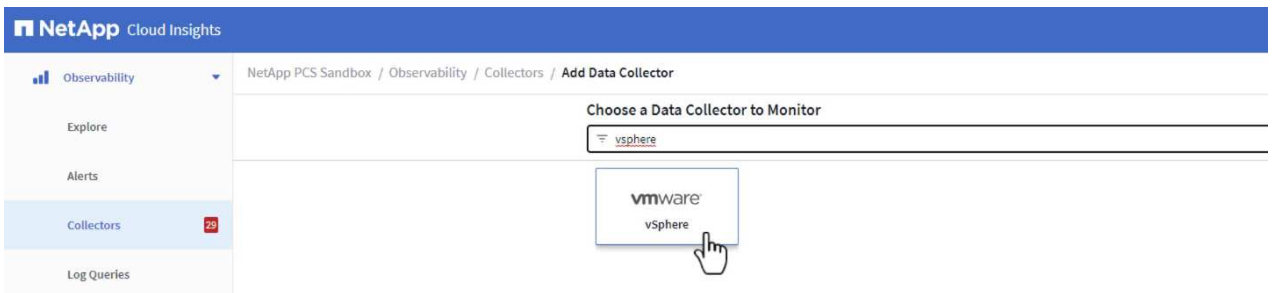


Ajoutez un Data Collector pour un cluster VMware vSphere

1. Une fois de plus, accédez à **observabilité > collecteurs > Data Collectors** et appuyez sur le bouton pour installer un nouveau Data Collector.



2. À partir d'ici, recherchez **vSphere** et cliquez sur **VMware vSphere**.



3. Sur la page **Configure Collector**, indiquez un nom pour le collecteur, indiquez l'unité **acquisition** correcte et fournissez les informations d'identification pour le serveur vCenter. Cliquez sur **Enregistrer et continuer**, puis sur **Terminer la configuration** en bas de la page pour terminer la configuration.



Configure Collector

Add credentials and required settings

[Need Help?](#)

| | |
|---------------------------------|------------------------------|
| Name ? VCSA7 | Acquisition Unit bxp-au01 |
|---------------------------------|------------------------------|

| | |
|--|--|
| Virtual Center IP Address 10.61.181.210 | User Name administrator@vsphere.local |
|--|--|

| |
|-------------------|
| Password ***** |
|-------------------|

| | |
|---|--|
| <input type="button" value="Complete Setup"/> | <input type="button" value="Test Connection"/> |
|---|--|

 Advanced Configuration

Collecting:

- Inventory
- VM Performance

| | |
|-------------------------------------|---------------------------|
| Inventory Poll Interval (min) 20 | Communication Port 443 |
|-------------------------------------|---------------------------|

| | |
|---------------------------|--|
| Filter VMs by ESX_HOST | Choose 'Exclude' or 'Include' to Specify a List Exclude |
|---------------------------|--|

| | |
|---|--|
| Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only) | Performance Poll Interval (sec) 300 |
|---|--|

 Collect basic performance metrics only

| | |
|---|--|
| <input type="button" value="Complete Setup"/> | <input type="button" value="Test Connection"/> |
|---|--|

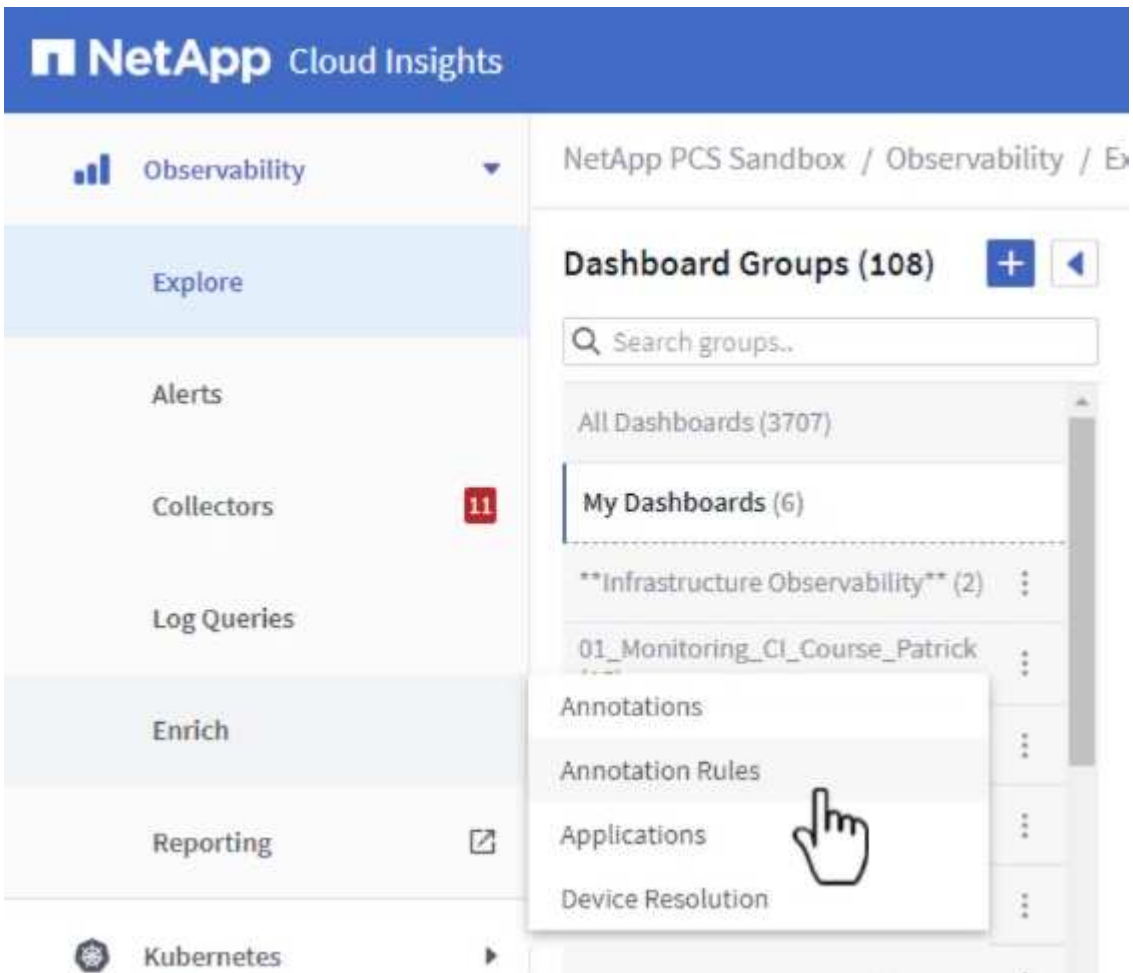
Ajouter des annotations aux actifs

Les annotations sont une méthode utile pour baliser les ressources de sorte qu'elles puissent être filtrées et identifiées dans les différentes vues et requêtes de mesures disponibles dans Cloud Insights.

Dans cette section, des annotations seront ajoutées aux ressources de la machine virtuelle pour filtrage par **Data Center**.

Utilisez les règles d'annotation pour marquer les actifs

1. Dans le menu de gauche, accédez à **observabilité** > **enrichir** > **règles d'annotation** et cliquez sur le bouton **+ Rule** en haut à droite pour ajouter une nouvelle règle.



2. Dans la boîte de dialogue **Ajouter une règle**, entrez un nom pour la règle, recherchez une requête à laquelle la règle sera appliquée, le champ d'annotation affecté et la valeur à renseigner.

Add Rule

Name
Add tags to Solutions Engineering VMs

Query
Solutions Engineering VMs

Annotation
DataCenter

Value
Solutions Engineering

Cancel Save

3. Enfin, dans le coin supérieur droit de la page **règles d'annotation**, cliquez sur **Exécuter toutes les règles** pour exécuter la règle et appliquer l'annotation aux actifs.

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Rules running... Run All Rules

Annotation rules (217)

| Name | Resource Type | Query | Annotation | Value |
|-------------------------------|---------------|---|------------|--------|
| Annotate Tier 1 Storage Pools | Storage Pool | Find Storage Pools (no aggro) for Tier... | Tier | Tier 1 |
| Annotate Tier 2 Storage Pools | Storage Pool | Find Storage Pools (no aggro) for Tier... | Tier | Tier 2 |

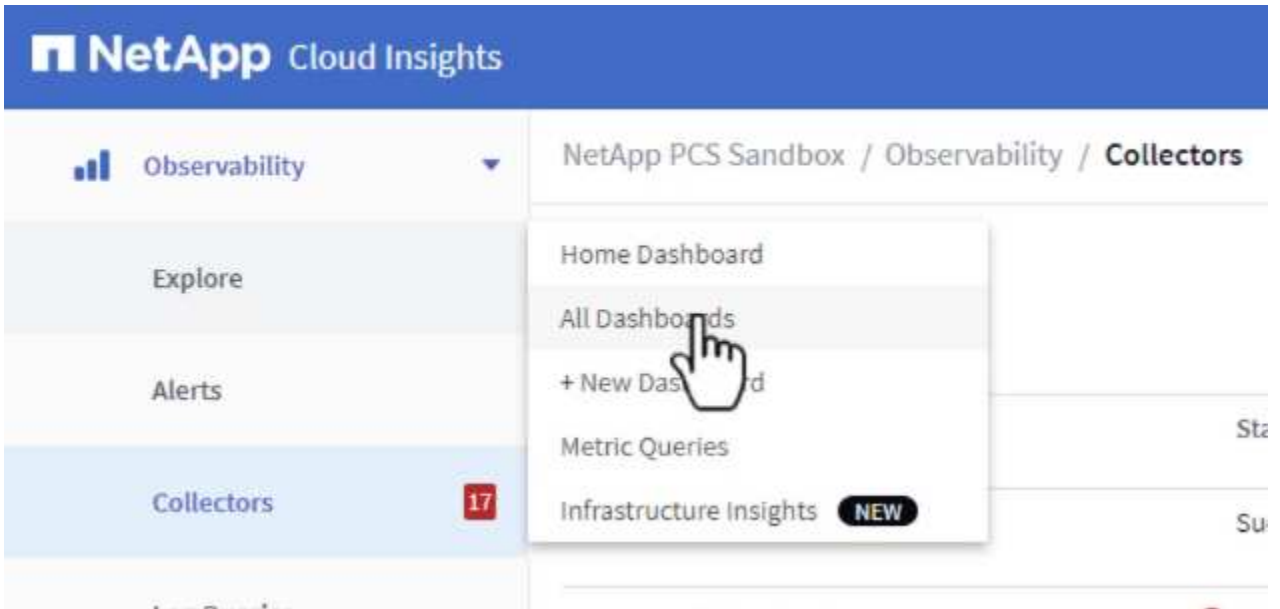
Explorez et mettez en corrélation les ressources

Cloud Insights tire des conclusions logiques sur les ressources fonctionnant ensemble sur vos systèmes de stockage et vos clusters vsphere.

Cette section explique comment utiliser les tableaux de bord pour mettre en corrélation les ressources.

Corréler les ressources à partir d'un tableau de bord des performances du stockage

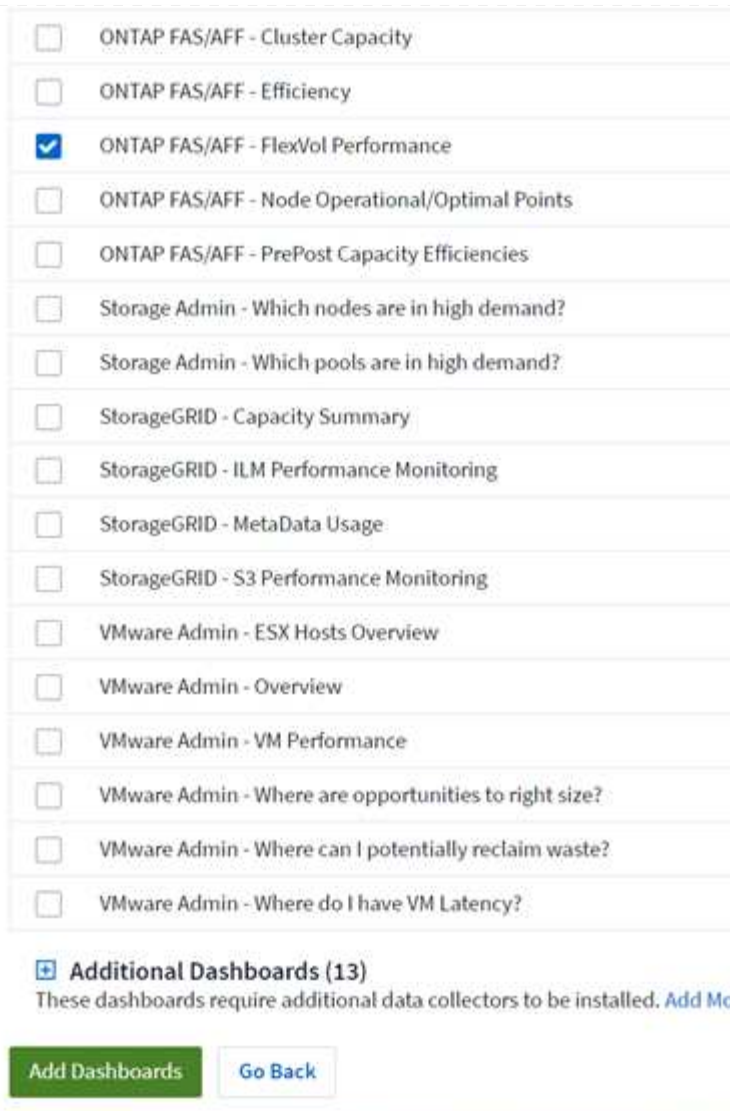
1. Dans le menu de gauche, accédez à **observabilité > Explorer > tous les tableaux de bord**.



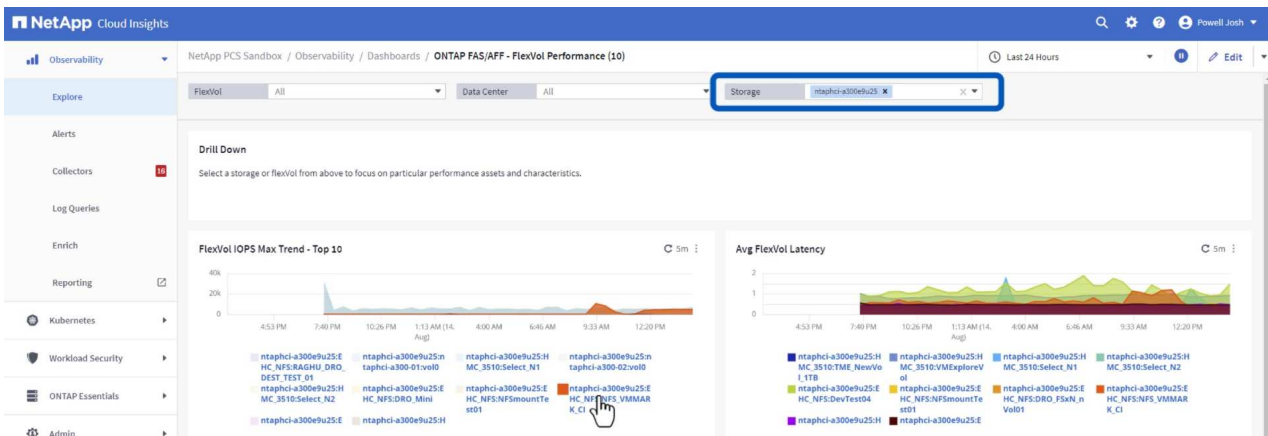
2. Cliquez sur le bouton **+** de la **Gallery** pour afficher la liste des tableaux de bord prêts à l'emploi pouvant être importés.



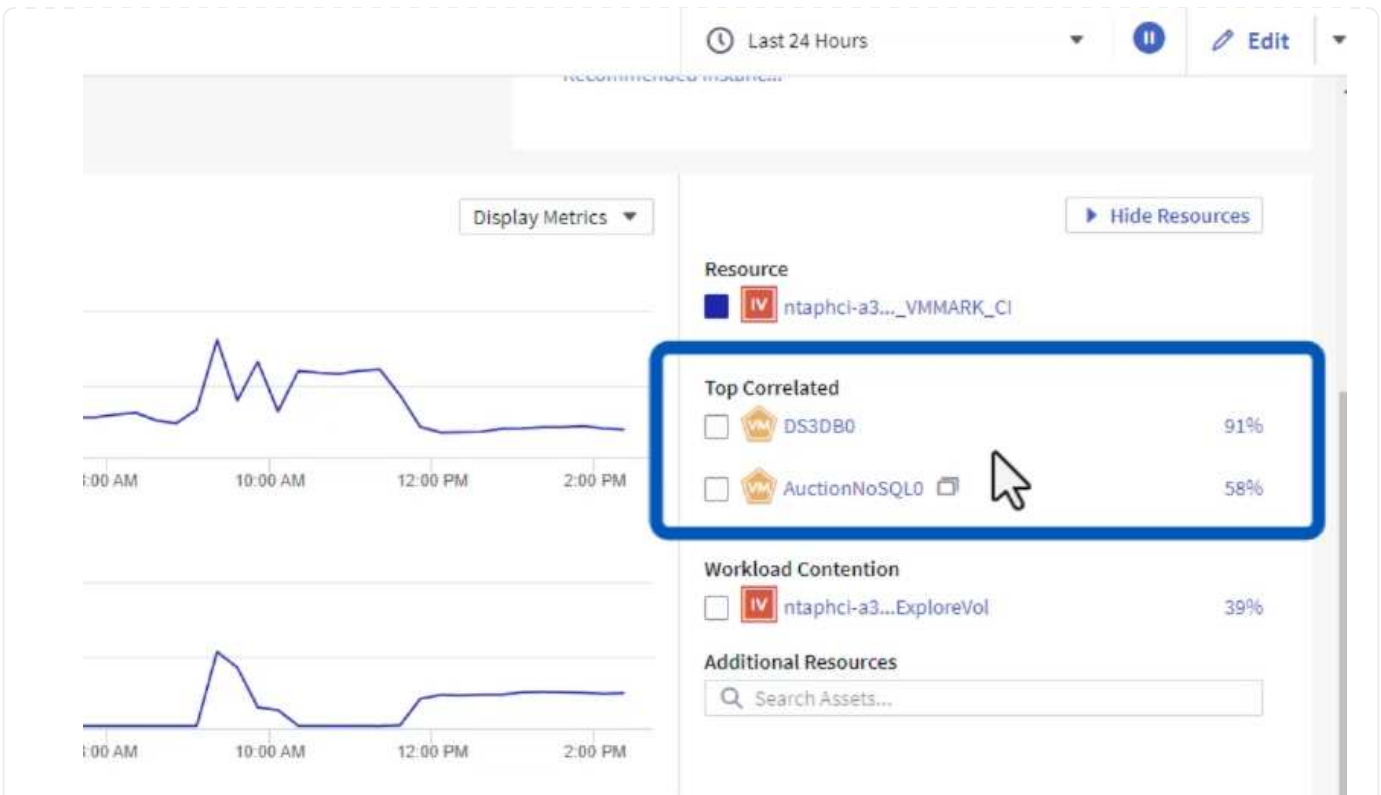
3. Choisissez un tableau de bord pour les performances FlexVol dans la liste et cliquez sur le bouton **Ajouter des tableaux de bord** en bas de la page.



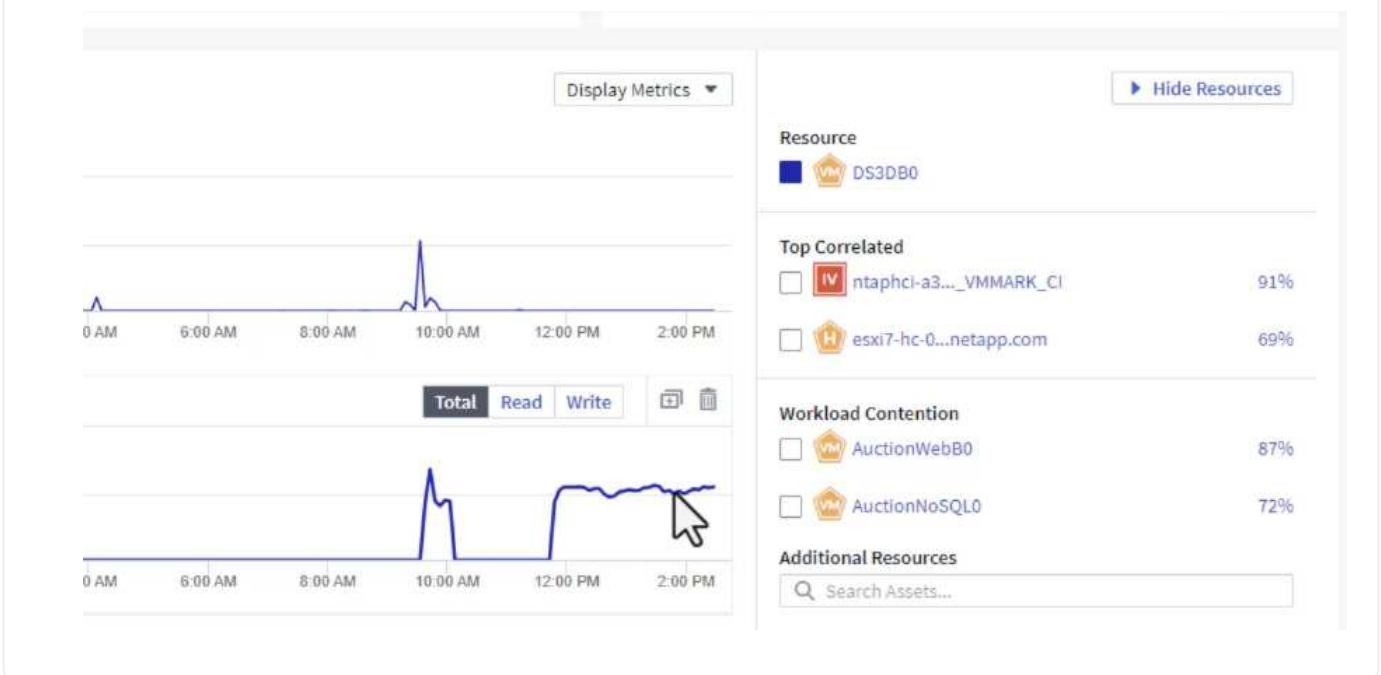
- Une fois importé, ouvrez le tableau de bord. De là, vous pouvez voir différents widgets avec des données de performances détaillées. Ajoutez un filtre pour afficher un système de stockage unique, puis sélectionnez un volume de stockage pour en savoir plus.



- Cette vue permet de visualiser différents metrics liés à ce volume de stockage ainsi que les machines virtuelles les plus utilisées et corrélées s'exécutant sur le volume.



6. En cliquant sur la machine virtuelle présentant le taux d'utilisation le plus élevé, les mesures correspondant à cette machine virtuelle sont prises pour afficher les problèmes potentiels.

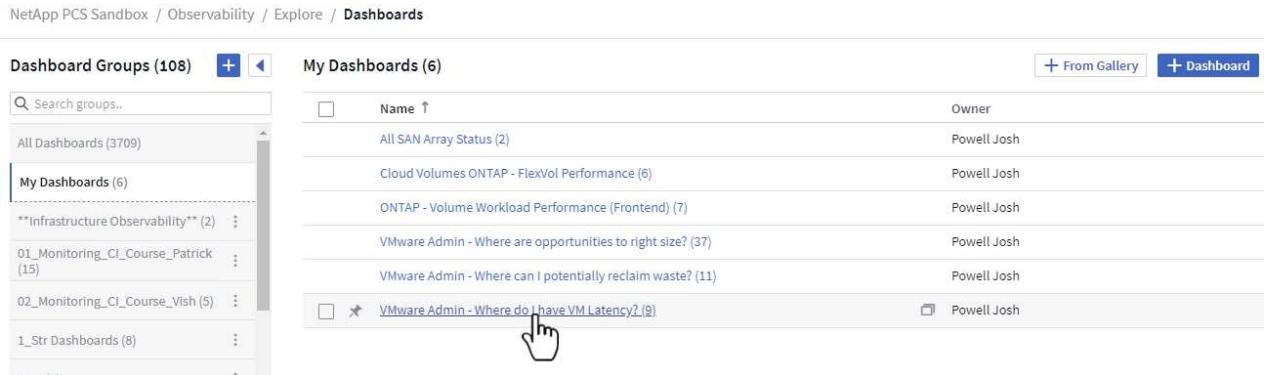


Utilisez Cloud Insights pour identifier les voisins bruyants

Cloud Insights comporte des tableaux de bord capables d'isoler facilement les machines virtuelles homologues qui ont un impact négatif sur d'autres machines virtuelles qui s'exécutent sur le même volume de stockage.

Utilisez un tableau de bord Top VM Latency pour isoler les voisins bruyants

1. Dans cet exemple, accédez à un tableau de bord disponible dans la **Gallery** appelé **VMware Admin - où ai-je une latence VM ?**



2. Ensuite, filtrez par l'annotation **Data Center** créée à l'étape précédente pour afficher un sous-ensemble de ressources.



3. Ce tableau de bord répertorie les 10 machines virtuelles les plus utilisées en termes de latence moyenne. Cliquez ici sur le VM concerné pour en savoir plus.

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

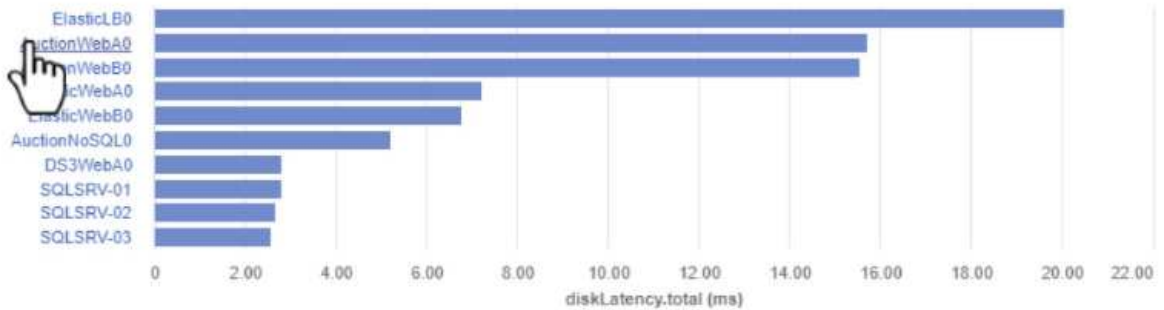
5m

1.55 ms

diskLatency.total

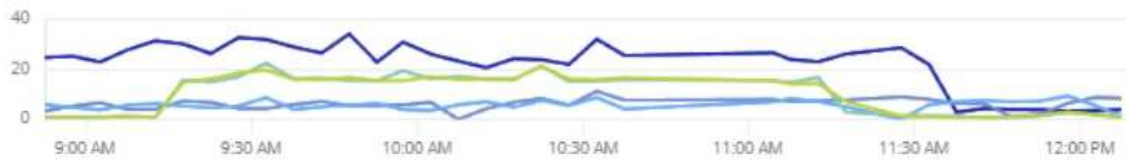
Avg VM Latency - Top 10

5m

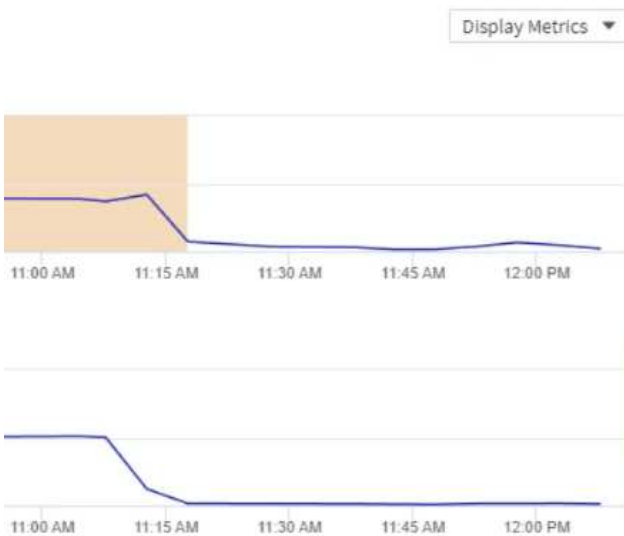


Top 5 Avg VM Latency Trend

30s



4. Les ordinateurs virtuels susceptibles d'entraîner des conflits de charges de travail sont répertoriés et disponibles. Examinez ces mesures de performances des machines virtuelles pour examiner tout problème potentiel.



Resource

VM AuctionWebA0

Top Correlated

esxi7-hc-0...netapp.com 91%

ntaphci-a3..._VMMARK_CI 84%

Workload Contention

AuctionNoSQL0 92%

AuctionWebB0 57%

Additional Resources

Search Assets...

Afficher les ressources sous-utilisées dans Cloud Insights

En adaptant les ressources des ordinateurs virtuels aux exigences réelles des charges de travail, l'utilisation des ressources peut être optimisée, ce qui permet de réaliser des économies sur l'infrastructure et les services cloud. Les données de Cloud Insights peuvent être personnalisées de façon à s'afficher facilement sur ou sous-utilisées des machines virtuelles.

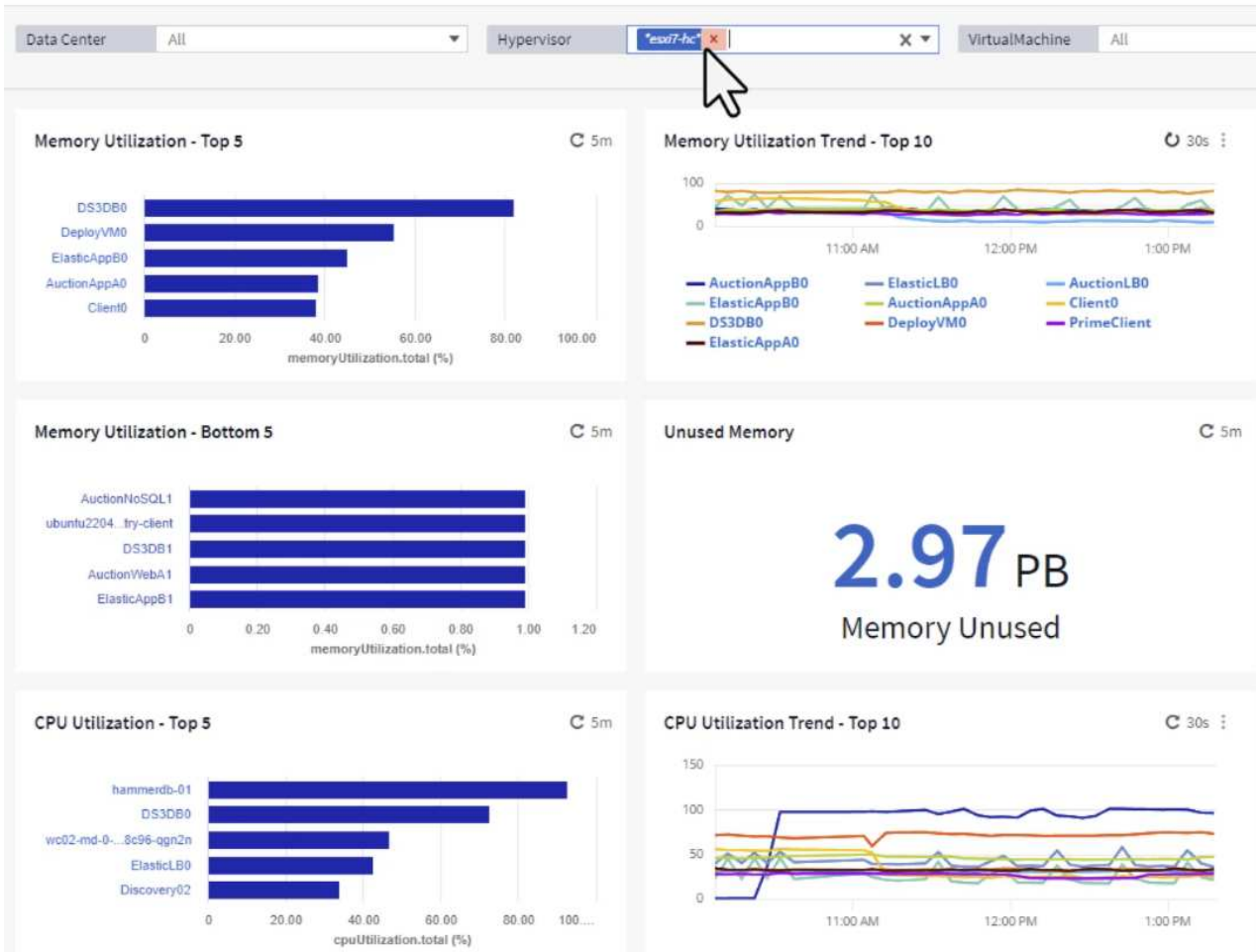
Identifier les opportunités d'adapter la taille des VM

1. Dans cet exemple, accédez à un tableau de bord disponible dans la **Gallery** appelé **VMware Admin - où sont les opportunités de taille correcte ?**

My Dashboards (6)

| <input type="checkbox"/> | Name ↑ |
|--------------------------|---|
| | All SAN Array Status (2) |
| | Cloud Volumes ONTAP - FlexVol Performance (6) |
| | ONTAP - Volume Workload Performance (Frontend) (7) |
| <input type="checkbox"/> | ★ <u>VMware Admin - Where are opportunities to right size? (37)</u> |
| | VMware Admin - Where do I have VMs that potentially reclaim waste? (11) |
| | VMware Admin - Where do I have VM Latency? (9) |

2. Premier filtre par tous les hôtes ESXi du cluster. Vous pouvez ensuite voir le classement des VM supérieures et inférieures en fonction de l'utilisation de la mémoire et du CPU.



3. Les tables permettent le tri et fournissent plus de détails en fonction des colonnes de données choisies.

Memory Usage

5m

121 items found

| Virtual Machine | memory (MiB) | memoryUt... ↓ |
|-----------------------------------|--------------|---------------|
| DS3DB0 | 768.0 | 81.64 |
| DeployVM0 | 92.0 | 55.06 |
| ElasticAppB0 | 92.0 | 44.91 |
| AuctionAppA0 | 336.0 | 38.42 |
| Client0 | 480.0 | 37.98 |
| AuctionAppB0 | 336.0 | 37.83 |
| ElasticAppA0 | 92.0 | 35.63 |
| ElasticLB0 | 96.0 | 35.13 |
| user-cluster1-8872k-78c65dd794... | 92.0 | 32.47 |
| PrimeClient | 48.0 | 30.30 |

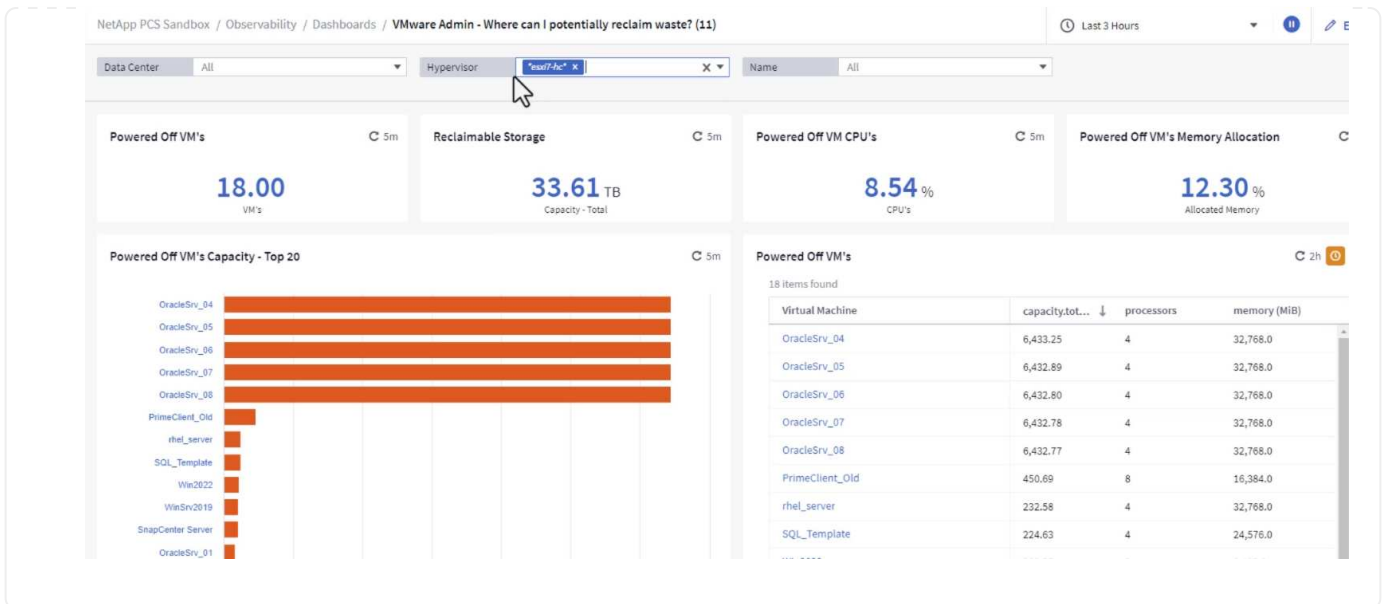
CPU Utilization

5m

121 items found

| Virtual Machine | name |
|---------------------------------|--------------------------------|
| hammerdb-01 | hammerdb-01 |
| DS3DB0 | DS3DB0 |
| wc02-md-0-xwdgb-8cf48c96-qgn... | wc02-md-0-xwdgb-8cf48c96-qg... |
| ElasticLB0 | ElasticLB0 |

4. Un autre tableau de bord appelé **VMware Admin** - où puis-je potentiellement récupérer le **gaspillage** ? affiche les ordinateurs virtuels éteints triés en fonction de leur utilisation de la capacité.

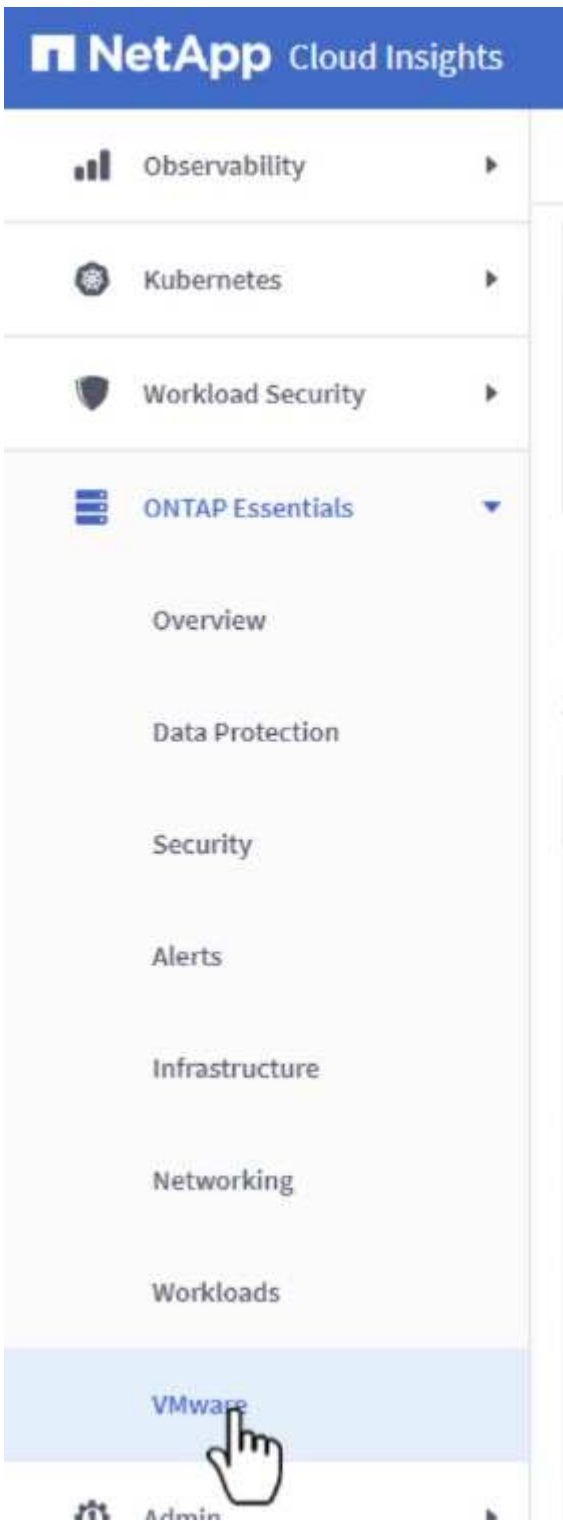


Utilisez des requêtes pour isoler et trier les mesures

La quantité de données capturées par Cloud Insights est assez complète. Les requêtes de mesures constituent un moyen efficace de trier et d'organiser de grandes quantités de données de manière efficace.

Affichez une requête VMware détaillée sous ONTAP Essentials

1. Accédez à **ONTAP Essentials > VMware** pour accéder à une requête complète de mesure VMware.



2. Dans cette vue, plusieurs options de filtrage et de regroupement des données s'affichent en haut. Toutes les colonnes de données sont personnalisables et des colonnes supplémentaires peuvent être facilement ajoutées.

The screenshot shows a dashboard for 'Virtual Machines' with filters for 'storageResources.storage.vendor' (NetApp) and 'host.Los' (vmware). The table below lists 281 items found, with columns for name, powerState, capacity, and disk performance metrics.

| Virtual Machine | name | powerState | capacity.used (GiB) | capacity.total (GiB) | capacityRatio.us... | diskIops.total (I/O/s) | diskLatency.total... | diskThroughput... |
|---------------------|---------------------|------------|---------------------|----------------------|---------------------|------------------------|----------------------|-------------------|
| 01rfk8sprodclient | 01rfk8sprodclient | On | 49.38 | 69.86 | 70.68 | 1.21 | 8.13 | 0.01 |
| 02rfk8sprodserver | 02rfk8sprodserver | On | 63.64 | 74.06 | 85.93 | 22.80 | 4.13 | 0.11 |
| 03rfk8sprodmaster01 | 03rfk8sprodmaster01 | On | 65.13 | 77.21 | 84.36 | 26.64 | 5.64 | 0.20 |
| 04rfk8sprodmaster02 | 04rfk8sprodmaster02 | On | 63.89 | 76.27 | 83.77 | 26.82 | 5.14 | 0.16 |
| 05rfk8sprodmaster03 | 05rfk8sprodmaster03 | On | 63.77 | 75.58 | 84.38 | 28.23 | 4.63 | 0.17 |
| AIQUM 9.11 (vApp) | AIQUM 9.11 (vApp) | On | 152.00 | 152.00 | 100.00 | 23.24 | 0.19 | 0.41 |
| AIQUM 9.12 (Linux) | AIQUM 9.12 (Linux) | On | 55.28 | 100.00 | 55.28 | 0.01 | 11.83 | 0.00 |
| AN-JumpHost01 | AN-JumpHost01 | On | 90.00 | 90.00 | 100.00 | 1.39 | 0.19 | 0.01 |
| AuctionAppA0 | AuctionAppA0 | On | 9.38 | 16.00 | 58.62 | 1.21 | 0.44 | 0.12 |
| AuctionAppA1 | AuctionAppA1 | On | 6.44 | 16.00 | 40.26 | 0.00 | 3.00 | 0.00 |

Conclusion

Cette solution a été conçue comme une amorce pour découvrir comment démarrer avec NetApp Cloud Insights et comment présenter les fonctionnalités puissantes de cette solution d'observabilité. Le produit intègre des centaines de tableaux de bord et de requêtes de metrics qui facilitent la mise en œuvre immédiate. La version complète de Cloud Insights est disponible sous forme d'essai de 30 jours et la version de base est disponible gratuitement pour les clients NetApp.

Informations supplémentaires

Pour en savoir plus sur les technologies présentées dans cette solution, consultez les informations complémentaires suivantes.

- ["Page d'accueil de NetApp BlueXP et Cloud Insights"](#)
- ["Documentation NetApp Cloud Insights"](#)

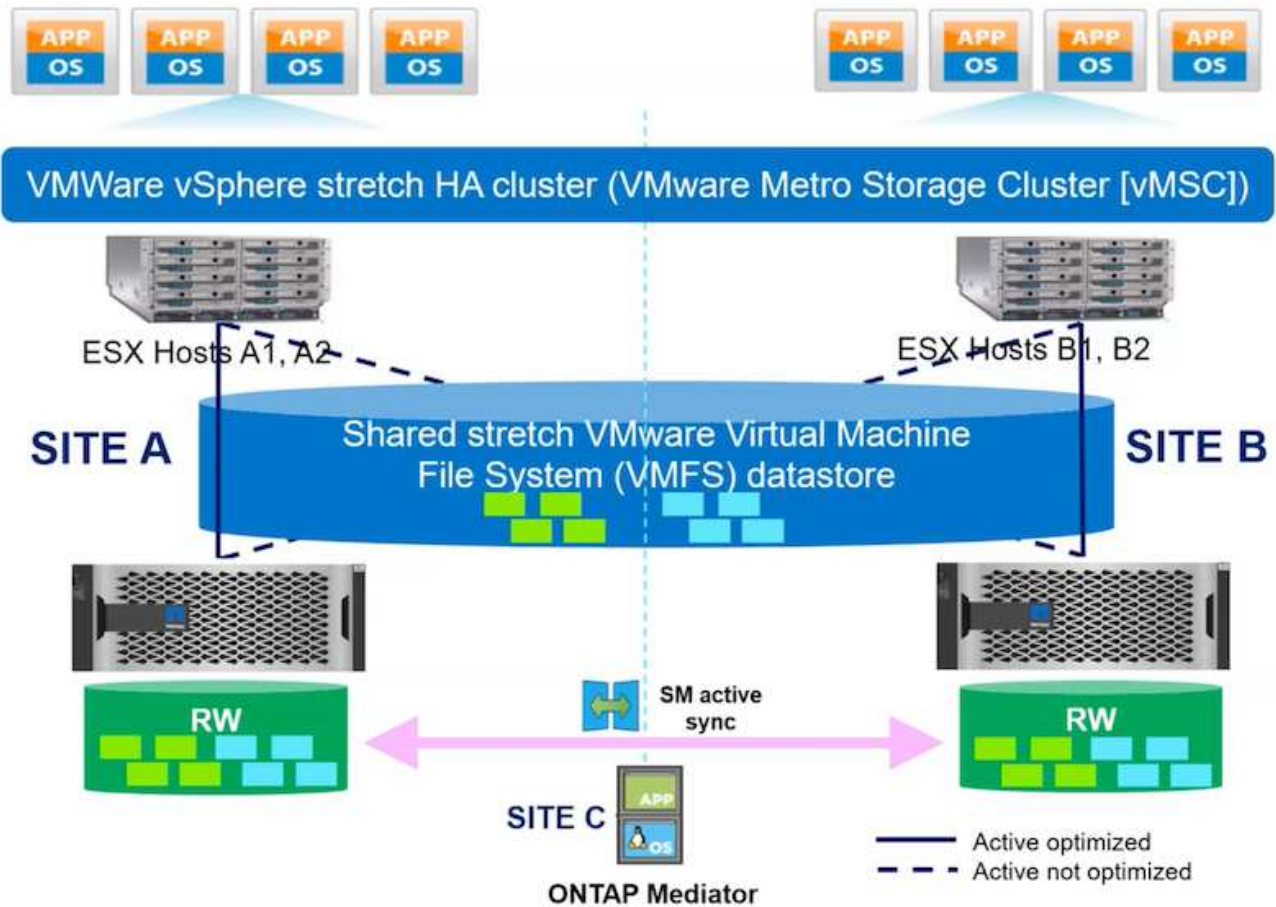
Cluster de stockage VMware vSphere Metro avec synchronisation active SnapMirror

"Cluster de stockage Metro VMware vSphere (vMSC)" Est une solution de cluster étendue à différents domaines de défaillance pour assurer * la mobilité des charges de travail entre les zones de disponibilité ou les sites. * prévention des temps d'arrêt * prévention des catastrophes * récupération rapide

Ce document fournit des informations détaillées sur l'implémentation du vMSC avec l' "[Synchronisation active SnapMirror \(SM-AS\)](#)" utilisation de System Manager et des outils ONTAP. Elle montre également comment protéger la machine virtuelle en effectuant une réplication sur un troisième site et en la gérant avec le plug-in SnapCenter pour VMware vSphere.

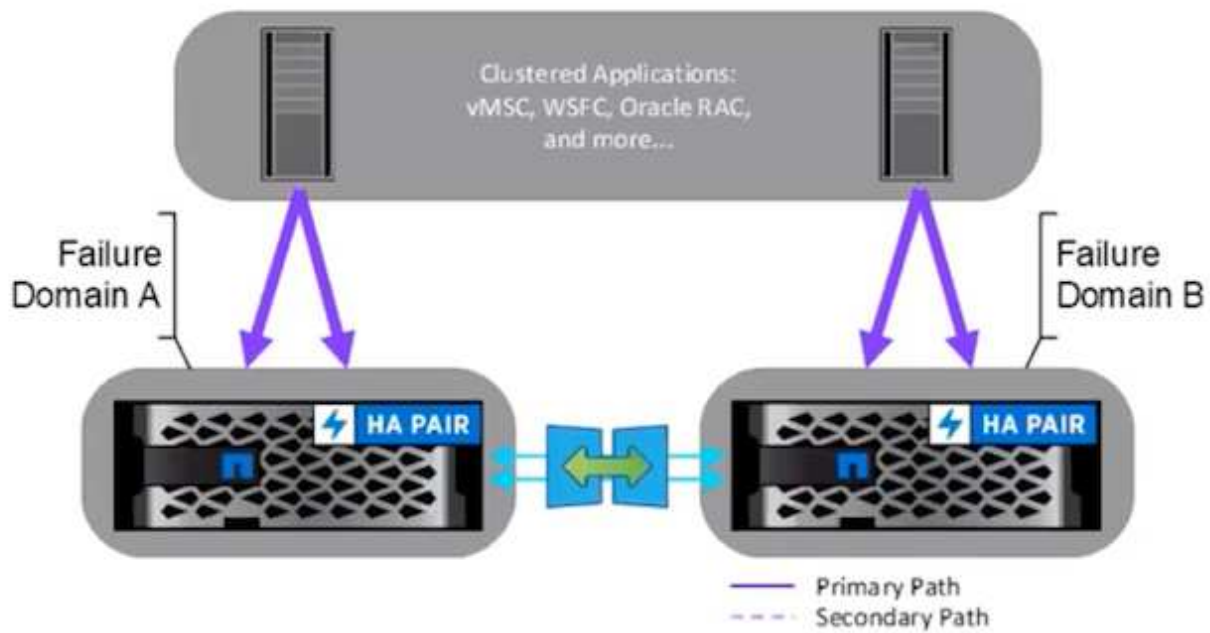
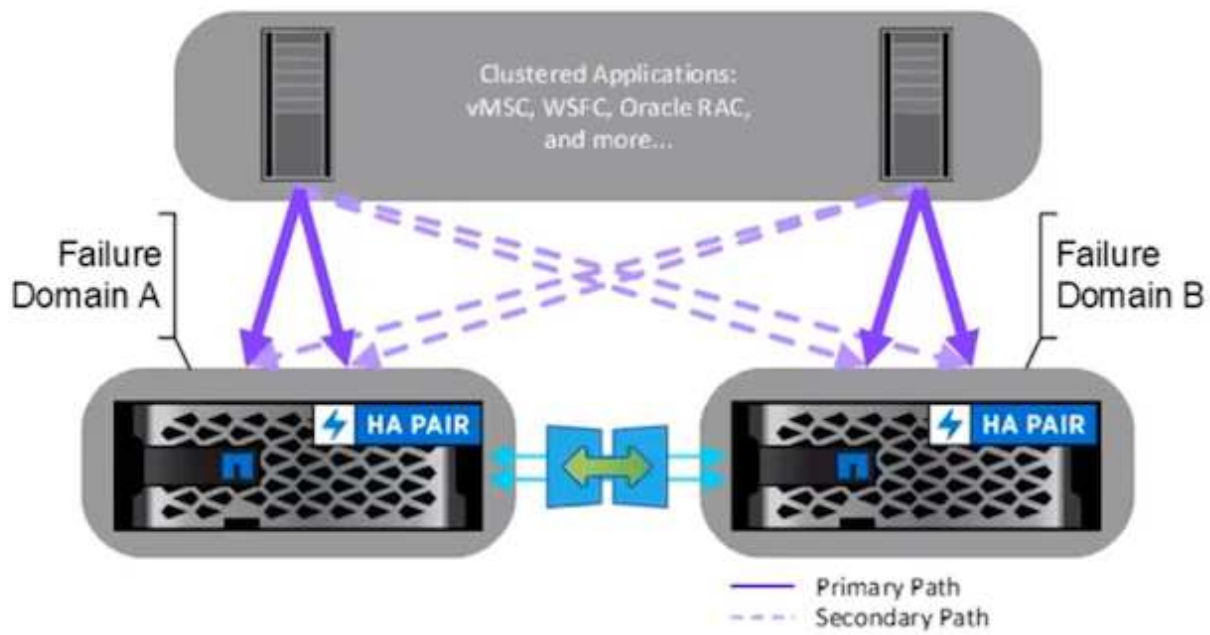
SnapMirror active sync

General availability release 9.15.1 for symmetric configuration



La synchronisation active SnapMirror prend en charge les baies de stockage ASA, AFF et FAS. Il est recommandé d'utiliser le même type (modèles Performance/Capacity) sur les deux domaines de défaillance. Actuellement, seuls les protocoles de bloc tels que FC et iSCSI sont pris en charge. Pour plus d'informations, reportez-vous aux sections "[Matrice d'interopérabilité](#)" et "[Hardware Universe](#)"

VMSC prend en charge deux modèles de déploiement différents nommés accès hôte uniforme et accès hôte non uniforme. Dans une configuration d'accès hôte uniforme, chaque hôte du cluster a accès à la LUN sur les deux domaines de défaillance. Elle est généralement utilisée dans différentes zones de disponibilité dans un même data Center.



Dans une configuration d'accès hôte non uniforme, l'hôte n'a accès qu'au domaine de pannes local. Il est généralement utilisé sur différents sites où l'exécution de plusieurs câbles sur les domaines de défaillance est une option restrictive.



En mode d'accès hôte non uniforme, les machines virtuelles seront redémarrées dans un autre domaine de défaillance par vSphere HA. La disponibilité de l'application sera influencée par sa conception. Le mode d'accès hôte non uniforme est pris en charge uniquement avec ONTAP 9.15 et versions ultérieures.

Prérequis

- "Hôtes VMware vSphere déployés avec une structure de stockage double (deux HBA ou VLAN double pour iSCSI) par hôte".
- "Les baies de stockage sont déployées avec une agrégation de liens pour les ports de données (pour iSCSI)".
- "Des VM et LIF de stockage sont disponibles"
- "Le temps d'aller-retour de latence entre clusters doit être inférieur à 10 millisecondes".
- "Le serveur virtuel du médiateur ONTAP est déployé sur un autre domaine de défaillance"
- "La relation entre clusters est établie"
- "La relation entre les pairs SVM est établie"
- "Mediator ONTAP enregistré sur le cluster ONTAP"



Si vous utilisez un certificat auto-signé, le certificat de l'autorité de certification peut être récupéré dans <installation path>/ontap_médiateur/Server_config/ca.crt sur la machine virtuelle médiateur.

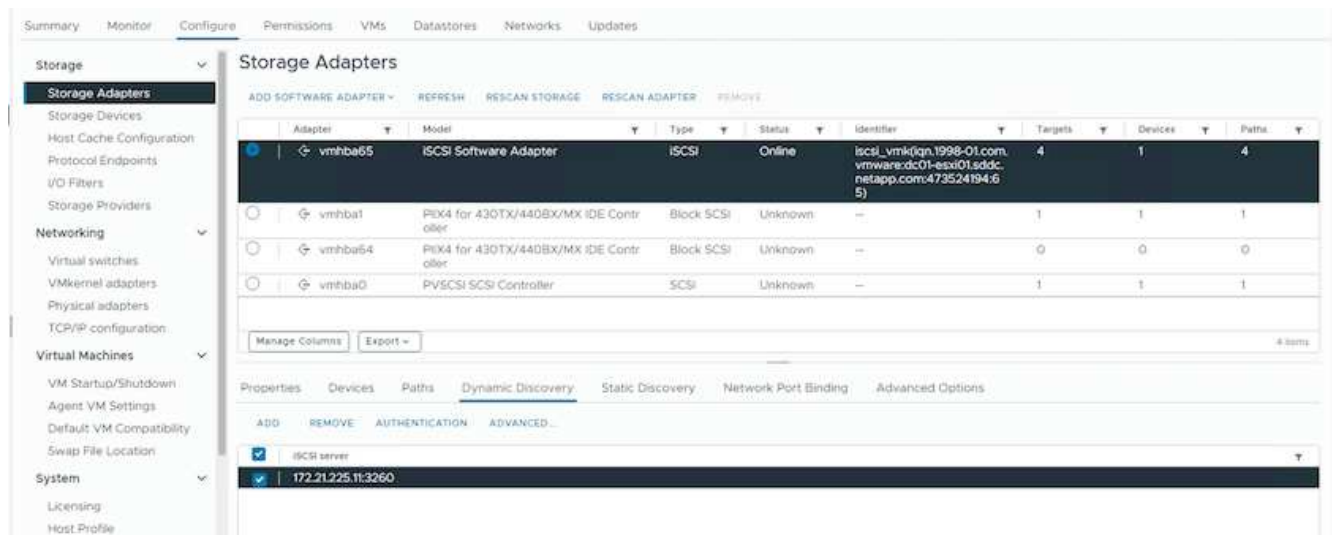
Accès hôte non uniforme VMSC avec l'interface utilisateur de ONTAP System Manager.

Remarque : les outils ONTAP 10.2 ou version ultérieure peuvent être utilisés pour provisionner un datastore étendu avec un mode d'accès hôte non uniforme sans changer d'interface utilisateur. Cette section est fournie à titre de référence uniquement si les outils ONTAP ne sont pas utilisés.

1. Notez l'une des adresses IP de la lif de données iSCSI de la matrice de stockage du domaine de pannes local.

| Name | Status | Storage VM | IPspace | Address | Current node | Current p... | Portset | Protocols | Ty... | Throughput |
|---------|--------|------------|---------|---------------|--------------|--------------|---------|-----------|-------|------------|
| iscsi02 | ✓ | zonea | Default | 172.21.226.11 | E13A300_1 | a0a-3482 | | iSCSI | D... | 0 |
| iscsi03 | ✓ | zonea | Default | 172.21.225.12 | E13A300_2 | a0a-3481 | | iSCSI | D... | 0.33 |
| iscsi04 | ✓ | zonea | Default | 172.21.226.12 | E13A300_2 | a0a-3482 | | iSCSI | D... | 0.01 |
| iscsi01 | ✓ | zonea | Default | 172.21.225.11 | E13A300_1 | a0a-3481 | | iSCSI | D... | 0 |

2. Sur l'adaptateur de stockage iSCSI hôte vSphere, ajoutez cette adresse IP iSCSI sous l'onglet Dynamic Discovery (détection dynamique).



Pour le mode d'accès uniforme, vous devez fournir l'adresse lif de données iSCSI du domaine de pannes source et cible.

- Répétez l'étape ci-dessus sur les hôtes vSphere pour l'autre domaine de pannes en ajoutant son adresse IP lif de données iSCSI locales dans l'onglet Dynamic Discovery.
- Avec une connectivité réseau appropriée, quatre connexions iSCSI doivent exister par hôte vSphere disposant de deux cartes réseau VMKernel iSCSI et de deux lif de données iSCSI par contrôleur de stockage.

```
E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.225.71
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zonea        iscsi01      23    0 172.21.225.11 172.21.225.71 0
zonea        iscsi03      17    0 172.21.225.12 172.21.225.71 0
2 entries were displayed.

E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.226.71
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zonea        iscsi02      24    0 172.21.226.11 172.21.226.71 0
zonea        iscsi04      16    0 172.21.226.12 172.21.226.71 0
2 entries were displayed.
```

- Créer un LUN à l'aide du Gestionnaire système ONTAP, configurer SnapMirror avec la règle de réplication AutomatedFailOverDuplex, sélectionner les initiateurs hôtes et définir la proximité de l'hôte.

Add LUNs ✕

NAME PREFIX

DISK/CD ROM

Group with related LUNs ⓘ

Storage and optimization

NUMBER OF LUNS: CAPACITY PER LUN: GB

PERFORMANCE SERVICE LEVEL

Not sure? [Get help selecting type](#)

Apply the performance limits enforcement to each LUN. If unchecked, these limits will be applied to the entire set of LUNs.

Protection

Enable Snapshot copies (vSAN)

Enable SnapMirror (local or remote)

RESTRICTION ADJUST

 Show legacy policies ⓘ

Source

CLUSTER: E13A200
 STORAGE VOL: zohba
 CONSISTENCY GROUP:

Destination

CLUSTER: Refresh
 STORAGE VOL:

Destination settings

ⓘ You should manually create anigroup by adding replicated hosts in the destination cluster and map the group to the newly created LUNs.

Host information

HOST OPERATING SYSTEM: LUN POWER:

HOST VENDOR

Existing initiator group

New initiator group using existing initiator groups

Host initiators

INITIATOR GROUP NAME

iSCSI Initiators (2)

| Name | Description | In proximity to |
|---|-------------|-----------------|
| <input type="checkbox"/> ipn.1954-01.com.redhat.51c1788998b | - | None |
| <input type="checkbox"/> ipn.1954-01.com.redhat.a3435046678 | - | None |
| <input checked="" type="checkbox"/> ipn.1958-01.com.vmware.s01-aaa01.s0... | - | Source |
| <input checked="" type="checkbox"/> ipn.1958-01.com.vmware.s01-aaa02.s12... | - | Source |
| <input type="checkbox"/> ipn.1958-01.com.vmware.s01-aaa01.s0... | - | Destination |

[+ Add initiator](#)

6. Sur une autre baie de stockage de domaine de panne, créez le groupe initiateur SAN avec ses initiateurs hôtes vSphere et définissez la proximité de l'hôte.

Overview Mapped LUNs

STORAGE VM
zonebTYPE
VMwarePROTOCOL
Mixed (iSCSI & FC)COMMENT
-PORTSET
-CONNECTION STATUS ?OK

Initiators

| Name | De... | Connection status ? | In proximity to |
|--|-------|----------------------------------|-----------------|
| iqn.1998-01.com.vmware:dc02-esxi01.sddc.netap... | - | OK | zoneb |
| iqn.1998-01.com.vmware:dc02-esxi02.sddc.netap... | - | OK | zoneb |



En mode d'accès uniforme, le groupe initiateur peut être répliqué à partir du domaine de pannes source.

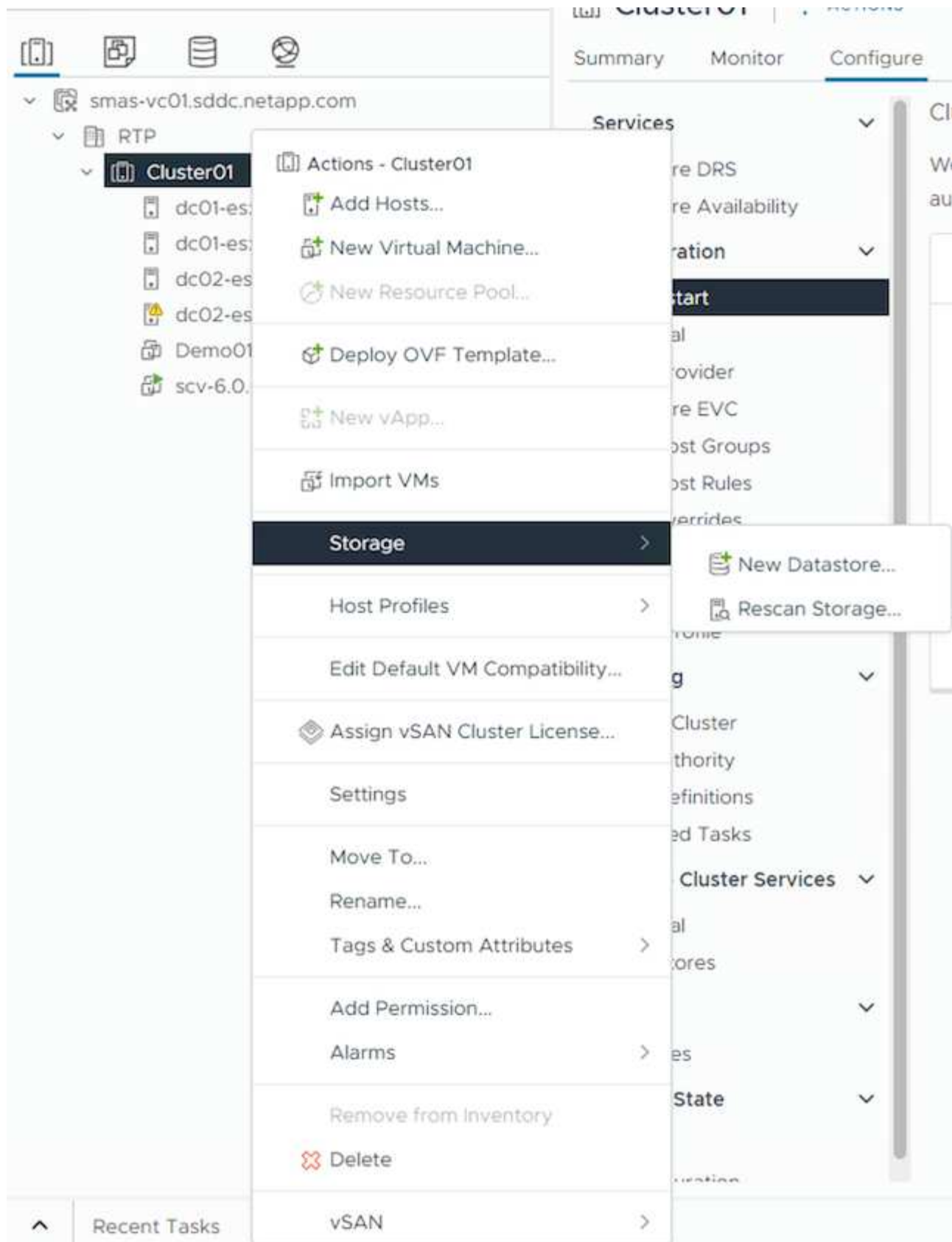
7. Mappez la LUN répliquée avec le même ID de mappage que dans le domaine de pannes source.

Overview Mapped LUNs

[+ Add](#) [Map LUNs](#)[Filter](#)

| <input type="checkbox"/> | Name | ID |
|--------------------------|------|----|
| <input type="checkbox"/> | ds02 | 1 |
| <input type="checkbox"/> | ds01 | 0 |

8. Dans vCenter, cliquez avec le bouton droit de la souris sur le cluster vSphere et sélectionnez Rescan Storage option (Réanalyser le stockage).



9. Sur l'un des hôtes vSphere du cluster, vérifiez que le nouveau périphérique s'affiche et que le datastore n'est pas utilisé.

dc01-esxi01.sddc.netapp.com | ACTIONS

Summary Monitor **Configure** Permissions VMs Datastores Networks Updates

Storage

- Storage Adapters**
 - Storage Devices
 - Host Cache Configuration
 - Protocol Endpoints
 - I/O Filters
 - Storage Providers
- Networking**
 - Virtual switches
 - VMkernel adapters
 - Physical adapters
 - TCP/IP configuration
- Virtual Machines**
 - VM Startup/Shutdown
 - Agent VM Settings
 - Default VM Compatibility
 - Swap File Location
- System**
 - Licensing
 - Host Profile
 - Time Configuration
 - Authentication Services

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

| Adapter | Model | Type | Status | Identifier | Targets | Devices | Paths |
|---------|---|------------|---------|--|---------|---------|-------|
| vmhba65 | ISCSI Software Adapter | ISCSI | Online | iscsi_vmk1(qn.1998-01.com,vmware:dc01-esxi01.sddc.netapp.com:473524194.65) | 4 | 2 | 8 |
| vmhba1 | PIIX4 for 430TX/440BX/MX IDE Contr other | Block SCSI | Unknown | -- | 1 | 1 | 1 |
| vmhba64 | PIIX4 for 430TX/440BX/MX IDE Contr other | Block SCSI | Unknown | -- | 0 | 0 | 0 |
| vmhba0 | PVSCSI SCSI Controller | SCSI | Unknown | -- | 1 | 1 | 1 |

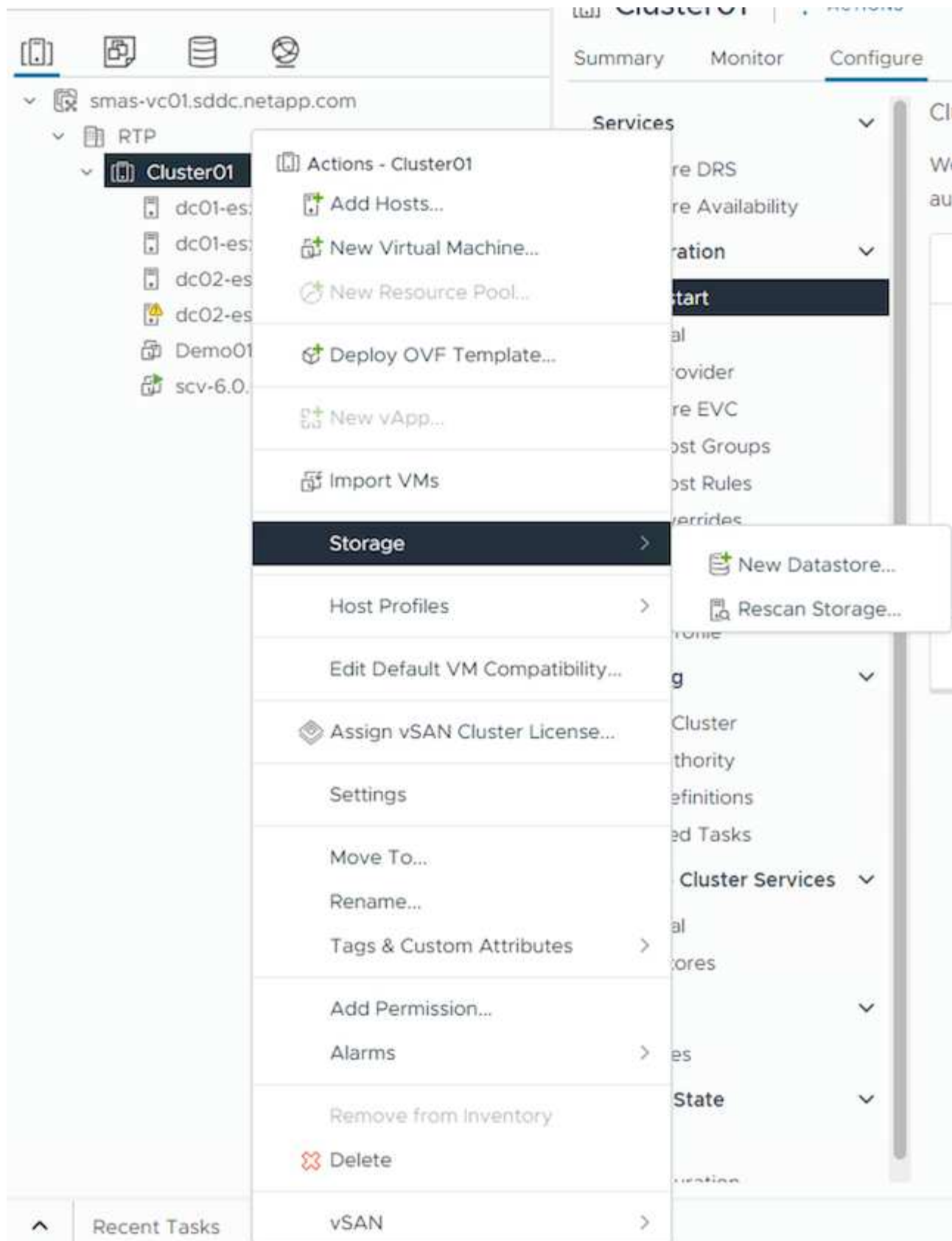
Manage Columns Export ▾ 4 items

Properties **Devices** Paths Dynamic Discovery Static Discovery Network Port Binding Advanced Options

REFRESH ATTACH DETACH RENAME

| Name | LUN | Type | Capacity | Datastore | Operational State | Hardware Acceleration | Drive Type | Transport |
|--|-----|------|-----------|--------------|-------------------|-----------------------|------------|-----------|
| NETAPP iSCSI Disk (naa.600a0980383038467724524975577933) | 0 | disk | 250.00 GB | DS01 | Attached | Supported | Flash | iSCSI |
| NETAPP iSCSI Disk (naa.600a0980383038467724524975577933) | 1 | disk | 300.00 GB | Not Consumed | Attached | Supported | Flash | iSCSI |

10. Dans vCenter, cliquez avec le bouton droit de la souris sur le cluster vSphere et sélectionnez l'option Nouveau datastore.



11. Dans l'assistant, n'oubliez pas de fournir le nom du datastore et de sélectionner le périphérique avec la capacité et l'ID de périphérique appropriés

New Datastore

- Type
- Name and device selection**
- VMFS version
- Partition configuration
- Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name:

Info: The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

Select a host:
Select a host to view its accessible disks/LUNs:

| | Name | LUN | Capacity | Hardware Acceleration | Drive Type | Sector Format | Ch... |
|----------------------------------|--|-----|------------|-----------------------|------------|---------------|-------|
| <input checked="" type="radio"/> | NETAPP iSCSI Disk (naa.600a0980383038467724524975577933) | 1 | 300.00 G B | Supported | Flash | 512e | Nc |
| <input type="radio"/> | Local VMware Disk (mpx.vmhba0:CO:T:LO) | 0 | 100.00 G B | Not support ed | HDD | 512n | Nc |

Manage Columns | Export v | 2 items

CANCEL | BACK | NEXT

12. Vérifiez que le datastore est monté sur tous les hôtes du cluster sur les deux domaines de panne.

DS02 | ACTIONS

Summary | Monitor | **Configure** | Permissions | Files | Hosts | VMs

Alarm Definitions
 Scheduled Tasks
 General
 Device Backing
Connectivity and Multipathing
 Hardware Acceleration
 Capability sets
 SnapCenter Plug-in for VMware
 Resource Groups
 Backups

Connectivity and Multipathing

Mount | Unmount

| | Host | Datastore Mounted | Datastore Connectivity | Mount Point |
|----------------------------------|-----------------------------|-------------------|------------------------|---|
| <input checked="" type="radio"/> | dc01-esxi01.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e |
| <input type="radio"/> | dc01-esxi02.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e |
| <input type="radio"/> | dc02-esxi01.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e |
| <input type="radio"/> | dc02-esxi02.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e |

Manage Columns | 4 items

Device NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)
 ACTIONS v

- Path Selection Policy: Round Robin (VMware)
- Storage Array Type Policy: VMW_SATP_ALUA
- Owner Plugin: NMP

Paths REFRESH | ENABLE | DISABLE

| | Runtime Name | Status | Target | LUN | Preferred |
|-----------------------|-------------------|--------------|--|-----|-----------|
| <input type="radio"/> | vmhba65:CO:T:LO:1 | Active | iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56-vs-28-172.21.225.11:3260 | 1 | No |
| <input type="radio"/> | vmhba65:C2:T:LO:1 | Active (I/O) | iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56-vs-28-172.21.225.12:3260 | 1 | No |
| <input type="radio"/> | vmhba65:C3:T:LO:1 | Active | iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56-vs-28-172.21.226.11:3260 | 1 | No |
| <input type="radio"/> | vmhba65:C1:T:LO:1 | Active (I/O) | iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a7:0d56-vs-28-172.21.226.12:3260 | 1 | No |

DS02 ACTIONS

Summary Monitor **Configure** Permissions Files Hosts VMs

Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity and Multipathing
Hardware Acceleration
Capability sets
SnapCenter Plug-in for VMware
Resource Groups
Backups

Connectivity and Multipathing

Mount UNMOUNT

| Host | Host | Datastore Mounted | Datastore Connectivity | Mount Point |
|-----------------------------|---------|-------------------|---|-------------|
| dc01-esxi01.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e | |
| dc01-esxi02.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e | |
| dc02-esxi01.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e | |
| dc02-esxi02.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e | |

Manage Columns 4 items

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577933) ↗

Multipathing Policies ACTIONS

- Path Selection Policy: Round Robin (VMware)
- Storage Array Type: VMW_SATP_ALUA
- Policy:
- Owner Plugin: NMP

Paths

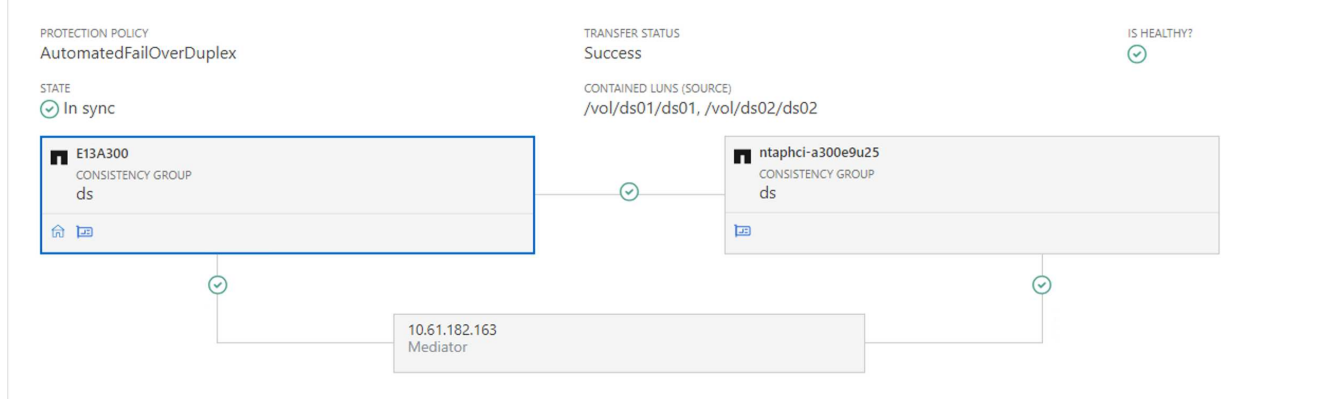
REFRESH ENABLE DISABLE

| Route Name | Status | Target | LLN | Preferred |
|------------------|--------------|--|-----|-----------|
| vmhba65:C2:T0:L1 | Active (I/O) | iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.225.22.3260 | 1 | No |
| vmhba65:C0:T0:L1 | Active | iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.225.22.3260 | 1 | No |
| vmhba65:C3:T0:L1 | Active (I/O) | iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.226.21.3260 | 1 | No |
| vmhba65:C1:T0:L1 | Active | iqn.1992-08.com.netapp:sn.133a93efce6b1edbb10000a098b46a21vs.12.172.21.226.22.3260 | 1 | No |



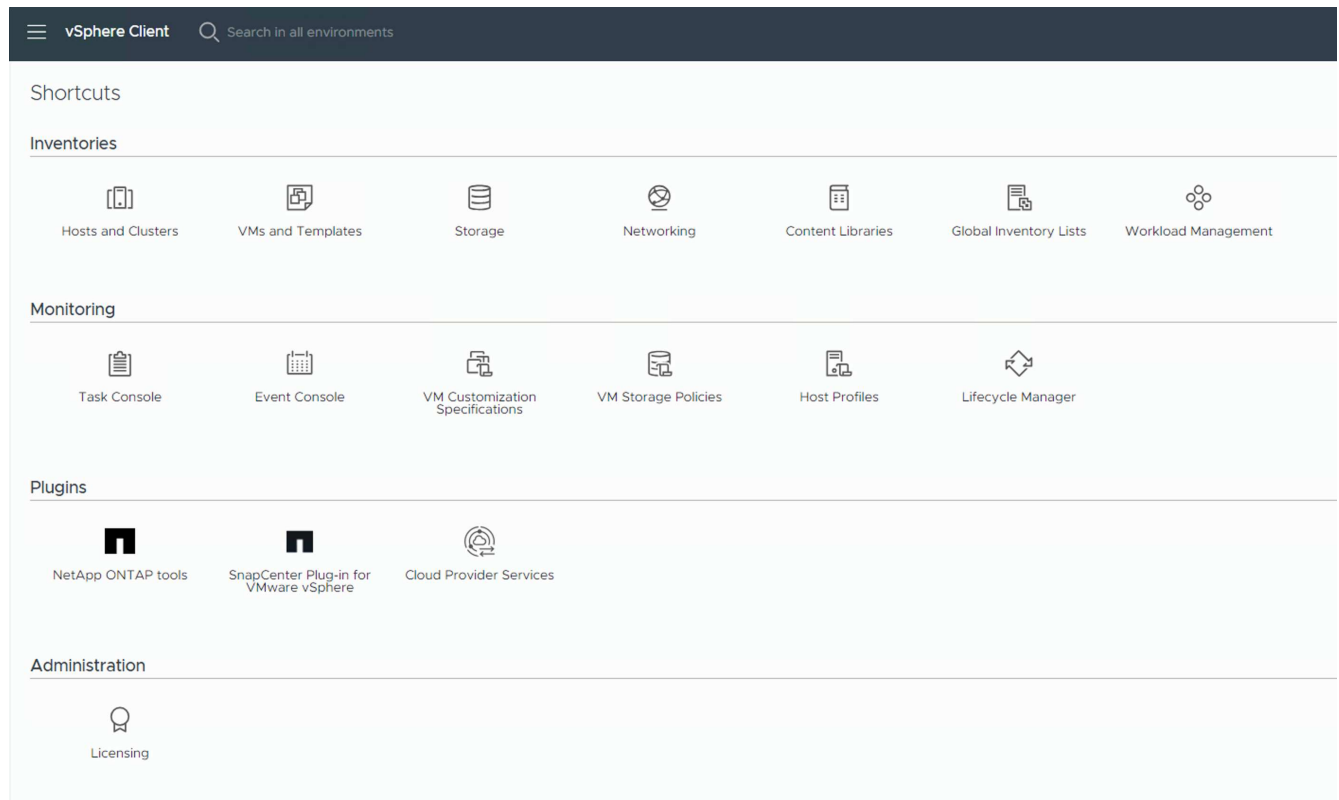
Les captures d'écran ci-dessus montrent les E/S actives sur un seul contrôleur depuis que nous avons utilisé AFF. Pour ASA, elle aura des E/S actives sur tous les chemins.

- Lorsque des datastores supplémentaires sont ajoutés, n'oubliez pas d'étendre le groupe de cohérence existant pour qu'il soit cohérent dans l'ensemble du cluster vSphere.



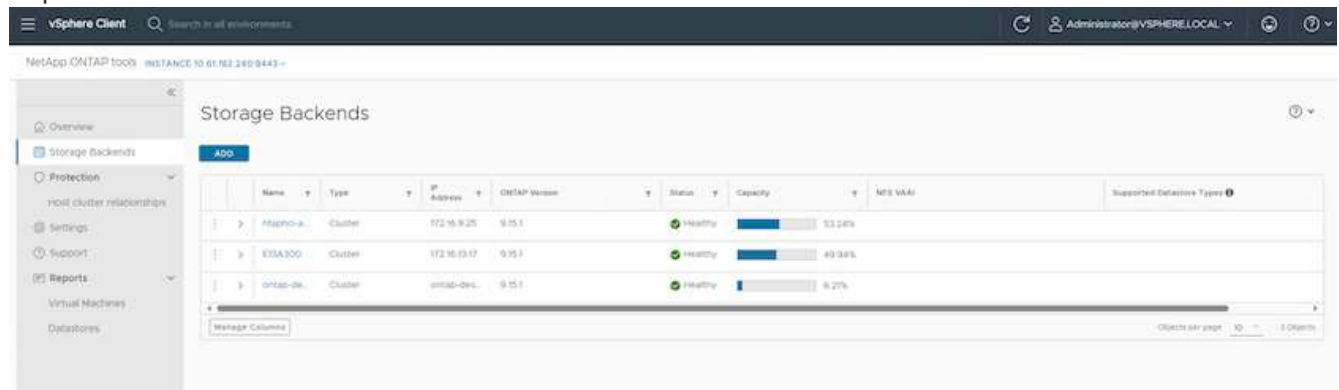
Mode d'accès hôte uniforme VMSC avec les outils ONTAP.

- Assurez-vous que les outils NetApp ONTAP sont déployés et enregistrés dans vCenter.



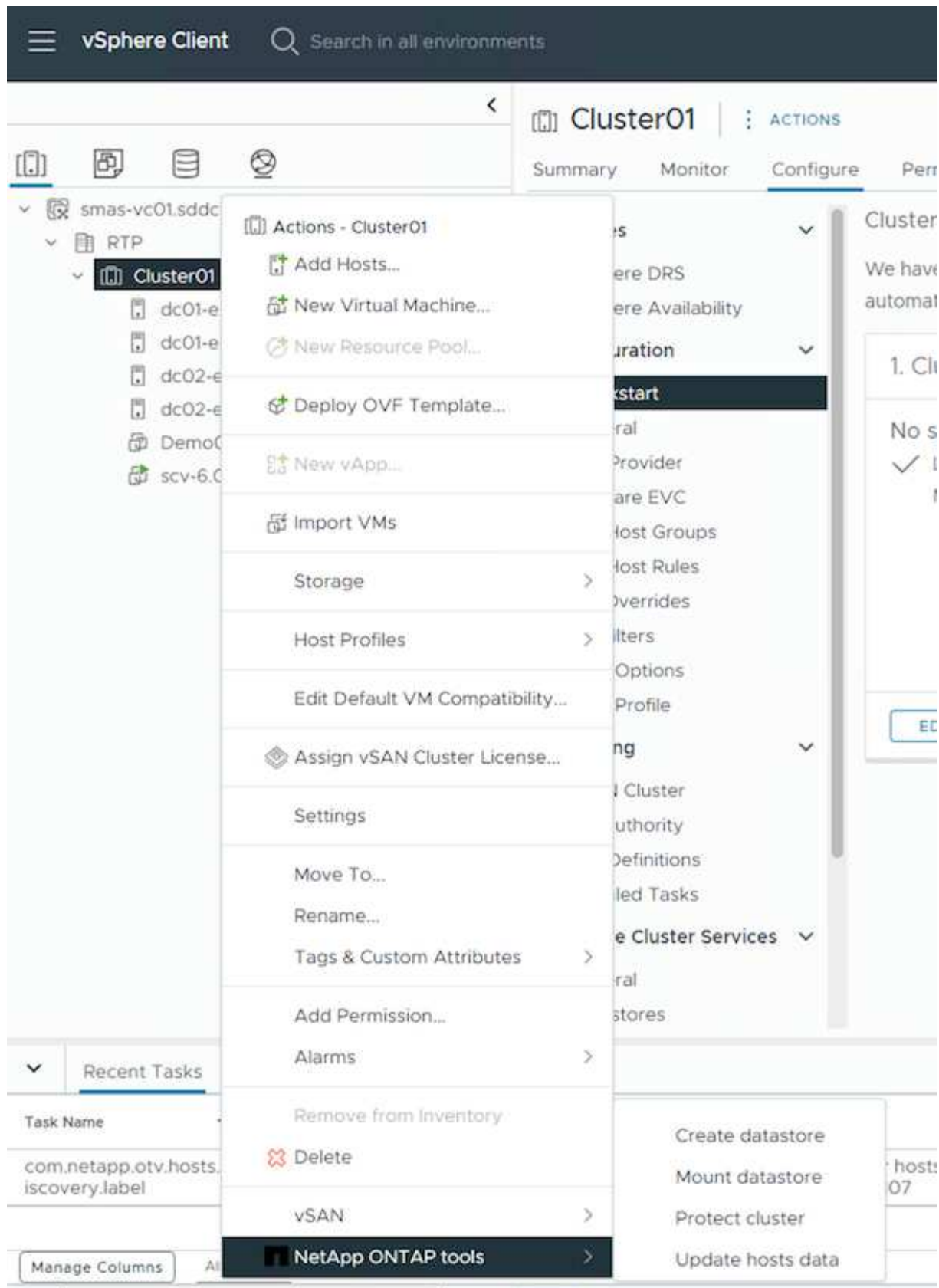
Si ce n'est pas le cas, suivez "[Déploiement des outils ONTAP](#)" les étapes et "[Ajoutez une instance de serveur vCenter](#)"

- Assurez-vous que les systèmes de stockage ONTAP sont enregistrés dans les outils ONTAP. Cela inclut à la fois les systèmes de stockage de domaine de panne et la troisième pour la réplication asynchrone à distance à utiliser pour la protection des machines virtuelles avec le plug-in SnapCenter pour VMware vSphere.



Sinon, suivez les instructions "[Ajoutez le système back-end de stockage à l'aide de l'interface client vSphere](#)"

- Mettre à jour les données des hôtes pour les synchroniser avec les outils ONTAP, puis, "[créer un datastore](#)".



4. Pour activer SM-AS, cliquez avec le bouton droit de la souris sur le cluster vSphere et sélectionnez protéger le cluster dans les outils NetApp ONTAP (voir la capture d'écran ci-dessus).
5. Il affiche les datastores existants pour ce cluster, ainsi que les détails des SVM. Le nom par défaut du groupe de cohérence est <Nom du cluster vSphere>_<SVM name>. Cliquez sur le bouton Ajouter une relation.

Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. [Learn more](#)


Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
[2 datastores](#)

Consistency group name: * Cluster01_zonea

SnapMirror settings

[ADD RELATIONSHIP](#)

| Target storage VM | Policy | Uniform Host Configuration | Host proximity |
|---|--------|----------------------------|----------------|
|  No SnapMirror relationship found. You can protect datastores using one or more SnapMirror relationships. | | | |
| Objects per page 5 0 Object | | | |

[CANCEL](#)

[PROTECT](#)

6. Choisir le SVM cible et définir la politique sur AutomatedFailOverDuplex pour SM-AS. Il existe un commutateur à bascule pour la configuration d'hôte uniforme. Définissez la proximité pour chaque hôte.

Add SnapMirror Relationship

Source storage VM: * E13A300 / zonea

Target storage VM: * zoneb
Cluster: ntaphci-a300e9u25

Policy: * AutomatedFailOverDuplex

Uniform host configuration:

Host proximity settings

 As part of protection, all datastores will be mounted on all hosts.

SET PROXIMAL TO ▾

| <input type="checkbox"/> | Hosts | Proximal to |
|--------------------------|-----------------------------|-------------|
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | dc01-esxi02.sddc.netapp.com | Source ▾ |
| <input type="checkbox"/> | dc02-esxi01.sddc.netapp.com | Target ▾ |

4 Objects

CANCEL

ADD

7. Vérifiez les informations de proximité de l'hôte et d'autres détails. Ajoutez une autre relation au site tiers avec la règle de réplication asynchrone si nécessaire. Cliquez ensuite sur protéger.

Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. [Learn more](#)

Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
[2 datastores](#)

Consistency group name: * Cluster01_zonea

SnapMirror settings

[ADD RELATIONSHIP](#)

| Target storage VM | Policy | Uniform Host Configuration | Host proximity |
|-----------------------------|-------------------------|----------------------------|------------------------|
| ⋮ ntaphci-a300e9u25 / zoneb | AutomatedFailOverDuplex | Yes | Source (2), Target (2) |

Objects per page 1 Object

[CANCEL](#) [PROTECT](#)

REMARQUE : si vous prévoyez d'utiliser le plug-in SnapCenter pour VMware vSphere 6.0, la réplication doit être configurée au niveau du volume plutôt qu'au niveau du groupe de cohérence.

8. Avec un accès hôte uniforme, l'hôte dispose d'une connexion iSCSI aux deux matrices de stockage de domaine de panne.

The screenshot shows the NetApp ONTAP interface for volume DS01. The 'Connectivity and Multipathing' section is active, displaying a table of connections to the host.

| Host | Datastore Mounted | Datastore Connectivity | Mount Point |
|----------------------------|-------------------|------------------------|---|
| dc02-esx01.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e |
| dc01-esx02.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e |
| dc02-esx02.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e |
| dc01-esx01.sddc.netapp.com | Mounted | Connected | /vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e |

Below the connectivity table, the 'Multipathing Policies' section shows:

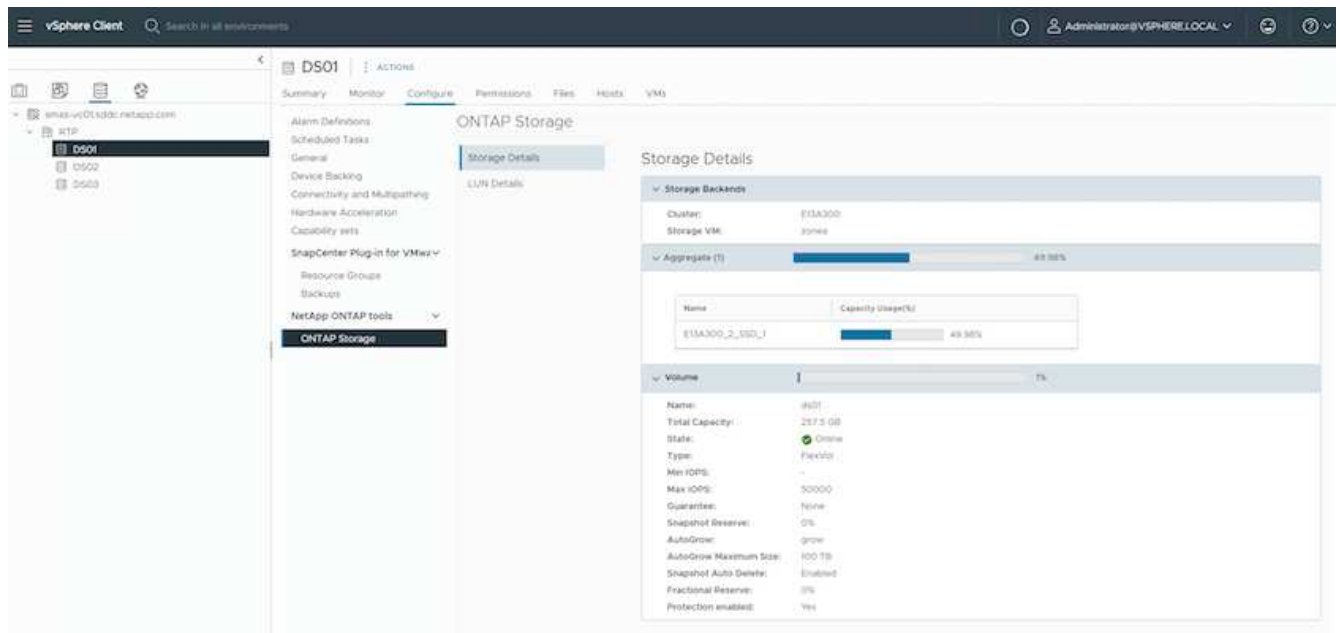
- Path Selection Policy: Round Robin (VMware)
- Storage Array Type Policy: VMW_SATP_ALUA
- Owner Plugin: NMP

The 'Paths' table shows the status of various paths:

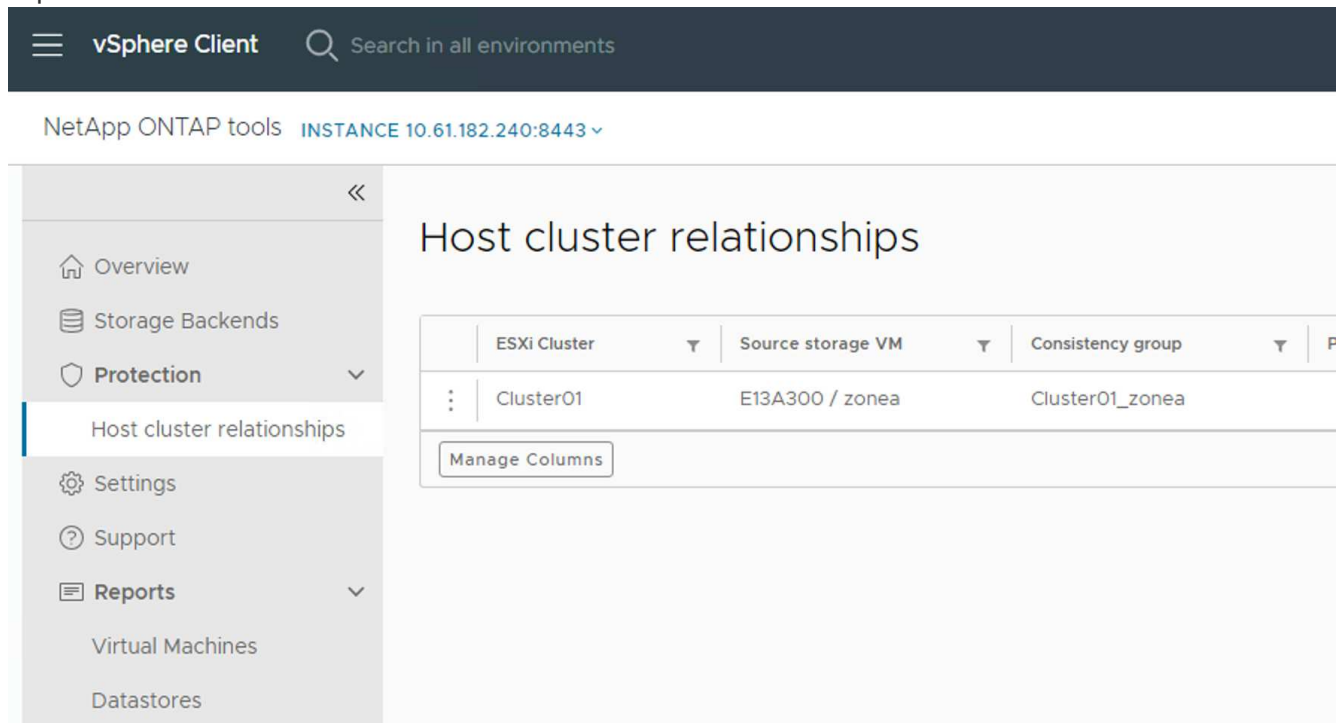
| Runtime Name | Status | Target | LUN |
|------------------|-------------|---|-----|
| vmhba65:C3:T1:L0 | Active | iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.225.12.3260 | 0 |
| vmhba65:C2:T1:L0 | Active | iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.226.12.3260 | 0 |
| vmhba65:C1:T1:L0 | Active | iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.225.11.3260 | 0 |
| vmhba65:C3:T0:L0 | Active (VO) | iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.226.21.3260 | 0 |
| vmhba65:C0:T1:L0 | Active | iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.226.11.3260 | 0 |
| vmhba65:C2:T0:L0 | Active (VO) | iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.225.21.3260 | 0 |
| vmhba65:C1:T0:L0 | Active | iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.226.22.3260 | 0 |
| vmhba65:C0:T0:L0 | Active | iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.225.22.3260 | 0 |

REMARQUE : la capture d'écran ci-dessus provient de AFF. En cas de ASA, les E/S ACTIVES doivent se trouver sur tous les chemins disposant de connexions réseau appropriées.

9. Le plug-in Outils ONTAP indique également que le volume est protégé ou non.

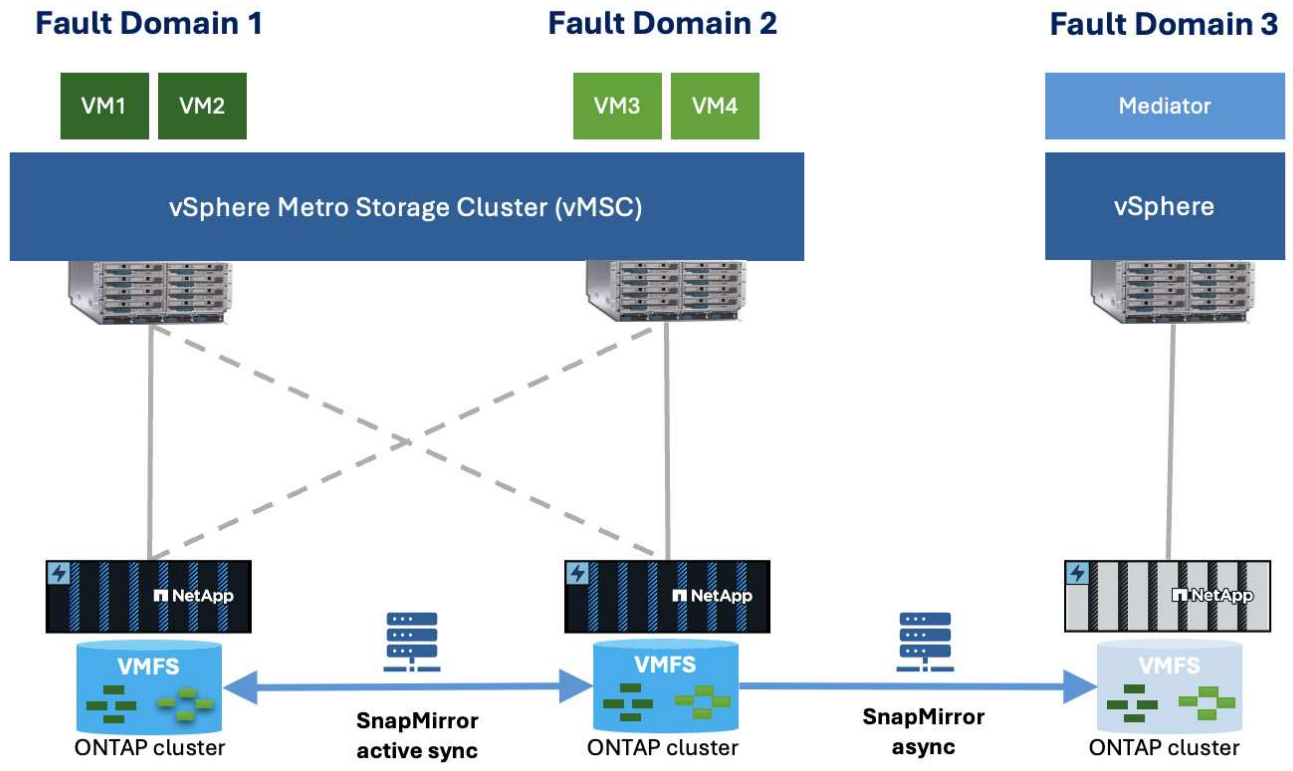


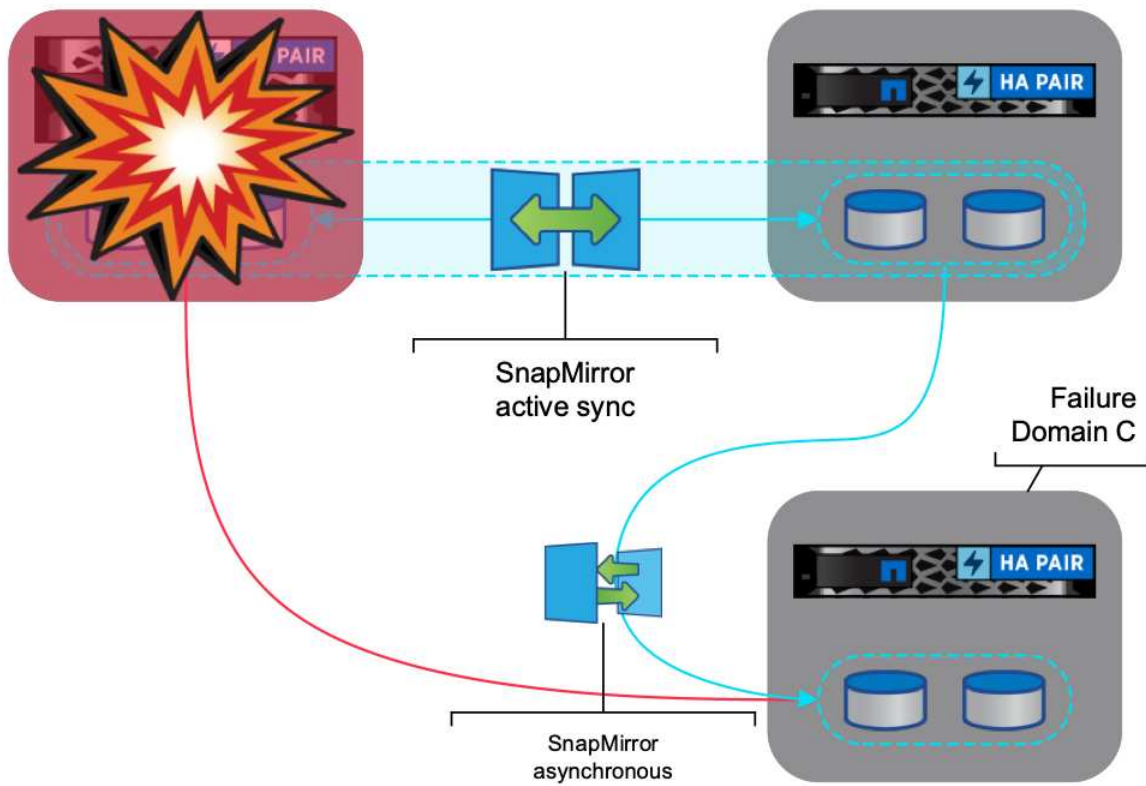
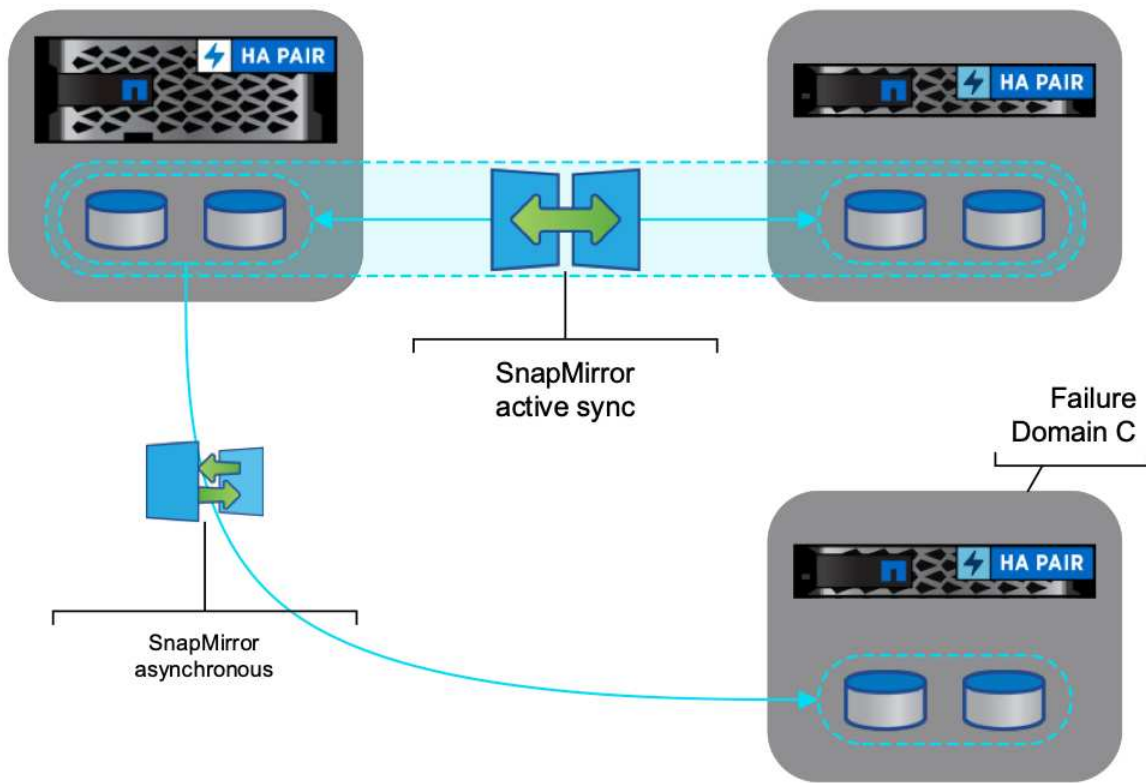
10. Pour plus de détails et pour mettre à jour les informations de proximité de l'hôte, vous pouvez utiliser l'option relations de cluster hôte sous les outils ONTAP.



Protection des machines virtuelles avec le plug-in SnapCenter pour VMware vSphere.

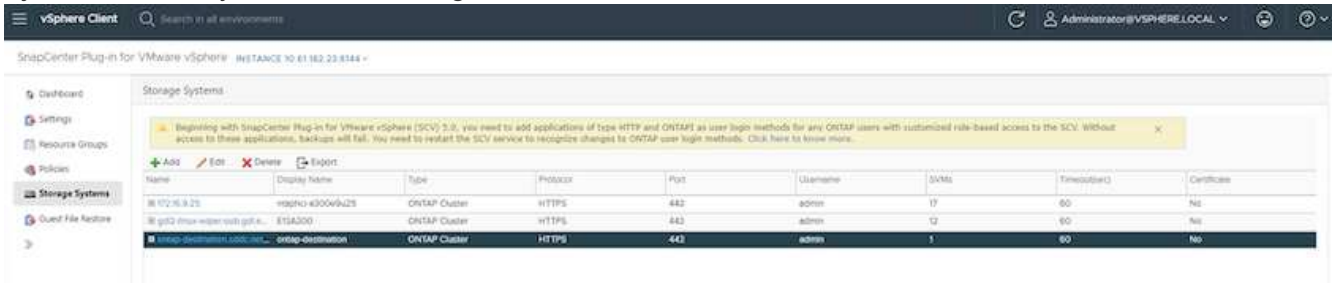
Le plug-in SnapCenter pour VMware vSphere (SCV) 6.0 ou version ultérieure prend en charge la synchronisation active SnapMirror et également en association avec SnapMirror Async pour la réplication vers le troisième domaine de panne.



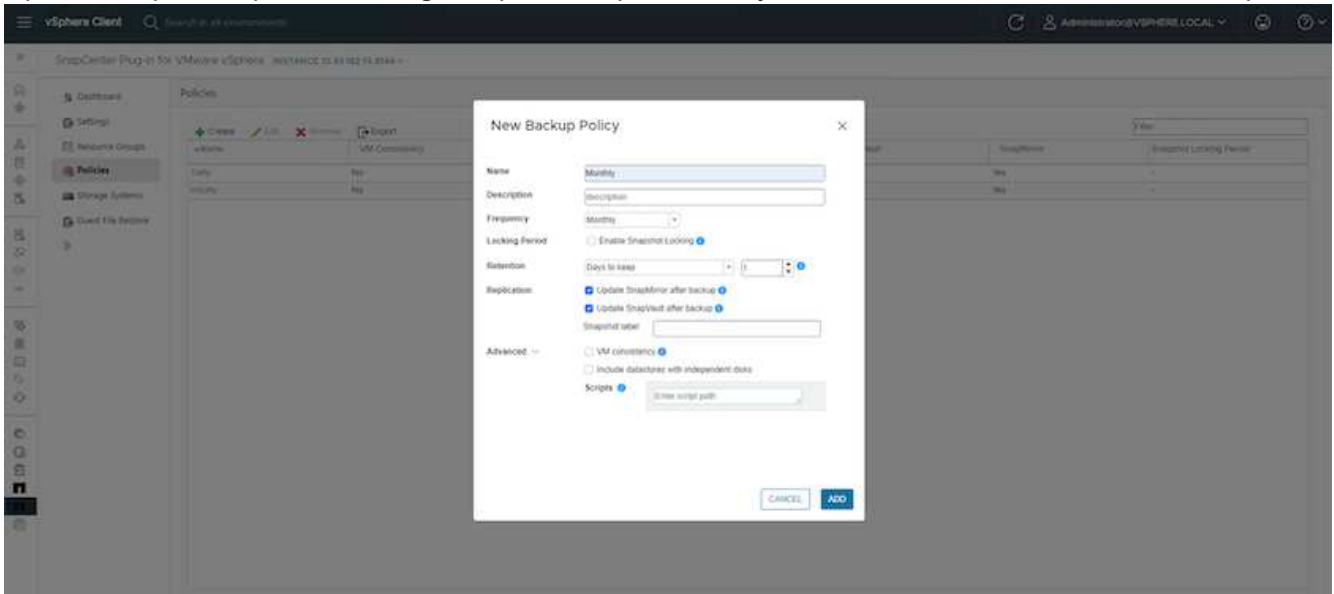


Les cas d'utilisation pris en charge sont les suivants : * sauvegarde et restauration de la machine virtuelle ou du datastore à partir de l'un des domaines de défaillance avec synchronisation active SnapMirror. * Restaurer les ressources à partir du troisième domaine de panne.

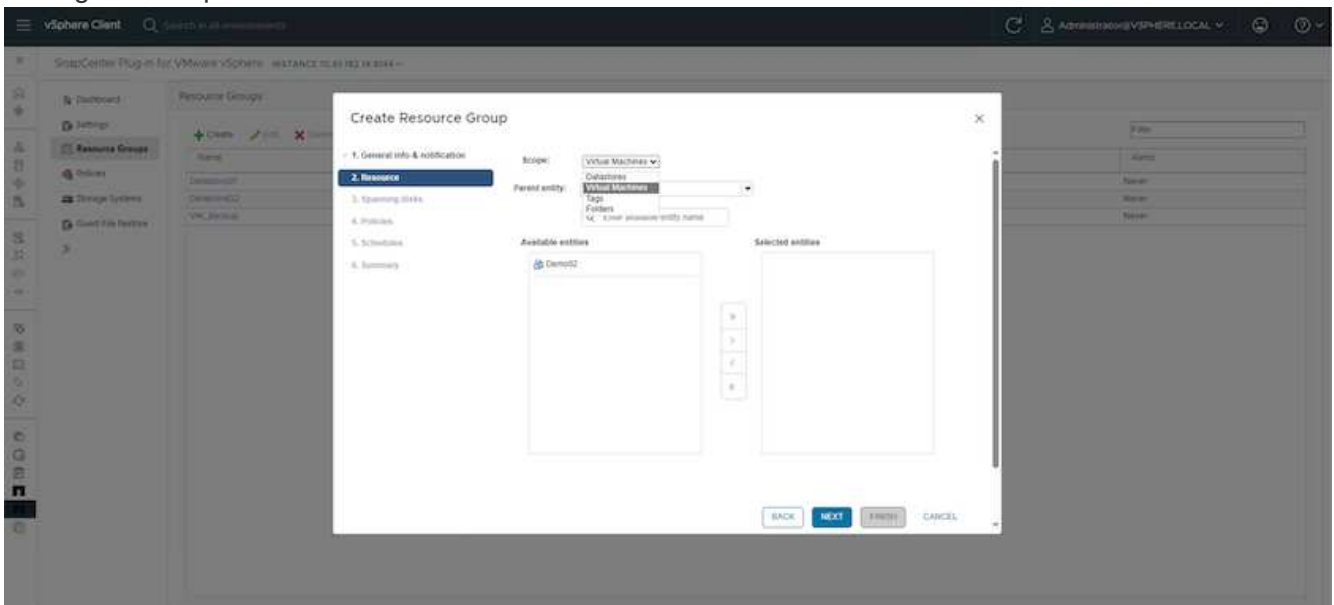
1. Ajouter tous les systèmes de stockage ONTAP devant être utilisés dans SCV.



2. Créer une règle. Assurez-vous que l'option Update SnapMirror After backup est cochée pour SM-AS et Update SnapVault après la sauvegarde pour la réplication asynchrone vers le troisième domaine de panne.

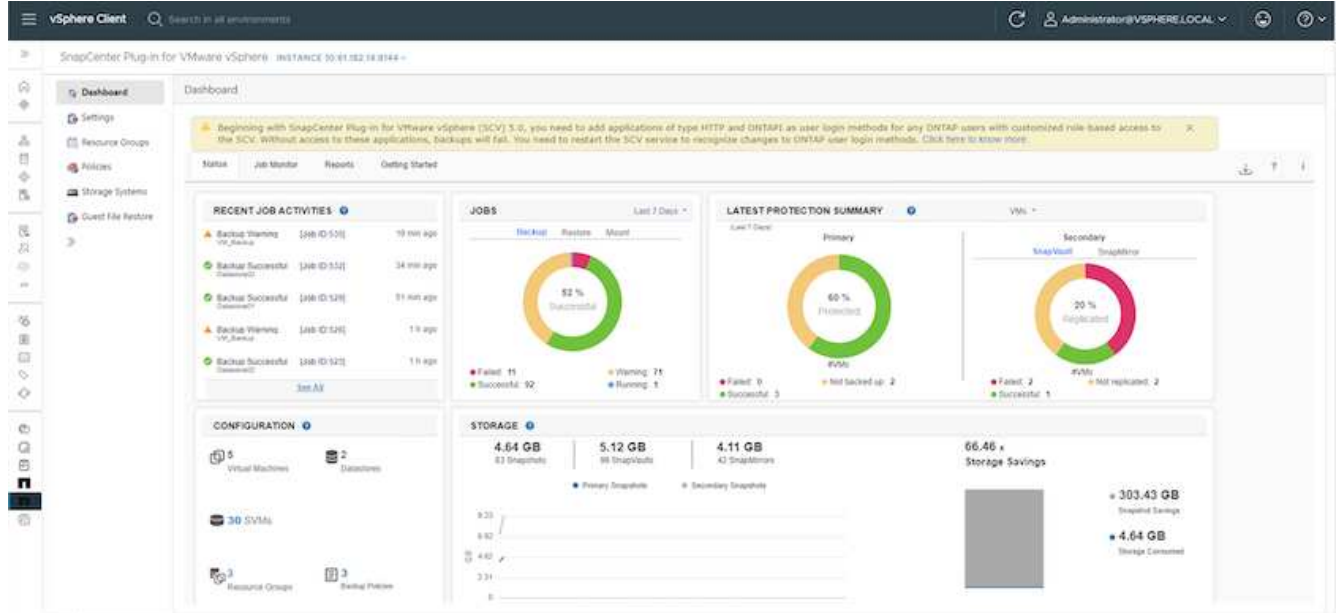


3. Créez un groupe de ressources avec des éléments désélectionnés qui doivent être protégés, associés à la stratégie et à la planification.



REMARQUE : le nom de snapshot se terminant par _Recent n'est pas pris en charge avec SM-AS.

- Les sauvegardes ont lieu à une heure planifiée en fonction de la stratégie associée au groupe de ressources. Les tâches peuvent être surveillées à partir du moniteur de tâches du tableau de bord ou des informations de sauvegarde de ces ressources.



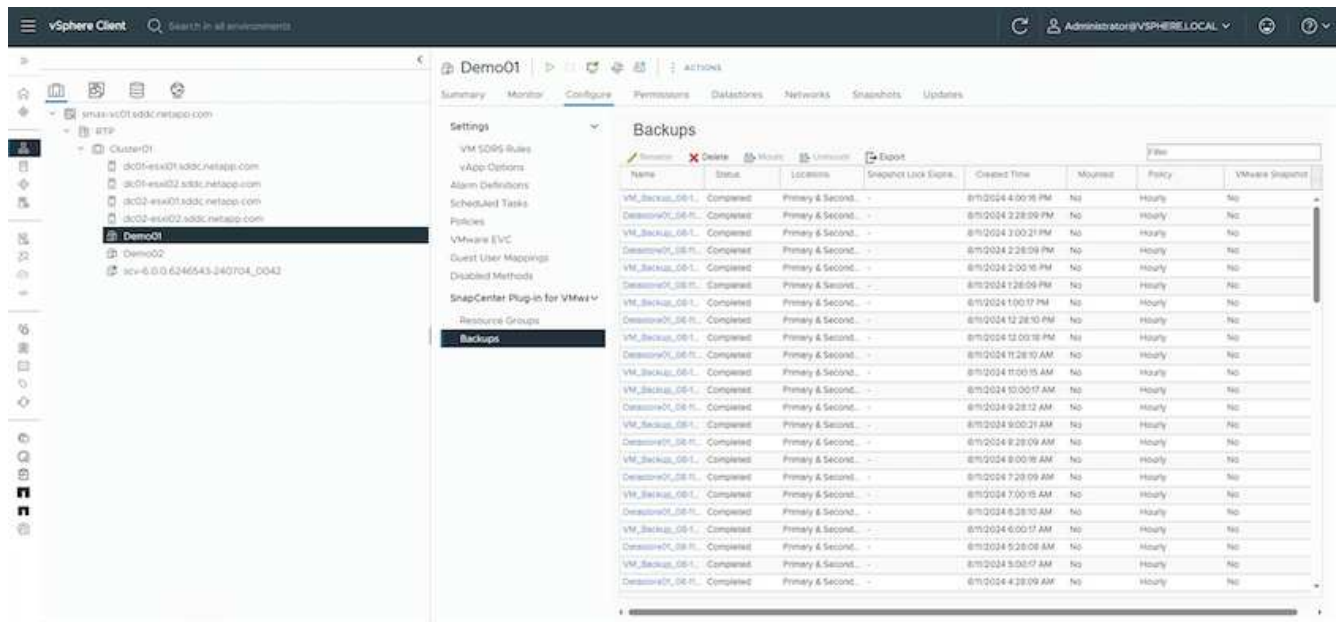
Datastore01 | ACTIONS

Summary | Monitor | **Configure** | Permissions | Files | Hosts | VMs

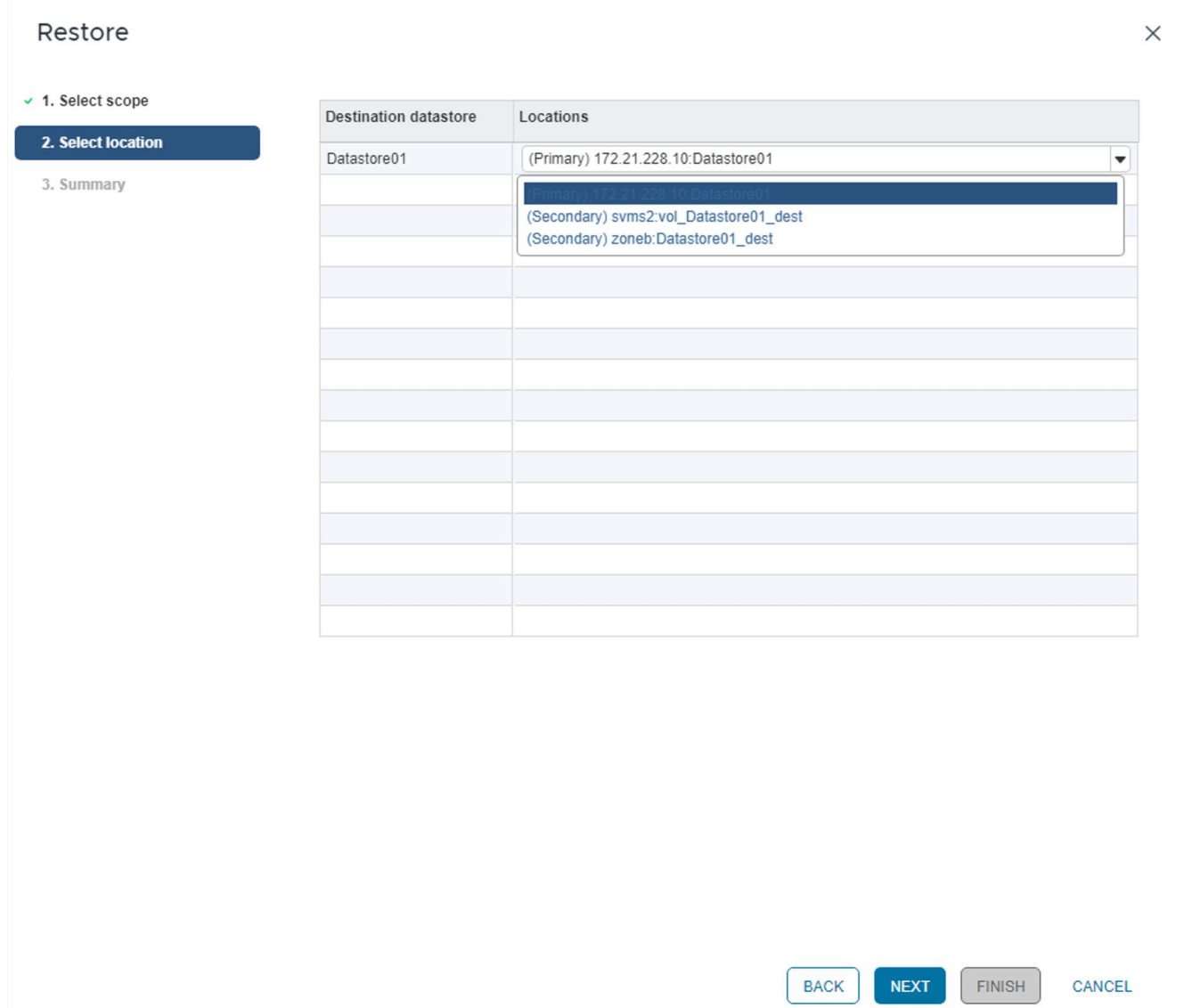
Alarm Definitions
Scheduled Tests
General
Device Backing
Connectivity and Multipathing
Hardware Acceleration
Capacity sets
NetApp ONTAP tools
SnapCenter Plug-in for VMazv
Resource Groups
Backups

Backups

| Name | Status | Location | Snapshot Lock Expt. | Created Time | Mounted | Policy | Where Snapshot |
|-------------------|-----------|------------------|---------------------|-----------------------|---------|--------|----------------|
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 4:00:16 PM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 3:28:09 PM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 3:00:21 PM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 2:28:09 PM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 2:00:16 PM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 1:28:09 PM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 1:00:17 PM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 12:28:10 PM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 12:00:18 PM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 9:28:10 AM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 9:00:21 AM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 8:28:09 AM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 8:00:16 AM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 7:28:09 AM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 7:00:15 AM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 6:28:10 AM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 6:00:17 AM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 5:28:09 AM | No | Hourly | No |
| VM_Backup_08-11 | Completed | Primary & Second | - | 8/15/2024 5:00:16 AM | No | Hourly | No |
| Datastore01_08-11 | Completed | Primary & Second | - | 8/15/2024 4:28:09 AM | No | Hourly | No |



5. Les machines virtuelles peuvent être restaurées dans le même serveur vCenter ou un autre serveur à partir du SVM sur le domaine de pannes principal ou de l'un des sites secondaires.



6. Une option similaire est également disponible pour le montage du datastore.

Mount Backup ✕

ESXi host name

Selected backup VM_Backup_08-11-2024_16.00.02.0270

Select datastore

| <input type="checkbox"/> | Name | Location |
|--------------------------|-------------|--|
| <input type="checkbox"/> | Datastore01 | Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270 ▼ |
| <input type="checkbox"/> | Datastore02 | Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270 Secondary:svms2:vol_Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270 Secondary:zoneb:Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270 |
| <input type="checkbox"/> | | |
| <input type="checkbox"/> | | |

⚠ Warning for ONTAP 9.12.1 and below version ✕ ▼

Pour obtenir de l'aide sur les opérations supplémentaires avec le distributeur auxiliaire, se reporter à ["Documentation du plug-in SnapCenter pour VMware vSphere"](#)

Socle cloud VMware

Socle cloud VMware

VMware Cloud Foundation (VCF) est un ensemble de technologies qui facilite l'accès à une expérience de cloud hybride. Dans la solution VCF, la prise en charge est assurée pour les workloads Kubernetes natifs et basés sur des machines virtuelles. Les services essentiels comme VMware vSphere, VMware VSAN, VMware NSX-T Data Center et VMware vRealize Cloud Management font partie intégrante du package VCF. Ces services permettent ainsi d'établir une infrastructure Software-defined capable de gérer le calcul, le stockage, la mise en réseau, la sécurité et la gestion du cloud. Cette infrastructure collective offre une expérience hybride dans laquelle la structure VCF étend l'environnement du data Center sur site à Amazon Web Services (AWS), Azure et Google Cloud.

Ressources de documentation

Pour plus d'informations sur les offres NetApp pour VMware Cloud Foundation, consultez la série de blogs à quatre (4) parties :

- ["NetApp et VMware Cloud Foundation en toute simplicité 1re partie : mise en route"](#)

- ["La Fondation NetApp et VMware Cloud en toute simplicité 2e partie : stockage principal VCF et ONTAP"](#)
- ["La base du cloud NetApp et VMware est simplifiée partie 3 : stockage principal VCF et Element"](#)
- ["NetApp et VMware Cloud Foundation en toute simplicité - partie 4 : Outils ONTAP pour VMware et stockage supplémentaire"](#)

VMware Cloud Foundation avec les baies SAN 100 % Flash NetApp

- ["VCF avec baies NetApp ASA, Présentation et présentation de la technologie"](#)
- ["Utilisez les outils ONTAP pour déployer les datastores iSCSI dans un domaine de gestion VCF"](#)
- ["Utilisez les outils ONTAP pour déployer les datastores vVols \(iSCSI\) dans un domaine de charges de travail VI"](#)
- ["Configurez les datastores NVMe sur TCP pour une utilisation dans un domaine de charges de travail VI"](#)
- ["Déployer et utiliser le plug-in SnapCenter pour VMware vSphere pour protéger et restaurer des machines virtuelles dans un domaine de charges de travail VI"](#)

VMware Cloud Foundation avec les baies AFF 100 % Flash NetApp

- ["VCF avec baies NetApp AFF, Présentation et présentation de la technologie"](#)
- ["Utilisez ONTAP avec NFS comme stockage principal pour les domaines des charges de travail VI"](#)
- ["Utilisez les outils ONTAP pour déployer les datastores NFS dans un domaine de charges de travail VI"](#)

Solutions NetApp FlexPod pour VMware Cloud Foundation

- ["L'extension du cloud hybride FlexPod avec VMware Cloud Foundation"](#)
- ["FlexPod en tant que domaine de charge de travail pour VMware Cloud Foundation"](#)
- ["Guide de conception de la base FlexPod en tant que domaine de charge de travail pour VMware Cloud"](#)

VCF avec baies NetApp ASA

VMware Cloud Foundation avec les baies SAN 100 % Flash NetApp

VMware Cloud Foundation (VCF) est une plateforme de data Center Software-defined intégrée qui fournit une pile complète d'infrastructure Software-defined pour exécuter les applications d'entreprise dans un environnement de cloud hybride. Elle réunit les fonctionnalités de calcul, de stockage, de mise en réseau et de gestion dans une plateforme unifiée, offrant ainsi une expérience opérationnelle cohérente dans les clouds privés et publics.

Auteur: Josh Powell

Ce document fournit des informations sur les options de stockage disponibles pour VMware Cloud Foundation utilisant la baie SAN 100 % Flash NetApp. Les options de stockage prises en charge sont couvertes par des instructions spécifiques pour le déploiement de datastores iSCSI en tant que stockage supplémentaire pour les domaines de gestion et les datastores vVol (iSCSI) et NVMe/TCP en tant que datastores supplémentaires pour les domaines de charge de travail. La protection des données des machines virtuelles et des datastores avec SnapCenter pour VMware vSphere est également couverte.

Cas d'utilisation

Cas d'utilisation décrits dans cette documentation :

- Options de stockage pour les clients à la recherche d'environnements uniformes sur les clouds privés et publics.
- Solution automatisée pour le déploiement d'infrastructures virtuelles pour les domaines de charge de travail.
- Solution de stockage évolutive et adaptée à l'évolution des besoins, même lorsqu'elle n'est pas directement alignée sur les besoins en ressources de calcul.
- Déployez du stockage supplémentaire pour les domaines de gestion et de charges de travail VI à l'aide des outils ONTAP pour VMware vSphere.
- Protection des machines virtuelles et des datastores à l'aide du plug-in SnapCenter pour VMware vSphere.

Public

Cette solution est destinée aux personnes suivantes :

- Architectes de solutions qui recherchent des options de stockage plus flexibles pour les environnements VMware conçus pour optimiser le TCO.
- Architectes de solutions à la recherche d'options de stockage VCF offrant des options de protection des données et de reprise d'activité avec les principaux fournisseurs cloud.
- Les administrateurs de stockage qui souhaitent obtenir des instructions spécifiques sur la configuration de VCF avec le stockage principal et supplémentaire.
- Les administrateurs du stockage qui souhaitent des instructions spécifiques sur la protection des VM et datastores résidant sur le stockage ONTAP

Présentation de la technologie

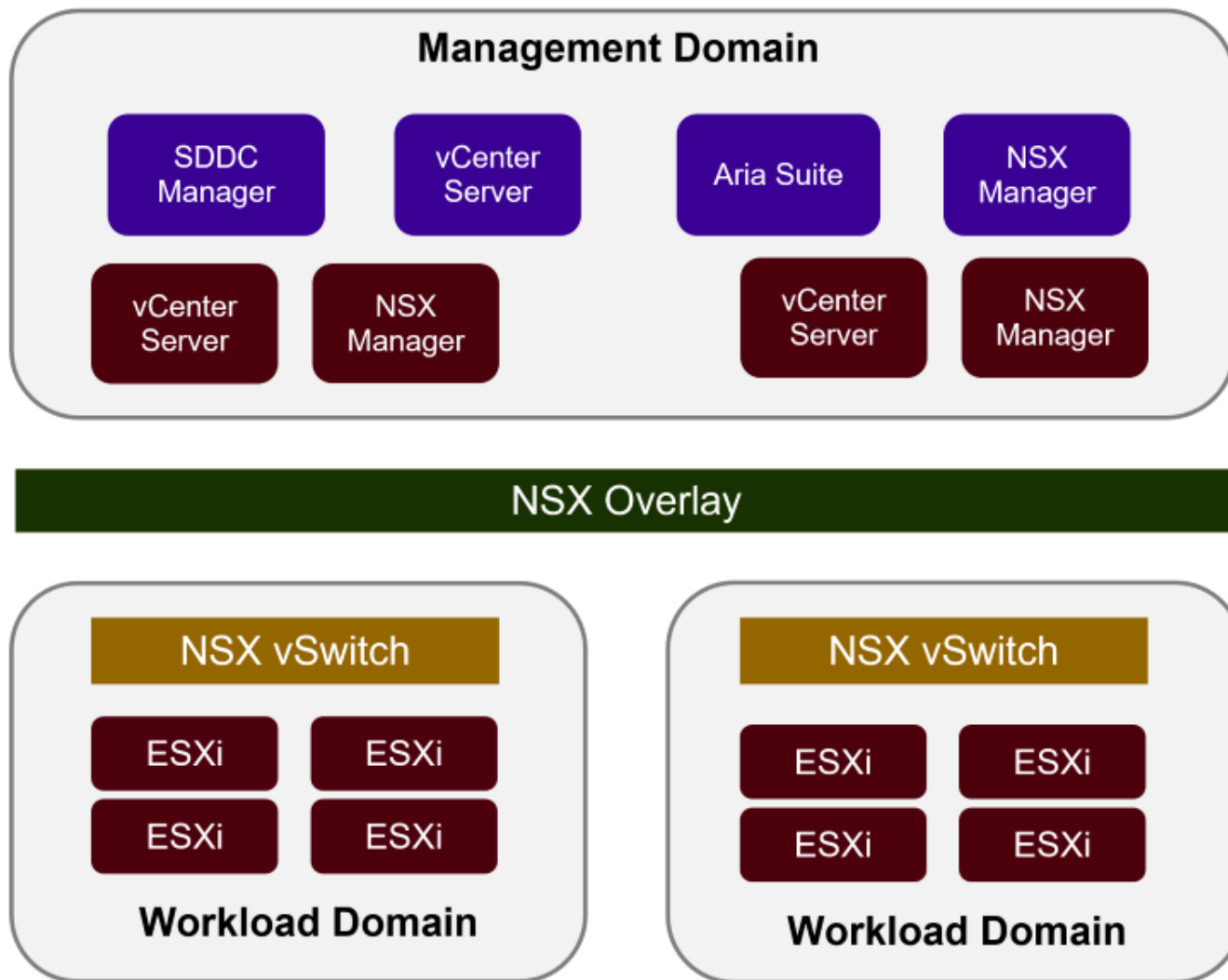
La solution VCF avec NetApp ASA comprend les principaux composants suivants :

Socle cloud VMware

VMware Cloud Foundation étend les offres d'hyperviseur vSphere de VMware en combinant des composants clés tels que SDDC Manager, vSphere, VSAN, NSX et VMware Aria Suite pour créer un data Center Software-defined.

La solution VCF prend en charge les workloads Kubernetes natifs et basés sur des machines virtuelles. Les services clés tels que VMware vSphere, VMware VSAN, VMware NSX-T Data Center et VMware Aria Cloud Management font partie intégrante du package VCF. Ces services permettent d'établir une infrastructure Software-defined capable de gérer efficacement le calcul, le stockage, la mise en réseau, la sécurité et la gestion du cloud.

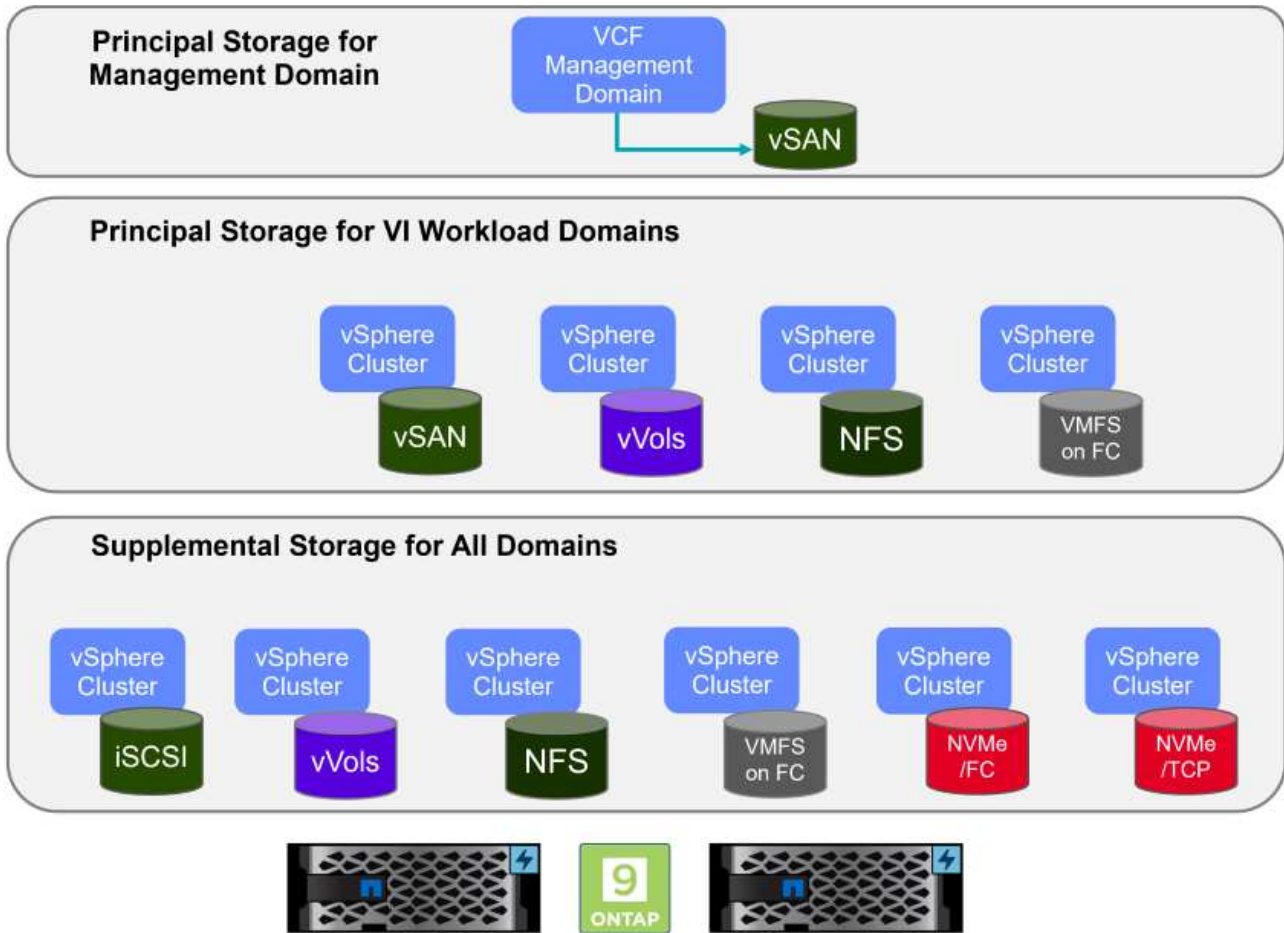
VCF comprend un seul domaine de gestion et jusqu'à 24 domaines de charge de travail VI, chacun représentant une unité d'infrastructure prête pour les applications. Un domaine de charges de travail comprend un ou plusieurs clusters vSphere gérés par une seule instance vCenter.



Pour plus d'informations sur l'architecture et la planification VCF, reportez-vous à la section "[Modèles d'architecture et types de domaine de charge de travail dans VMware Cloud Foundation](#)".

Options de stockage VCF

VMware divise les options de stockage pour VCF en stockage **principal** et **supplémentaire**. Le domaine de gestion VCF doit utiliser VSAN comme stockage principal. Cependant, il existe de nombreuses options de stockage supplémentaires pour le domaine de gestion et des options de stockage principal et supplémentaire disponibles pour les domaines de charges de travail VI.



Stockage principal pour les domaines de charge de travail

Le terme stockage principal désigne tout type de stockage pouvant être directement connecté à un domaine de charge de travail VI pendant le processus de configuration dans SDDC Manager. Le stockage principal est déployé avec le gestionnaire SDDC dans le cadre de l'orchestration de création de cluster. Il s'agit du premier datastore configuré pour un domaine de charge de travail. Notamment VSAN, vVols (VMFS), NFS et VMFS sur Fibre Channel.

Stockage supplémentaire pour les domaines de gestion et de charge de travail

Le stockage supplémentaire correspond au type de stockage qui peut être ajouté aux domaines de gestion ou de charge de travail à tout moment après la création du cluster. Le stockage supplémentaire représente le plus grand nombre d'options de stockage prises en charge, toutes prises en charge sur les baies NetApp ASA. Un stockage supplémentaire peut être déployé à l'aide des outils ONTAP pour VMware vSphere pour la plupart des types de protocoles de stockage.

Ressources de documentation supplémentaires pour VMware Cloud Foundation :

- * ["Documentation de VMware Cloud Foundation"](#)
- * ["Types de stockage pris en charge pour VMware Cloud Foundation"](#)
- * ["Gestion du stockage dans VMware Cloud Foundation"](#)

Baies SAN 100 % Flash de NetApp

La baie SAN 100 % Flash (ASA) NetApp est une solution de stockage haute performance conçue pour répondre aux exigences élevées des data centers modernes. Il associe la vitesse et la fiabilité du stockage Flash aux fonctionnalités avancées de gestion des données de NetApp pour assurer des performances, une

évolutivité et une protection des données exceptionnelles.

La gamme ASA comprend à la fois des modèles de la série A et des modèles de la série C.

Les baies Flash NetApp A-Series 100 % NVMe sont conçues pour les workloads haute performance. Elles offrent une latence ultra faible et une résilience élevée. Elles sont donc adaptées aux applications stratégiques.



Les baies Flash C-Series QLC sont destinées à des cas d'utilisation de capacité supérieure, offrant la vitesse de la technologie Flash et l'économie du Flash hybride.



Pour plus d'informations, reportez-vous au ["Page d'accueil NetApp ASA"](#).

Prise en charge des protocoles de stockage

La baie ASA prend en charge tous les protocoles SAN standard, notamment iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) et NVMe over Fabrics.

iSCSI - NetApp ASA fournit une prise en charge robuste pour iSCSI, permettant un accès au niveau des blocs aux périphériques de stockage sur les réseaux IP. Il offre une intégration transparente avec les initiateurs iSCSI pour un provisionnement et une gestion efficaces des LUN iSCSI. Fonctionnalités avancées d'ONTAP, telles que les chemins d'accès multiples, l'authentification CHAP et la prise en charge ALUA.

Pour obtenir des conseils de conception sur les configurations iSCSI, reportez-vous au ["Documentation de référence sur la configuration SAN"](#).

Fibre Channel - NetApp ASA offre une prise en charge complète de Fibre Channel (FC), une technologie de réseau haut débit couramment utilisée dans les réseaux de stockage (SAN). ONTAP s'intègre en toute transparence à l'infrastructure FC, offrant ainsi un accès fiable et efficace au niveau des blocs aux systèmes de stockage. Elle offre des fonctionnalités telles que le zoning, les chemins d'accès multiples et la connexion à

la fabric (FLOGI) pour optimiser les performances, améliorer la sécurité et assurer la connectivité transparente dans les environnements FC.

Pour obtenir des conseils de conception sur les configurations Fibre Channel, reportez-vous au ["Documentation de référence sur la configuration SAN"](#).

NVMe over Fabrics - NetApp ONTAP et ASA prennent en charge NVMe over Fabrics. NVMe/FC permet d'utiliser des périphériques de stockage NVMe sur l'infrastructure Fibre Channel et NVMe/TCP sur les réseaux de stockage IP.

Pour obtenir des conseils de conception sur NVMe, reportez-vous à la section ["Configuration, prise en charge et limitations de NVMe"](#)

Technologie active/active

Les baies SAN 100 % Flash de NetApp autorisent des chemins de données actif-actif à travers les deux contrôleurs, ce qui évite au système d'exploitation hôte d'attendre la panne d'un chemin actif avant d'activer le chemin alternatif. Cela signifie que l'hôte peut utiliser tous les chemins disponibles sur tous les contrôleurs, en veillant à ce que les chemins actifs soient toujours présents, que le système soit dans un état stable ou qu'il ait subi un basculement de contrôleur.

De plus, la fonctionnalité NetApp ASA améliore considérablement la vitesse de basculement du SAN. Chaque contrôleur réplique en continu les métadonnées de LUN essentielles à son partenaire. Par conséquent, chaque contrôleur est prêt à reprendre les responsabilités liées à la transmission de données en cas de panne soudaine de son partenaire. Cette préparation est possible car le contrôleur possède déjà les informations nécessaires pour commencer à utiliser les lecteurs précédemment gérés par le contrôleur défectueux.

Avec les chemins d'accès actif-actif, les basculements planifiés et non planifiés bénéficient de délais de reprise des E/S de 2-3 secondes.

Pour plus d'informations, voir ["Tr-4968, Baie 100 % SAS NetApp – disponibilité et intégrité des données avec le NetApp ASA"](#).

Garanties de stockage

NetApp propose un ensemble unique de garanties de stockage grâce aux baies SAN 100 % Flash de NetApp. Ses avantages uniques incluent :

Garantie d'efficacité du stockage : atteignez une haute performance tout en réduisant les coûts de stockage grâce à la garantie d'efficacité du stockage. Ratio de 4:1 pour les workloads SAN

6 Nines (99.9999 %) garantie de disponibilité des données : garantit la correction des temps d'arrêt imprévus de plus de 31.56 secondes par an.

Garantie de restauration ransomware : garantie de récupération des données en cas d'attaque par ransomware.

Voir la ["Portail produit NetApp ASA"](#) pour en savoir plus.

Outils NetApp ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere permettent aux administrateurs de gérer le stockage NetApp

directement à partir du client vSphere. Les outils ONTAP vous permettent de déployer et de gérer des datastores, ainsi que de provisionner des datastores VVol.

Les outils ONTAP permettent de mapper les datastores aux profils de capacité de stockage qui déterminent un ensemble d'attributs de système de stockage. Il est ainsi possible de créer des datastores dotés d'attributs spécifiques tels que les performances du stockage et la qualité de service.

Les outils ONTAP incluent également un fournisseur * VMware vSphere API for Storage Awareness (VASA)* pour les systèmes de stockage ONTAP, qui permet le provisionnement de datastores VMware Virtual volumes (vVols), la création et l'utilisation de profils de fonctionnalités de stockage, la vérification de conformité et la surveillance des performances.

Pour plus d'informations sur les outils NetApp ONTAP, reportez-vous au "[Documentation sur les outils ONTAP pour VMware vSphere](#)" page.

Plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter pour VMware vSphere (SCV) est une solution logicielle de NetApp qui protège intégralement les données dans les environnements VMware vSphere. Son objectif est de simplifier et de rationaliser le processus de protection et de gestion des machines virtuelles et des datastores. SCV utilise un snapshot basé sur le stockage et la réplication sur des baies secondaires pour atteindre des objectifs de durée de restauration plus faibles.

Le plug-in SnapCenter pour VMware vSphere offre les fonctionnalités suivantes dans une interface unifiée, intégrée au client vSphere :

Snapshots basés sur des règles - SnapCenter vous permet de définir des règles pour la création et la gestion de snapshots cohérents au niveau des applications de machines virtuelles dans VMware vSphere.

Automatisation - la création et la gestion automatisées de snapshots basées sur des règles définies permettent d'assurer une protection cohérente et efficace des données.

Protection au niveau VM - la protection granulaire au niveau VM permet une gestion et une récupération efficaces des machines virtuelles individuelles.

Fonctionnalités d'efficacité du stockage - l'intégration aux technologies de stockage NetApp fournit des fonctionnalités d'efficacité du stockage telles que la déduplication et la compression pour les snapshots, ce qui réduit les besoins en stockage.

Le plug-in SnapCenter orchestre la mise en veille des machines virtuelles en association avec des snapshots matériels sur des baies de stockage NetApp. La technologie SnapMirror permet de répliquer des copies de sauvegarde sur les systèmes de stockage secondaires, y compris dans le cloud.

Pour plus d'informations, reportez-vous à la "[Documentation du plug-in SnapCenter pour VMware vSphere](#)".

L'intégration de BlueXP active 3-2-1 stratégies de sauvegarde qui étendent les copies de données au stockage objet dans le cloud.

Pour plus d'informations sur les stratégies de sauvegarde 3-2-1 avec BlueXP, rendez-vous sur "[3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration BlueXP pour les VM](#)".

Présentation de la solution

Les scénarios présentés dans cette documentation expliquent comment utiliser les systèmes de stockage ONTAP en tant que stockage supplémentaire dans des domaines de gestion et de charge de travail. En outre, le plug-in SnapCenter pour VMware vSphere est utilisé pour protéger les VM et les datastores.

Scénarios traités dans cette documentation :

- **Utilisez les outils ONTAP pour déployer les datastores iSCSI dans un domaine de gestion VCF.** Cliquez sur "[ici](#)" pour les étapes de déploiement.
- **Utilisez les outils ONTAP pour déployer les datastores vVols (iSCSI) dans un domaine de charge de travail VI.** Cliquez sur "[ici](#)" pour les étapes de déploiement.
- **Configurer les datastores NVMe sur TCP pour une utilisation dans un domaine de charge de travail VI.** Cliquez sur "[ici](#)" pour les étapes de déploiement.
- **Déployer et utiliser le plug-in SnapCenter pour VMware vSphere pour protéger et restaurer des machines virtuelles dans un domaine de charges de travail VI.** Cliquez sur "[ici](#)" pour les étapes de déploiement.

Utilisez les outils ONTAP pour configurer le stockage supplémentaire pour les domaines de gestion VCF

Dans ce scénario, nous allons montrer comment déployer et utiliser les outils ONTAP pour VMware vSphere (OTV) pour configurer un datastore iSCSI pour un domaine de gestion VCF.

Auteur: Josh Powell

Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

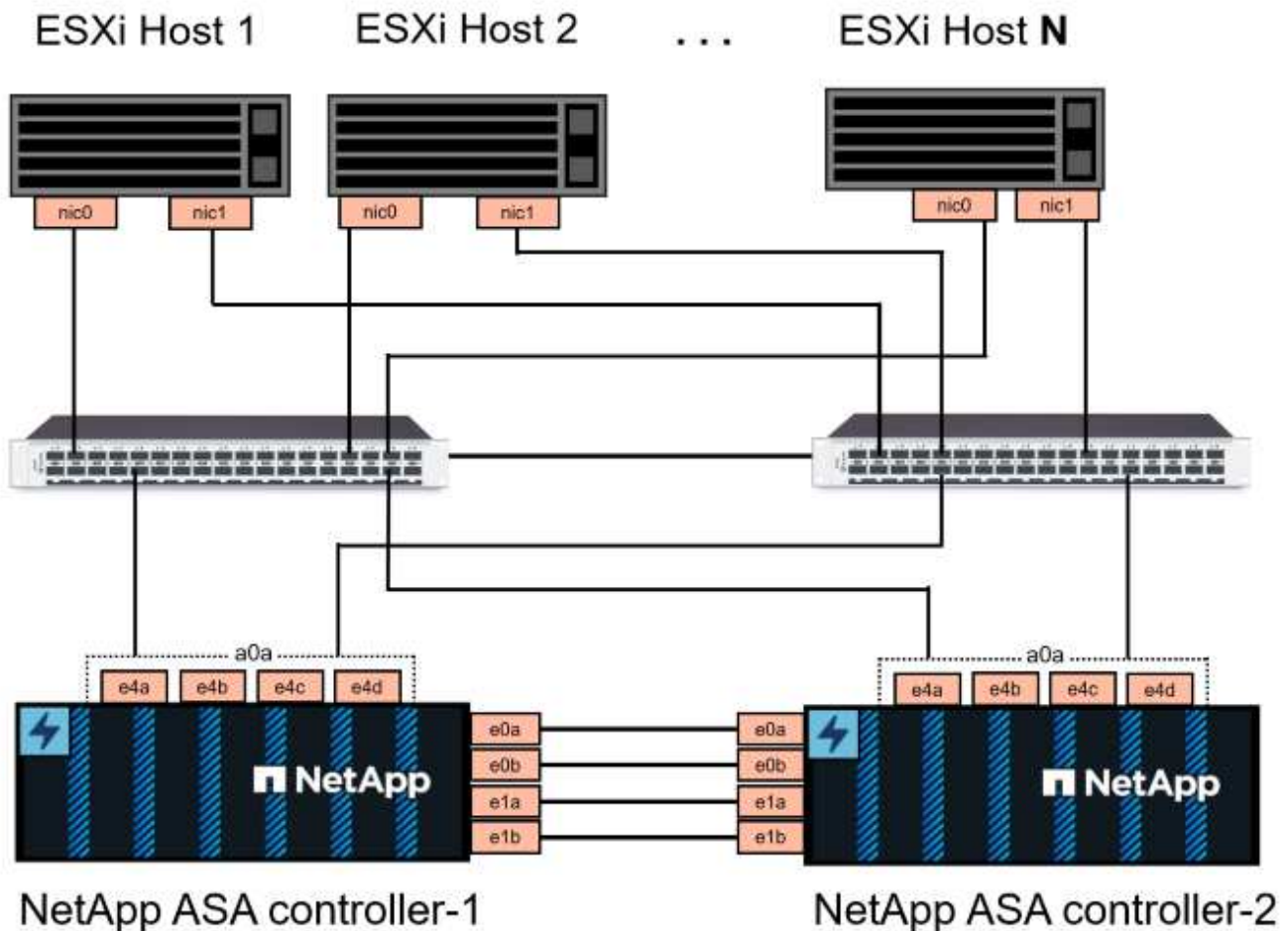
- Créez un SVM (Storage Virtual machine) avec des interfaces logiques (LIF) pour le trafic iSCSI.
- Créez des groupes de ports distribués pour les réseaux iSCSI sur le domaine de gestion VCF.
- Créez des adaptateurs vmkernel pour iSCSI sur les hôtes ESXi pour le domaine de gestion VCF.
- Déployez les outils ONTAP sur le domaine de gestion VCF.
- Créez un nouveau datastore VMFS sur le domaine de gestion VCF.

Prérequis

Ce scénario nécessite les composants et configurations suivants :

- Un système de stockage ONTAP ASA doté de ports de données physiques sur des commutateurs ethernet dédiés au trafic de stockage.
- Le déploiement du domaine de gestion VCF est terminé et le client vSphere est accessible.

NetApp recommande des configurations réseau entièrement redondantes pour iSCSI. Le schéma suivant illustre un exemple de configuration redondante, fournissant une tolérance aux pannes pour les systèmes de stockage, les commutateurs, les cartes réseau et les systèmes hôtes. Reportez-vous au NetApp "[Référence de configuration SAN](#)" pour plus d'informations.



Pour les chemins d'accès multiples et le basculement sur plusieurs chemins, NetApp recommande de disposer d'au moins deux LIF par nœud de stockage dans des réseaux ethernet distincts pour tous les SVM dans les configurations iSCSI.

Cette documentation explique le processus de création d'un SVM et de spécification des informations d'adresse IP pour créer plusieurs LIFs pour le trafic iSCSI. Pour ajouter de nouvelles LIFs à un SVM existant, voir "[Créer une LIF \(interface réseau\)](#)".

Pour plus d'informations sur l'utilisation de datastores iSCSI VMFS avec VMware, reportez-vous à la section "[Datastore VMFS vSphere - stockage iSCSI back-end avec ONTAP](#)".



Dans les cas où plusieurs adaptateurs VMkernel sont configurés sur le même réseau IP, il est recommandé d'utiliser la liaison logicielle des ports iSCSI sur les hôtes ESXi afin de garantir l'équilibrage de la charge sur les adaptateurs. Reportez-vous à l'article de la base de connaissances "[Considérations relatives à l'utilisation de la liaison logicielle du port iSCSI dans ESX/ESXi \(2038869\)](#)".

Étapes de déploiement

Pour déployer les outils ONTAP et les utiliser pour créer un datastore VMFS sur le domaine de gestion VCF, procédez comme suit :

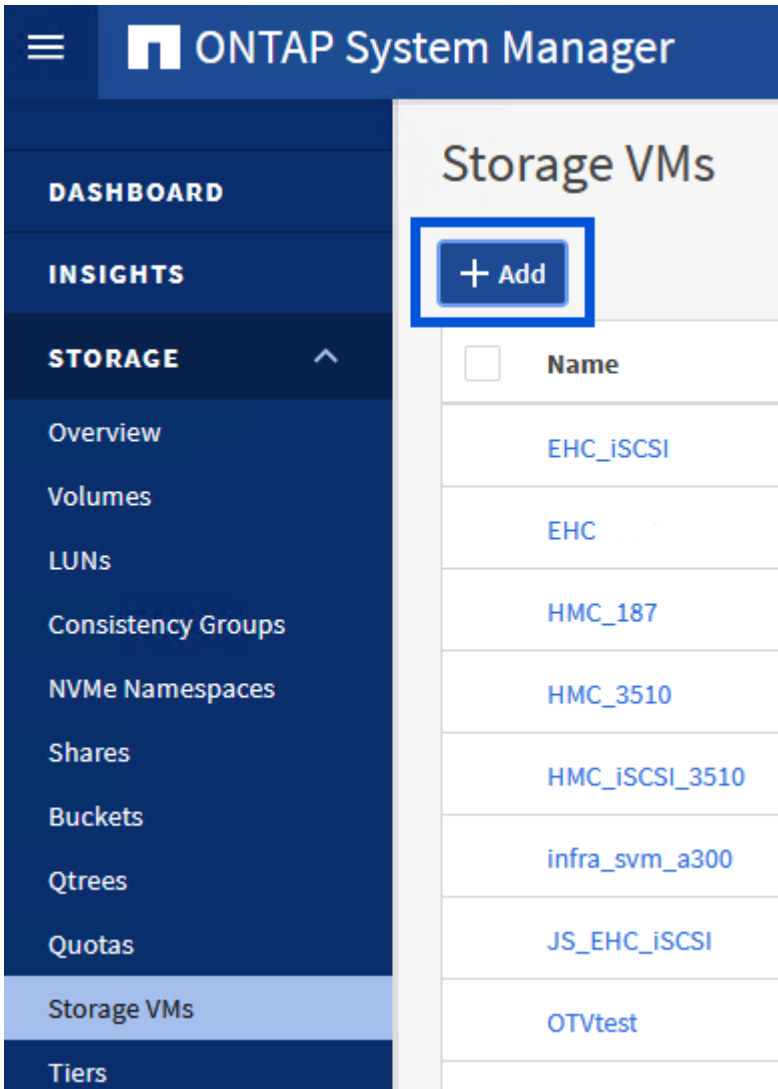
Créez un SVM et des LIF sur un système de stockage ONTAP

L'étape suivante s'effectue dans ONTAP System Manager.

Créez la VM de stockage et les LIF

Effectuer les étapes suivantes pour créer un SVM avec plusieurs LIF pour le trafic iSCSI.

1. Dans le Gestionnaire système ONTAP, accédez à **Storage VMs** dans le menu de gauche et cliquez sur **+ Add** pour démarrer.



2. Dans l'assistant **Add Storage VM**, indiquez un **Name** pour le SVM, sélectionnez **IP Space**, puis, sous **Access Protocol**, cliquez sur l'onglet ***iSCSI** et cochez la case **Enable iSCSI**.

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. Dans la section **interface réseau**, remplissez les champs **adresse IP**, **masque de sous-réseau** et **domaine de diffusion et Port** pour la première LIF. Pour les LIF suivantes, la case à cocher peut être activée pour utiliser des paramètres communs à toutes les LIF restantes ou pour utiliser des paramètres distincts.



Pour les chemins d'accès multiples et le basculement sur plusieurs chemins, NetApp recommande de disposer d'au moins deux LIF par nœud de stockage dans des réseaux Ethernet distincts pour tous les SVM dans les configurations iSCSI.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Indiquez si vous souhaitez activer le compte Storage VM Administration (pour les environnements en colocation) et cliquez sur **Save** pour créer le SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

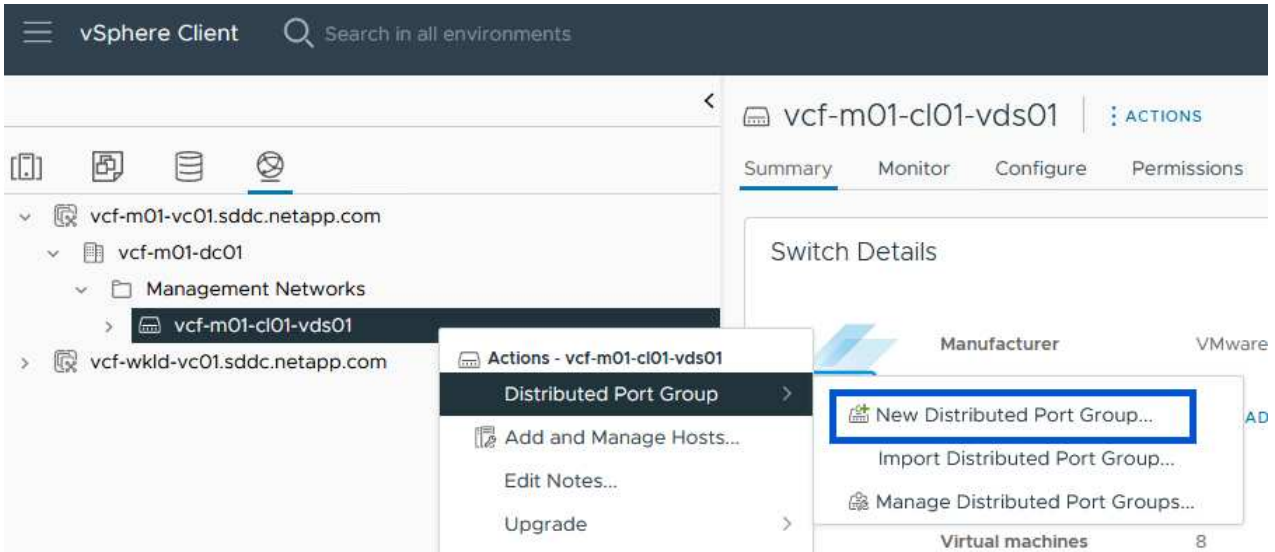
Configuration de la mise en réseau iSCSI sur les hôtes ESXi

Les étapes suivantes sont effectuées sur le cluster de domaine de gestion VCF à l'aide du client vSphere.

Créez des groupes de ports distribués pour le trafic iSCSI

Pour créer un nouveau groupe de ports distribués pour chaque réseau iSCSI, procédez comme suit :

1. Dans le client vSphere pour le cluster de domaine de gestion, accédez à **Inventory > Networking**. Naviguez jusqu'au commutateur distribué existant et choisissez l'action pour créer **Nouveau groupe de ports distribués...**



2. Dans l'assistant **Nouveau groupe de ports distribués**, entrez un nom pour le nouveau groupe de ports et cliquez sur **Suivant** pour continuer.
3. Sur la page **configurer les paramètres**, remplissez tous les paramètres. Si des VLAN sont utilisés, assurez-vous de fournir l'ID de VLAN correct. Cliquez sur **Suivant** pour continuer.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding Static binding

Port allocation Elastic ⓘ

Number of ports 8

Network resource pool (default)

VLAN

VLAN type VLAN

VLAN ID 3374

Advanced

Customize default policies configuration

CANCEL

BACK

NEXT

4. Sur la page **prêt à terminer**, passez en revue les modifications et cliquez sur **Terminer** pour créer le nouveau groupe de ports distribués.
5. Répétez ce processus pour créer un groupe de ports distribués pour le deuxième réseau iSCSI utilisé et assurez-vous d'avoir saisi l'ID **VLAN** correct.
6. Une fois les deux groupes de ports créés, naviguez jusqu'au premier groupe de ports et sélectionnez l'action **Modifier les paramètres...**

The screenshot shows the vSphere Client interface. The top navigation bar includes the vSphere Client logo and a search bar. The main content area is divided into a left-hand navigation pane and a right-hand details pane. The left pane shows a tree view of the environment, with the following structure:

- vcf-m01-vc01.sddc.netapp.com
 - vcf-m01-dc01
 - Management Networks
 - vcf-m01-cl01-vds01
 - SDDC-DPortGroup-VM-Mgmt
 - vcf-m01-cl01-vds-DVUplinks-19
 - vcf-m01-cl01-vds01-pg-iscsi-a**
 - vcf-m01-cl01-vds0
 - vcf-m01-cl01-vds0
 - vcf-m01-cl01-vds0
 - vcf-m01-cl01-vds0
- vcf-wkld-vc01.sddc.netapp.com

The right-hand pane displays the details for the selected port group, **vcf-m01-cl01-vds01-pg-iscsi-a**. The details are as follows:

| Property | Value |
|--------------------------|-------------------|
| Port binding | Static binding |
| Port allocation | Elastic |
| VLAN ID | 3374 |
| Distributed switch | vcf-m01-cl01-vds0 |
| Network protocol profile | -- |
| Network resource pool | -- |
| Hosts | 4 |

An action menu is open over the selected port group, showing the following options:

- Actions - vcf-m01-cl01-vds01-pg-iscsi-a
- Edit Settings...**
- Export Configuration...
- Restore Configuration...

7. Sur la page **Distributed Port Group - Edit Settings**, accédez à **Teaming and failover** dans le menu de gauche et cliquez sur **uplink2** pour le déplacer vers **uplinks** inutilisés.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

| | | |
|-----------------------------|----------------------------------|--|
| General | Load balancing | Route based on originating virtual por ▾ |
| Advanced | Network failure detection | Link status only ▾ |
| VLAN | Notify switches | Yes ▾ |
| Security | Failback | Yes ▾ |
| Traffic shaping | | |
| Teaming and failover | | |
| Monitoring | | |
| Miscellaneous | | |

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

8. Répétez cette étape pour le deuxième groupe de ports iSCSI. Cependant, cette fois, déplacez **uplink1** vers **uplinks** inutilisés.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual por 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 

MOVE UP MOVE DOWN

Active uplinks

 uplink2

Standby uplinks

Unused uplinks

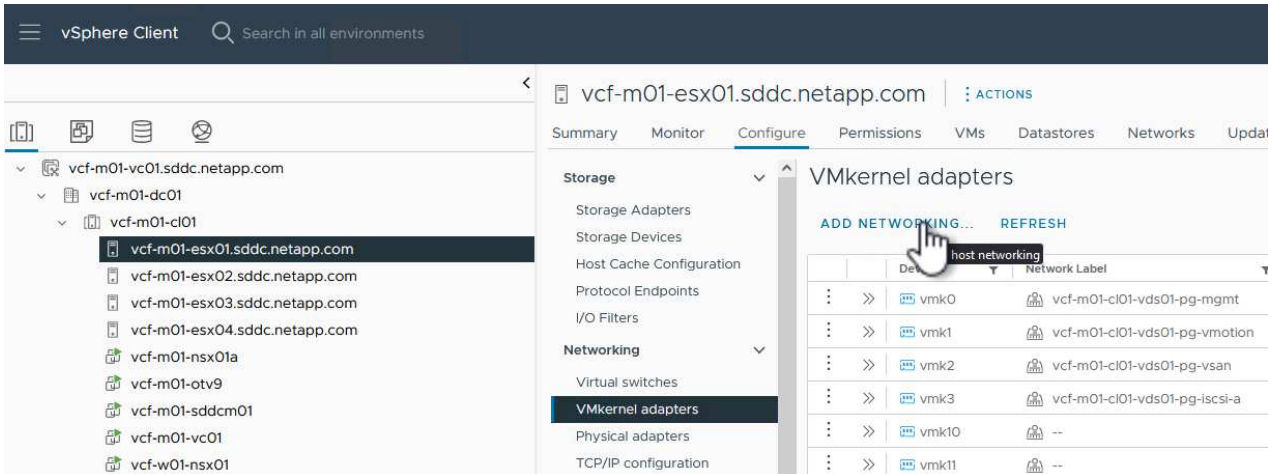
 uplink1



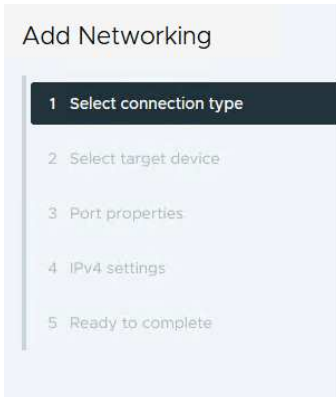
Créez des adaptateurs VMkernel sur chaque hôte ESXi

Répétez ce processus sur chaque hôte ESXi du domaine de gestion.

1. À partir du client vSphere, accédez à l'un des hôtes ESXi dans l'inventaire du domaine de gestion. Dans l'onglet **configurer**, sélectionnez **adaptateurs VMkernel** et cliquez sur **Ajouter réseau...** pour démarrer.



2. Dans la fenêtre **Select connection type**, choisissez **VMkernel Network adapter** et cliquez sur **Next** pour continuer.



Select connection type

Select a connection type to create.

- VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.
- Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

3. Sur la page **Sélectionner le périphérique cible**, choisissez l'un des groupes de ports distribués pour iSCSI créés précédemment.

Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

| | Name | NSX Port Group ID | Distributed Switch |
|----------------------------------|-------------------------------|-------------------|--------------------|
| <input type="radio"/> | SDDC-DPortGroup-VM-Mgmt | -- | vcf-m01-cl01-vds01 |
| <input checked="" type="radio"/> | vcf-m01-cl01-vds01-pg-iscsi-a | -- | vcf-m01-cl01-vds01 |
| <input type="radio"/> | vcf-m01-cl01-vds01-pg-iscsi-b | -- | vcf-m01-cl01-vds01 |
| <input type="radio"/> | vcf-m01-cl01-vds01-pg-mgmt | -- | vcf-m01-cl01-vds01 |
| <input type="radio"/> | vcf-m01-cl01-vds01-pg-vmotion | -- | vcf-m01-cl01-vds01 |
| <input type="radio"/> | vcf-m01-cl01-vds01-pg-vsan | -- | vcf-m01-cl01-vds01 |

Manage Columns 6 items

CANCEL

BACK

NEXT

4. Sur la page **Port properties**, conservez les valeurs par défaut et cliquez sur **Next** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties**
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN
- vSAN Witness
- vSphere Backup NFC
- NVMe over TCP
- NVMe over RDMA

5. Sur la page **IPv4 settings**, remplissez **adresse IP**, **masque de sous-réseau** et fournissez une nouvelle adresse IP de passerelle (uniquement si nécessaire). Cliquez sur **Suivant** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

6. Consultez vos sélections sur la page **prêt à terminer** et cliquez sur **Terminer** pour créer l'adaptateur VMkernel.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-m01-cl01-vds01-pg-iscsi-a

Distributed switch vcf-m01-cl01-vds01
- ▼ Port properties

New port group vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.114 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

7. Répétez cette procédure pour créer un adaptateur VMkernel pour le second réseau iSCSI.

Déployer et utiliser les outils ONTAP pour configurer le stockage

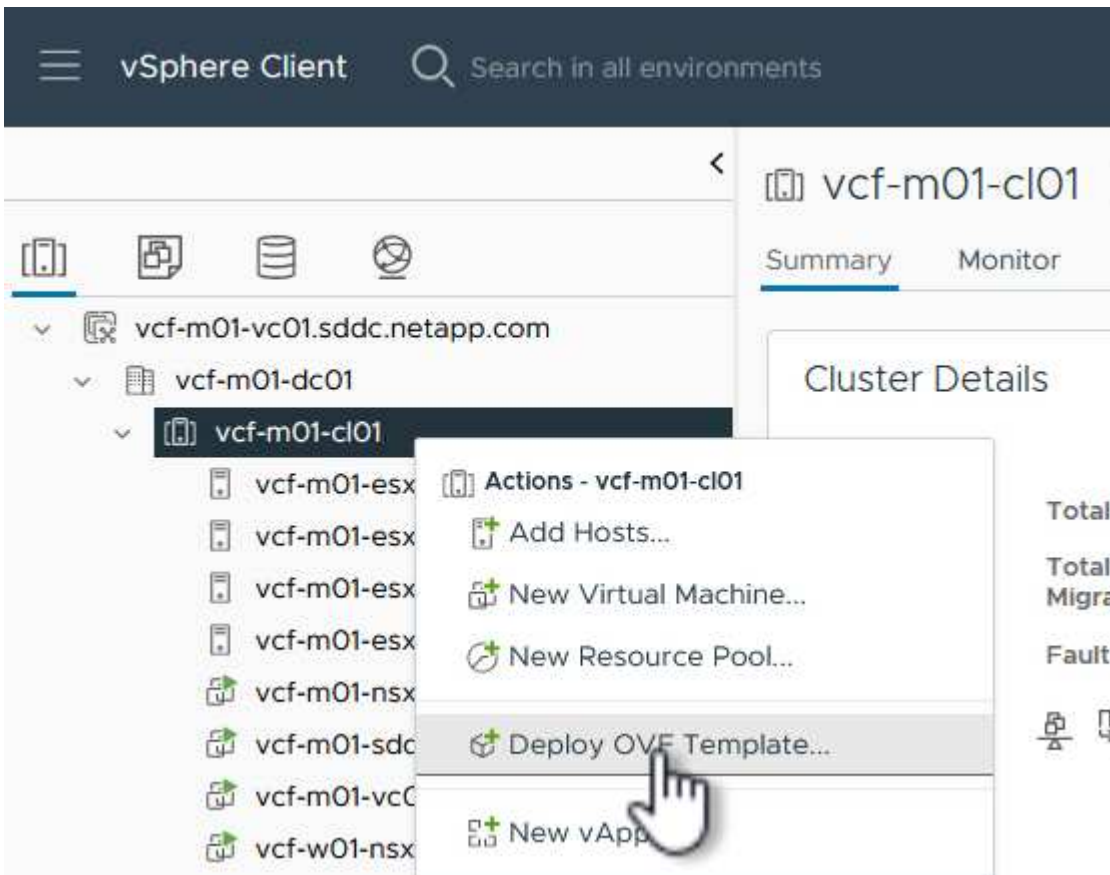
Les étapes suivantes sont effectuées sur le cluster de domaine de gestion VCF à l'aide du client vSphere et impliquent le déploiement d'OTV, la création d'un datastore iSCSI VMFS et la migration des VM de gestion vers le nouveau datastore.

Déployez les outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere (OTV) sont déployés en tant qu'appliance de machine virtuelle et fournissent une interface utilisateur vCenter intégrée pour la gestion du stockage ONTAP.

Procédez comme suit pour déployer les outils ONTAP pour VMware vSphere :

1. Obtenir l'image OVA des outils ONTAP à partir du "[Site de support NetApp](#)" et télécharger dans un dossier local.
2. Connectez-vous à l'appliance vCenter pour le domaine de gestion VCF.
3. Dans l'interface de l'appliance vCenter, cliquez avec le bouton droit de la souris sur le cluster de gestion et sélectionnez **déployer le modèle OVF...**



4. Dans l'assistant **déployer modèle OVF**, cliquez sur le bouton radio **fichier local** et sélectionnez le fichier OVA des outils ONTAP téléchargé à l'étape précédente.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Pour les étapes 2 à 5 de l'assistant, sélectionnez un nom et un dossier pour la machine virtuelle, sélectionnez la ressource de calcul, vérifiez les détails et acceptez le contrat de licence.
6. Pour l'emplacement de stockage des fichiers de configuration et des fichiers disque, sélectionnez le datastore VSAN du cluster du domaine de gestion VCF.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

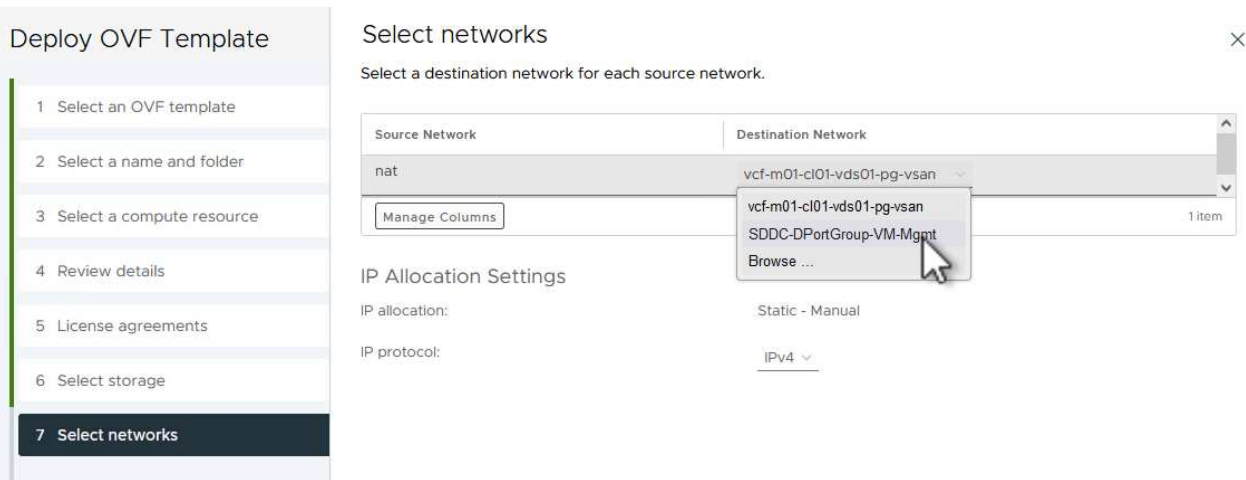
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

| | Name | Storage Compatibility | Capacity | Provisioned | Free | T |
|----------------------------------|-------------------------------------|-----------------------|-----------|-------------|-----------|---|
| <input checked="" type="radio"/> | vcf-m01-c01-ds-vsant01 | -- | 999.97 GB | 7.17 TB | 225.72 GB | v |
| <input type="radio"/> | vcf-m01-esx01-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx02-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx03-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx04-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |

Manage Columns Items per page 10 5 items

7. Sur la page Sélectionner le réseau, sélectionnez le réseau utilisé pour le trafic de gestion.



8. Sur la page Personnaliser le modèle, remplissez toutes les informations requises :

- Mot de passe à utiliser pour l'accès administratif à OTV.
- Adresse IP du serveur NTP.
- Mot de passe du compte de maintenance OTV.
- Mot de passe OTV Derby DB.
- Ne cochez pas la case **Activer VMware Cloud Foundation (VCF)**. Le mode VCF n'est pas requis pour le déploiement de stockage supplémentaire.
- Nom de domaine complet ou adresse IP de l'appliance vCenter et informations d'identification pour vCenter.
- Renseignez les champs de propriétés réseau requis.

Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

❗ 2 properties have invalid values ✕

| System Configuration | 4 settings |
|--------------------------------------|--|
| Application User Password (*) | Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character. |
| | Password <input type="password" value="....."/> |
| | Confirm Password <input type="password" value="....."/> |
| NTP Servers | A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. <input type="text" value="172.21.166.1"/> |
| Maintenance User Password (*) | Password to assign to maint user account. |
| | Password <input type="password" value="....."/> |
| | Confirm Password <input type="password" value="....."/> |

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

| Configure vCenter or Enable VCF | 5 settings |
|---|---|
| Enable VMware Cloud Foundation (VCF) | vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/> |
| vCenter Server Address (*) | Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="172.21.166.140"/> |
| Port (*) | Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/> |
| Username (*) | Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/> |
| Password (*) | Specify the password of an existing vCenter to register to. |
| | Password <input type="password" value="....."/> |
| | Confirm Password <input type="password" value="....."/> |

| Network Properties | 8 settings |
|--------------------|---|
| Host Name | Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-m01-otv9"/> |
| IP Address | Specify the IP address for the appliance. (Leave blank if DHCP is |

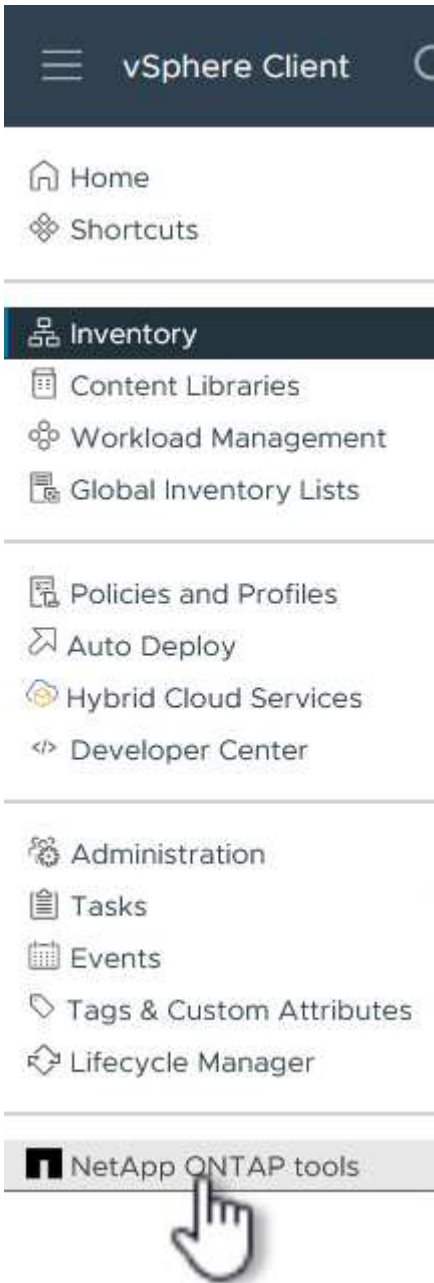
CANCEL BACK NEXT

9. Passez en revue toutes les informations de la page prêt à terminer et cliquez sur Terminer pour commencer à déployer l'appliance OTV.

Configurez un datastore iSCSI VMFS sur le domaine de gestion à l'aide d'OTV

Procédez comme suit pour utiliser OTV pour configurer un datastore iSCSI VMFS en tant que stockage supplémentaire sur le domaine de gestion :

1. Dans le client vSphere, accédez au menu principal et sélectionnez **Outils NetApp ONTAP**.



2. Une fois dans **Outils ONTAP**, à partir de la page mise en route (ou de **systèmes de stockage**), cliquez sur **Ajouter** pour ajouter un nouveau système de stockage.

vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview

- Storage Systems
- Storage capability profile
- Storage Mapping
- Settings
- Reports
 - Datastore Report
 - Virtual Machine Report
 - vVols Datastore Report
 - vVols Virtual Machine Report
 - Log Integrity Report


ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.


Add Storage System

Add storage systems to ONTAP tools for VMware vSphere.





Provision Datastore

Create traditional or vVols datastores.



Next Steps

 [View Dashboard](#)
View and monitor the datastores in ONTAP tools for VMware vSphere.

 [Settings](#)
Configure administrative settings such as credentials, alarm thresholds.

What's new?

September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management



Resources

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

3. Indiquez l'adresse IP et les informations d'identification du système de stockage ONTAP, puis cliquez sur **Ajouter**.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

| | |
|---------------------|--|
| vCenter server | vcf-m01-vc01.sddc.netapp.com  |
| Name or IP address: | 172.16.9.25 |
| Username: | admin |
| Password: | ●●●●●●●● |
| Port: | 443 |
| Advanced options |  |


CANCEL

SAVE & ADD MORE

ADD 

4. Cliquez sur **Oui** pour autoriser le certificat de cluster et ajouter le système de stockage.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

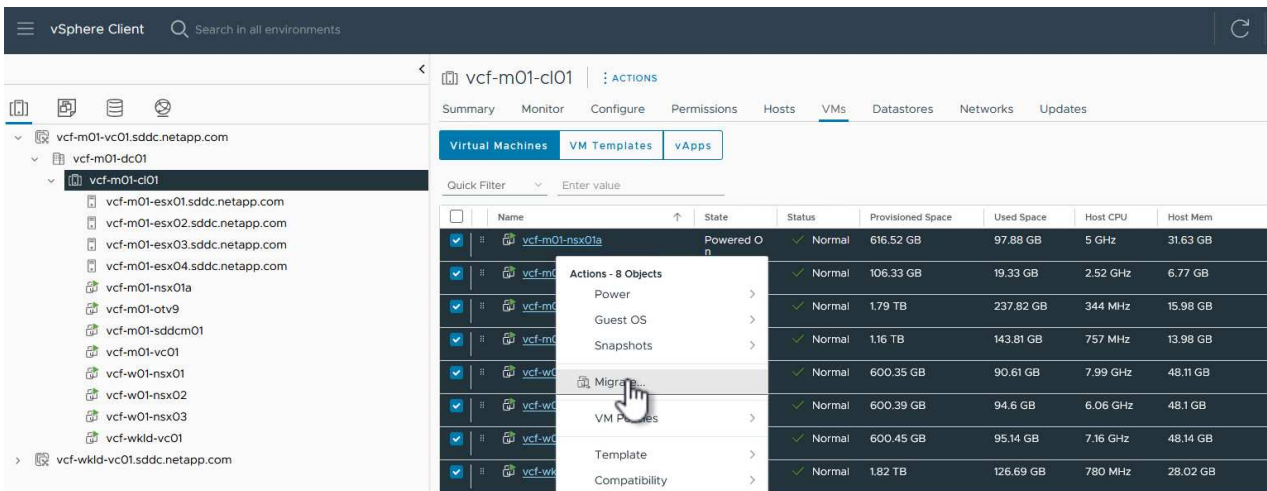
ADD

Migrer la VM de gestion's vers un datastore iSCSI

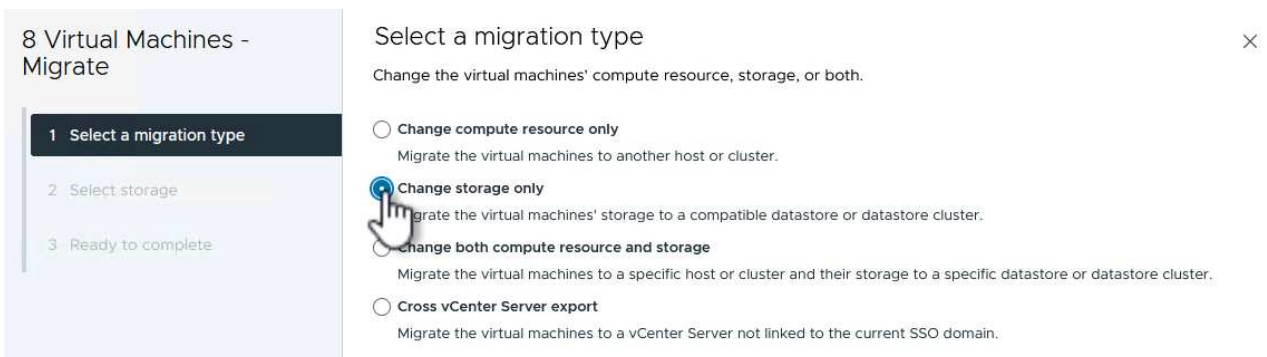
Lorsqu'il est préférable d'utiliser le stockage ONTAP pour protéger la VM de gestion VCF, vMotion peut être utilisé pour migrer les VM vers le nouveau datastore iSCSI.

Procédez comme suit pour migrer la VM de gestion VCF vers le datastore iSCSI.

1. Dans le client vSphere, naviguez jusqu'au cluster du domaine de gestion et cliquez sur l'onglet **VM**.
2. Sélectionnez les machines virtuelles à migrer vers le datastore iSCSI, cliquez avec le bouton droit de la souris et sélectionnez **migrer..**



3. Dans l'assistant **ordinateurs virtuels - migration**, sélectionnez **changer le stockage uniquement** comme type de migration et cliquez sur **Suivant** pour continuer.



4. Sur la page **Sélectionner le stockage**, sélectionnez le datastore iSCSI et sélectionnez **Suivant** pour continuer.

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

| Name | Storage Compatibility | Capacity | Provisioned | Free |
|------------------------|-----------------------|-----------|-------------|----------|
| mgmt_01_iscsi | -- | 3 TB | 1.46 GB | 3 TB |
| vcf-m01-cl01-ds-vsan01 | -- | 999.97 GB | 7.28 TB | 52.38 GB |

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Vérifiez les sélections et cliquez sur **Terminer** pour démarrer la migration.

6. L'état de la relocalisation peut être affiché à partir du volet **tâches récentes**.

| Task Name | Target | Status | Details |
|--------------------------|---------------------------------|--------|--|
| Relocate virtual machine | vcf-w01-nsx03 | 38% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-wkld-vc01 | 42% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-m01-otv9 | 36% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-m01-nsx01a | 49% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-w01-nsx02 | 47% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-m01-sddcm01 | 39% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-w01-nsx01 | 42% | Migrating Virtual Machine active state |
| Relocate virtual machine | vcf-m01-vc01 | 44% | Migrating Virtual Machine active state |

Informations supplémentaires

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au ["Documentation ONTAP 9"](#) centre.

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section ["Documentation de VMware Cloud Foundation"](#).

Vidéo de démonstration de cette solution

[Datastores iSCSI en tant que stockage supplémentaire pour les domaines de gestion VCF](#)

Utilisez les outils ONTAP pour configurer le stockage supplémentaire (vVols) pour les domaines de charge de travail VCF

Dans ce scénario, nous allons montrer comment déployer et utiliser les outils ONTAP pour VMware vSphere pour configurer un datastore **vVols** pour un domaine de charge de travail VCF.

iSCSI est utilisé comme protocole de stockage pour le datastore vVols.

Auteur: Josh Powell

Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

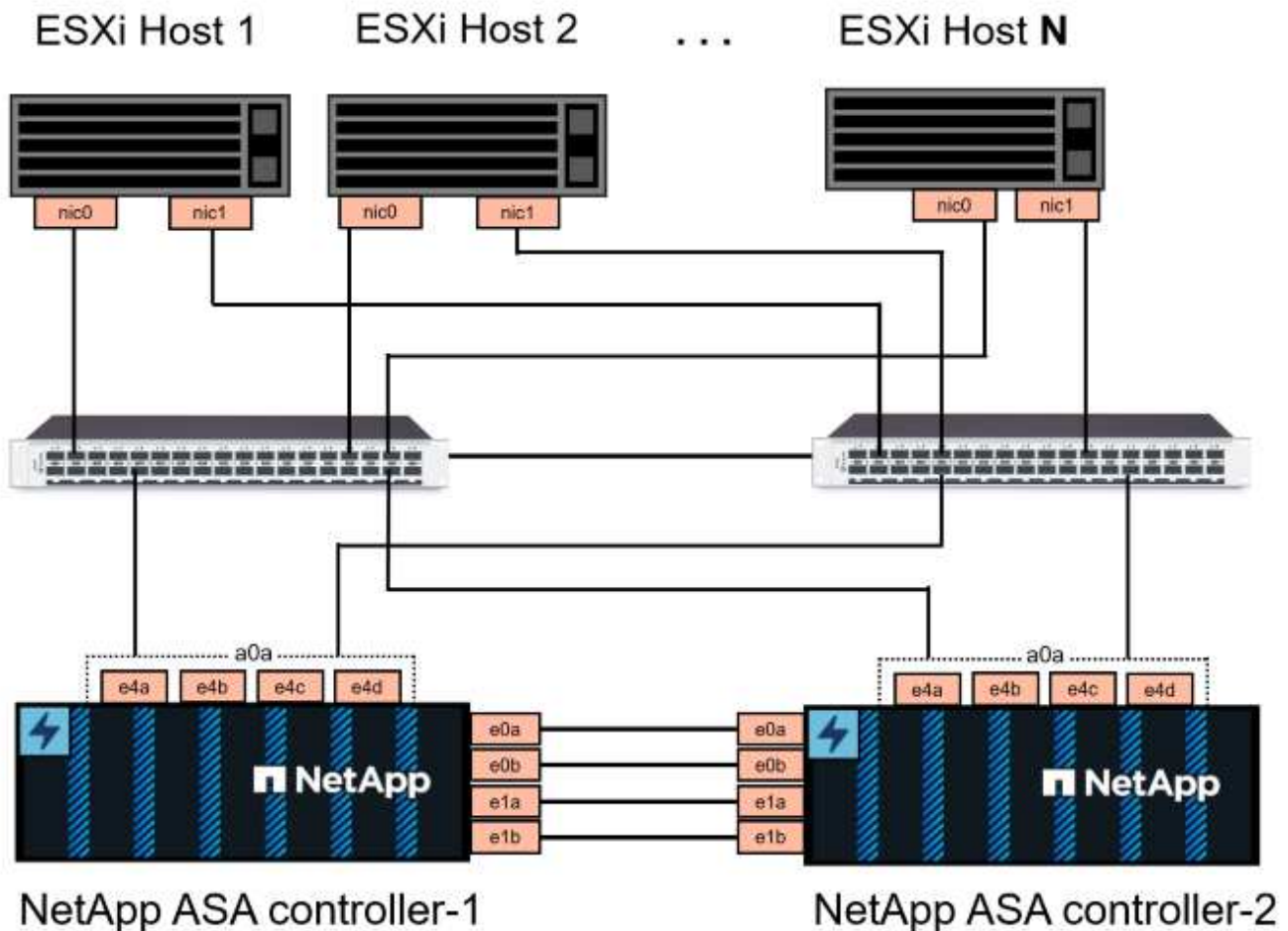
- Créez un SVM (Storage Virtual machine) avec des interfaces logiques (LIF) pour le trafic iSCSI.
- Créez des groupes de ports distribués pour les réseaux iSCSI sur le domaine de la charge de travail VI.
- Créez des adaptateurs vmkernel pour iSCSI sur les hôtes ESXi pour le domaine de charge de travail VI.
- Déployez les outils ONTAP sur le domaine de charge de travail VI.
- Créez un nouveau datastore vVols sur le domaine de la charge de travail VI.

Prérequis

Ce scénario nécessite les composants et configurations suivants :

- Un système de stockage ONTAP ASA doté de ports de données physiques sur des commutateurs ethernet dédiés au trafic de stockage.
- Le déploiement du domaine de gestion VCF est terminé et le client vSphere est accessible.
- Un domaine de charge de travail VI a déjà été déployé.

NetApp recommande des configurations réseau entièrement redondantes pour iSCSI. Le schéma suivant illustre un exemple de configuration redondante, fournissant une tolérance aux pannes pour les systèmes de stockage, les commutateurs, les cartes réseau et les systèmes hôtes. Reportez-vous au NetApp ["Référence de configuration SAN"](#) pour plus d'informations.



Pour les chemins d'accès multiples et le basculement sur plusieurs chemins, NetApp recommande de disposer d'au moins deux LIF par nœud de stockage dans des réseaux ethernet distincts pour tous les SVM dans les configurations iSCSI.

Cette documentation explique le processus de création d'un SVM et de spécification des informations d'adresse IP pour créer plusieurs LIFs pour le trafic iSCSI. Pour ajouter de nouvelles LIFs à un SVM existant, voir "[Créer une LIF \(interface réseau\)](#)".



Dans les cas où plusieurs adaptateurs VMkernel sont configurés sur le même réseau IP, il est recommandé d'utiliser la liaison logicielle des ports iSCSI sur les hôtes ESXi afin de garantir l'équilibrage de la charge sur les adaptateurs. Reportez-vous à l'article de la base de connaissances "[Considérations relatives à l'utilisation de la liaison logicielle du port iSCSI dans ESX/ESXi \(2038869\)](#)".

Pour plus d'informations sur l'utilisation de datastores iSCSI VMFS avec VMware, reportez-vous à la section "[Datastore VMFS vSphere - stockage iSCSI back-end avec ONTAP](#)".

Étapes de déploiement

Pour déployer les outils ONTAP et les utiliser pour créer un datastore vVols sur le domaine de gestion VCF, effectuez les opérations suivantes :

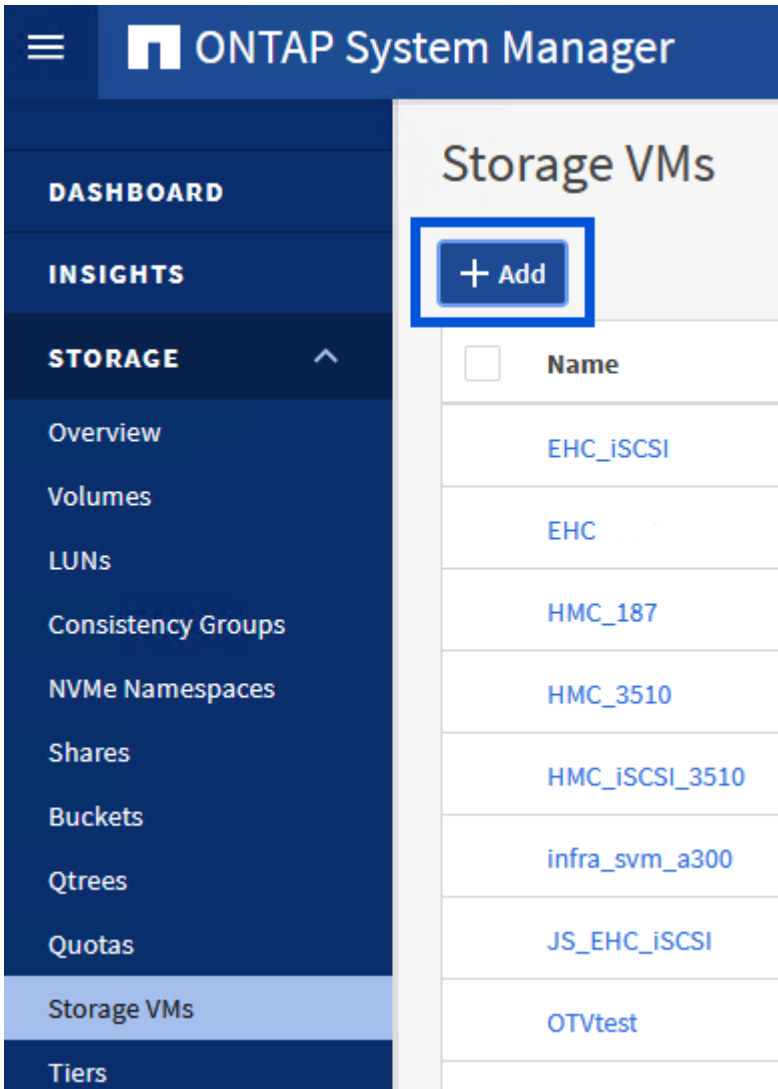
Créez un SVM et des LIF sur un système de stockage ONTAP

L'étape suivante s'effectue dans ONTAP System Manager.

Créez la VM de stockage et les LIF

Effectuer les étapes suivantes pour créer un SVM avec plusieurs LIF pour le trafic iSCSI.

1. Dans le Gestionnaire système ONTAP, accédez à **Storage VMs** dans le menu de gauche et cliquez sur **+ Add** pour démarrer.



2. Dans l'assistant **Add Storage VM**, indiquez un **Name** pour le SVM, sélectionnez **IP Space**, puis, sous **Access Protocol**, cliquez sur l'onglet **iSCSI** et cochez la case **Enable iSCSI**.

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. Dans la section **interface réseau**, remplissez les champs **adresse IP**, **masque de sous-réseau** et **domaine de diffusion et Port** pour la première LIF. Pour les LIF suivantes, la case à cocher peut être activée pour utiliser des paramètres communs à toutes les LIF restantes ou pour utiliser des paramètres distincts.



Pour les chemins d'accès multiples et le basculement sur plusieurs chemins, NetApp recommande de disposer d'au moins deux LIF par nœud de stockage dans des réseaux Ethernet distincts pour tous les SVM dans les configurations iSCSI.

NETWORK INTERFACE

ntaphci-a300-01

| | | | |
|---|---------------------------------|--------------------------------------|--|
| IP ADDRESS | SUBNET MASK | GATEWAY | BROADCAST DOMAIN AND PORT |
| <input type="text" value="172.21.118.179"/> | <input type="text" value="24"/> | Add optional gateway | <input type="text" value="NFS_iSCSI"/> |

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

| | |
|---|---------------------------------------|
| IP ADDRESS | PORT |
| <input type="text" value="172.21.119.179"/> | <input type="text" value="a0a-3375"/> |

ntaphci-a300-02

| | |
|---|---------------------------------------|
| IP ADDRESS | PORT |
| <input type="text" value="172.21.118.180"/> | <input type="text" value="a0a-3374"/> |

| | |
|---|---------------------------------------|
| IP ADDRESS | PORT |
| <input type="text" value="172.21.119.180"/> | <input type="text" value="a0a-3375"/> |

- Indiquez si vous souhaitez activer le compte Storage VM Administration (pour les environnements en colocation) et cliquez sur **Save** pour créer le SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

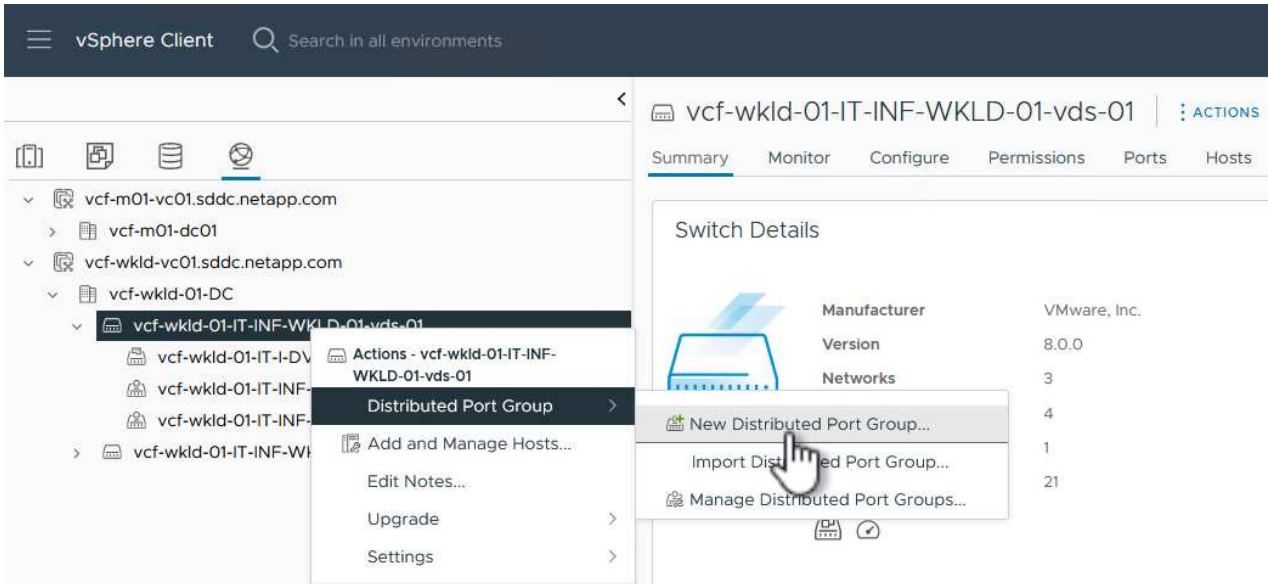
Configuration de la mise en réseau iSCSI sur les hôtes ESXi

Les étapes suivantes sont effectuées sur le cluster VI Workload Domain à l'aide du client vSphere. Dans ce cas, l'authentification unique vCenter est utilisée, de sorte que le client vSphere est commun aux domaines de gestion et de charge de travail.

Créez des groupes de ports distribués pour le trafic iSCSI

Pour créer un nouveau groupe de ports distribués pour chaque réseau iSCSI, procédez comme suit :

1. Dans le client vSphere , accédez à **Inventory > Networking** pour le domaine de charge de travail. Naviguez jusqu'au commutateur distribué existant et choisissez l'action pour créer **Nouveau groupe de ports distribués....**



2. Dans l'assistant **Nouveau groupe de ports distribués**, entrez un nom pour le nouveau groupe de ports et cliquez sur **Suivant** pour continuer.
3. Sur la page **configurer les paramètres**, remplissez tous les paramètres. Si des VLAN sont utilisés, assurez-vous de fournir l'ID de VLAN correct. Cliquez sur **Suivant** pour continuer.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

| | |
|---|----------------|
| Port binding | Static binding |
| Port allocation | Elastic ⓘ |
| Number of ports | 8 |
| Network resource pool | (default) |
| VLAN | |
| VLAN type | VLAN |
| VLAN ID | 3374 |
| Advanced | |
| <input type="checkbox"/> Customize default policies configuration | |

CANCEL

BACK

NEXT

4. Sur la page **prêt à terminer**, passez en revue les modifications et cliquez sur **Terminer** pour créer le nouveau groupe de ports distribués.
5. Répétez ce processus pour créer un groupe de ports distribués pour le deuxième réseau iSCSI utilisé et assurez-vous d'avoir saisi l'ID **VLAN** correct.
6. Une fois les deux groupes de ports créés, naviguez jusqu'au premier groupe de ports et sélectionnez l'action **Modifier les paramètres...**

The screenshot shows the vSphere Client interface. On the left, a tree view displays the environment structure, with the path **vcf-wkld-01-iscsi-a** selected. A context menu is open over this selection, showing options like **Actions - vcf-wkld-01-iscsi-a** and **Edit Settings...**. On the right, the **Distributed Port Group Details** panel is visible, showing the following configuration:

| | |
|--------------------------|---|
| Port binding | Static binding |
| Port allocation | Elastic |
| VLAN ID | 3374 |
| Distributed switch | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| Network protocol profile | -- |

7. Sur la page **Distributed Port Group - Edit Settings**, accédez à **Teaming and failover** dans le menu de gauche et cliquez sur **uplink2** pour le déplacer vers **uplinks** inutilisés.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a ×

| | | |
|-----------------------------|----------------------------------|---|
| General | Load balancing | Route based on originating virtual por ▼ |
| Advanced | Network failure detection | Link status only ▼ |
| VLAN | Notify switches | Yes ▼ |
| Security | Failback | Yes ▼ |
| Traffic shaping | | |
| Teaming and failover | | |
| Monitoring | | |
| Miscellaneous | | |

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL **OK**

8. Répétez cette étape pour le deuxième groupe de ports iSCSI. Cependant, cette fois, déplacez **uplink1** vers **uplinks** inutilisés.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

| | | |
|-----------------------------|----------------------------------|---|
| General | Load balancing | Route based on originating virtual por ▼ |
| Advanced | Network failure detection | Link status only ▼ |
| VLAN | Notify switches | Yes ▼ |
| Security | Failback | Yes ▼ |
| Traffic shaping | | |
| Teaming and failover | | |
| Monitoring | | |
| Miscellaneous | | |

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

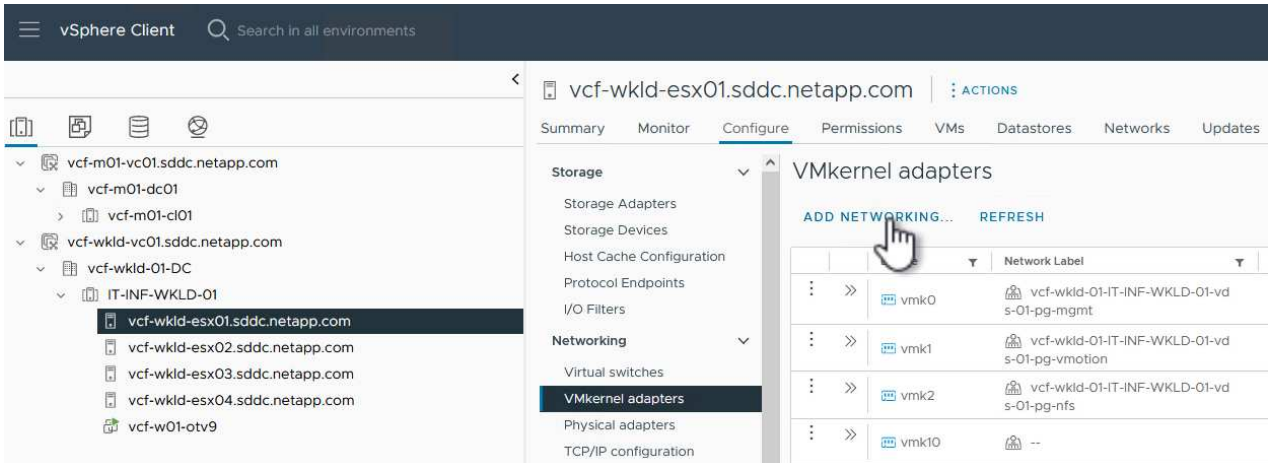
Unused uplinks

uplink1

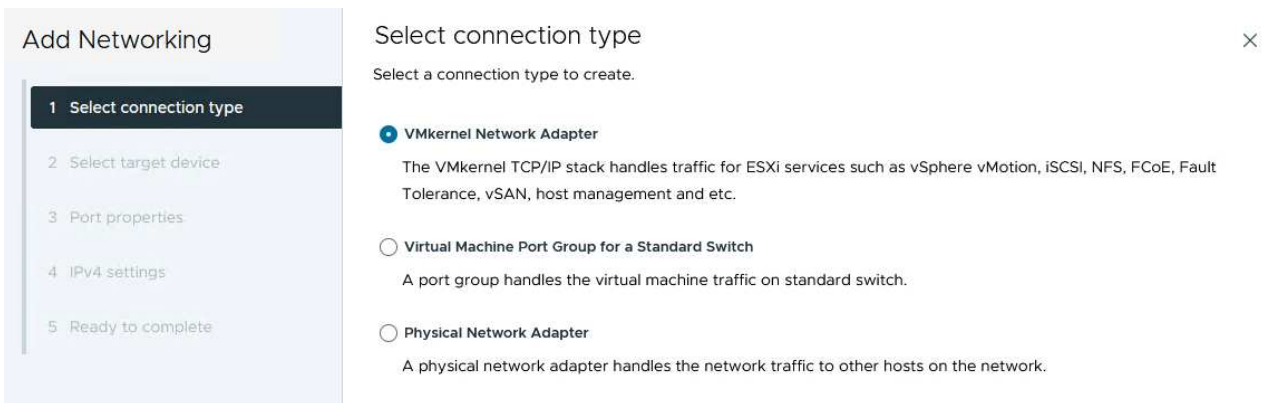
Créez des adaptateurs VMkernel sur chaque hôte ESXi

Répétez ce processus sur chaque hôte ESXi du domaine de charge de travail.

1. À partir du client vSphere, accédez à l'un des hôtes ESXi de l'inventaire du domaine de charge de travail. Dans l'onglet **configurer**, sélectionnez **adaptateurs VMkernel** et cliquez sur **Ajouter réseau...** pour démarrer.



2. Dans la fenêtre **Select connection type**, choisissez **VMkernel Network adapter** et cliquez sur **Next** pour continuer.



3. Sur la page **Sélectionner le périphérique cible**, choisissez l'un des groupes de ports distribués pour iSCSI créés précédemment.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete






Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

| | Name | NSX Port Group ID | Distributed Switch |
|----------------------------------|--|-------------------|-----------------------------------|
| <input checked="" type="radio"/> |  vcf-wkld-01-iscsi-a | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> |  vcf-wkld-01-iscsi-b | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> |  vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> |  vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-02 |
| <input type="radio"/> |  vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |

Manage Columns 5 items

CANCEL

BACK

NEXT

4. Sur la page **Port properties**, conservez les valeurs par défaut et cliquez sur **Next** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN
- vSAN Witness
- vSphere Backup NFC
- NVMe over TCP
- NVMe over RDMA

5. Sur la page **IPv4 settings**, remplissez **adresse IP**, **masque de sous-réseau** et fournissez une nouvelle adresse IP de passerelle (uniquement si nécessaire). Cliquez sur **Suivant** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

6. Consultez vos sélections sur la page **prêt à terminer** et cliquez sur **Terminer** pour créer l'adaptateur VMkernel.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-wkld-01-iscsi-a

Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
- ▼ Port properties

New port group vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.127 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

7. Répétez cette procédure pour créer un adaptateur VMkernel pour le second réseau iSCSI.

Déployer et utiliser les outils ONTAP pour configurer le stockage

Les étapes suivantes sont effectuées sur le cluster de domaine de gestion VCF à l'aide du client vSphere et impliquent le déploiement des outils ONTAP, la création d'un datastore iSCSI vVols et la migration des machines virtuelles de gestion vers le nouveau datastore.

Pour les domaines de charge de travail VI, les outils ONTAP sont installés sur le cluster de gestion VCF, mais enregistrés avec vCenter associé au domaine de charge de travail VI.

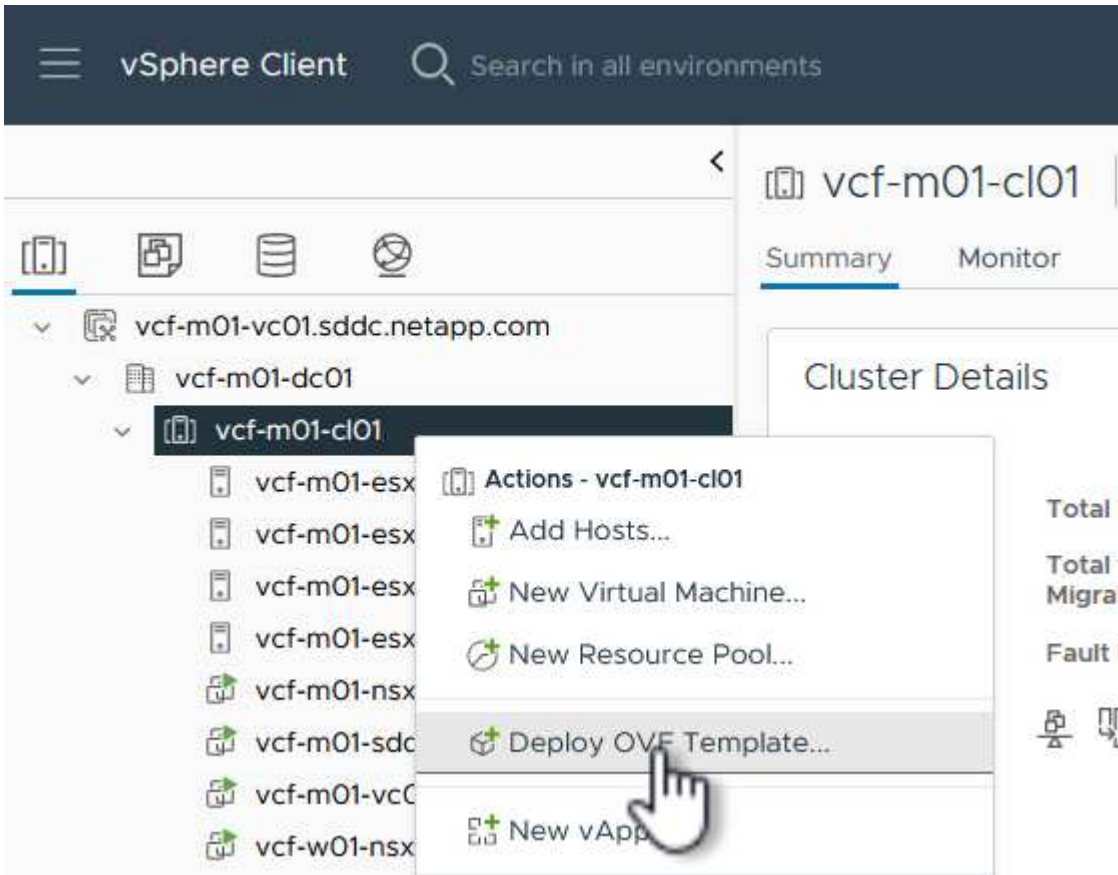
Pour plus d'informations sur le déploiement et l'utilisation des outils ONTAP dans un environnement à plusieurs serveurs vCenter, reportez-vous à la section ["Conditions requises pour l'enregistrement des outils ONTAP dans un environnement de plusieurs serveurs vCenter"](#).

Déployez les outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere sont déployés en tant qu'appliance de machine virtuelle et fournissent une interface utilisateur vCenter intégrée pour la gestion du stockage ONTAP.

Procédez comme suit pour déployer les outils ONTAP pour VMware vSphere :

1. Obtenir l'image OVA des outils ONTAP à partir du "[Site de support NetApp](#)" et télécharger dans un dossier local.
2. Connectez-vous à l'appliance vCenter pour le domaine de gestion VCF.
3. Dans l'interface de l'appliance vCenter, cliquez avec le bouton droit de la souris sur le cluster de gestion et sélectionnez **déployer le modèle OVF...**



4. Dans l'assistant **déployer modèle OVF**, cliquez sur le bouton radio **fichier local** et sélectionnez le fichier OVA des outils ONTAP téléchargé à l'étape précédente.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Pour les étapes 2 à 5 de l'assistant, sélectionnez un nom et un dossier pour la machine virtuelle, sélectionnez la ressource de calcul, vérifiez les détails et acceptez le contrat de licence.
6. Pour l'emplacement de stockage des fichiers de configuration et des fichiers disque, sélectionnez le datastore VSAN du cluster du domaine de gestion VCF.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [i](#)

Select virtual disk format

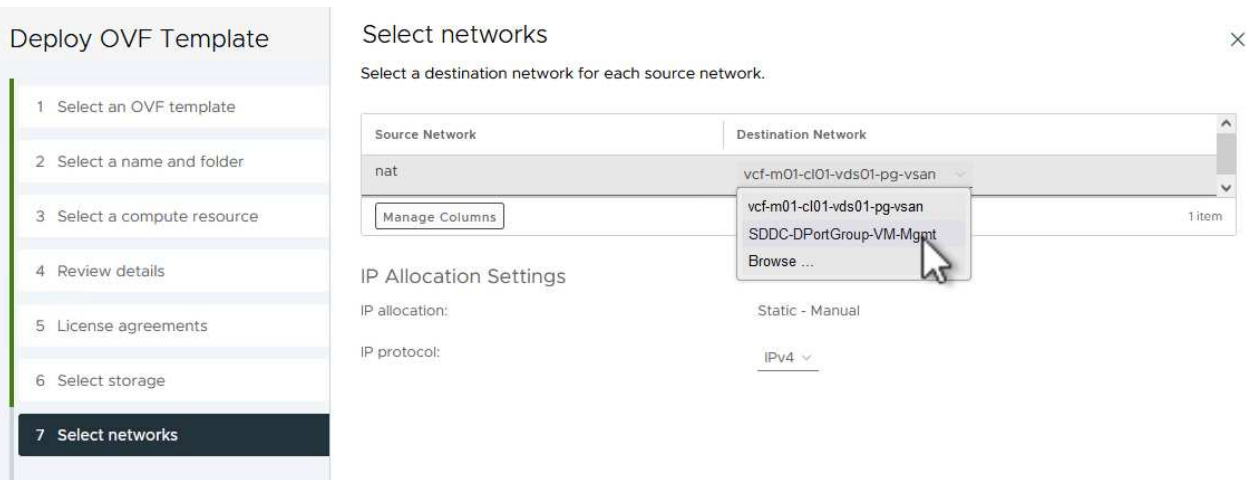
VM Storage Policy

Disable Storage DRS for this virtual machine

| | Name | Storage Compatibility | Capacity | Provisioned | Free | T |
|----------------------------------|-------------------------------------|-----------------------|-----------|-------------|-----------|---|
| <input checked="" type="radio"/> | vcf-m01-c01-ds-vsant01 | -- | 999.97 GB | 7.17 TB | 225.72 GB | v |
| <input type="radio"/> | vcf-m01-esx01-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx02-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx03-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx04-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |

Manage Columns Items per page 10 5 items

7. Sur la page Sélectionner le réseau, sélectionnez le réseau utilisé pour le trafic de gestion.



8. Sur la page Personnaliser le modèle, remplissez toutes les informations requises :

- Mot de passe à utiliser pour l'accès administratif aux outils ONTAP.
- Adresse IP du serveur NTP.
- Mot de passe du compte de maintenance des outils ONTAP.
- ONTAP Outils Derby DB mot de passe.
- Ne cochez pas la case **Activer VMware Cloud Foundation (VCF)**. Le mode VCF n'est pas requis pour le déploiement de stockage supplémentaire.
- FQDN ou adresse IP de l'appliance vCenter pour le **VI Workload Domain**
- Informations d'identification pour l'appliance vCenter du **VI Workload Domain**
- Renseignez les champs de propriétés réseau requis.

Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

! 2 properties have invalid values X

System Configuration 4 settings

Application User Password (*) Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password

Confirm Password

NTP Servers A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

Maintenance User Password (*) Password to assign to maint user account.

Password

Confirm Password

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Configure vCenter or Enable vCF 3 settings

Enable VMware Cloud Foundation (VCF) vCenter server and user details are ignored when VCF is enabled.

vCenter Server Address (*) Specify the IP address/hostname of an existing vCenter to register to.

Port (*) Specify the HTTPS port of an existing vCenter to register to.

Username (*) Specify the username of an existing vCenter to register to.

Password (*) Specify the password of an existing vCenter to register to.

Password

Confirm Password

Network Properties 8 settings

Host Name Specify the hostname for the appliance. (Leave blank if DHCP is desired)

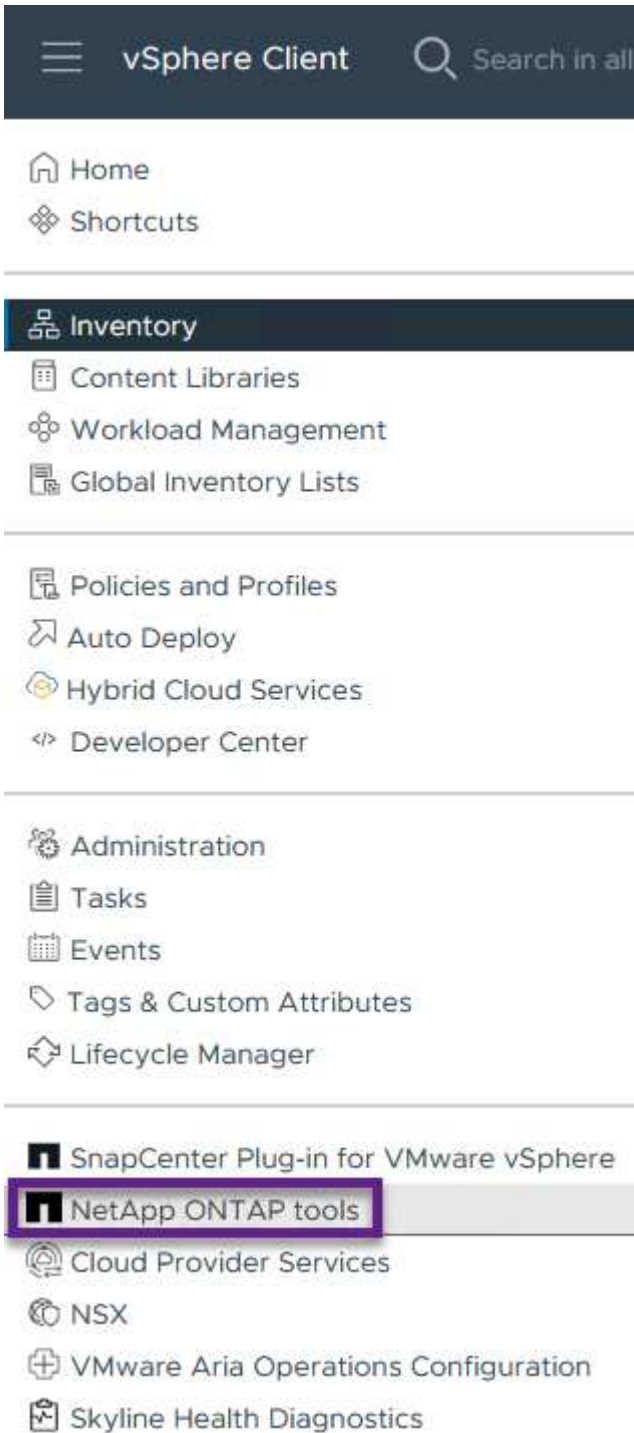
IP Address Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL BACK NEXT

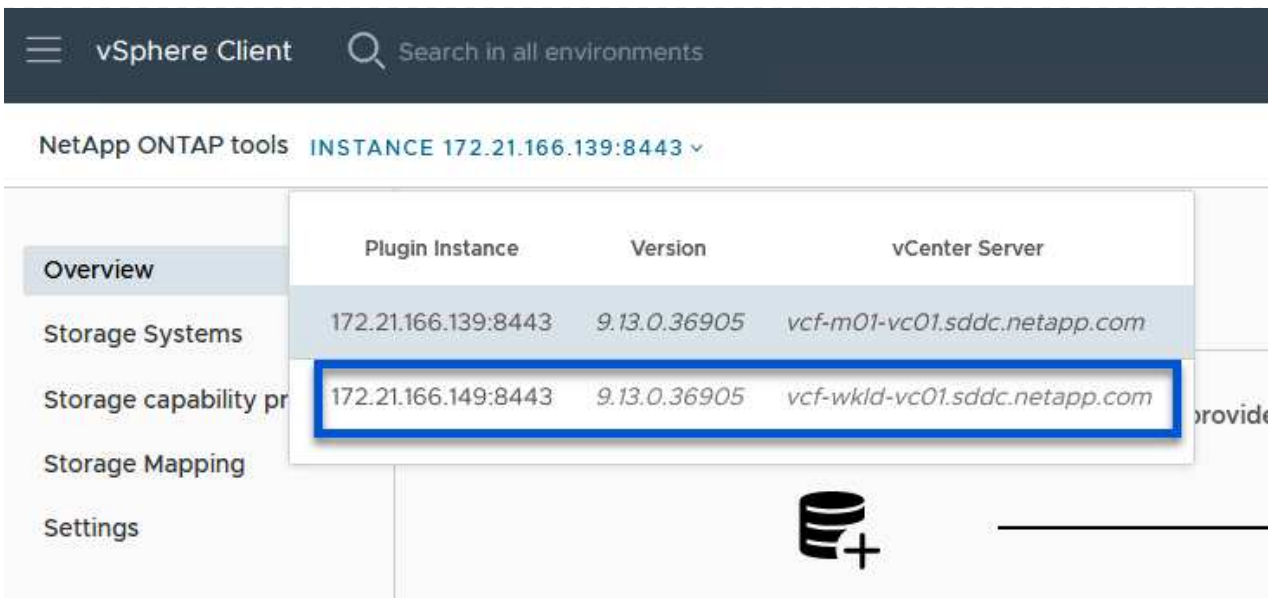
9. Passez en revue toutes les informations de la page prêt à terminer et cliquez sur Terminer pour commencer à déployer l'appliance Outils ONTAP.

Ajoutez un système de stockage aux outils ONTAP.

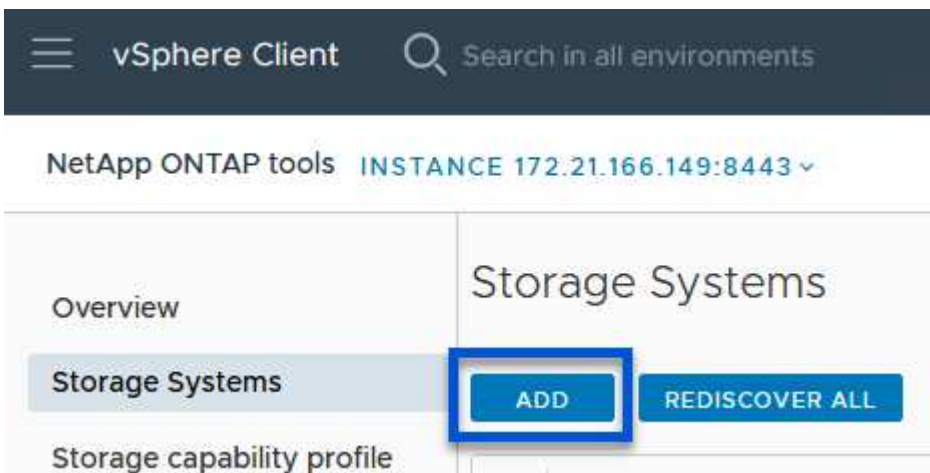
1. Accédez aux outils NetApp ONTAP en les sélectionnant dans le menu principal du client vSphere.



2. Dans le menu déroulant **INSTANCE** de l'interface de l'outil ONTAP, sélectionnez l'instance Outils ONTAP associée au domaine de charge de travail à gérer.



3. Dans Outils ONTAP, sélectionnez **systèmes de stockage** dans le menu de gauche, puis appuyez sur **Ajouter**.




4. Indiquez l'adresse IP, les informations d'identification du système de stockage et le numéro de port. Cliquez sur **Ajouter** pour lancer le processus de découverte.



VVol requiert des informations d'identification de cluster ONTAP plutôt que des informations d'identification de SVM. Pour plus d'informations, reportez-vous à la section "[Ajout de systèmes de stockage](#)" Dans la documentation Outils ONTAP.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server vcf-m01-vc01.sddc.netapp.com 

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options 

ONTAP Cluster Certificate: Automatically fetch Manually upload

CANCEL

SAVE & ADD MORE

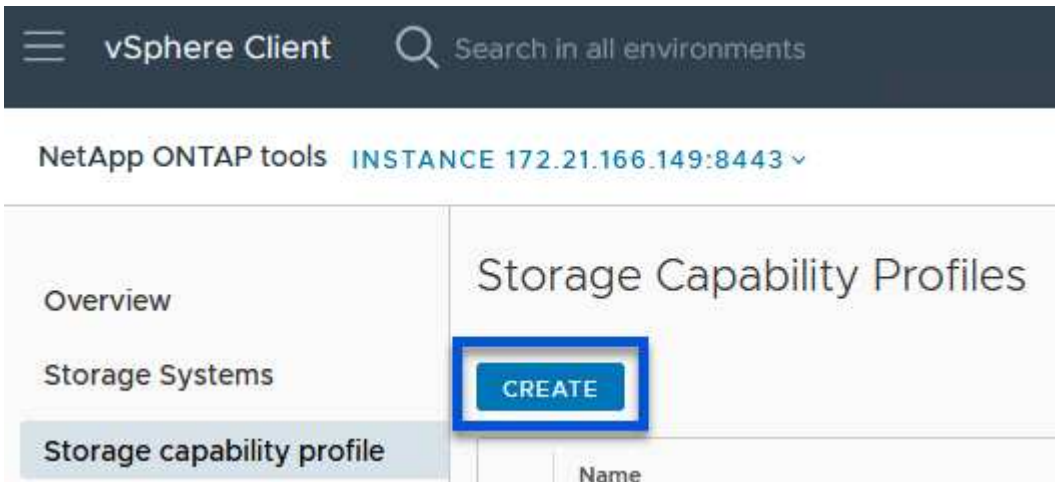
ADD

Créez un profil de capacité de stockage dans les outils ONTAP

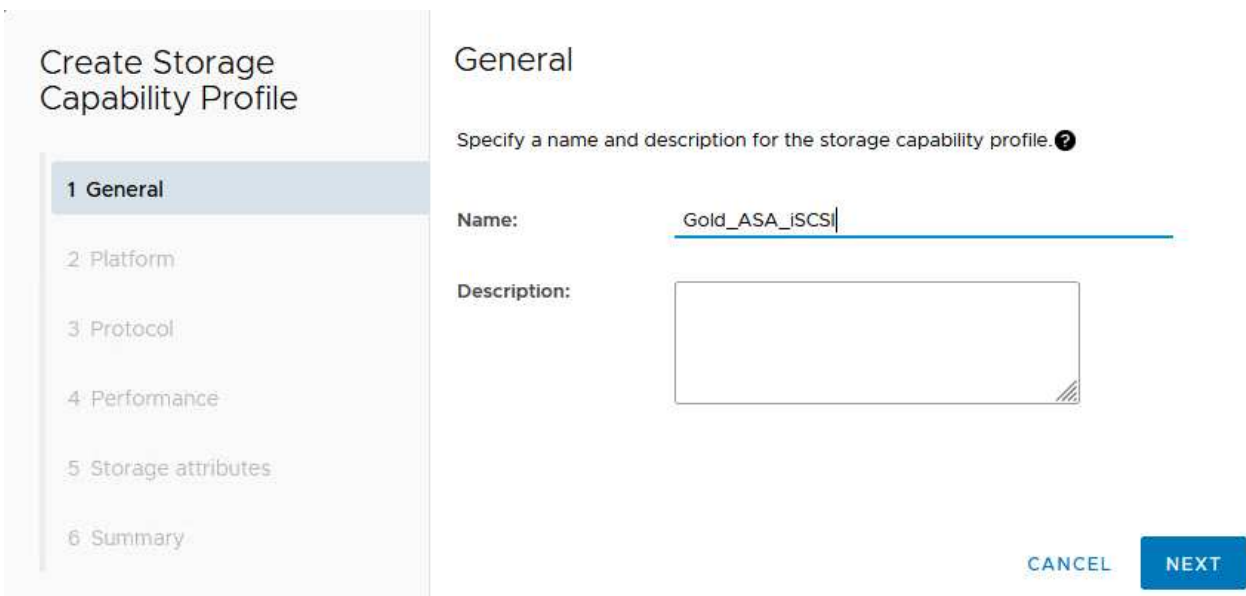
Les profils de capacité de stockage décrivent les fonctionnalités fournies par une baie de stockage ou un système de stockage. Ils incluent des définitions de qualité de service et sont utilisés pour sélectionner des systèmes de stockage qui répondent aux paramètres définis dans le profil. Vous pouvez utiliser l'un des profils fournis ou en créer de nouveaux.

Pour créer un profil de capacité de stockage dans les outils ONTAP, procédez comme suit :

1. Dans Outils ONTAP, sélectionnez **profil de capacité de stockage** dans le menu de gauche, puis appuyez sur **Créer**.



2. Dans l'assistant **Créer un profil de capacité de stockage**, indiquez un nom et une description du profil et cliquez sur **Suivant**.



3. Sélectionnez le type de plate-forme et pour spécifier que le système de stockage doit être un ensemble de baies SAN 100 % Flash **asymétrique** sur **FALSE**.

Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. Ensuite, sélectionnez le protocole ou **n'importe quel** pour autoriser tous les protocoles possibles. Cliquez sur **Suivant** pour continuer.

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. La page **performance** permet de définir la qualité de service sous la forme d'IOPS minimum et maximum autorisées.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

6. Complétez la page **Storage Attributes** en sélectionnant l'efficacité du stockage, la réservation d'espace, le cryptage et toute règle de hiérarchisation, le cas échéant.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Storage attributes

Deduplication:

Yes



Compression:

Yes



Space reserve:

Thin



Encryption:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

7. Enfin, passez en revue le résumé et cliquez sur Terminer pour créer le profil.

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

Summary

| | |
|------------------------------|----------------|
| Name: | ASA_Gold_iSCSI |
| Description: | N/A |
| Platform: | Performance |
| Asymmetric: | No |
| Protocol: | Any |
| Max IOPS: | 6000 IOPS |
| Space reserve: | Thin |
| Deduplication: | Yes |
| Compression: | Yes |
| Encryption: | Yes |
| Tiering policy (FabricPool): | None |

CANCEL

BACK

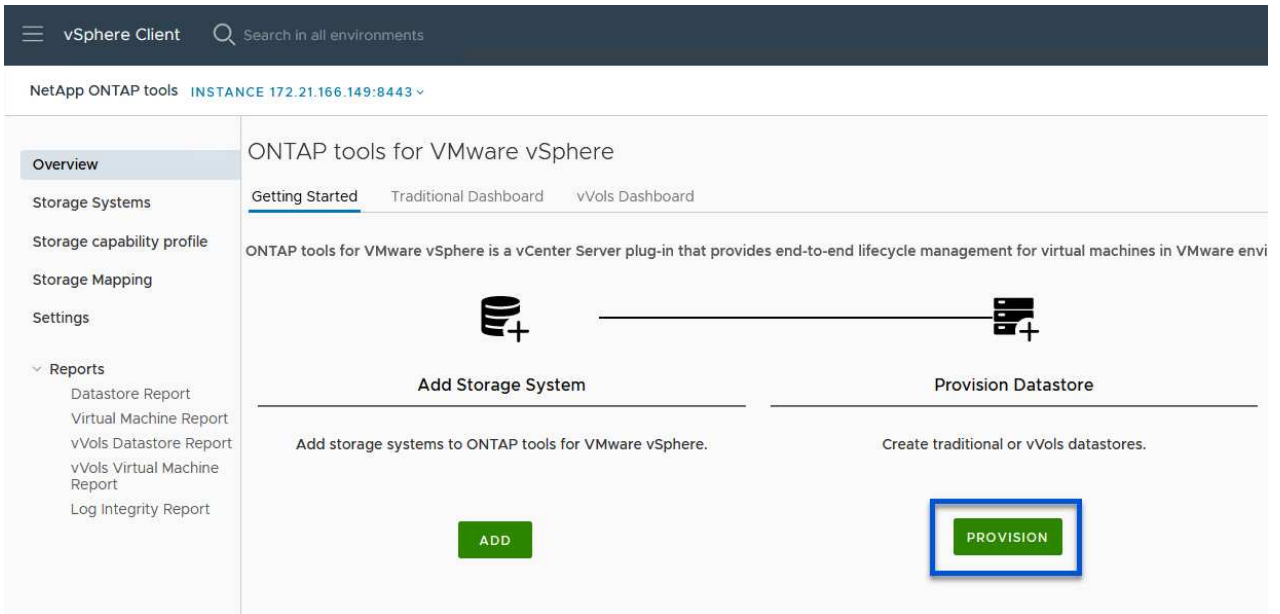
FINISH



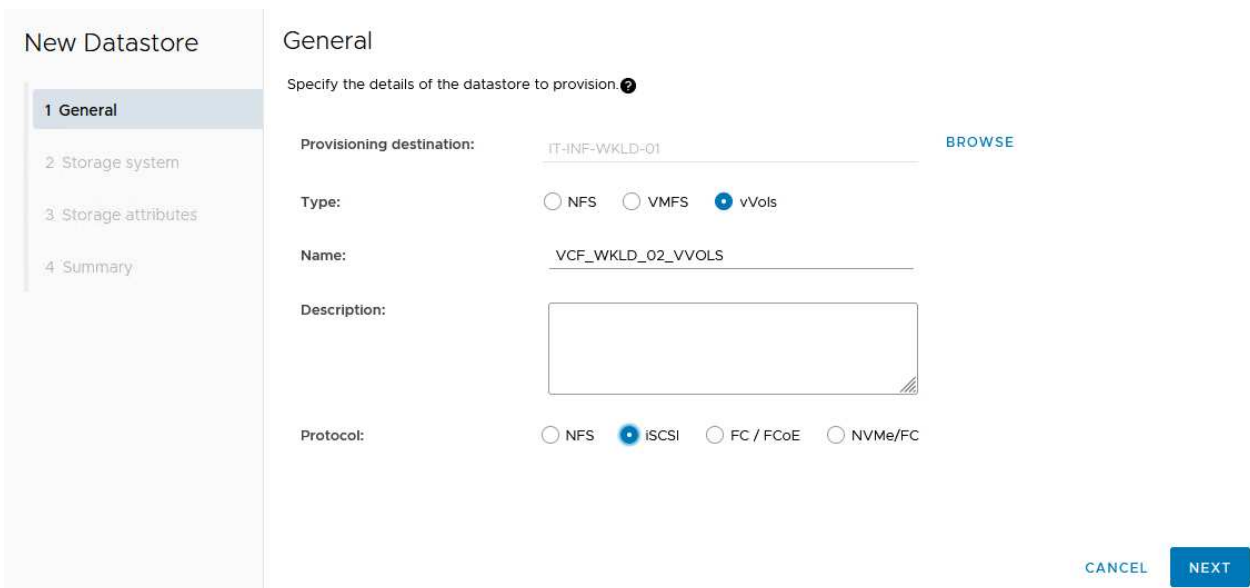
Créez un datastore vVols dans les outils ONTAP

Pour créer un datastore vVols dans les outils ONTAP, procédez comme suit :

1. Dans Outils ONTAP, sélectionnez **Présentation** et dans l'onglet **mise en route**, cliquez sur **Provision** pour démarrer l'assistant.



2. Sur la page **général** de l'assistant Nouveau datastore, sélectionnez le centre de données vSphere ou la destination du cluster. Sélectionnez **vVols** comme type de datastore, indiquez un nom pour le datastore et sélectionnez **iSCSI** comme protocole. Cliquez sur **Suivant** pour continuer.



3. Sur la page **système de stockage**, sélectionner le profil de capacité de stockage, le système de stockage et le SVM. Cliquez sur **Suivant** pour continuer.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

- AFF_Encrypted_Min50_ASA_A
- FAS_Default
- FAS_Max20
- Custom profiles
- ASA_Gold_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_iSCSI

CANCEL BACK NEXT

4. Sur la page **attributs de stockage**, sélectionnez pour créer un nouveau volume pour le datastore et remplissez les attributs de stockage du volume à créer. Cliquez sur **Ajouter** pour créer le volume, puis sur **Suivant** pour continuer.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

| Name | Size | Storage Capability Profile | Aggregate |
|---|------|----------------------------|-----------|
|  FlexVol volumes are not added. | | | |

| Name | Size(GB) ⓘ | Storage capability profile | Aggregates | Space reserve |
|-----------------|------------|----------------------------|-------------------------|---------------|
| f_wkld_02_vvols | 3000 | ASA_Gold_iSCSI | EHCaggr02 - (27053.3 GE | Thin |

ADD
CANCEL BACK NEXT

5. Enfin, passez en revue le résumé et cliquez sur **Finish** pour lancer le processus de création du datastore vVol.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

Datastore type: vVols
Protocol: iSCSI
Storage capability profile: ASA_Gold_iSCSI

Storage system details

Storage system: ntaphcl-a300e9u25
SVM: VCF_iSCSI

Storage attributes

| New FlexVol Name | New FlexVol Size | Aggregate | Storage Capability Profile |
|-------------------|------------------|-----------|----------------------------|
| vcf_wkld_02_vvols | 3000 GB | EHCAGgr02 | ASA_Gold_iSCSI |

Click 'Finish' to provision this datastore.

CANCEL
BACK
FINISH

Informations supplémentaires

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au ["Documentation ONTAP 9"](#) centre.

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section ["Documentation de VMware Cloud Foundation"](#).

Configuration du stockage supplémentaire NVMe/TCP pour les domaines de charge de travail VCF

Dans ce scénario, nous montrerons comment configurer du stockage supplémentaire NVMe/TCP pour un domaine de charge de travail VCF.

Auteur: Josh Powell

Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

- Créez une machine virtuelle de stockage (SVM) avec des interfaces logiques (LIF) pour le trafic NVMe/TCP.
- Créez des groupes de ports distribués pour les réseaux iSCSI sur le domaine de la charge de travail VI.
- Créez des adaptateurs vmkernel pour iSCSI sur les hôtes ESXi pour le domaine de charge de travail VI.
- Ajout d'adaptateurs NVMe/TCP sur les hôtes ESXi
- Déployez un datastore NVMe/TCP.

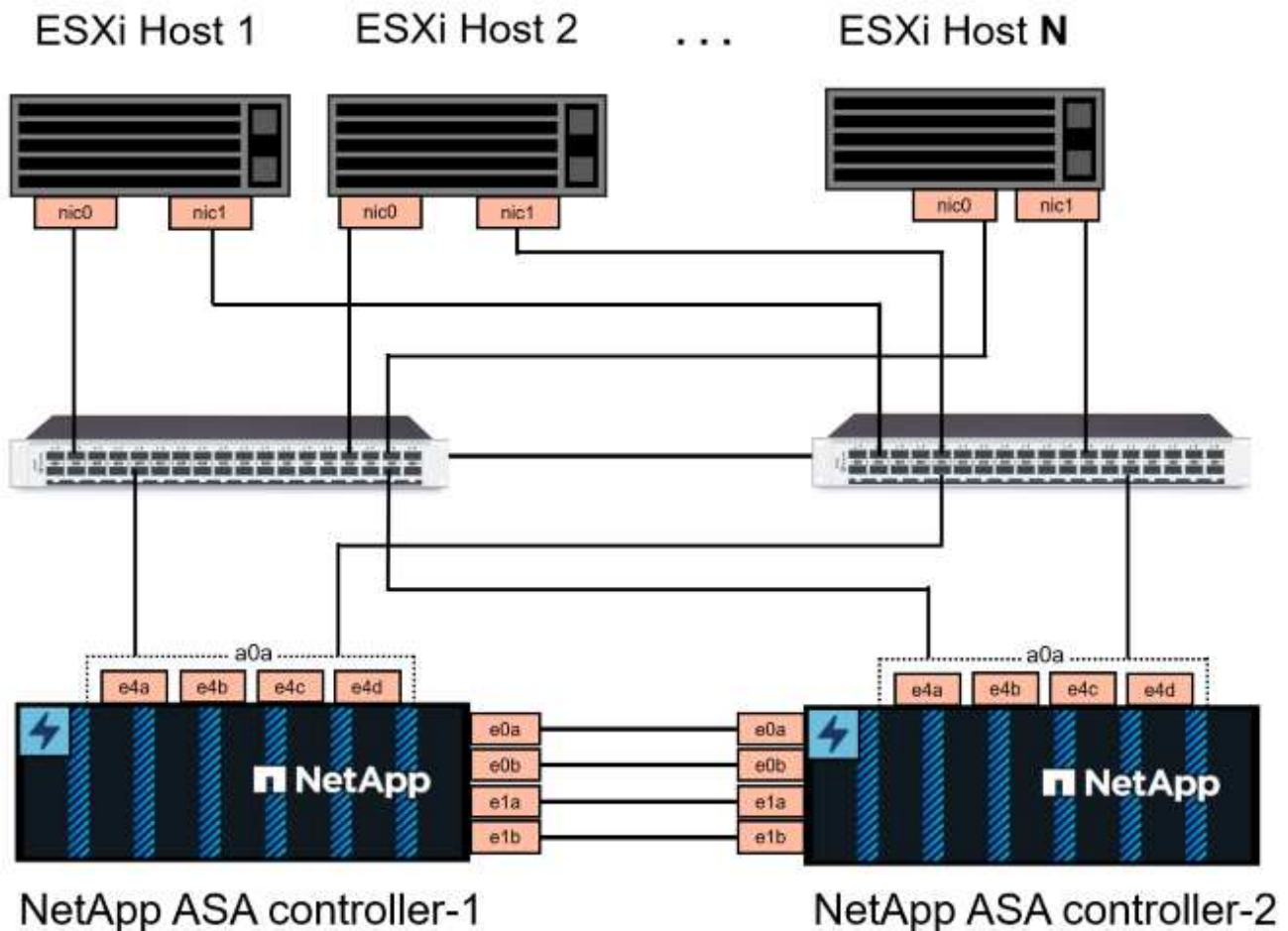
Prérequis

Ce scénario nécessite les composants et configurations suivants :

- Un système de stockage ONTAP ASA doté de ports de données physiques sur des commutateurs ethernet dédiés au trafic de stockage.

- Le déploiement du domaine de gestion VCF est terminé et le client vSphere est accessible.
- Un domaine de charge de travail VI a déjà été déployé.

NetApp recommande des designs réseau entièrement redondants pour NVMe/TCP. Le schéma suivant illustre un exemple de configuration redondante, fournissant une tolérance aux pannes pour les systèmes de stockage, les commutateurs, les cartes réseau et les systèmes hôtes. Reportez-vous au NetApp ["Référence de configuration SAN"](#) pour plus d'informations.



Pour les chemins d'accès multiples et le basculement sur plusieurs chemins, NetApp recommande de disposer d'au moins deux LIF par nœud de stockage dans des réseaux ethernet distincts pour tous les SVM dans des configurations NVMe/TCP.

Cette documentation explique le processus de création d'un SVM et de spécification des informations d'adresse IP pour créer plusieurs LIFs pour le trafic NVMe/TCP. Pour ajouter de nouvelles LIFs à un SVM existant, voir ["Créer une LIF \(interface réseau\)"](#).

Pour plus d'informations sur les considérations relatives à la conception NVMe des systèmes de stockage ONTAP, reportez-vous à la section ["Configuration, prise en charge et limitations de NVMe"](#).

Étapes de déploiement

Pour créer un datastore VMFS sur un domaine de charge de travail VCF à l'aide de NVMe/TCP, procédez comme suit.

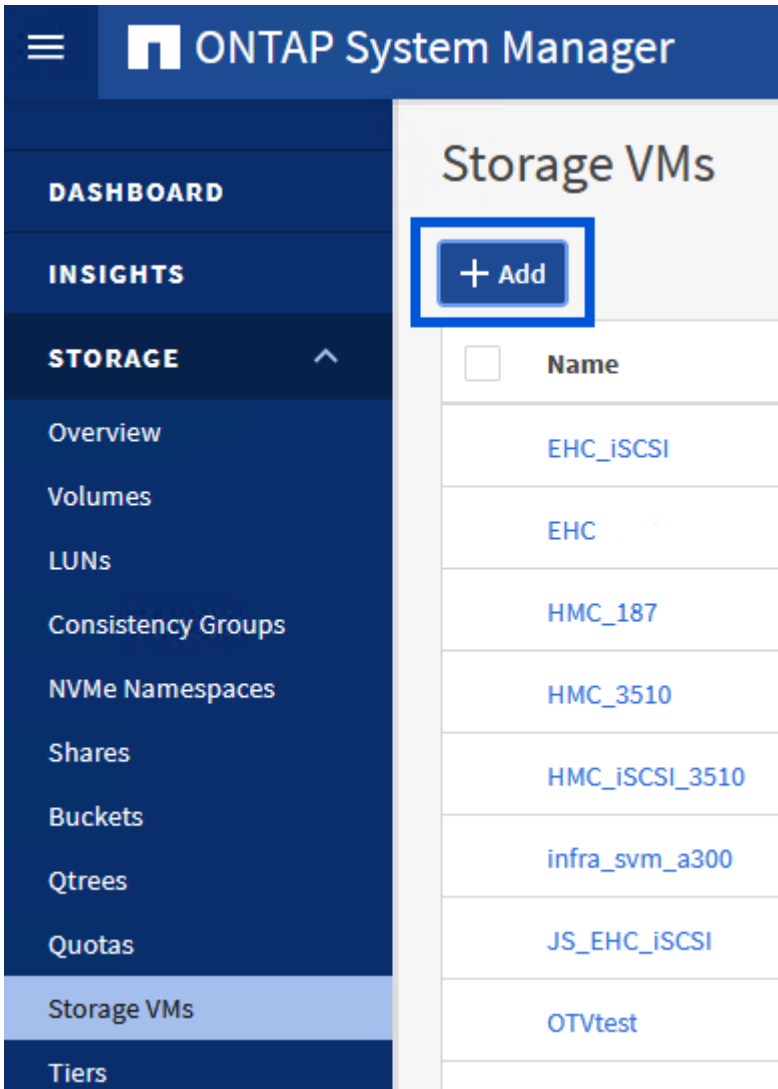
Créez un SVM, des LIF et un namespace NVMe sur un système de stockage ONTAP

L'étape suivante s'effectue dans ONTAP System Manager.

Créez la VM de stockage et les LIF

Effectuez les étapes suivantes pour créer un SVM avec plusieurs LIF pour le trafic NVMe/TCP.

1. Dans le Gestionnaire système ONTAP, accédez à **Storage VMs** dans le menu de gauche et cliquez sur **+ Add** pour démarrer.



2. Dans l'assistant **Add Storage VM**, indiquez un **Name** pour le SVM, sélectionnez **IP Space**, puis, sous **Access Protocol**, cliquez sur l'onglet **NVMe** et cochez la case **Enable NVMe/TCP**.

Add Storage VM



STORAGE VM NAME

VCF_NVMe

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable NVMe/FC

Enable NVMe/TCP

3. Dans la section **interface réseau**, remplissez les champs **adresse IP**, **masque de sous-réseau** et **domaine de diffusion et Port** pour la première LIF. Pour les LIF suivantes, la case à cocher peut être activée pour utiliser des paramètres communs à toutes les LIF restantes ou pour utiliser des paramètres distincts.



Pour les chemins d'accès multiples et le basculement sur plusieurs chemins, NetApp recommande de disposer d'au moins deux LIF par nœud de stockage dans des réseaux Ethernet distincts pour tous les SVM dans des configurations NVMe/TCP.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189


SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT 


NFS_iSCSI 

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.189

PORT


a0a-3375 

ntaphci-a300-02

IP ADDRESS

172.21.118.190


PORT

a0a-3374 

IP ADDRESS

172.21.119.190

PORT

a0a-3375 

Storage VM Administration

Manage administrator account

Save

Cancel

- Indiquez si vous souhaitez activer le compte Storage VM Administration (pour les environnements en colocation) et cliquez sur **Save** pour créer le SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

Créez le namespace NVMe

Les espaces de noms NVMe sont analogues aux LUN pour iSCSI ou FC. L'espace de noms NVMe doit être créé avant de pouvoir déployer un datastore VMFS à partir du client vSphere. Pour créer l'espace de noms NVMe, vous devez d'abord obtenir le nom NQN (NVMe Qualified Name) de chaque hôte ESXi du cluster. Le NQN est utilisé par ONTAP pour fournir un contrôle d'accès à l'espace de noms.

Pour créer un namespace NVMe, procédez comme suit :

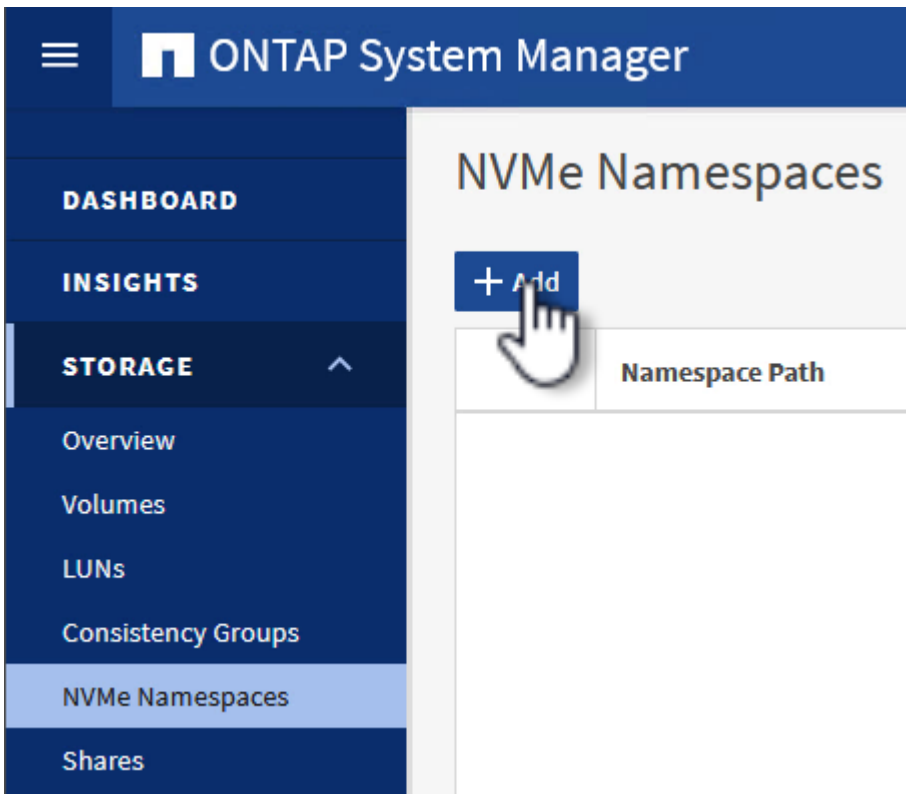
1. Ouvrez une session SSH avec un hôte ESXi dans le cluster pour obtenir son NQN. Utilisez la commande suivante depuis l'interface de ligne de commande :

```
esxcli nvme info get
```

Une sortie similaire à la suivante doit s'afficher :

```
Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
```

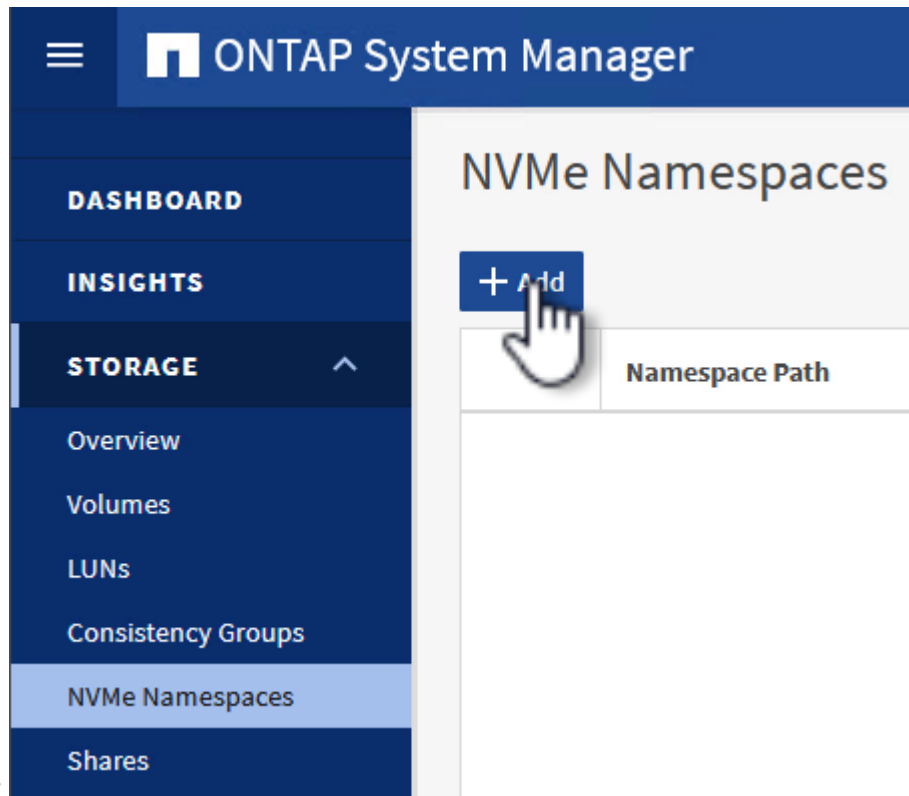
2. Enregistrez le NQN pour chaque hôte ESXi du cluster
3. Dans le Gestionnaire système ONTAP, naviguez jusqu'à **Namespaces NVMe** dans le menu de gauche et cliquez sur **+ Add** pour démarrer.



4. Sur la page **Ajouter un espace de noms NVMe**, indiquez un préfixe de nom, le nombre d'espaces de noms à créer, la taille de l'espace de noms et le système d'exploitation hôte qui accédera à

l'espace de noms. Dans la section **Host NQN**, créez une liste séparée par des virgules des NQN précédemment collectés auprès des hôtes ESXi qui accéderont aux espaces de noms.

Cliquez sur **plus d'options** pour configurer des éléments supplémentaires tels que la stratégie de protection des snapshots. Enfin, cliquez sur **Save** pour créer l'espace de noms NVMe.



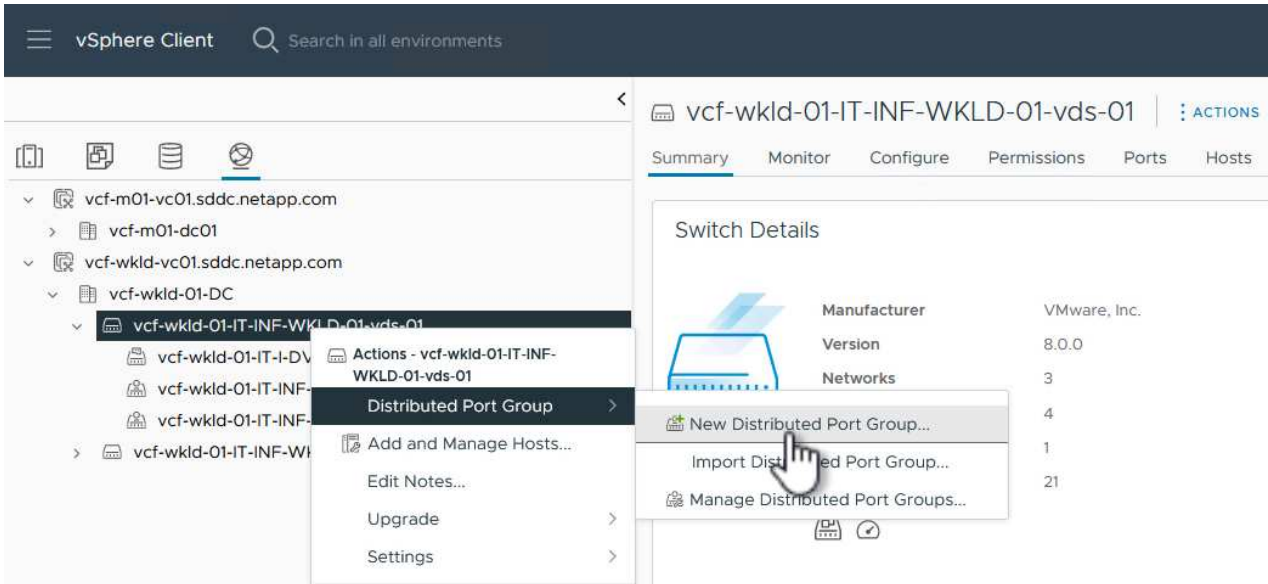
Configuration du réseau et des adaptateurs logiciels NVMe sur des hôtes ESXi

Les étapes suivantes sont effectuées sur le cluster du domaine de la charge de travail VI à l'aide du client vSphere. Dans ce cas, l'authentification unique vCenter est utilisée, de sorte que le client vSphere est commun aux domaines de la gestion et de la charge de travail.

Créez des groupes de ports distribués pour le trafic NVMe/TCP

Pour créer un nouveau groupe de ports distribués pour chaque réseau NVMe/TCP, procédez comme suit :

1. Dans le client vSphere , accédez à **Inventory > Networking** pour le domaine de charge de travail. Naviguez jusqu'au commutateur distribué existant et choisissez l'action pour créer **Nouveau groupe de ports distribués....**



2. Dans l'assistant **Nouveau groupe de ports distribués**, entrez un nom pour le nouveau groupe de ports et cliquez sur **Suivant** pour continuer.
3. Sur la page **configurer les paramètres**, remplissez tous les paramètres. Si des VLAN sont utilisés, assurez-vous de fournir l'ID de VLAN correct. Cliquez sur **Suivant** pour continuer.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

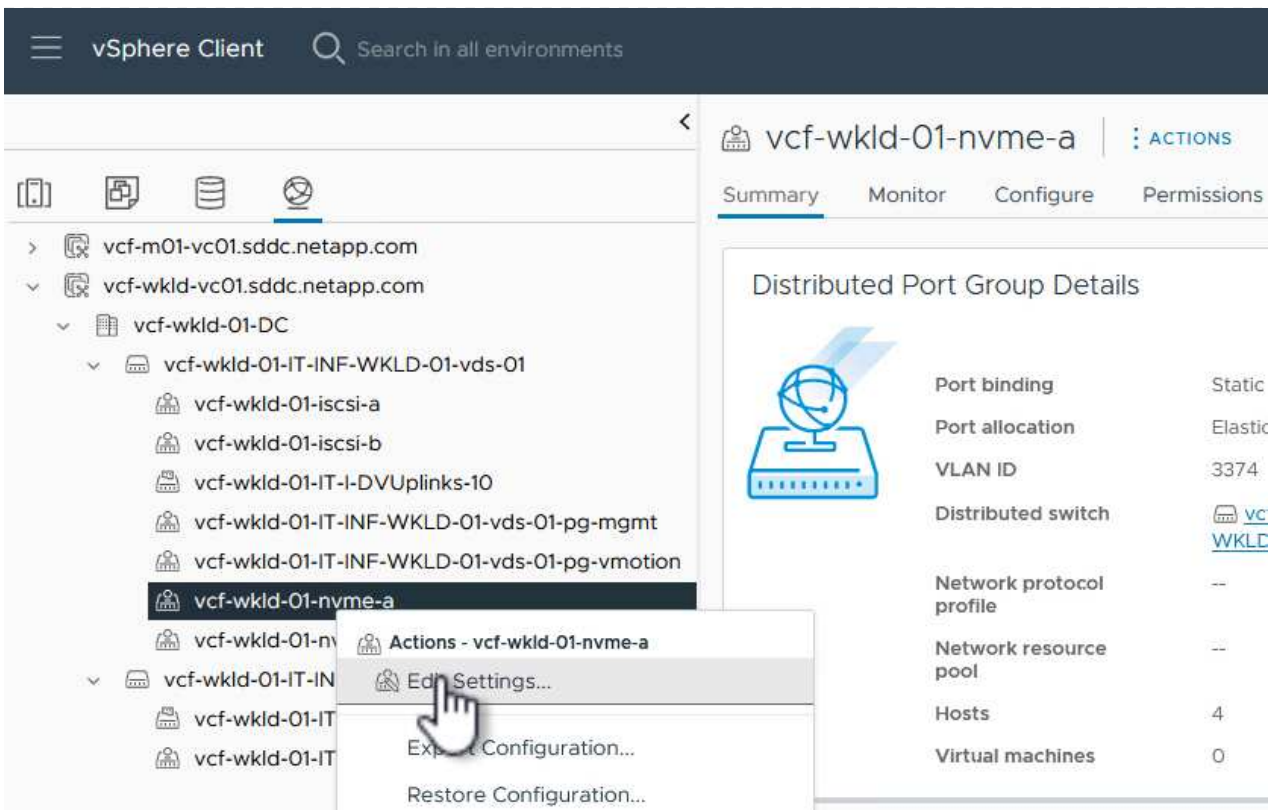
| | |
|---|------------------------|
| Port binding | Static binding |
| Port allocation | Elastic ? |
| Number of ports | 8 |
| Network resource pool | (default) |
| VLAN | |
| VLAN type | VLAN |
| VLAN ID | 3374 |
| Advanced | |
| <input type="checkbox"/> Customize default policies configuration | |

CANCEL

BACK

NEXT

4. Sur la page **prêt à terminer**, passez en revue les modifications et cliquez sur **Terminer** pour créer le nouveau groupe de ports distribués.
5. Répétez ce processus pour créer un groupe de ports distribués pour le deuxième réseau NVMe/TCP utilisé et assurez-vous que vous avez entré l'ID **VLAN** correct.
6. Une fois les deux groupes de ports créés, naviguez jusqu'au premier groupe de ports et sélectionnez l'action **Modifier les paramètres...**



7. Sur la page **Distributed Port Group - Edit Settings**, accédez à **Teaming and failover** dans le menu de gauche et cliquez sur **uplink2** pour le déplacer vers **uplinks** inutilisés.

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing Route based on originating virtual port

Network failure detection Link status only

Notify switches Yes

Failback Yes

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

8. Répétez cette étape pour le deuxième groupe de ports NVMe/TCP. Cependant, cette fois, déplacez

uplink1 vers uplinks inutilisés.

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and fallover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual por 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 


[MOVE UP](#) [MOVE DOWN](#)

Active uplinks

 uplink2

Standby uplinks

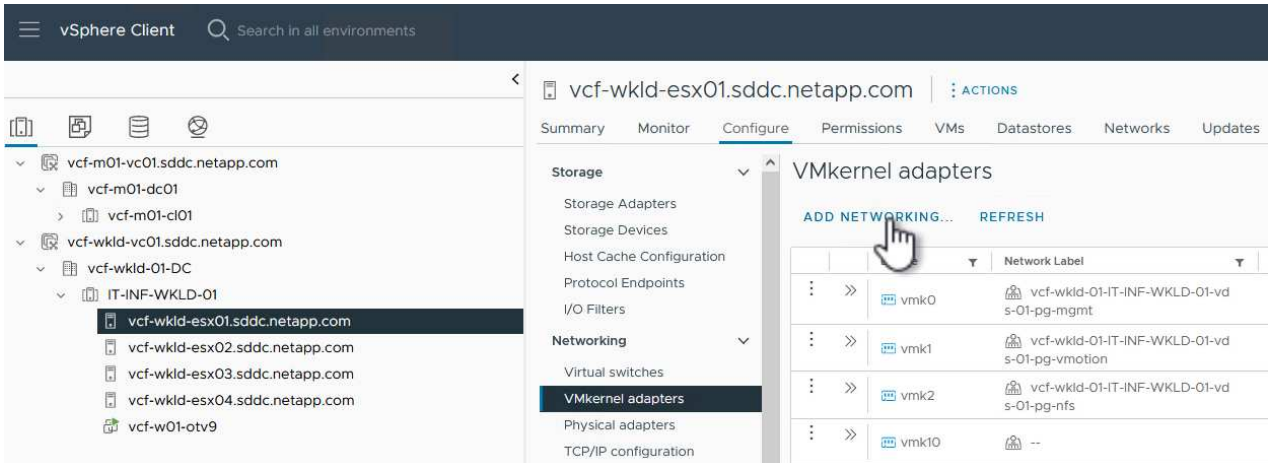
Unused uplinks

 uplink1

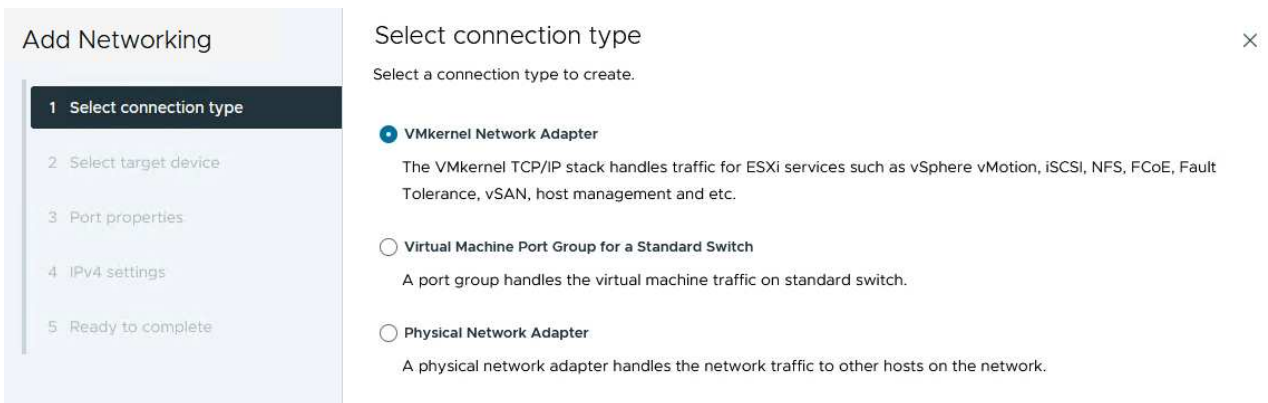
Créez des adaptateurs VMkernel sur chaque hôte ESXi

Répétez ce processus sur chaque hôte ESXi du domaine de charge de travail.

1. À partir du client vSphere, accédez à l'un des hôtes ESXi de l'inventaire du domaine de charge de travail. Dans l'onglet **configurer**, sélectionnez **adaptateurs VMkernel** et cliquez sur **Ajouter réseau...** pour démarrer.



2. Dans la fenêtre **Select connection type**, choisissez **VMkernel Network adapter** et cliquez sur **Next** pour continuer.



3. Sur la page **Sélectionner le périphérique cible**, choisissez l'un des groupes de ports distribués pour iSCSI créés précédemment.

Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device



Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

| | Name | NSX Port Group ID | Distributed Switch |
|----------------------------------|--|-------------------|-----------------------------------|
| <input type="radio"/> | vcf-wkld-01-iscsi-a | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-iscsi-b | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-02 |
| <input type="radio"/> | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input checked="" type="radio"/> | vcf-wkld-01-nvme-a | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-nvme-b | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |

Manage Columns 7 Items

CANCEL

BACK

NEXT



Packages

4. Sur la page **Port properties**, cliquez sur la case **NVMe over TCP** et cliquez sur **Next** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Port properties ✕

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

| | | |
|--|---|---|
| <input checked="" type="checkbox"/> vMotion | <input type="checkbox"/> vSphere Replication NFC | <input type="checkbox"/> NVMe over RDMA |
| <input type="checkbox"/> Provisioning | <input type="checkbox"/> vSAN | |
| <input type="checkbox"/> Fault Tolerance logging | <input type="checkbox"/> vSAN Witness | |
| <input type="checkbox"/> Management | <input type="checkbox"/> vSphere Backup NFC | |
| <input type="checkbox"/> vSphere Replication | <input checked="" type="checkbox"/> NVMe over TCP | |

5. Sur la page **IPv4 settings**, remplissez **adresse IP**, **masque de sous-réseau** et fournissez une nouvelle adresse IP de passerelle (uniquement si nécessaire). Cliquez sur **Suivant** pour continuer.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings ✕

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically

Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

6. Consultez vos sélections sur la page **prêt à terminer** et cliquez sur **Terminer** pour créer l'adaptateur VMkernel.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

| | |
|------------------------|-----------------------------------|
| Distributed port group | vcf-wkld-01-nvme-a |
| Distributed switch | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |

▼ Port properties

| | |
|-------------------------|--|
| New port group | vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01) |
| MTU | 9000 |
| vMotion | Disabled |
| Provisioning | Disabled |
| Fault Tolerance logging | Disabled |
| Management | Disabled |
| vSphere Replication | Disabled |
| vSphere Replication NFC | Disabled |
| vSAN | Disabled |
| vSAN Witness | Disabled |
| vSphere Backup NFC | Disabled |
| NVMe over TCP | Enabled |
| NVMe over RDMA | Disabled |

▼ IPv4 settings

| | |
|--------------|-------------------------|
| IPv4 address | 172.21.118.191 (static) |
| Subnet mask | 255.255.255.0 |

CANCEL

BACK

FINISH

Packages

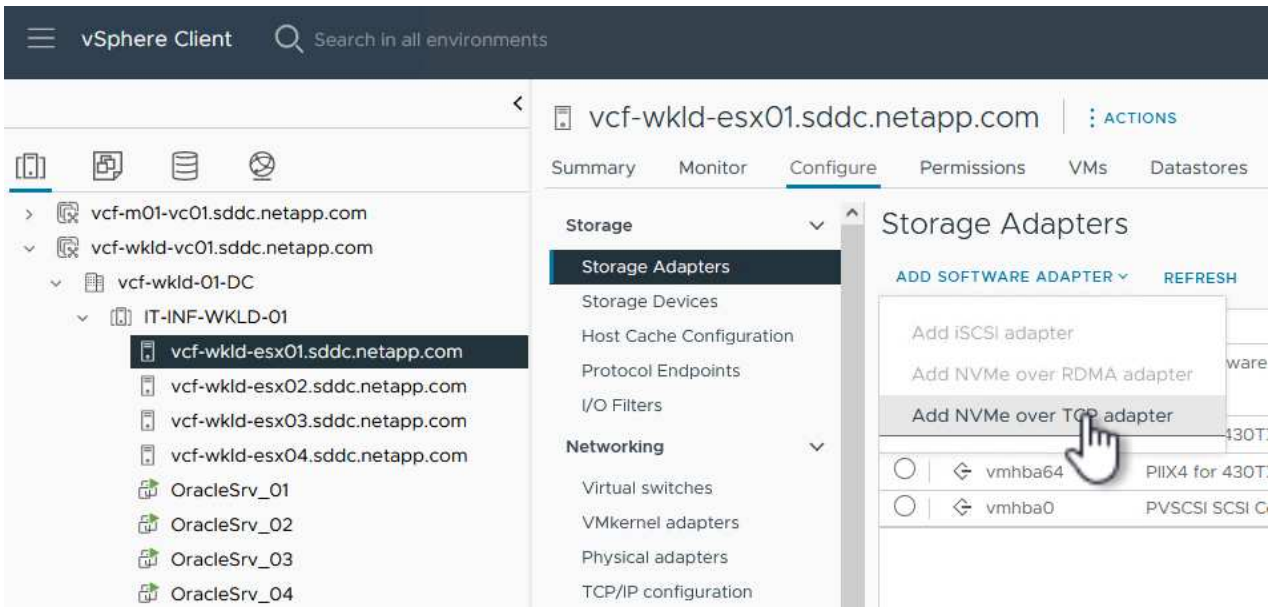
7. Répétez cette procédure pour créer un adaptateur VMkernel pour le second réseau iSCSI.

Ajout de l'adaptateur NVMe over TCP

Chaque hôte ESXi du cluster de domaine de charge de travail doit disposer d'un adaptateur logiciel NVMe over TCP installé pour chaque réseau NVMe/TCP établi dédié au trafic de stockage.

Pour installer les adaptateurs NVMe over TCP et découvrir les contrôleurs NVMe, effectuez les opérations suivantes :

1. Dans le client vSphere, accédez à l'un des hôtes ESXi du cluster du domaine de charge de travail. Dans l'onglet **Configure**, cliquez sur **Storage Adapters** dans le menu, puis, dans le menu déroulant **Add Software adapter**, sélectionnez **Add NVMe over TCP adapter**.



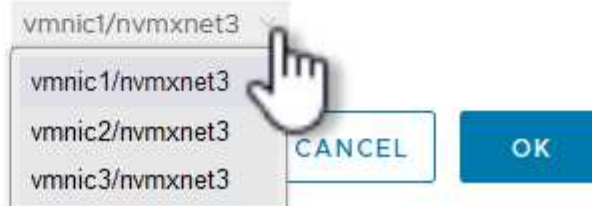
2. Dans la fenêtre **Add Software NVMe over TCP adapter**, accédez au menu déroulant **Physical Network adapter** et sélectionnez l'adaptateur réseau physique approprié sur lequel activer l'adaptateur NVMe.

Add Software NVMe over TCP adapter

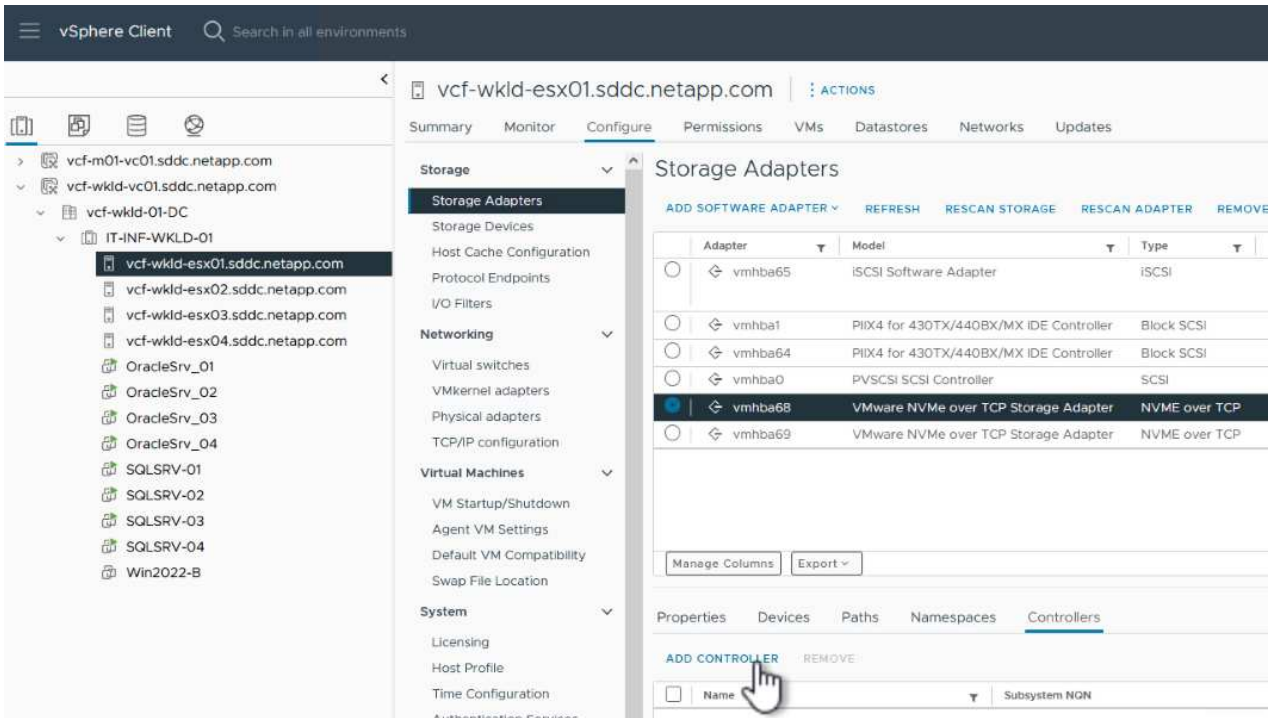
vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter



3. Répétez cette procédure pour le second réseau attribué au trafic NVMe sur TCP, en attribuant l'adaptateur physique approprié.
4. Sélectionnez l'un des adaptateurs NVMe over TCP récemment installés et, dans l'onglet **contrôleurs**, sélectionnez **Ajouter un contrôleur**.



5. Dans la fenêtre **Ajouter contrôleur**, sélectionnez l'onglet **automatiquement** et procédez comme suit.
 - Remplissez les adresses IP de l'une des interfaces logiques du SVM sur le même réseau que l'adaptateur physique affecté à cet adaptateur NVMe over TCP.
 - Cliquez sur le bouton **détecter contrôleurs**.
 - Dans la liste des contrôleurs découverts, cochez la case des deux contrôleurs dont les adresses réseau sont alignées sur cet adaptateur NVMe over TCP.
 - Cliquez sur le bouton **OK** pour ajouter les contrôleurs sélectionnés.

Add controller | vmhba68



Automatically

Manually

Host NQN

nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

COPY

IP

172.21.118.189

Enter IPv4 / IPv6 address

Central discovery controller

Port Number

Range more from 0

Digest parameter

Header digest

Data digest

DISCOVER CONTROLLERS

Select which controller to connect

| <input type="checkbox"/> | Id | Subsystem NQN | Transport Type | IP | Port Number |
|-------------------------------------|-------|--|----------------|----------------|-------------|
| <input checked="" type="checkbox"/> | 65535 | nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe | nvme | 172.21.118.189 | 4420 |
| <input checked="" type="checkbox"/> | 65535 | nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF | nvme | 172.21.118.190 | 4420 |

Manage Columns 4 items

3

4

OK

6. Au bout de quelques secondes, l'espace de nom NVMe s'affiche dans l'onglet Devices.

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

| <input type="radio"/> | Adapter | Model | Type | Status | Identifier | Targets | Devices | Paths |
|----------------------------------|---------|---|---------------|---------|---|---------|---------|-------|
| <input type="radio"/> | vmhba65 | iSCSI Software Adapter | iSCSI | Online | iscsi_vmk(ign.1998-01.com.vmware:vcf-wkld-esx01.sddc.netapp.com:794177624:65) | 4 | 2 | 8 |
| <input type="radio"/> | vmhba1 | PIIX4 for 430TX/440BX/MX IDE Controller | Block SCSI | Unknown | -- | 1 | 1 | 1 |
| <input type="radio"/> | vmhba64 | PIIX4 for 430TX/440BX/MX IDE Controller | Block SCSI | Unknown | -- | 0 | 0 | 0 |
| <input type="radio"/> | vmhba0 | PVSCSI SCSI Controller | SCSI | Unknown | -- | 3 | 3 | 3 |
| <input checked="" type="radio"/> | vmhba68 | VMware NVMe over TCP Storage Adapter | NVME over TCP | Online | -- | 1 | 1 | 1 |
| <input type="radio"/> | vmhba69 | VMware NVMe over TCP Storage Adapter | NVME over TCP | Online | -- | 0 | 0 | 0 |

Manage Columns 6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

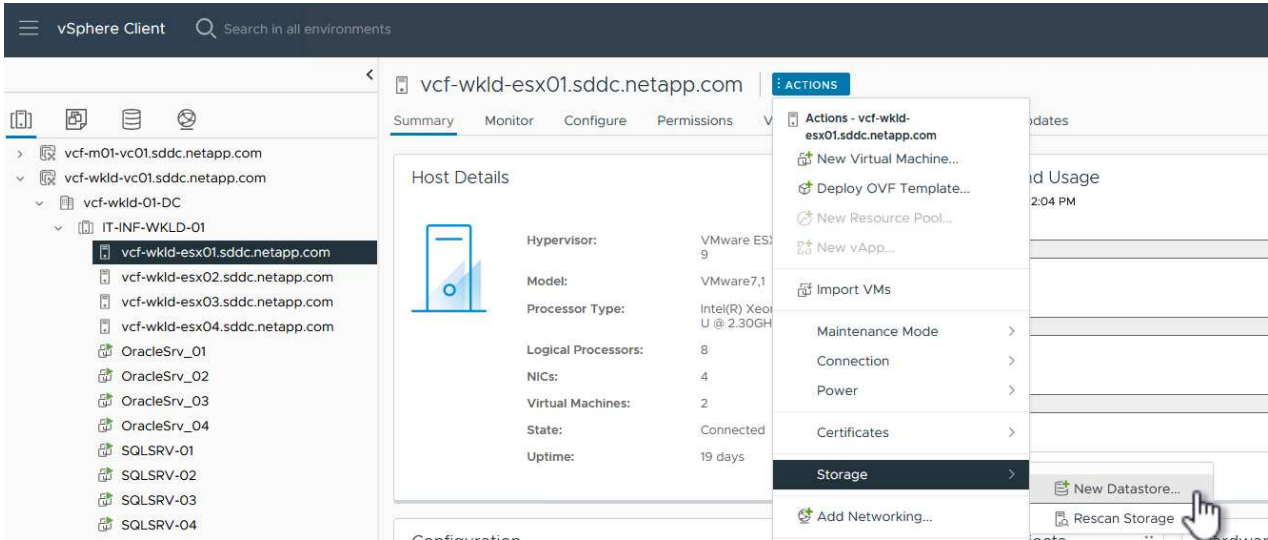
| <input type="checkbox"/> | Name | LUN | Type | Capacity | Datastore | Operational State | Hardware Acceleration | Drive Type | Transport |
|--------------------------|---|-----|------|----------|--------------|-------------------|-----------------------|------------|-----------|
| <input type="checkbox"/> | NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076) | 0 | disk | 3.00 TB | Not Consumed | Attached | Supported | Flash | TCPRTRAN |

7. Répétez cette procédure pour créer un adaptateur NVMe over TCP pour le second réseau établi pour le trafic NVMe/TCP.

Déployez le datastore NVMe over TCP

Pour créer un datastore VMFS sur l'espace de noms NVMe, effectuez les opérations suivantes :

1. Dans le client vSphere, accédez à l'un des hôtes ESXi du cluster du domaine de charge de travail. Dans le menu **actions**, sélectionnez **stockage > Nouveau datastore...**



2. Dans l'assistant **Nouveau datastore**, sélectionnez **VMFS** comme type. Cliquez sur **Suivant** pour continuer.
3. Sur la page **sélection du nom et du périphérique**, indiquez un nom pour le datastore et sélectionnez l'espace de noms NVMe dans la liste des périphériques disponibles.

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name VCF_WKLD_04_NVMe

| | Name | LUN | Capacity | Hardware Acceleration | Drive Type | Sector Format | Cl V S |
|----------------------------------|--|-----|----------|-----------------------|------------|---------------|--------|
| <input checked="" type="radio"/> | NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076) | 0 | 3.00 TB | Supported | Flash | 512e | N |
| <input type="radio"/> | Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036) | 0 | 4.00 GB | Not supported | Flash | 512n | N |
| <input type="radio"/> | Local VMware Disk (naa.6000c291464644a835bc23d384813ac0) | 0 | 75.00 GB | Not supported | Flash | 512n | N |

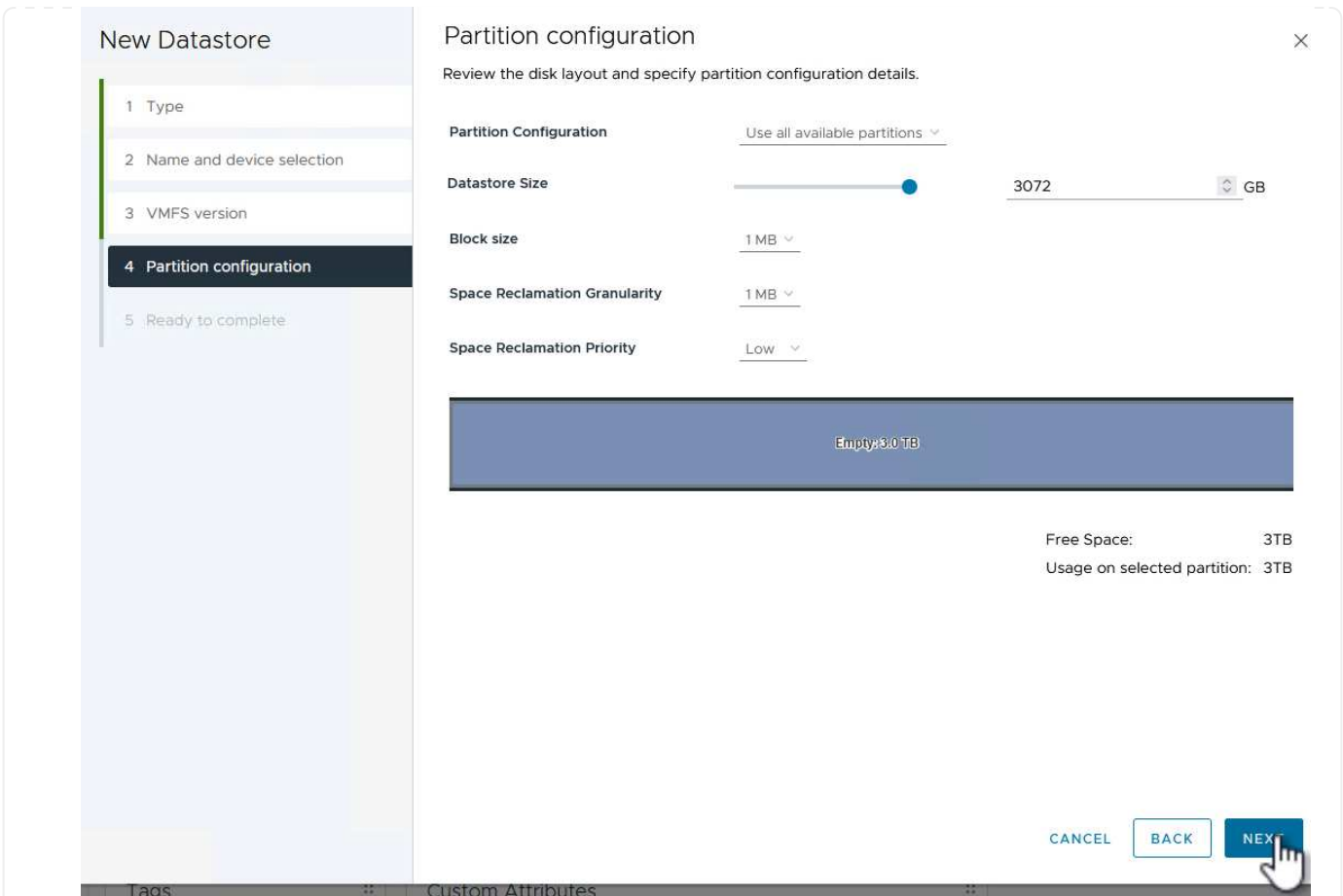
Manage Columns Export 3 items

CANCEL

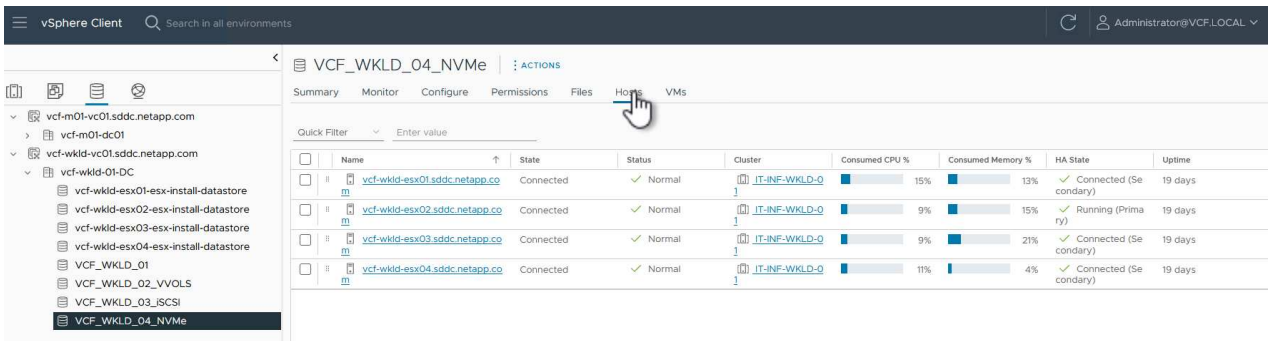
BACK

NEXT

4. Sur la page **VMFS version**, sélectionnez la version de VMFS pour le datastore.
5. Sur la page **partition configuration**, apportez les modifications souhaitées au schéma de partition par défaut. Cliquez sur **Suivant** pour continuer.



6. Sur la page **prêt à terminer**, passez en revue le résumé et cliquez sur **Terminer** pour créer le datastore.
7. Naviguez jusqu'au nouveau datastore de l'inventaire et cliquez sur l'onglet **hosts**. S'il est configuré correctement, tous les hôtes ESXi du cluster doivent être répertoriés et avoir accès au nouveau datastore.



Informations supplémentaires

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au ["Documentation ONTAP 9"](#) centre.

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section "[Documentation de VMware Cloud Foundation](#)".

Utilisez le plug-in SnapCenter pour VMware vSphere pour protéger les machines virtuelles sur les domaines de charge de travail VCF

Dans ce scénario, nous allons montrer comment déployer et utiliser le plug-in SnapCenter pour VMware vSphere (SCV) pour sauvegarder et restaurer des machines virtuelles et des datastores sur un domaine de charge de travail VCF. SCV utilise la technologie snapshot ONTAP pour effectuer des copies de sauvegarde rapides et efficaces des volumes de stockage ONTAP hébergeant des datastores vSphere. Les technologies SnapMirror et SnapVault permettent de créer des sauvegardes secondaires sur un système de stockage séparé avec des règles de conservation qui imitent le volume d'origine ou peuvent être indépendantes du volume d'origine pour une conservation à long terme.

ISCSI est utilisé comme protocole de stockage pour le datastore VMFS dans cette solution.

Auteur: Josh Powell

Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

- Déployer le plug-in SnapCenter pour VMware vSphere (SCV) sur le domaine des charges de travail VI.
- Ajouter des systèmes de stockage au distributeur sélectif.
- Créer des politiques de sauvegarde dans SCV.
- Créer des groupes de ressources dans SCV.
- Utilisez SCV pour sauvegarder des datastores ou des machines virtuelles spécifiques.
- Utiliser SCV pour restaurer les machines virtuelles à un autre emplacement dans le cluster.
- Utilisez SCV pour restaurer les fichiers dans un système de fichiers Windows.

Prérequis

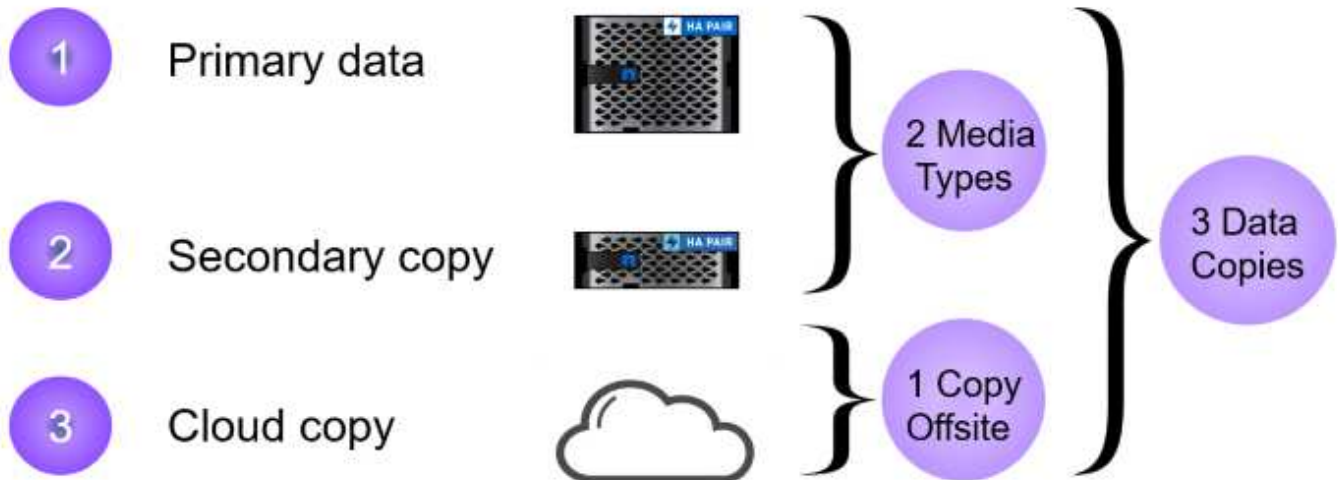
Ce scénario nécessite les composants et configurations suivants :

- Un système de stockage ONTAP ASA avec datastores VMFS iSCSI alloués au cluster de domaine de charge de travail.
- Un système de stockage ONTAP secondaire configuré pour recevoir des sauvegardes secondaires à l'aide de SnapMirror.
- Le déploiement du domaine de gestion VCF est terminé et le client vSphere est accessible.
- Un domaine de charge de travail VI a déjà été déployé.
- Les machines virtuelles sont présentes sur le bloc de distributeurs sélectifs est désigné pour protéger.

Pour plus d'informations sur la configuration des datastores VMFS iSCSI en tant que stockage supplémentaire, reportez-vous à la section "[ISCSI comme stockage supplémentaire pour les domaines de gestion](#)" dans cette documentation. Le processus d'utilisation d'OTV pour déployer les datastores est identique pour les domaines de gestion et de charge de travail.



En plus de la réplication des sauvegardes effectuées avec SCV sur le stockage secondaire, des copies hors site des données peuvent être effectuées sur le stockage objet sur l'un des trois (3) principaux fournisseurs cloud à l'aide de la sauvegarde et de la restauration NetApp BlueXP pour les machines virtuelles. Pour plus d'informations, reportez-vous à la solution "[3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration BlueXP pour les VM](#)".



Étapes de déploiement

Pour déployer le plug-in SnapCenter et l'utiliser pour créer des sauvegardes et restaurer des machines virtuelles et des datastores, procédez comme suit :

Déployer et utiliser SCV pour protéger les données dans un domaine de charge de travail VI

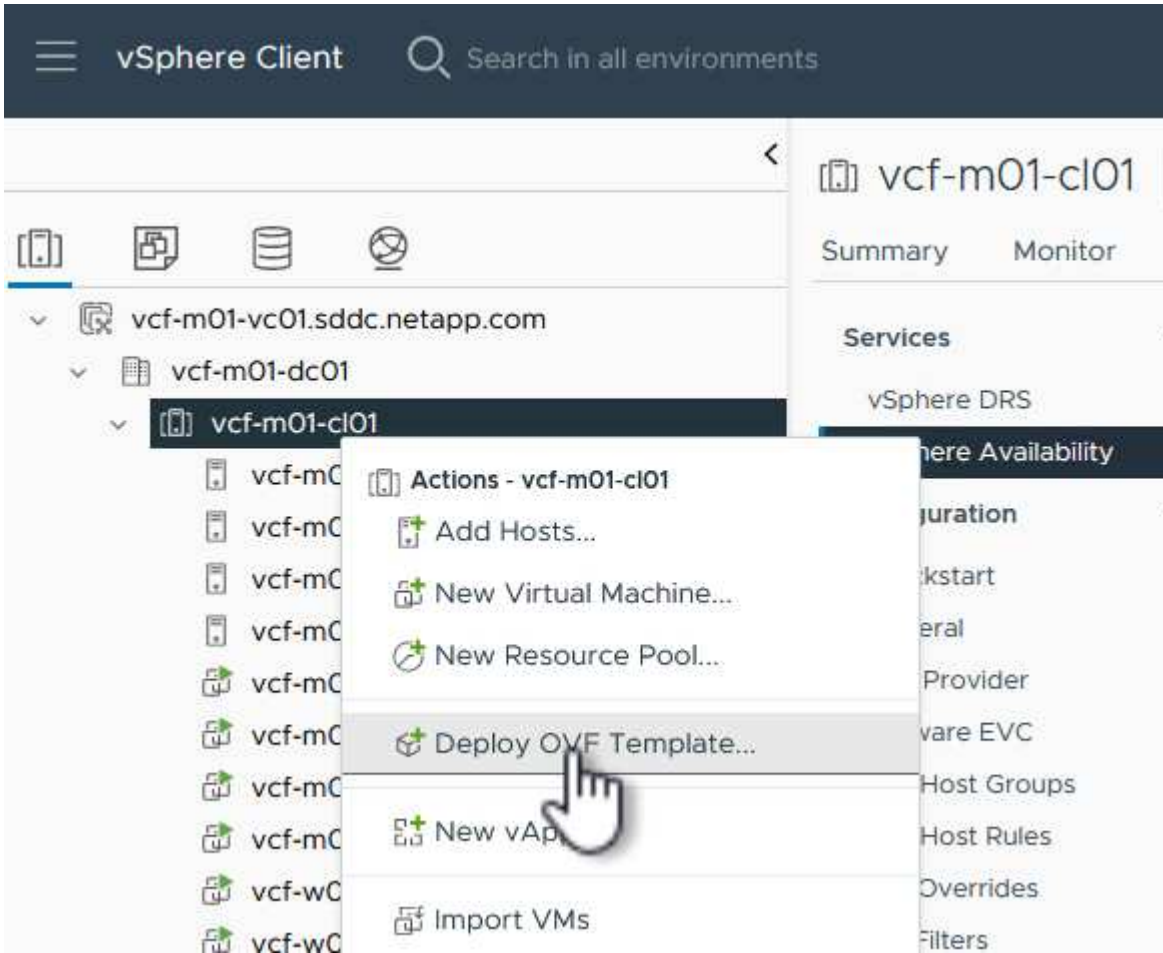
Procédez comme suit pour déployer, configurer et utiliser SCV pour protéger les données dans un domaine de charge de travail VI :

Déployez le plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter est hébergé sur le domaine de gestion VCF, mais enregistré dans vCenter pour le domaine de charge de travail VI. Une instance SCV est requise pour chaque instance vCenter. Notez qu'un domaine de charge de travail peut inclure plusieurs clusters gérés par une seule instance vCenter.

Effectuez les étapes suivantes à partir du client vCenter pour déployer SCV dans le domaine de la charge de travail VI :

1. Télécharger le fichier OVA pour le déploiement des distributeurs sélectifs à partir de la zone de téléchargement du site d'assistance NetApp "ICI".
2. Dans le domaine de gestion vCenter client, sélectionnez **déployer le modèle OVF...**



3. Dans l'assistant **Deploy OVF Template**, cliquez sur le bouton radio **local file**, puis sélectionnez pour télécharger le modèle OVF précédemment téléchargé. Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

UPLOAD FILES

scv-5.OP2-240310_1514.ova

4. Sur la page **Sélectionner le nom et le dossier**, indiquez un nom pour le serveur virtuel du courtier de données SCV et un dossier sur le domaine de gestion. Cliquez sur **Suivant** pour continuer.
5. Sur la page **Sélectionner une ressource de calcul**, sélectionnez le cluster de domaine de gestion ou un hôte ESXi spécifique au sein du cluster sur lequel installer la machine virtuelle.
6. Passez en revue l'information relative au modèle OVF sur la page **consulter les détails** et acceptez les conditions de licence sur la page **accords de licence**.
7. Sur la page **Select Storage**, choisissez le datastore sur lequel la machine virtuelle sera installée et sélectionnez **Virtual disk format** et **VM Storage Policy**. Dans cette solution, la machine virtuelle sera installée sur un datastore VMFS iSCSI situé sur un système de stockage ONTAP, comme précédemment déployé dans une section distincte de cette documentation. Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format

VM Storage Policy

Disable Storage DRS for this virtual machine

| Name | Storage Compatibility | Capacity | Provisioned | Free | |
|---|-----------------------|-----------|-------------|-----------|--|
| <input checked="" type="radio"/> mgmt_01_iscsi | -- | 3 TB | 3.71 TB | 2.5 TB | |
| <input type="radio"/> vcf-m01-cl01-ds-vsan01 | -- | 999.97 GB | 49.16 GB | 957.54 GB | |
| <input type="radio"/> vcf-m01-esx01-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | |
| <input type="radio"/> vcf-m01-esx02-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | |
| <input type="radio"/> vcf-m01-esx03-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | |
| <input type="radio"/> vcf-m01-esx04-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | |

Manage Columns Items per page: 10 6 items

Compatibility

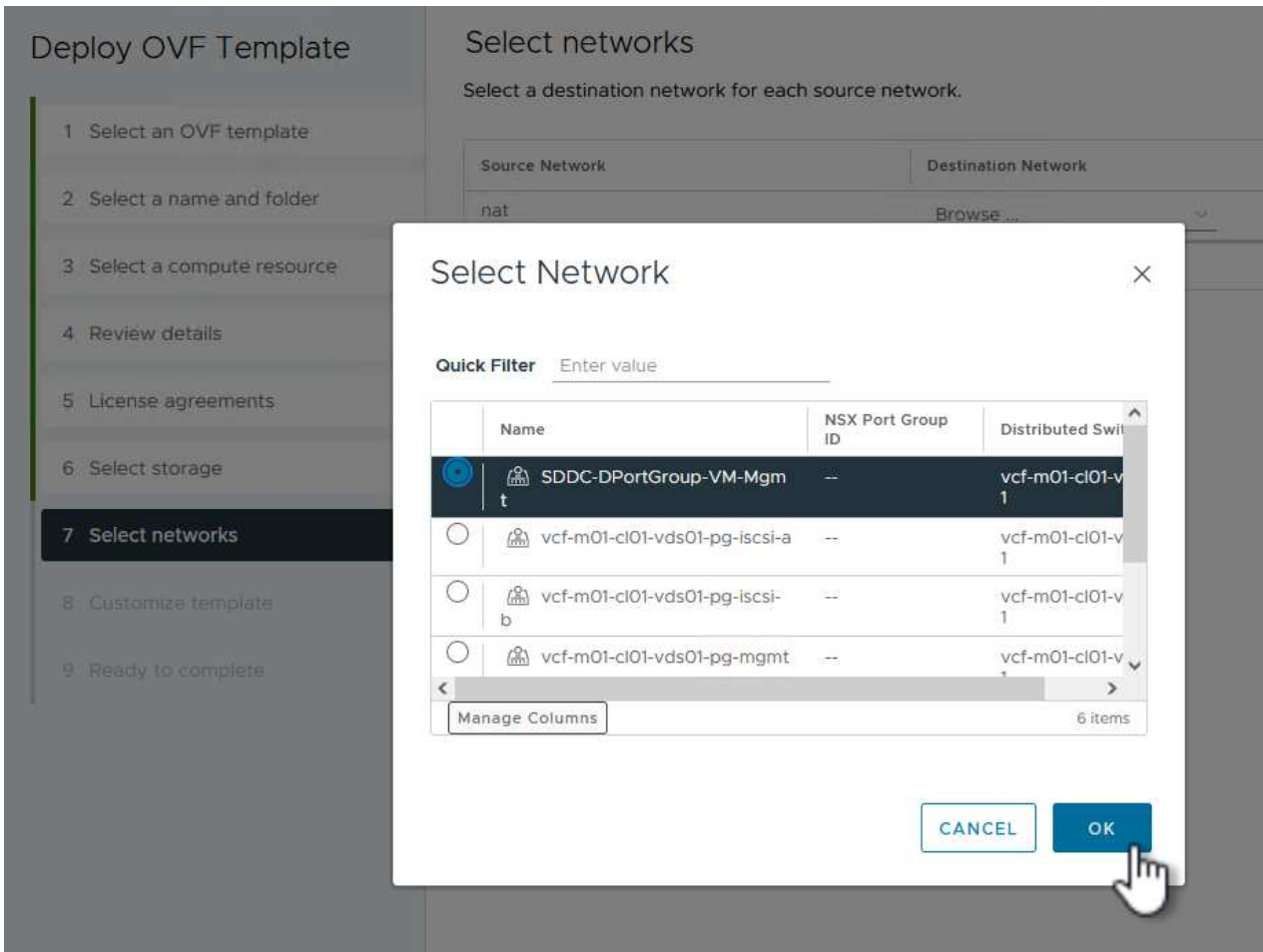
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Sur la page **Sélectionner réseau**, sélectionnez le réseau de gestion capable de communiquer avec l'apppliance vCenter du domaine de charge de travail et les systèmes de stockage ONTAP principal et secondaire.



9. Sur la page **Personnaliser le modèle**, remplissez toutes les informations requises pour le déploiement :

- FQDN ou IP, et informations d'identification pour l'apppliance vCenter du domaine de charge de travail.
- Informations d'identification pour le compte d'administration SCV.
- Informations d'identification pour le compte d'entretien du distributeur auxiliaire.
- Détails des propriétés réseau IPv4 (IPv6 peut également être utilisé).
- Paramètres de date et d'heure.

Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

| | | |
|--|---|--|
| 1. Register to existing vCenter | | 4 settings |
| 1.1 vCenter Name(FQDN) or IP Address | <input type="text" value="cf-wkld-vc01.sddc.netapp.com"/> | |
| 1.2 vCenter username | <input type="text" value="administrator@vcf.local"/> | |
| 1.3 vCenter password | Password | <input type="password" value="....."/> |
| | Confirm Password | <input type="password" value="....."/> |
| 1.4 vCenter port | <input type="text" value="443"/> | |
| 2. Create SCV Credentials | | 2 settings |
| 2.1 Username | <input type="text" value="admin"/> | |
| 2.2 Password | Password | <input type="password" value="....."/> |
| | Confirm Password | <input type="password" value="....."/> |
| 3. System Configuration | | 1 settings |

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

| | | |
|--|---|------------|
| 4.2 Setup IPv4 Network Properties | | 6 settings |
| 4.2.1 IPv4 Address | IP address for the appliance. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.148"/> | |
| 4.2.2 IPv4 Netmask | Subnet to use on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="255.255.255.0"/> | |
| 4.2.3 IPv4 Gateway | Gateway on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.1"/> | |
| 4.2.4 IPv4 Primary DNS | Primary DNS server's IP address. (Leave blank if DHCP is desired) <input type="text" value="10.61.185.231"/> | |
| 4.2.5 IPv4 Secondary DNS | Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) <input type="text" value="10.61.186.231"/> | |
| 4.2.6 IPv4 Search Domains (optional) | Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) <input type="text" value="netapp.com,sddc.netapp.com"/> | |
| 3.3 Setup IPv6 Network Properties | | 6 settings |
| 4.3.1 IPv6 Address | IP address for the appliance. (Leave blank if DHCP is desired) <input type="text"/> | |
| 4.3.2 IPv6 PrefixLen | Prefix length to use on the deployed network. (Leave blank if DHCP is desired) <input type="text"/> | |

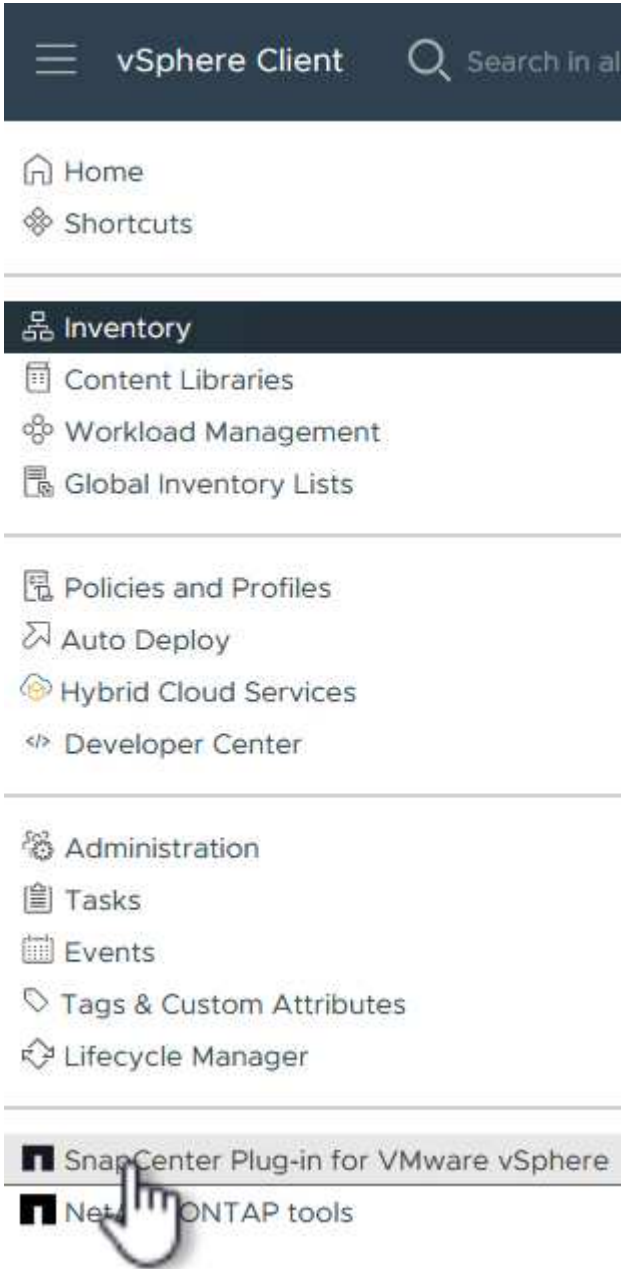


10. Enfin, sur la page **prêt à terminer**, passez en revue tous les paramètres et cliquez sur Terminer pour démarrer le déploiement.

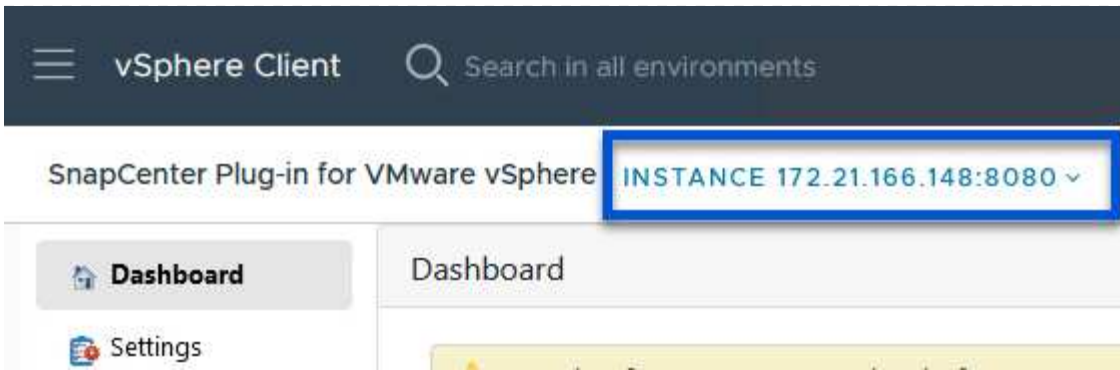
Ajouter des systèmes de stockage au distributeur sélectif

Une fois le plug-in SnapCenter installé, procédez comme suit pour ajouter des systèmes de stockage au distributeur sélectif :

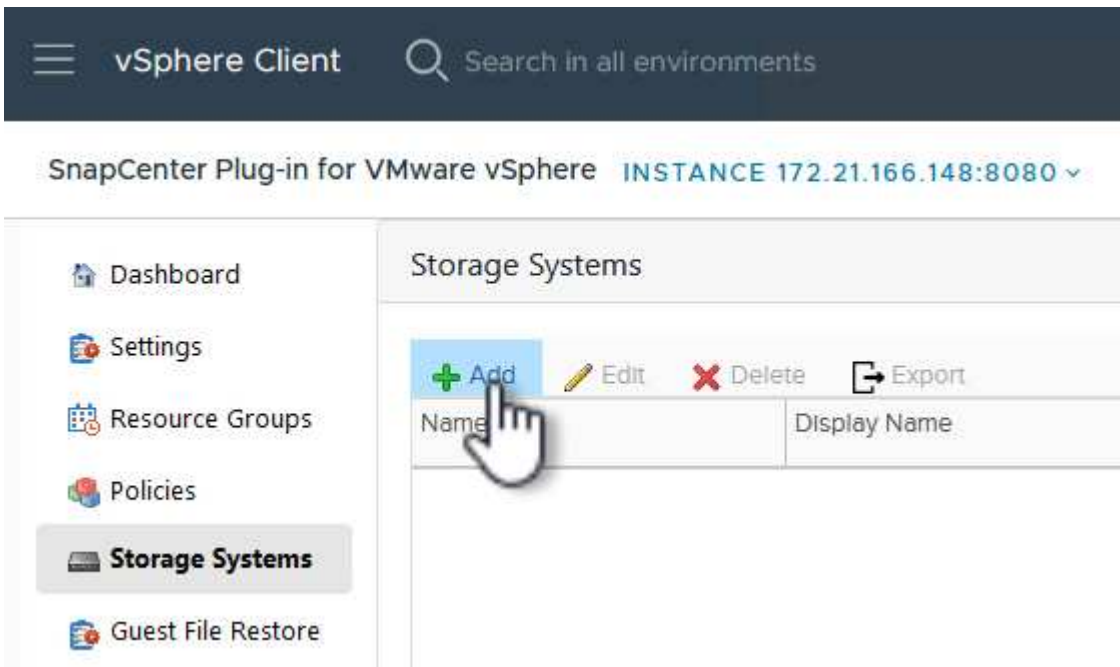
1. Vous pouvez accéder à SCV à partir du menu principal du client vSphere.



2. En haut de l'interface utilisateur SCV, sélectionnez l'instance SCV qui correspond au cluster vSphere à protéger.



3. Accédez à **Storage Systems** dans le menu de gauche et cliquez sur **Add** pour commencer.



4. Dans le formulaire **Ajouter un système de stockage**, entrez l'adresse IP et les informations d'identification du système de stockage ONTAP à ajouter, puis cliquez sur **Ajouter** pour terminer l'action.

Add Storage System



| | |
|---------------------------------------|--|
| Storage System | <input type="text" value="172.16.9.25"/> |
| Authentication Method | <input checked="" type="radio"/> Credentials <input type="radio"/> Certificate |
| Username | <input type="text" value="admin"/> |
| Password | <input type="password" value="••••••••"/> |
| Protocol | <input type="text" value="HTTPS"/> |
| Port | <input type="text" value="443"/> |
| Timeout | <input type="text" value="60"/> Seconds |
| <input type="checkbox"/> Preferred IP | <input type="text" value="Preferred IP"/> |

Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



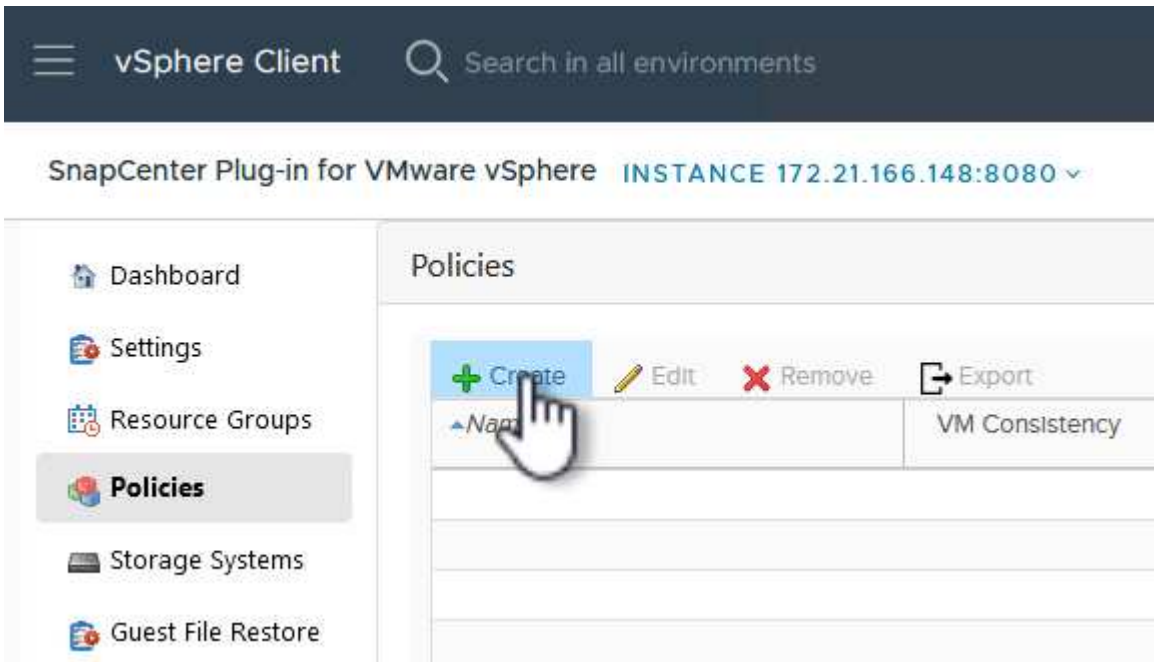
5. Répétez cette procédure pour tous les systèmes de stockage supplémentaires à gérer, y compris tous les systèmes à utiliser comme cibles de sauvegarde secondaires.

Configurer les politiques de sauvegarde dans SCV

Pour plus d'informations sur la création de politiques de sauvegarde SCV, voir "[Créez des règles de sauvegarde pour les VM et les datastores](#)".

Pour créer une nouvelle règle de sauvegarde, procédez comme suit :

1. Dans le menu de gauche, sélectionnez **politiques** et cliquez sur **Créer** pour commencer.



2. Sur le formulaire **Nouvelle stratégie de sauvegarde**, indiquez un **Nom** et une **Description** pour la stratégie, la **fréquence** à laquelle les sauvegardes auront lieu et la période **rétenion** qui spécifie la durée de conservation de la sauvegarde.

Période de verrouillage permet à la fonction ONTAP SnapLock de créer des instantanés inviolables et de configurer la période de verrouillage.

Pour **réplication** sélectionnez cette option pour mettre à jour les relations SnapMirror ou SnapVault sous-jacentes du volume de stockage ONTAP.



SnapMirror et la réplication SnapVault sont similaires dans la mesure où ils utilisent la technologie ONTAP SnapMirror pour répliquer de manière asynchrone des volumes de stockage vers un système secondaire afin d'améliorer la protection et la sécurité. Pour les relations SnapMirror, le planning de conservation spécifié dans la règle de sauvegarde SCV régit la conservation des volumes principal et secondaire. Avec les relations SnapVault, il est possible d'établir un calendrier de conservation distinct sur le système de stockage secondaire pour les plannings de conservation à plus long terme ou différents. Dans ce cas, l'étiquette d'instantané est spécifiée dans la stratégie de sauvegarde SCV et dans la stratégie associée au volume secondaire, pour identifier les volumes auxquels appliquer le programme de rétention indépendant.

Choisissez des options avancées supplémentaires et cliquez sur **Ajouter** pour créer la stratégie.

New Backup Policy



Name

Description

Frequency

Locking Period Enable Snapshot Locking ⓘ

Retention ⓘ

Replication Update SnapMirror after backup ⓘ
 Update SnapVault after backup ⓘ

Snapshot label

Advanced ▾ VM consistency ⓘ
 Include datastores with independent disks

Scripts ⓘ

CANCEL

ADD

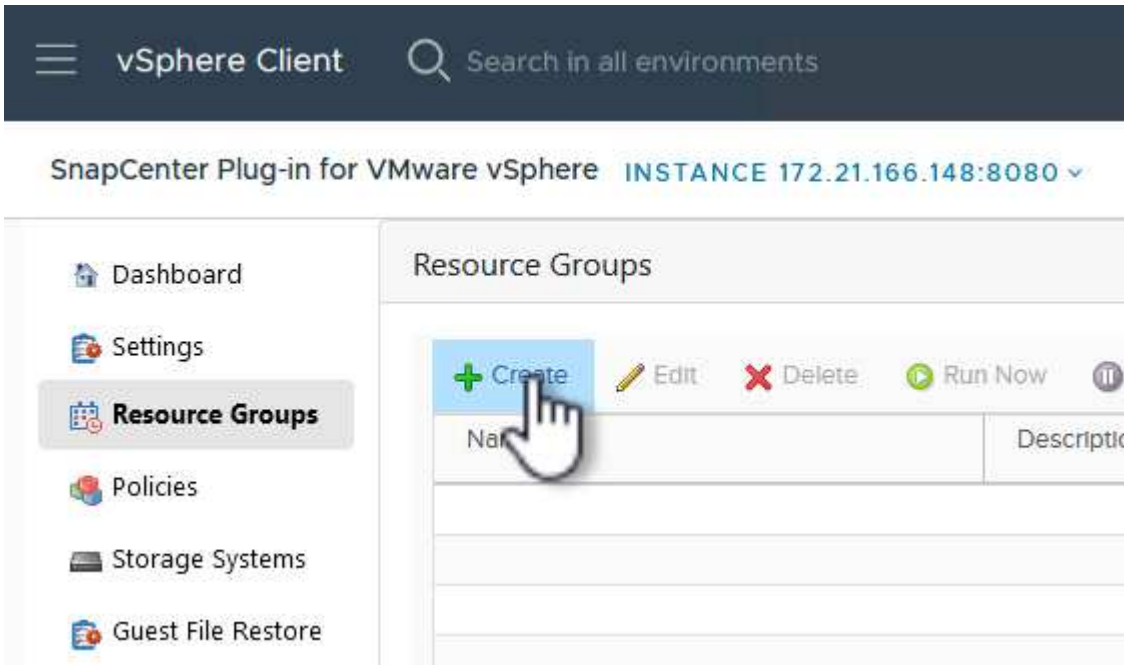


Créer des groupes de ressources dans SCV

Pour plus d'informations sur la création de groupes de ressources SCV, voir "[Créer des groupes de ressources](#)".

Pour créer un nouveau groupe de ressources, procédez comme suit :

1. Dans le menu de gauche, sélectionnez **groupes de ressources** et cliquez sur **Créer** pour commencer.



2. Sur la page **informations générales et notification**, indiquez un nom pour le groupe de ressources, les paramètres de notification et les options supplémentaires pour le nom des snapshots.
3. Sur la page **Resource**, sélectionnez les datastores et les machines virtuelles à protéger dans le groupe de ressources. Cliquez sur **Suivant** pour continuer.



Même si seules des machines virtuelles spécifiques sont sélectionnées, le datastore entier est toujours sauvegardé. En effet, ONTAP effectue des snapshots du volume hébergeant le datastore. Notez toutefois que la sélection de machines virtuelles spécifiques uniquement pour la sauvegarde limite la capacité de restauration de ces machines virtuelles uniquement.

Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities

OracleSrv_01
OracleSrv_02
OracleSrv_03
OracleSrv_04

Selected entities

SQLSRV-01
SQLSRV-02
SQLSRV-03
SQLSRV-04

BACK

NEXT

FINISH

CANCEL

4. Sur la page **Spanning Disks**, sélectionnez l'option permettant de gérer les machines virtuelles avec des VMDK qui couvrent plusieurs datastores. Cliquez sur **Suivant** pour continuer.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included ⓘ

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BACK

NEXT

FINISH

CANCEL

5. Sur la page **Policies**, sélectionnez une ou plusieurs stratégies créées précédemment qui seront utilisées avec ce groupe de ressources. Cliquez sur **Suivant** pour continuer.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

4. Policies

5. Schedules

6. Summary

+ Create

| <input type="checkbox"/> | Name | VM Consistent | Include independent di... | Schedule |
|-------------------------------------|------------------|---------------|---------------------------|----------|
| <input checked="" type="checkbox"/> | Daily_Snapmirror | No | No | Daily |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |
| <input type="checkbox"/> | | | | |

BACK NEXT FINISH CANCEL

6. Sur la page **Schedules**, définissez la date d'exécution de la sauvegarde en configurant la récurrence et l'heure de la journée. Cliquez sur **Suivant** pour continuer.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily_Snapmi... ▼

Type Daily

Every 1 Day(s)

Starting 04/04/2024

At 04 45 PM

BACK

NEXT

FINISH

CANCEL

7. Enfin, passez en revue le **Résumé** et cliquez sur **Terminer** pour créer le groupe de ressources.

Create Resource Group

- 1. General info & notification
- 2. Resource
- 3. Spanning disks
- 4. Policies
- 5. Schedules
- 6. Summary**

| Name | SQL_Servers | | | | | | |
|------------------------|---|-------------------------|-----------|-------------------------|------------------|-------|---|
| Description | | | | | | | |
| Send email | Never | | | | | | |
| Latest Snapshot name | None ⓘ | | | | | | |
| Custom snapshot format | None ⓘ | | | | | | |
| Entities | SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04 | | | | | | |
| Spanning | False | | | | | | |
| Policies | <table><thead><tr><th>Name</th><th>Frequency</th><th>Snapshot Locking Period</th></tr></thead><tbody><tr><td>Daily_Snapmir...</td><td>Daily</td><td>-</td></tr></tbody></table> | Name | Frequency | Snapshot Locking Period | Daily_Snapmir... | Daily | - |
| Name | Frequency | Snapshot Locking Period | | | | | |
| Daily_Snapmir... | Daily | - | | | | | |

BACK

NEXT

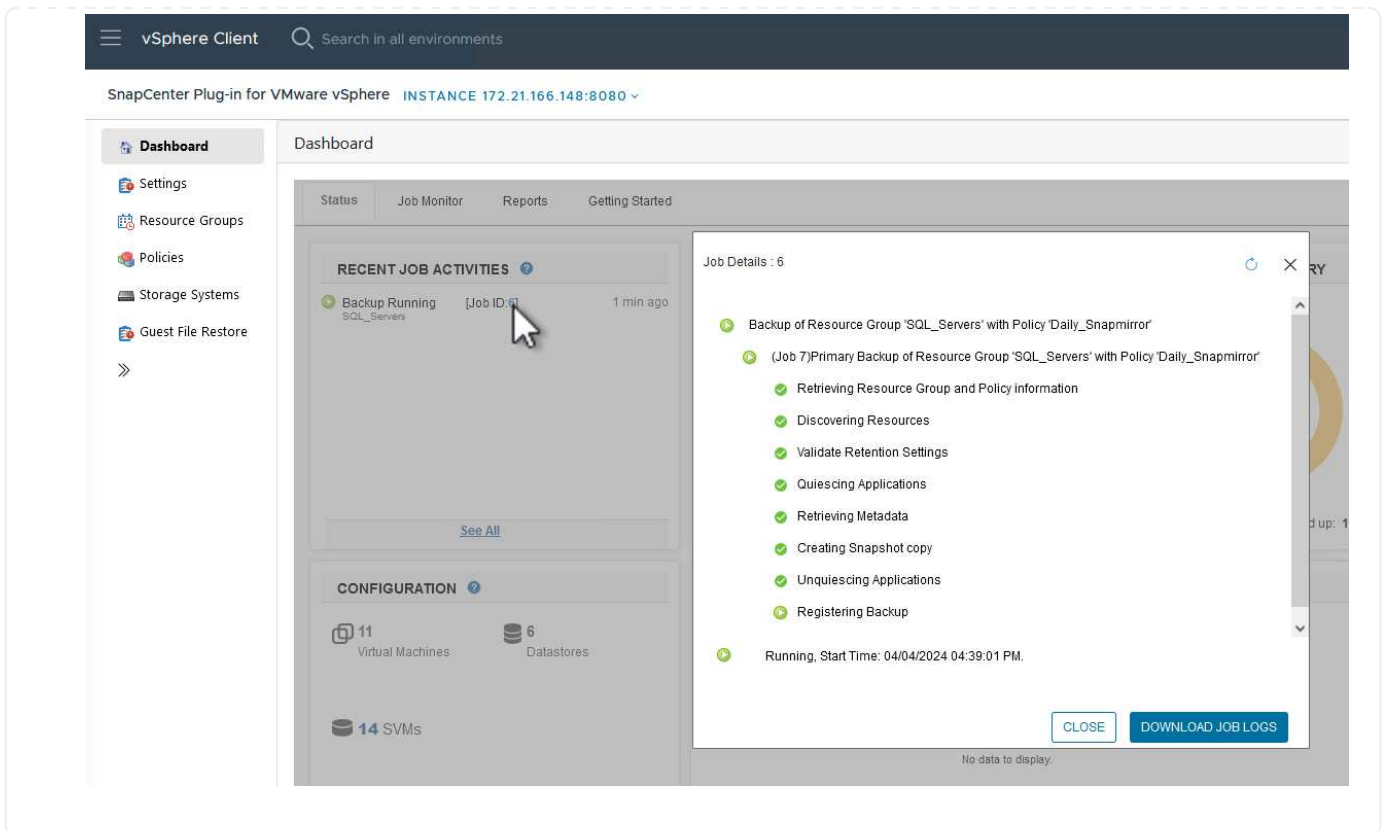
FINISH

CANCEL

8. Une fois le groupe de ressources créé, cliquez sur le bouton **Exécuter maintenant** pour exécuter la première sauvegarde.

The screenshot shows the vSphere Client interface. At the top, there is a search bar and the text 'vSphere Client'. Below that, it says 'SnapCenter Plug-in for VMware vSphere' and 'INSTANCE 172.21.166.148:8080'. On the left, there is a navigation menu with 'Resource Groups' selected. The main area shows a table of 'Resource Groups' with columns for Name, Description, and Policy. The 'SQL_Servers' group is highlighted. Above the table, there are action buttons: Create, Edit, Delete, Run Now (highlighted with a hand cursor), Suspend, Resume, and Export.

9. Accédez au **Tableau de bord** et, sous **activités récentes**, cliquez sur le numéro en regard de **ID travail** pour ouvrir le moniteur de travaux et afficher la progression du travail en cours.



Utilisez SCV pour restaurer des machines virtuelles, des VMDK et des fichiers

Le plug-in SnapCenter permet de restaurer des machines virtuelles, des VMDK, des fichiers et des dossiers à partir de sauvegardes primaires ou secondaires.

Les machines virtuelles peuvent être restaurées sur l'hôte d'origine ou sur un autre hôte du même serveur vCenter, ou sur un autre hôte ESXi géré par le même vCenter ou tout autre vCenter en mode lié.

Les VM vVol peuvent être restaurées sur l'hôte d'origine.

Dans les machines virtuelles classiques, les VMDK peuvent être restaurés sur le datastore d'origine ou sur un autre datastore.

Les VMDK des VM vVol peuvent être restaurés dans le datastore d'origine.

Les fichiers et dossiers individuels d'une session de restauration de fichiers invité peuvent être restaurés, ce qui joint une copie de sauvegarde d'un disque virtuel, puis restaure les fichiers ou dossiers sélectionnés.

Procédez comme suit pour restaurer des machines virtuelles, des VMDK ou des dossiers individuels.

Restaurer des machines virtuelles à l'aide du plug-in SnapCenter

Effectuer les étapes suivantes pour restaurer une machine virtuelle avec distributeur auxiliaire:

1. Accédez à la machine virtuelle à restaurer dans le client vSphere, cliquez avec le bouton droit de la souris et naviguez jusqu'à **SnapCenter Plug-in pour VMware vSphere**. Sélectionnez **Restaurer** dans le sous-menu.

OracleSrv_04 | Summary Monitor Configure Permissions

Guest OS Virtual Mac

Actions - OracleSrv_04

- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings...
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Remove from Inventory
- Delete from Disk
- vSAN
- NetApp ONTAP tools
- SnapCenter Plug-in for VMware vSphere
 - Create Resource Group
 - Add to Resource Group
 - Attach Virtual Disk(s)
 - Detach Virtual Disk(s)
 - Restore
 - File Restore

4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_ISCSI
(of 2) vcf-wkld-01-IT-INF-WKLD-01-vc (connected) | 00:50:56:83:02:f
Disconnected
ESXI 7.0 U2 and later (VM vers

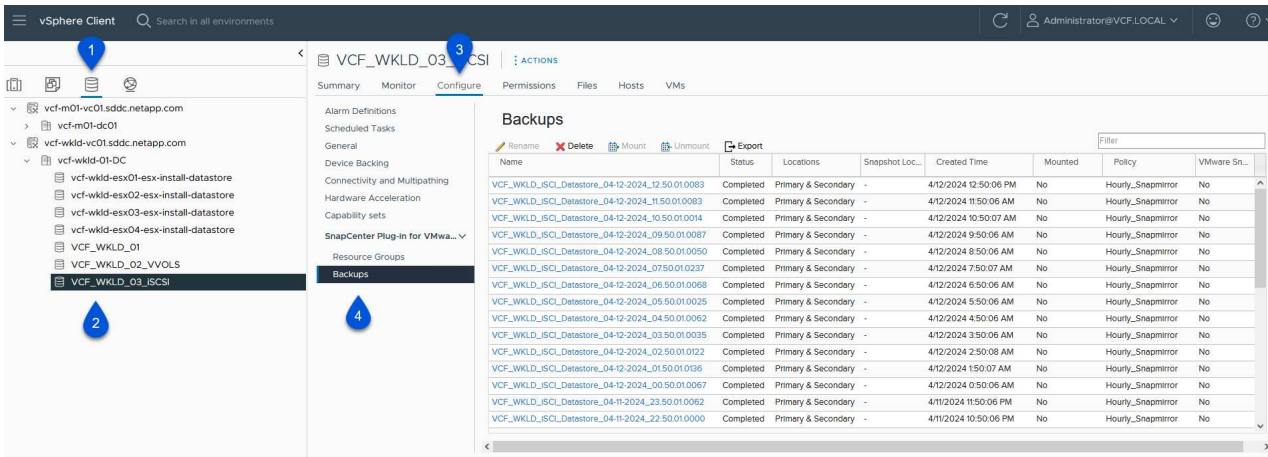
Recent Tasks

| Task Name |
|-----------|
|-----------|

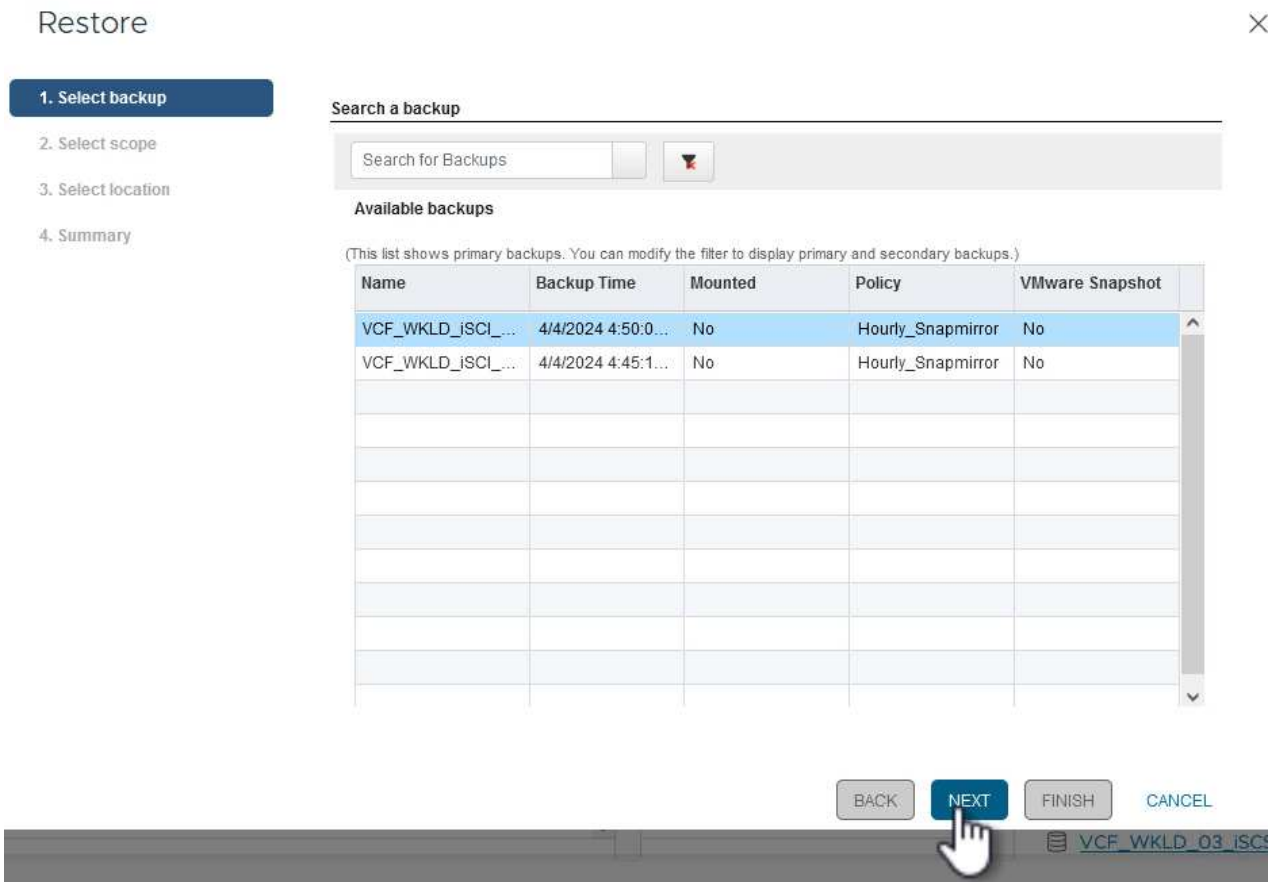
Manage Columns Run



Vous pouvez également naviguer jusqu'au datastore en inventaire, puis, sous l'onglet **configurer**, accédez à **Plug-in SnapCenter pour VMware vSphere > sauvegardes**. Dans la sauvegarde choisie, sélectionnez les machines virtuelles à restaurer.



2. Dans l'assistant **Restore**, sélectionnez la sauvegarde à utiliser. Cliquez sur **Suivant** pour continuer.



3. Sur la page **Select Scope**, remplissez tous les champs obligatoires :

- **Restore Scope** - sélectionnez cette option pour restaurer la machine virtuelle entière.
- **Redémarrer VM** - Choisissez de démarrer la VM après la restauration.
- **Restaurer l'emplacement** - Choisissez de restaurer l'emplacement original ou un autre emplacement. Lorsque vous choisissez un autre emplacement, sélectionnez les options de chacun des champs :
 - **Serveur vCenter de destination** - vCenter local ou autre vCenter en mode lié
 - **Hôte ESXi de destination**
 - **Réseau**
 - **Nom de la VM après la restauration**
 - **Sélectionnez datastore:**

Restore ×

1. Select backup
 2. Select scope
 3. Select location
 4. Summary

Restore scope: Entire virtual machine

Restart VM:

Restore Location:

- Original Location
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)
- Alternate Location
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server: 172.21.166.143

Destination ESXi host: vcf-wkld-esx04.sddc.netapp.com

Network: vcf-wkld-01-HT-INF-WKLD-01-vds-01-pg-

VM name after restore: OracleSrv_04_restored

Select Datastore: VCF_WKLD_03_iSCSI

VCF_WKLD_03_iSCSI

Cliquez sur **Suivant** pour continuer.

4. Sur la page **Sélectionner un emplacement**, choisissez de restaurer la machine virtuelle à partir du système de stockage ONTAP principal ou secondaire. Cliquez sur **Suivant** pour continuer.

Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location**
- 4. Summary

| Destination datastore | Locations |
|-----------------------|--|
| VCF_WKLD_03_iSCSI | (Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI |
| | (Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI |
| | (Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest |
| | < > |

5. Enfin, passez en revue le **Résumé** et cliquez sur **Terminer** pour lancer le travail de restauration.

Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary**

| | |
|---|---|
| Virtual machine to be restored | OracleSrv_04 |
| Backup name | VCF_WKLD_iSCSI_Datastore_04-04-2024_16.50.00.0940 |
| Restart virtual machine | No |
| Restore Location | Alternate Location |
| Destination vCenter Server | 172.21.166.143 |
| ESXi host to be used to mount the backup | vcf-wkld-esx04.sddc.netapp.com |
| VM Network | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt |
| Destination datastore | VCF_WKLD_03_iSCSI |
| VM name after restore | OracleSrv_04_restored |



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

FINISH

CANCEL

6. La progression de la tâche de restauration peut être surveillée à partir du volet **tâches récentes** du client vSphere et du moniteur de tâches de SCV.

- Dashboard
- Settings
- Resource Groups
- Policies
- Storage Systems
- Guest File Restore
- >>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago
VCF_WKLD_ISCI_Datastore_04-04-2024...
- Backup Successful [Job ID:15] 8 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:12] 13 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:9] 13 min ago
SQL_Servers
- Backup Successful [Job ID:6] 19 min ago
SQL_Servers

[See All](#)

CONFIGURATION

11 Virtual Machines 6 Datastores

14 SVMs

2 Resource Groups 2 Backup Policies

Job Details : 18

- Restoring backup with name: VCF_WKLD_ISCI_Datastore_04-04-2024_16:50:00.0940
- Preparing for Restore: Retrieving Backup metadata from Repository.
- Pre Restore
- Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

CLOSE DOWNLOAD JOB LOGS

No data to display.

Recent Tasks Alarms

| Task Name | Target | Status | Details | Initiator | Queued For | Start Time |
|------------------------|--|--------|---|-------------------------|------------|-------------------------|
| NetApp Mount Datastore | vcf-wkld-esx04.sdd c.netapp.com | 35% | Mount operation completed successfully. | VCF.LOCAL\Administrator | 6 ms | 04/04/2024, 4:58:27 P M |
| NetApp Restore | vcf-wkld-esx04.sdd c.netapp.com | 2% | Restore operation started. | VCF.LOCAL\Administrator | 10 ms | 04/04/2024, 4:58:27 P M |

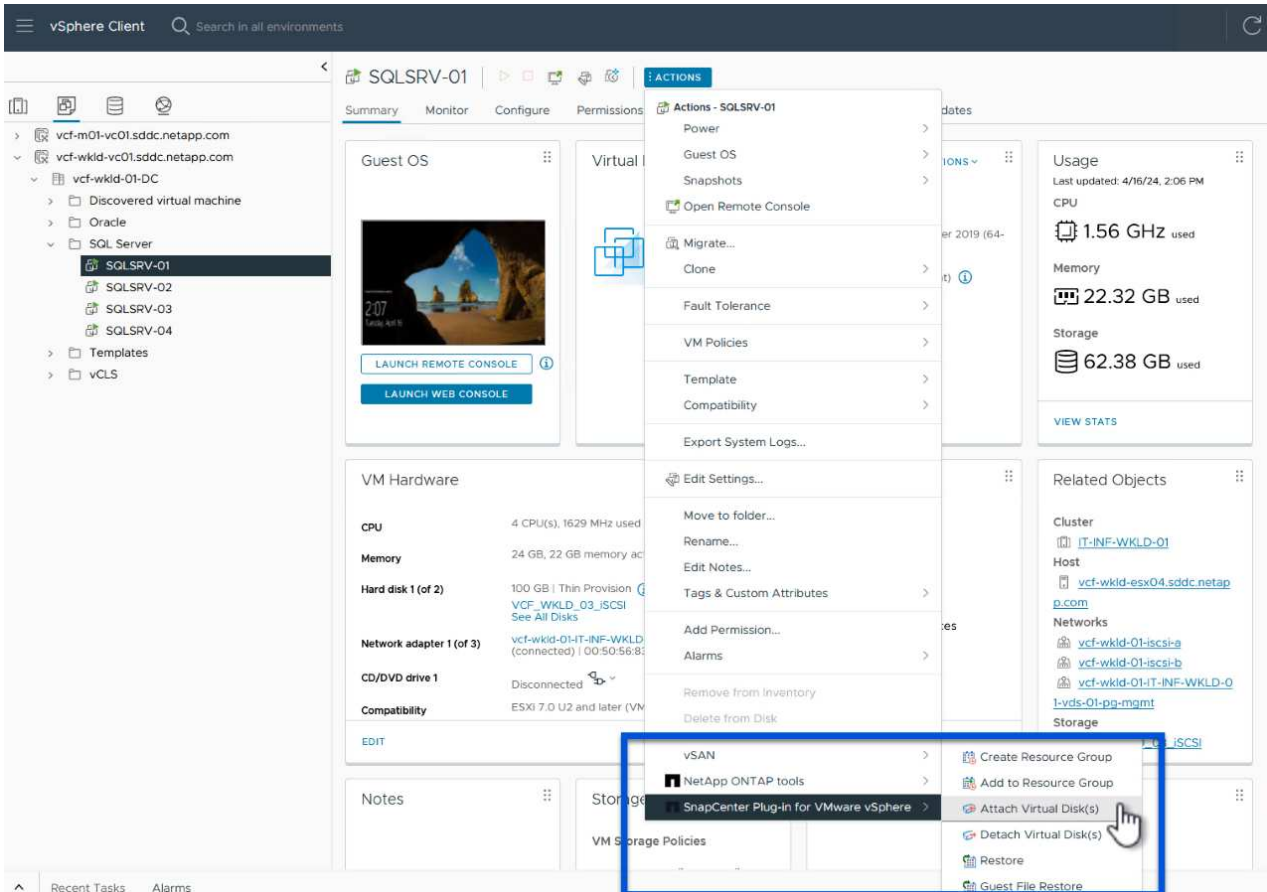
Manage Columns Running More Tasks

Restaurez des VMDK à l'aide du plug-in SnapCenter

Les outils ONTAP permettent une restauration complète des VMDK à leur emplacement d'origine ou la possibilité de rattacher un VMDK en tant que nouveau disque à un système hôte. Dans ce scénario, un VMDK sera rattaché à un hôte Windows afin d'accéder au système de fichiers.

Pour joindre un VMDK à partir d'une sauvegarde, procédez comme suit :

1. Dans le client vSphere, accédez à une machine virtuelle et, dans le menu **actions**, sélectionnez **SnapCenter Plug-in pour VMware vSphere > connecter un ou plusieurs disques virtuels**.



2. Dans l'assistant **Attach Virtual Disk(s)**, sélectionnez l'instance de sauvegarde à utiliser et le VMDK à connecter.

Attach Virtual Disk(s)



Click here to attach to alternate VM

Backup

(This list shows primary backups. **1** modify the filter to display primary and secondary backups.)

| Name | Backup Time | Mounted | Policy | VMware Snapshot |
|---|----------------------|---------|-------------------|-----------------|
| VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218 | 4/17/2024 9:50:01 AM | No | Hourly_Snapmirror | No |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223 | 4/17/2024 8:50:01 AM | No | Hourly_Snapmirror | No |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204 | 4/17/2024 7:50:00 AM | No | Hourly_Snapmirror | No |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194 | 4/17/2024 6:50:00 AM | No | Hourly_Snapmirror | No |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245 | 4/17/2024 5:50:01 AM | No | Hourly_Snapmirror | No |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231 | 4/17/2024 4:50:01 AM | No | Hourly_Snapmirror | No |

Select disks

| Virtual disk | Location |
|--|---|
| <input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk | Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0... |
| <input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v... | Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0... |

Les options de filtre permettent de localiser les sauvegardes et d'afficher les sauvegardes des systèmes de stockage primaire et secondaire.

Attach Virtual Disk(s)



Click here to attach to alternate VM

Backup

(This list shows primary backups)

| Name |
|---|
| VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218 |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223 |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204 |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194 |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245 |
| VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231 |

Select disks

| Virtual disk | Location |
|--|---|
| <input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk | Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0... |
| <input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v... | Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0... |

Time range

From

Hour Minute Second

To

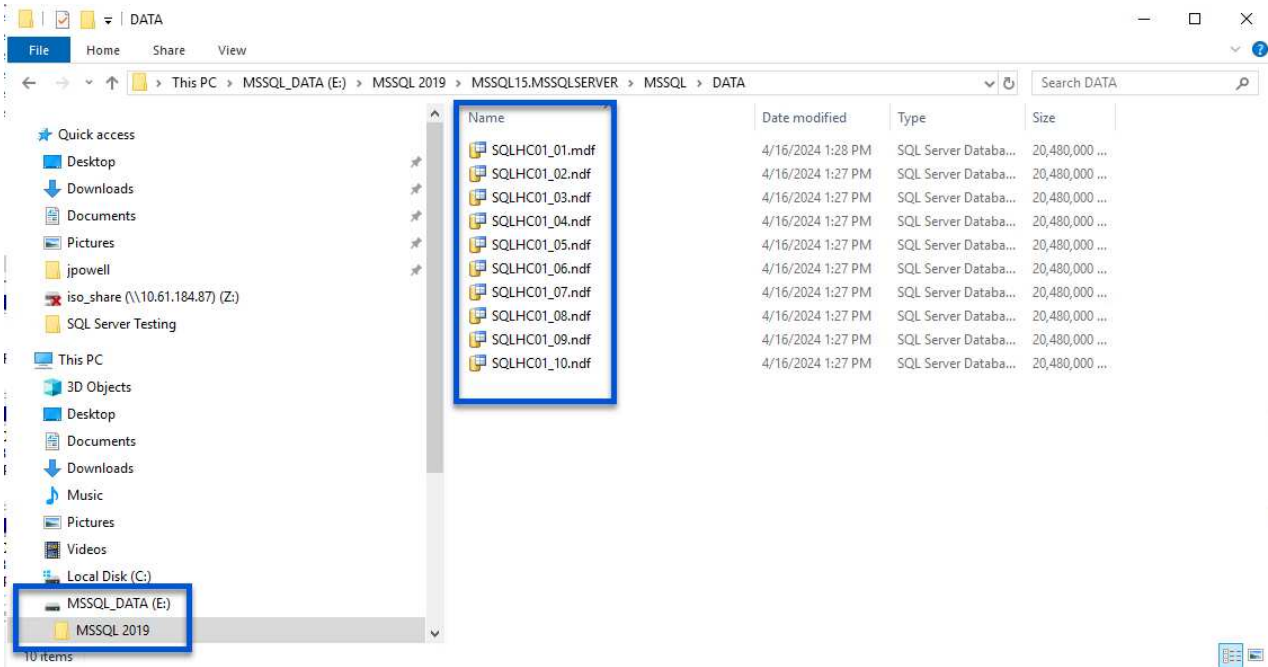
Hour Minute Second

VMware snapshot

Mounted

Location

3. Après avoir sélectionné toutes les options, cliquez sur le bouton **joindre** pour lancer le processus de restauration et joindre le VMDK à l'hôte.
4. Une fois la procédure de connexion terminée, le disque est accessible à partir du système d'exploitation du système hôte. Dans ce cas, SCV connecté le disque avec son système de fichiers NTFS au lecteur E: De notre serveur Windows SQL Server et les fichiers de base de données SQL sur le système de fichiers sont accessibles via l'Explorateur de fichiers.



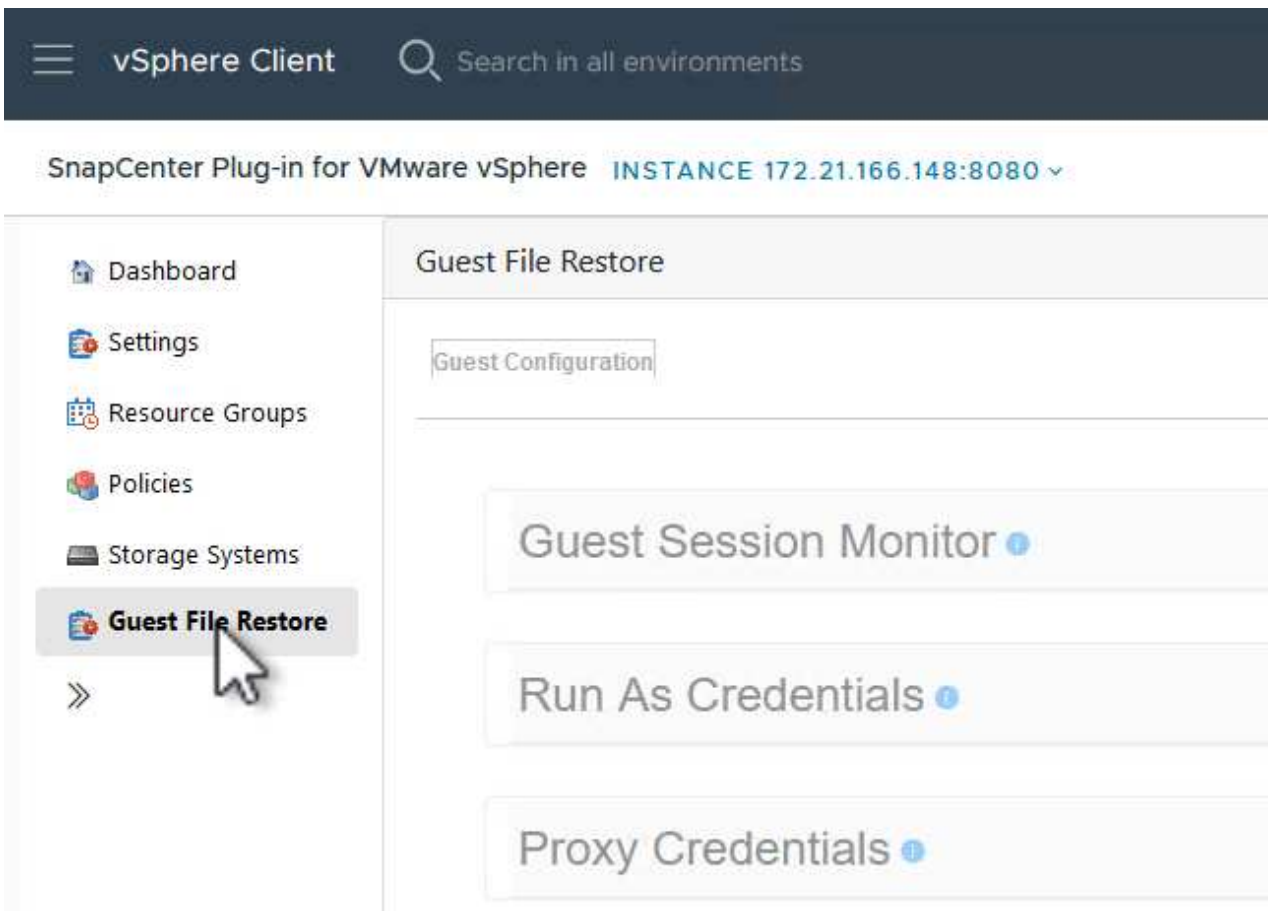
Restauration du système de fichiers invité à l'aide du plug-in SnapCenter

Les outils ONTAP incluent des restaurations de systèmes de fichiers invités à partir d'un VMDK sur les systèmes d'exploitation Windows Server. Ceci est préformé de manière centralisée à partir de l'interface du plug-in SnapCenter.

Pour plus d'informations, reportez-vous à la section "[Restaurez les fichiers et les dossiers invités](#)" Sur le site de documentation des distributeurs sélectifs.

Pour effectuer une restauration du système de fichiers invité sur un système Windows, procédez comme suit :

1. La première étape consiste à créer des informations d'identification Exécuter en tant que pour fournir un accès au système hôte Windows. Dans le client vSphere, accédez à l'interface du plug-in CSV et cliquez sur **Guest File Restore** dans le menu principal.

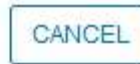


2. Sous **Exécuter en tant qu'informations d'identification**, cliquez sur l'icône + pour ouvrir la fenêtre **Exécuter en tant qu'informations d'identification**.
3. Saisissez un nom pour l'enregistrement des informations d'identification, un nom d'utilisateur et un mot de passe administrateur pour le système Windows, puis cliquez sur le bouton **Sélectionner VM** pour sélectionner une machine virtuelle proxy facultative à utiliser pour la restauration.

Run As Credentials



| | | |
|---------------------|--|--|
| Run As Name | <input type="text" value="Administrator"/> | |
| Username | <input type="text" value="administrator"/> | |
| Password | <input type="password" value="••••••••"/> | |
| Authentication Mode | <input type="text" value="Windows"/> | |
| VM Name | <input type="text"/> | |



4. Sur la page Proxy VM, indiquez le nom de la VM et recherchez-la en effectuant une recherche par hôte ESXi ou par nom. Une fois sélectionné, cliquez sur **Enregistrer**.

Proxy VM



VM Name

Search by ESXi Host

ESXi Host

Virtual Machine

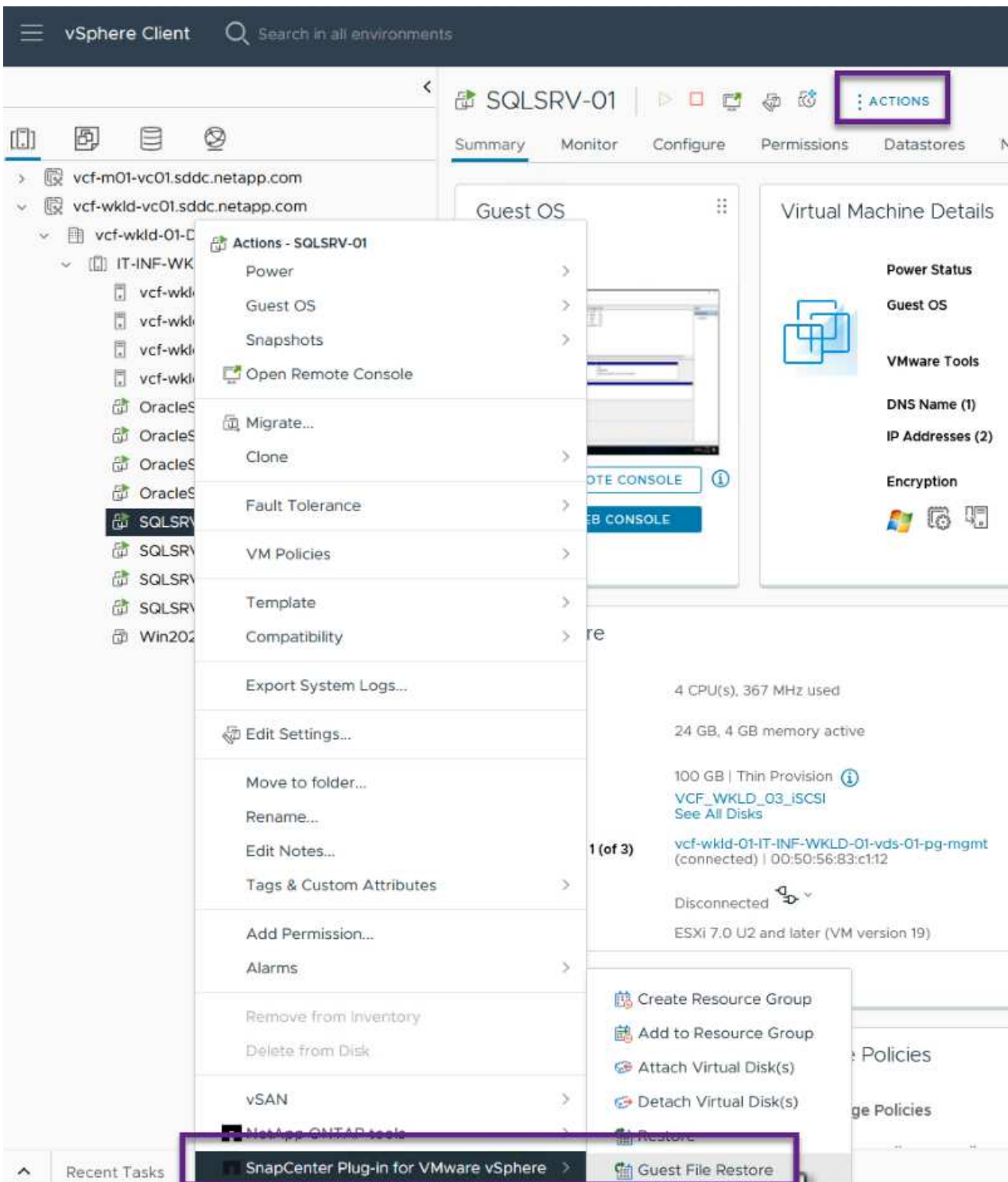
Search by Virtual Machine name

CANCEL

SAVE



5. Cliquez de nouveau sur **Enregistrer** dans la fenêtre **Exécuter en tant qu'informations d'identification** pour terminer l'enregistrement.
6. Ensuite, accédez à une machine virtuelle dans l'inventaire. Dans le menu **actions** ou en cliquant avec le bouton droit de la souris sur la machine virtuelle, sélectionnez **SnapCenter Plug-in pour VMware vSphere > Restauration des fichiers invités**.



7. Sur la page **Restore Scope** de l'assistant **Guest File Restore**, sélectionnez la sauvegarde à partir de laquelle effectuer la restauration, le VMDK spécifique et l'emplacement (principal ou secondaire) à partir duquel restaurer le VMDK. Cliquez sur **Suivant** pour continuer.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

| Backup Name | Start Time | End Time |
|-----------------------------------|----------------------|----------------------|
| SQL_Servers_04-16-2024_13.52.3... | 4/16/2024 1:52:34 PM | 4/16/2024 1:52:40 PM |
| VCF_WKLD_iscsi_Datastore_04-1... | 4/16/2024 1:50:01 PM | 4/16/2024 1:50:08 PM |
| | | |
| | | |

| VMDK |
|--|
| [VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01.vmdk |
| [VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01_1.vmdk |
| |
| |

| Locations |
|---|
| Primary:VCF_iscsi:VCF_WKLD_03_iscsi:SQL_Servers_04-16-2024_13.52.34.0329 |
| Secondary:svm_iscsi:VCF_WKLD_03_iscsi_dest:SQL_Servers_04-16-2024_13.52.34.0329 |
| |
| |

BACK NEXT FINISH CANCEL



8. Sur la page **Guest Details**, sélectionnez pour utiliser **Guest VM** ou **Use Gues File Restore proxy VM** pour la restauration. Remplissez également les paramètres de notification par e-mail ici si vous le souhaitez. Cliquez sur **Suivant** pour continuer.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Use Guest VM

Guest File Restore operation will attach disk to guest VM

| Run As Name | Username | Authentication Mode |
|---------------|---------------|---------------------|
| Administrator | administrator | WINDOWS |
| | | |
| | | |

Use Guest File Restore proxy VM

Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

- Enfin, consultez la page **Résumé** et cliquez sur **Terminer** pour commencer la session de restauration du système de fichiers invité.
- De retour dans l'interface du plug-in SnapCenter, naviguez à nouveau jusqu'à **Restauration de fichier invité** et affichez la session en cours sous **moniteur de session invité**. Cliquez sur l'icône sous **Parcourir les fichiers** pour continuer.

| Backup Name | Source VM | Disk Path | Guest Mount Path | Time To Expire | Browse Files |
|--------------------------------------|-----------|---------------------------------------|------------------|----------------|--------------|
| SQL_Servers_04-16-2024_13.52.34.0329 | SQLSRV-01 | [VCF_WKLD_03_JSCSI]sc-202404161419... | E:\ | 23h:58m | |

- Dans l'assistant **Guest File Browse**, sélectionnez le ou les fichiers à restaurer et l'emplacement du système de fichiers dans lequel les restaurer. Enfin, cliquez sur **Restaurer** pour lancer le processus **Restaurer**.

Guest File Browse



Select File(s)/Folder(s) to Restore



E:\MSSQL 2019

| | Name | Size | |
|--------------------------|---------------------|------|---|
| <input type="checkbox"/> | MSSQL15.MSSQLSERVER | | ^ |
| | | | v |

Selected 0 Files / 1 Directory

| Name | Path | Size | Delete | |
|------------|---------------|------|--------|---|
| MSSQL 2019 | E:\MSSQL 2019 | | | ^ |
| | | | | v |

Select Restore Location



Select address family for UNC path:

IPv4

IPv6

Either Files to Restore or Restore Location is not selected!

CANCEL

RESTORE

Select Restore Location

Select address family for UNC path:

IPv4

IPv6

Restore to path

Provide UNC path to the guest where files will be restored. eg: \\10.60.136.65\c\$

Run As Credentials while triggering the Guest File Restore workflow will be used to connect to the UNC path

If original file(s) exist:

Always overwrite

Always skip

Disconnect Guest Session after successful restore

CANCEL RESTORE

12. La tâche de restauration peut être surveillée à partir du volet des tâches du client vSphere.

Informations supplémentaires

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section "[Documentation de VMware Cloud Foundation](#)".

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au "[Documentation ONTAP 9](#)" centre.

Pour plus d'informations sur l'utilisation du plug-in SnapCenter pour VMware vSphere, reportez-vous au "[Documentation du plug-in SnapCenter pour VMware vSphere](#)".

VCF avec baies NetApp AFF

Socle cloud VMware avec baies NetApp AFF

VMware Cloud Foundation (VCF) est une plateforme de data Center Software-defined intégrée qui fournit une pile complète d'infrastructure Software-defined pour exécuter les applications d'entreprise dans un environnement de cloud hybride. Elle réunit les fonctionnalités de calcul, de stockage, de mise en réseau et de gestion dans une plateforme unifiée, offrant ainsi une expérience opérationnelle cohérente dans les clouds privés et publics.

Auteur: Josh Powell, Ravi BCB

Ce document fournit des informations sur les options de stockage disponibles pour VMware Cloud Foundation avec le système de stockage AFF 100 % Flash de NetApp. Les options de stockage prises en charge sont couvertes par des instructions spécifiques pour la création de domaines de charge de travail avec des datastores NFS et vVol en tant que stockage principal, ainsi qu'un ensemble d'options de stockage supplémentaires.

Cas d'utilisation

Cas d'utilisation décrits dans cette documentation :

- Options de stockage pour les clients à la recherche d'environnements uniformes sur les clouds privés et publics.
- Solution automatisée pour le déploiement d'infrastructures virtuelles pour les domaines de charge de travail.
- Solution de stockage évolutive et adaptée à l'évolution des besoins, même lorsqu'elle n'est pas directement alignée sur les besoins en ressources de calcul.
- Déployez des domaines de charge de travail virtuels en utilisant ONTAP comme stockage principal.
- Déployez un stockage supplémentaire dans des domaines de charge de travail VI à l'aide des outils ONTAP pour VMware vSphere.

Public

Cette solution est destinée aux personnes suivantes :

- Architectes de solutions qui recherchent des options de stockage plus flexibles pour les environnements VMware conçus pour optimiser le TCO.
- Architectes de solutions à la recherche d'options de stockage VCF offrant des options de protection des données et de reprise d'activité avec les principaux fournisseurs cloud.
- Les administrateurs du stockage qui souhaitent comprendre comment configurer VCF avec le stockage principal et supplémentaire.

Présentation de la technologie

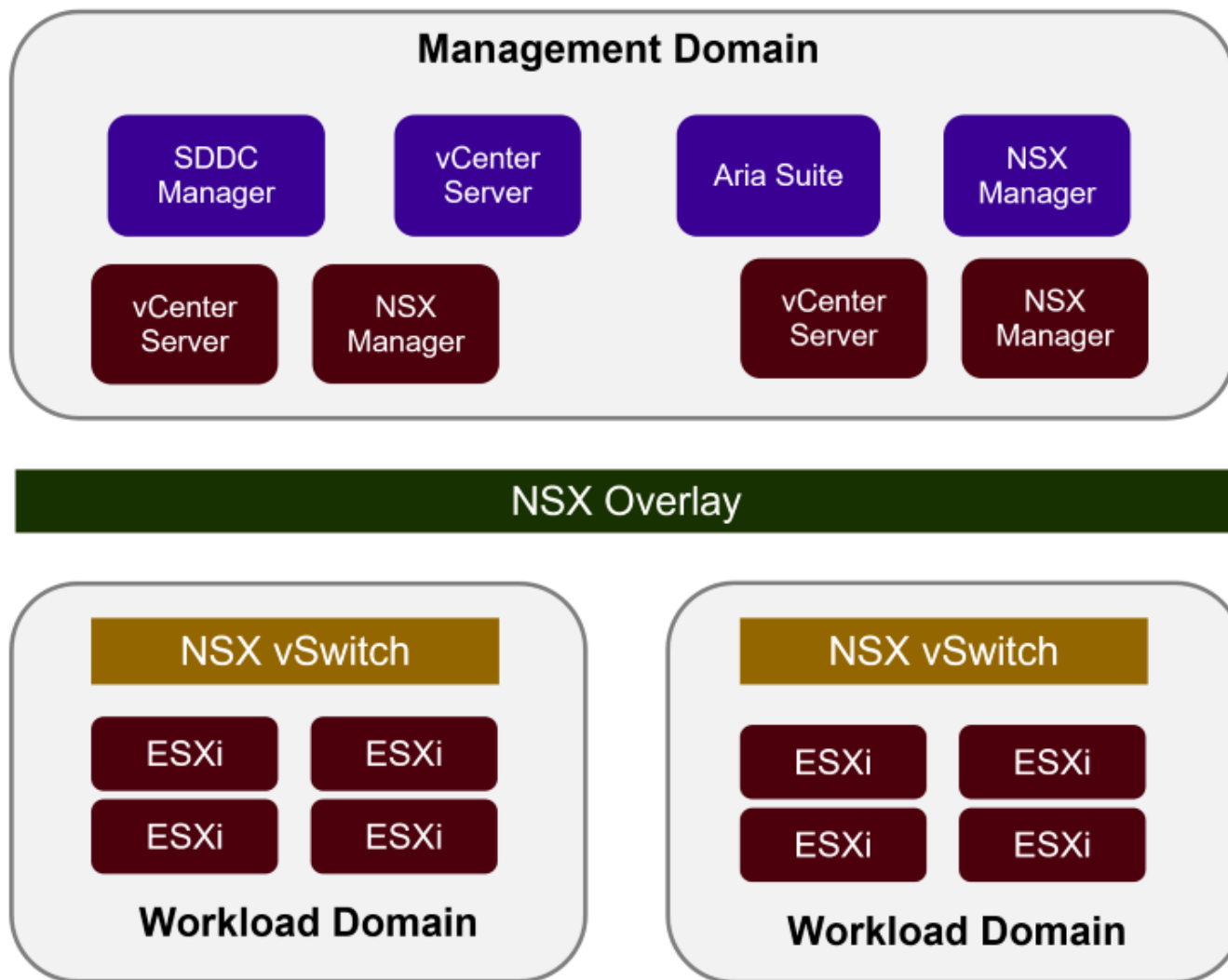
La solution VCF avec NetApp AFF comprend les principaux composants suivants :

Socle cloud VMware

VMware Cloud Foundation étend les offres d'hyperviseur vSphere de VMware en combinant des composants clés tels que SDDC Manager, vSphere, VSAN, NSX et VMware Aria Suite pour créer un data Center virtualisé.

La solution VCF prend en charge les workloads Kubernetes natifs et basés sur des machines virtuelles. Les services clés tels que VMware vSphere, VMware VSAN, VMware NSX-T Data Center et VMware vRealize Cloud Management font partie intégrante du package VCF. Ces services permettent d'établir une infrastructure Software-defined capable de gérer efficacement le calcul, le stockage, la mise en réseau, la sécurité et la gestion du cloud.

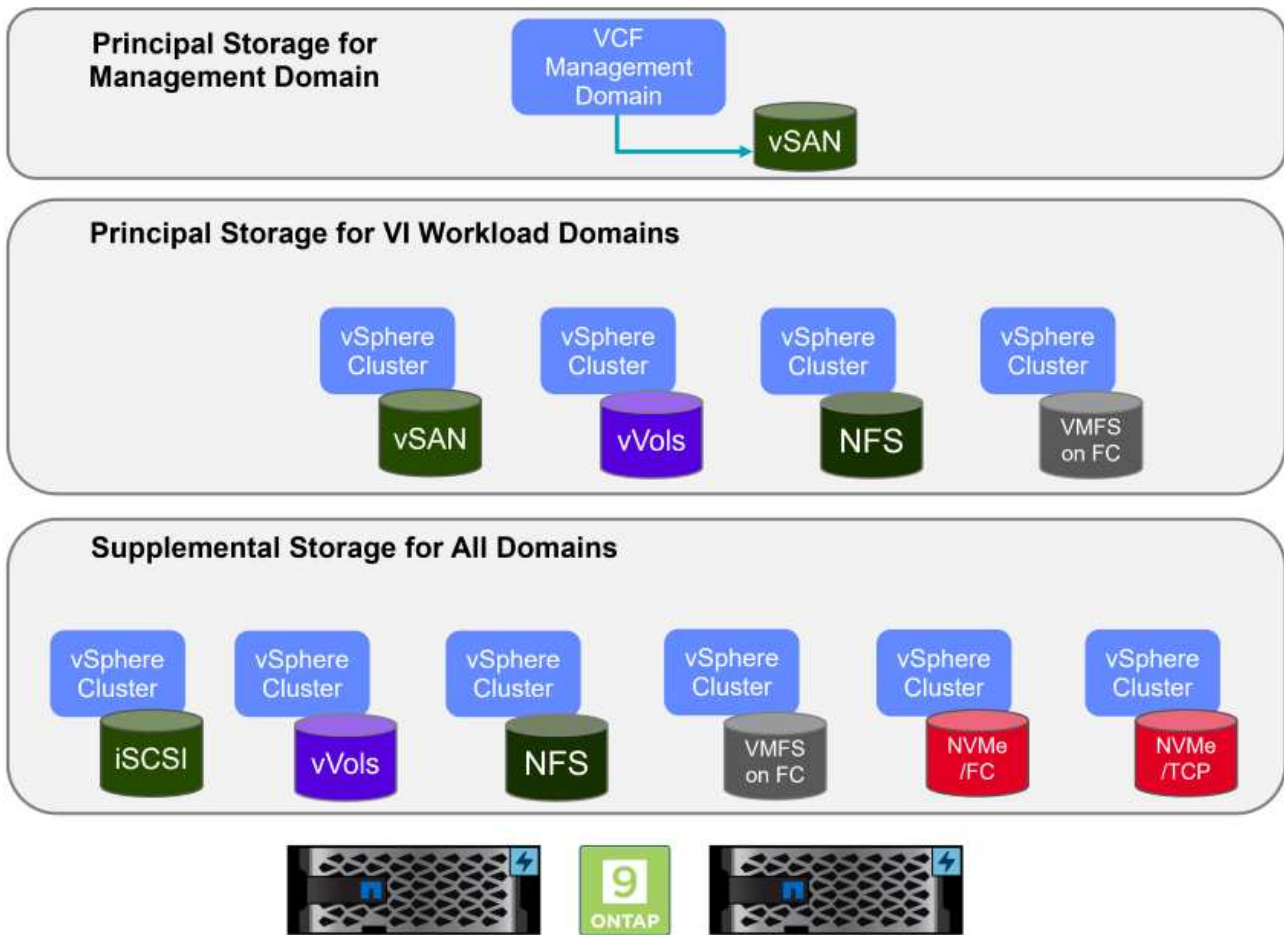
VCF comprend un seul domaine de gestion et jusqu'à 24 domaines de charge de travail VI qui représentent chacun une unité d'infrastructure prête pour les applications. Un domaine de charges de travail comprend un ou plusieurs clusters vSphere gérés par une seule instance vCenter.



Pour plus d'informations sur l'architecture et la planification VCF, reportez-vous à la section ["Modèles d'architecture et types de domaine de charge de travail dans VMware Cloud Foundation"](#).

Options de stockage VCF

VMware divise les options de stockage pour VCF en stockage **principal** et **supplémentaire**. Le domaine de gestion VCF doit utiliser VSAN comme stockage principal. Cependant, il existe de nombreuses options de stockage supplémentaires pour le domaine de gestion et des options de stockage principal et supplémentaire disponibles pour les domaines de charge de travail VI.



Stockage principal pour les domaines de charge de travail

Le stockage principal désigne tout type de stockage pouvant être directement connecté à un domaine de charge de travail VI pendant le processus de configuration dans SDDC Manager. Le stockage principal est le premier datastore configuré pour un domaine de charge de travail et inclut vSAN, vVols (VMFS), NFS et VMFS sur Fibre Channel.

Stockage supplémentaire pour les domaines de gestion et de charge de travail

Le stockage supplémentaire correspond au type de stockage qui peut être ajouté aux domaines de gestion ou de charge de travail à tout moment après la création du cluster. Le stockage supplémentaire représente le plus grand nombre d'options de stockage prises en charge, toutes prises en charge sur les baies NetApp AFF.

Ressources de documentation supplémentaires pour VMware Cloud Foundation :

- * ["Documentation de VMware Cloud Foundation"](#)
- * ["Types de stockage pris en charge pour VMware Cloud Foundation"](#)
- * ["Gestion du stockage dans VMware Cloud Foundation"](#)

Baies de stockage 100 % Flash NetApp

Les baies NetApp AFF (FAS 100 % Flash) sont des solutions de stockage haute performance conçues pour exploiter la vitesse et l'efficacité de la technologie Flash. Les baies AFF intègrent des fonctionnalités intégrées de gestion des données telles que les sauvegardes basées sur des snapshots, la réplication, le provisionnement fin et la protection des données.

Les baies NetApp AFF utilisent le système d'exploitation de stockage ONTAP et proposent une prise en charge complète des protocoles de stockage pour toutes les options de stockage compatibles avec VCF, le tout dans une architecture unifiée.

Les baies de stockage NetApp AFF sont disponibles dans les gammes A-Series et C-Series Flash QLC les plus performantes. Les deux gammes utilisent des disques Flash NVMe.

Pour plus d'informations sur les baies de stockage NetApp AFF A-Series, consultez le ["NetApp AFF A-Series"](#) page d'accueil.

Pour plus d'informations sur les baies de stockage NetApp C-Series, consultez le ["NetApp AFF série C."](#) page d'accueil.

Outils NetApp ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere (OTV) permettent aux administrateurs de gérer le stockage NetApp directement à partir du client vSphere. Les outils ONTAP vous permettent de déployer et de gérer des datastores, ainsi que de provisionner des datastores VVol.

Les outils ONTAP permettent de mapper les datastores aux profils de capacité de stockage qui déterminent un ensemble d'attributs de système de stockage. Il est ainsi possible de créer des datastores dotés d'attributs spécifiques tels que les performances du stockage et la qualité de service.

Les outils ONTAP incluent également un fournisseur * VMware vSphere API for Storage Awareness (VASA)* pour les systèmes de stockage ONTAP qui permet le provisionnement de datastores VMware Virtual volumes (vVols), la création et l'utilisation de profils de fonctionnalités de stockage, la vérification de conformité et la surveillance des performances.

Pour plus d'informations sur les outils NetApp ONTAP, reportez-vous au ["Documentation sur les outils ONTAP pour VMware vSphere"](#) page.

Présentation de la solution

Dans les scénarios présentés dans cette documentation, nous démontrerons comment utiliser les systèmes de stockage ONTAP comme stockage principal pour les déploiements VCF VI Workload Domain. En outre, nous installerons et utiliserons les outils ONTAP pour VMware vSphere pour configurer des datastores supplémentaires pour les domaines de charge de travail VI.

Scénarios traités dans cette documentation :

- **Configurer et utiliser un datastore NFS comme stockage principal pendant le déploiement de VI Workload Domain.** cliquez sur ["ici"](#) pour les étapes de déploiement.
- **Installez et démontrez l'utilisation des outils ONTAP pour configurer et monter des datastores NFS en tant que stockage supplémentaire dans des domaines de charge de travail VI.** cliquez sur ["ici"](#) pour les étapes de déploiement.

NFS en tant que stockage principal pour les domaines de charge de travail VI

Dans ce scénario, nous allons montrer comment configurer un datastore NFS en tant que stockage principal pour le déploiement d'un domaine de charge de travail VI dans VCF. Le cas échéant, nous nous référons à la documentation externe pour connaître les

étapes à suivre dans le gestionnaire SDDC de VCF, et nous aborderons les étapes spécifiques à la partie relative à la configuration du stockage.

Auteur: Josh Powell, Ravi BCB

Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

- Vérifier la mise en réseau de la machine virtuelle de stockage ONTAP (SVM) et qu'une interface logique (LIF) est présente pour le transport du trafic NFS.
- Créez une export policy pour permettre aux hôtes ESXi d'accéder au volume NFS.
- Créez un volume NFS sur le système de stockage ONTAP.
- Créez un pool réseau pour le trafic NFS et vMotion dans SDDC Manager.
- Commission des hôtes dans VCF pour une utilisation dans un domaine de charge de travail VI.
- Déployez un domaine de charge de travail VI dans VCF en utilisant un datastore NFS comme stockage principal.
- Installation du plug-in NetApp NFS pour VMware VAAI

Prérequis

Ce scénario nécessite les composants et configurations suivants :

- Système de stockage NetApp AFF avec une machine virtuelle de stockage (SVM) configurée pour autoriser le trafic NFS.
- L'interface logique (LIF) a été créée sur le réseau IP qui transporte le trafic NFS et est associée à la SVM.
- Le déploiement du domaine de gestion VCF est terminé et l'interface SDDC Manager est accessible.
- 4 hôtes ESXi configurés pour la communication sur le réseau de gestion VCF.
- Adresses IP réservées pour le trafic de stockage vMotion et NFS sur le VLAN ou le segment réseau établi à cet effet.



Lors du déploiement d'un domaine de charge de travail VI, VCF valide la connectivité au serveur NFS. Pour ce faire, utilisez l'adaptateur de gestion sur les hôtes ESXi avant d'ajouter un adaptateur vmkernel supplémentaire avec l'adresse IP NFS. Par conséquent, il faut s'assurer que 1) le réseau de gestion est routable vers le serveur NFS, ou 2) une LIF pour le réseau de gestion a été ajoutée au SVM hébergeant le volume du datastore NFS, pour s'assurer que la validation peut se poursuivre.

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au ["Documentation ONTAP 9"](#) centre.

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section ["Documentation de VMware Cloud Foundation"](#).

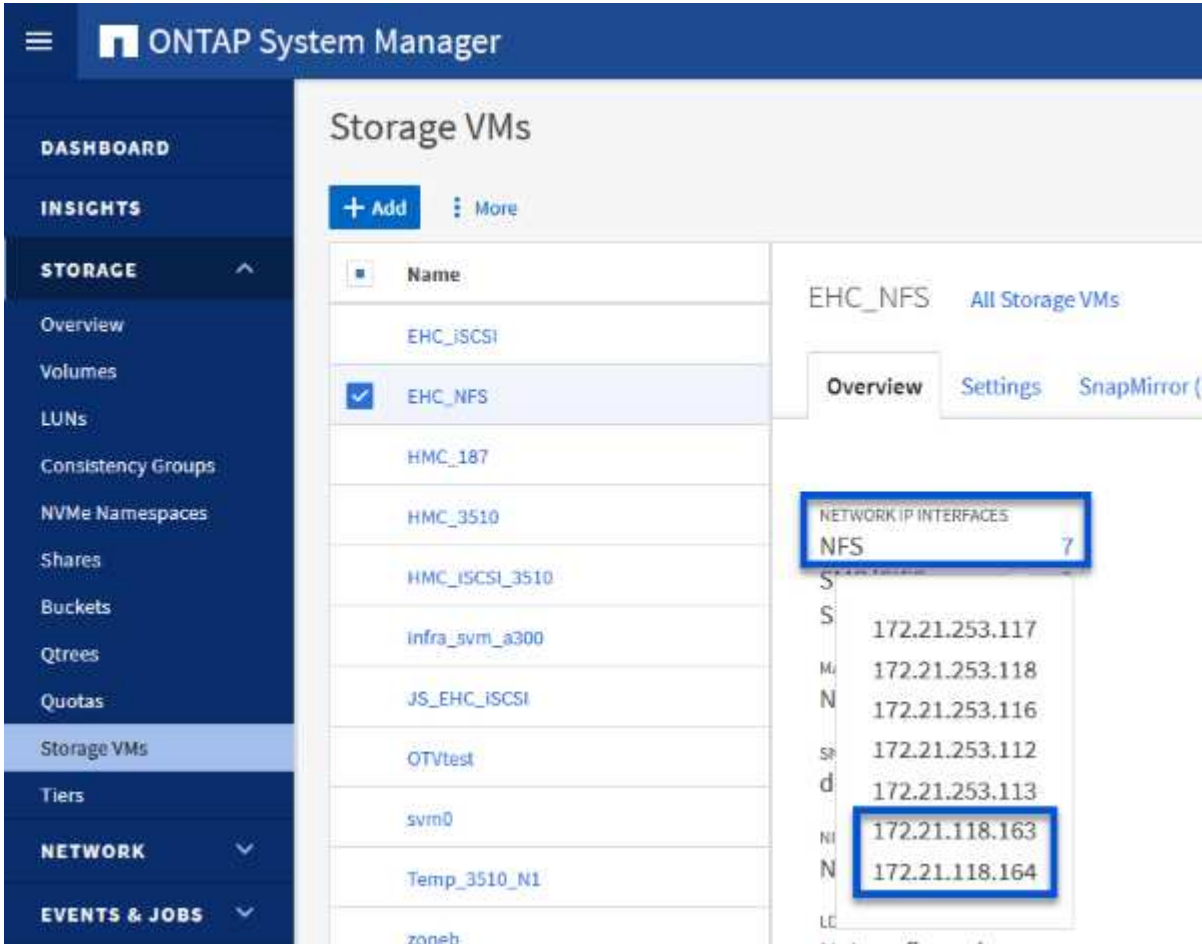
Étapes de déploiement

Pour déployer un domaine de charge de travail VI avec un datastore NFS comme stockage principal, procédez comme suit :

Vérifier la mise en réseau du SVM ONTAP

Vérifiez que les interfaces logiques requises ont été établies pour le réseau qui transportera le trafic NFS entre le cluster de stockage ONTAP et le domaine de charge de travail VI.

1. Depuis ONTAP System Manager, naviguez jusqu'à **Storage VM** dans le menu de gauche et cliquez sur le SVM à utiliser pour le trafic NFS. Dans l'onglet **vue d'ensemble**, sous **NETWORK IP INTERFACES**, cliquez sur la valeur numérique à droite de **NFS**. Vérifier dans la liste que les adresses IP LIF requises sont répertoriées.



The screenshot shows the ONTAP System Manager interface. The left sidebar contains a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE (expanded), and NETWORK. Under STORAGE, 'Storage VMs' is selected. The main area displays a list of Storage VMs, with 'EHC_NFS' selected. To the right, the 'Overview' tab for 'EHC_NFS' is active, showing 'All Storage VMs'. Below this, the 'NETWORK IP INTERFACES' section is visible, with 'NFS' selected. A dropdown menu shows a list of IP addresses, with '172.21.118.163' and '172.21.118.164' highlighted by blue boxes.

| Name |
|---|
| EHC_ISCSI |
| <input checked="" type="checkbox"/> EHC_NFS |
| HMC_187 |
| HMC_3510 |
| HMC_ISCSI_3510 |
| infra_svm_a300 |
| JS_EHC_ISCSI |
| OTVtest |
| svm0 |
| Temp_3510_N1 |
| zoneb |

NETWORK IP INTERFACES

| NFS | 7 |
|----------------|---|
| 172.21.253.117 | |
| 172.21.253.118 | |
| 172.21.253.116 | |
| 172.21.253.112 | |
| 172.21.253.113 | |
| 172.21.118.163 | |
| 172.21.118.164 | |

Vérifier alternativement les LIFs associées à un SVM depuis l'interface de ligne de commandes ONTAP avec la commande suivante :

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

1. Vérifiez que les hôtes VMware ESXi peuvent communiquer avec le serveur NFS ONTAP. Se connecter à l'hôte ESXi via SSH et envoyer une requête ping au LIF du SVM :

```
vmkping <IP Address>
```

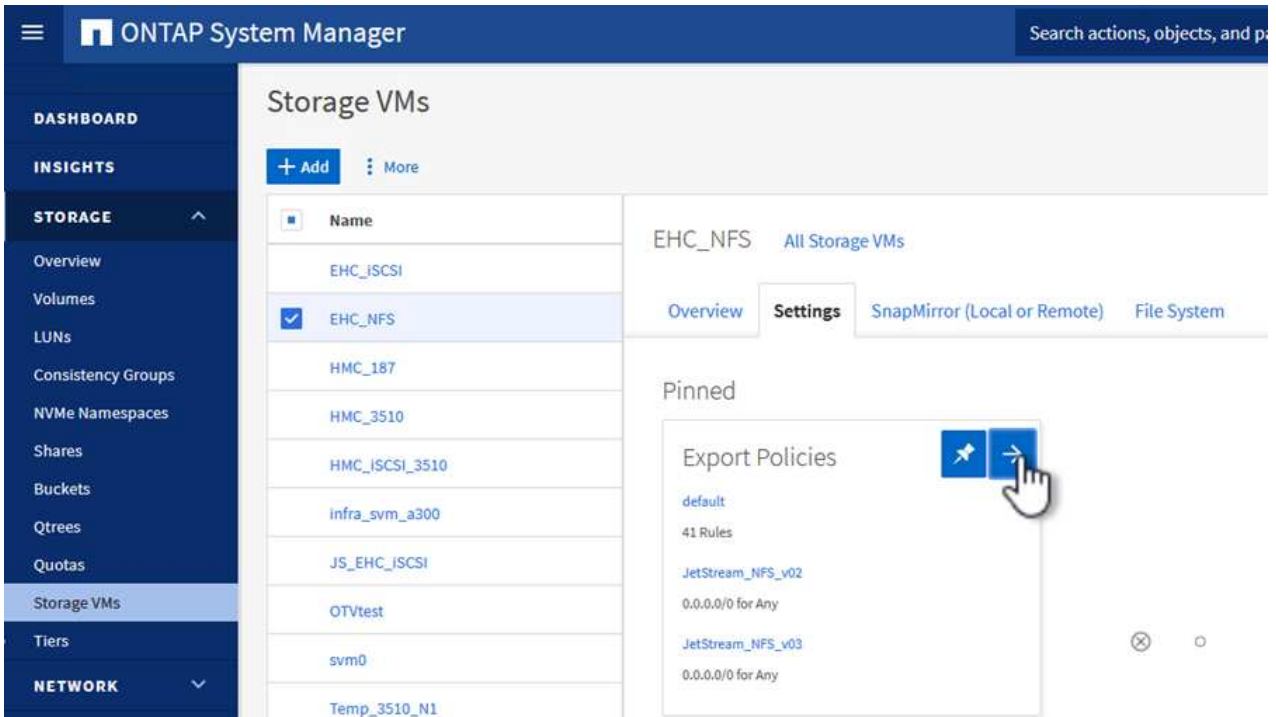


Lors du déploiement d'un domaine de charge de travail VI, VCF valide la connectivité au serveur NFS. Pour ce faire, utilisez l'adaptateur de gestion sur les hôtes ESXi avant d'ajouter un adaptateur vmkernel supplémentaire avec l'adresse IP NFS. Par conséquent, il faut s'assurer que 1) le réseau de gestion est routable vers le serveur NFS, ou 2) une LIF pour le réseau de gestion a été ajoutée au SVM hébergeant le volume du datastore NFS, pour s'assurer que la validation peut se poursuivre.

Créez une règle d'export pour le partage du volume NFS

Créez une export policy dans ONTAP System Manager afin de définir le contrôle d'accès des volumes NFS.

1. Dans ONTAP System Manager, cliquez sur **Storage VM** dans le menu de gauche et sélectionnez un SVM dans la liste.
2. Dans l'onglet **Paramètres**, localisez **règles d'exportation** et cliquez sur la flèche pour y accéder.



3. Dans la fenêtre **Nouvelle export policy**, ajoutez un nom pour la stratégie, cliquez sur le bouton **Ajouter de nouvelles règles**, puis sur le bouton **+Ajouter** pour commencer à ajouter une nouvelle règle.

New export policy

NAME

WKLD_DM01

Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

- Indiquez les adresses IP, la plage d'adresses IP ou le réseau que vous souhaitez inclure dans la règle. Décochez les cases **SMB/CIFS** et **FlexCache** et effectuez les sélections pour les détails d'accès ci-dessous. La sélection des cases UNIX suffit pour l'accès à l'hôte ESXi.

New Rule



CLIENT SPECIFICATION

ACCESS PROTOCOLS

 SMB/CIFS FlexCache NFS NFSv3 NFSv4

ACCESS DETAILS

| Type | Read-only Access | Read/Write Access | Superuser Access |
|-------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| All | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| All (As anonymous user) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| UNIX | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Kerberos 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Kerberos 5i | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Kerberos 5p | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| NTLM | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Cancel

Save



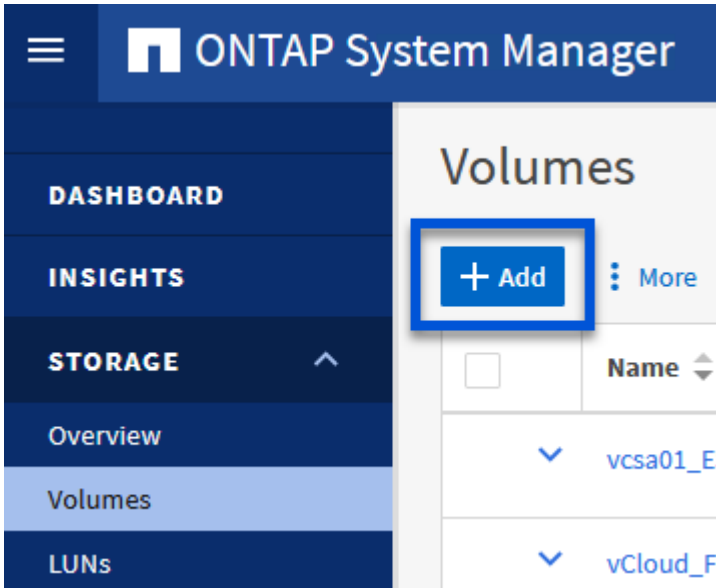
Lors du déploiement d'un domaine de charge de travail VI, VCF valide la connectivité au serveur NFS. Pour ce faire, utilisez l'adaptateur de gestion sur les hôtes ESXi avant d'ajouter un adaptateur vmkernel supplémentaire avec l'adresse IP NFS. Par conséquent, il est nécessaire de s'assurer que la politique d'exportation inclut le réseau de gestion VCF afin de permettre la validation.

- Une fois toutes les règles saisies, cliquez sur le bouton **Enregistrer** pour enregistrer la nouvelle politique d'exportation.
- Vous pouvez également créer des règles et des règles d'export dans l'interface de ligne de commandes de ONTAP. Reportez-vous aux étapes de création d'une export-policy et d'ajout de règles dans la documentation ONTAP.
 - Utilisez l'interface de ligne de commandes ONTAP pour "[Créer une export-policy](#)".
 - Utilisez l'interface de ligne de commandes ONTAP pour "[Ajouter une règle à une export-policy](#)".

Créer un volume NFS

Créez un volume NFS sur le système de stockage ONTAP à utiliser comme datastore dans le déploiement de domaine de charge de travail.

1. Dans le Gestionnaire système ONTAP, accédez à **stockage > volumes** dans le menu de gauche et cliquez sur **+Ajouter** pour créer un volume.



2. Ajoutez un nom au volume, remplissez la capacité souhaitée et sélectionnez la VM de stockage qui hébergera le volume. Cliquez sur **plus d'options** pour continuer.

Add Volume



NAME

VCF_WKLD_01

CAPACITY

5



TiB



STORAGE VM

EHC_NFS



Export via NFS

[More Options](#)

Cancel


Save

3. Sous autorisations d'accès, sélectionnez la politique d'exportation qui inclut le réseau de gestion VCF ou l'adresse IP et les adresses IP réseau NFS qui seront utilisées pour la validation du serveur NFS et du trafic NFS.

Access Permissions

Export via NFS

GRANT ACCESS TO HOST

default 

JetStream_NFS_v04
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01
3 rules

NFSmountTestReno01
Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv_VPN
Clients : 172.21.254.0/24 | Access protocols : Any

VCF_WKLD
2 rules

WKLD_DM01
2 rules

Wkld01_NFS
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.252.208

+



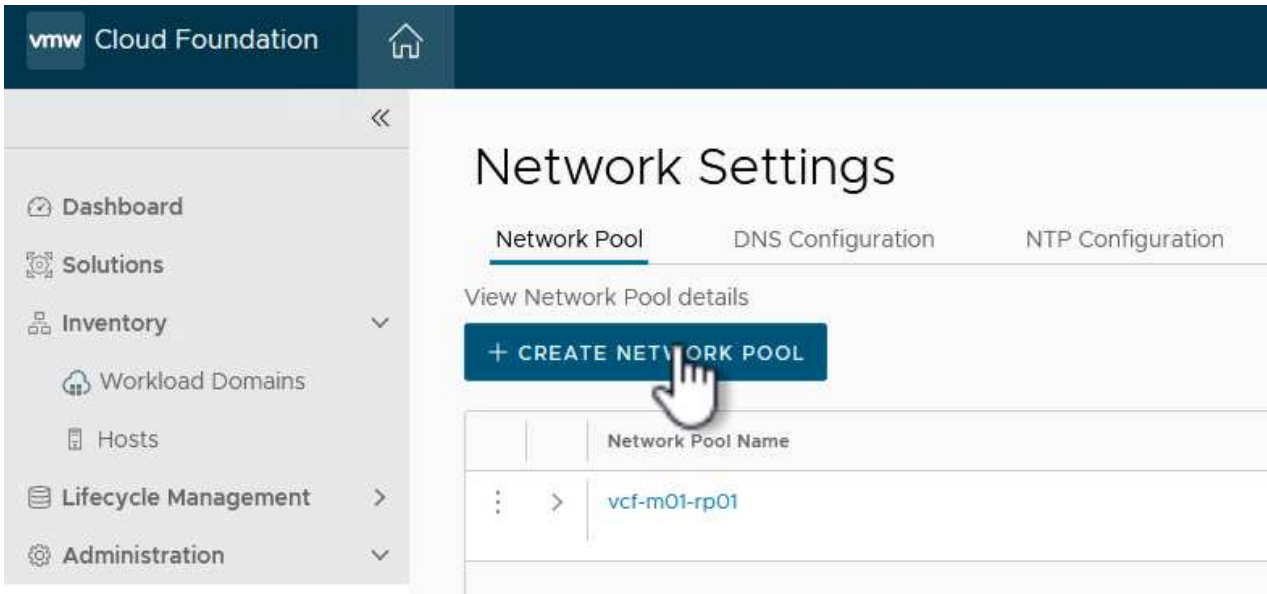
Lors du déploiement d'un domaine de charge de travail VI, VCF valide la connectivité au serveur NFS. Pour ce faire, utilisez l'adaptateur de gestion sur les hôtes ESXi avant d'ajouter un adaptateur vmkernel supplémentaire avec l'adresse IP NFS. Par conséquent, il faut s'assurer que 1) le réseau de gestion est routable vers le serveur NFS, ou 2) une LIF pour le réseau de gestion a été ajoutée au SVM hébergeant le volume du datastore NFS, pour s'assurer que la validation peut se poursuivre.

1. Les volumes ONTAP peuvent également être créés dans l'interface de ligne de commande ONTAP. Pour plus d'informations, reportez-vous à la ["la création de lun"](#) Dans la documentation des commandes ONTAP.

Créez un pool réseau dans SDDC Manager

Un Network Pool doit être créé dans SDDC Manager avant de mettre en service les hôtes ESXi, afin de préparer leur déploiement dans un domaine de charge de travail VI. Le pool réseau doit inclure les informations réseau et les plages d'adresses IP pour que les cartes VMkernel soient utilisées pour la communication avec le serveur NFS.

1. Dans l'interface Web du gestionnaire SDDC, naviguez jusqu'à **Paramètres réseau** dans le menu de gauche et cliquez sur le bouton **+ Créer un pool réseau**.



2. Indiquez un nom pour le pool réseau, cochez la case NFS et renseignez tous les détails de la mise en réseau. Répétez cette opération pour les informations du réseau vMotion.

The screenshot displays the VMware Cloud Foundation interface for configuring a network pool. The left sidebar shows the navigation menu with 'Network Settings' selected. The main content area is titled 'Network Settings' and 'Create Network Pool'. The 'Network Pool Name' is set to 'NFS_NPOOL'. The 'Network Type' is set to 'NFS'. Below this, there are two panels: 'NFS Network Information' and 'vMotion Network Information'. Each panel contains fields for 'VLAN ID', 'MTU', 'Network', 'Subnet Mask', and 'Default Gateway'. The 'Included IP Address Ranges' section for each network type shows a table with columns for 'From', 'To', and 'Action'. The 'NFS Network Information' panel has a 'SAVE' button at the bottom right.

| Field | Value |
|-----------------|---------------|
| VLAN ID | 3374 |
| MTU | 9000 |
| Network | 172.21.118.0 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 172.21.118.1 |

| Field | Value |
|-----------------|---------------|
| VLAN ID | 3423 |
| MTU | 9000 |
| Network | 172.21.167.0 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 172.21.167.1 |

| From | To | Action |
|-----------------|-----------------|--------|
| 172.21.118.145 | 172.21.118.148 | REMOVE |
| xxx.xxx.xxx.xxx | xxx.xxx.xxx.xxx | ADD |

| From | To | Action |
|-----------------|-----------------|--------|
| 172.21.167.121 | 172.21.167.124 | REMOVE |
| xxx.xxx.xxx.xxx | xxx.xxx.xxx.xxx | ADD |

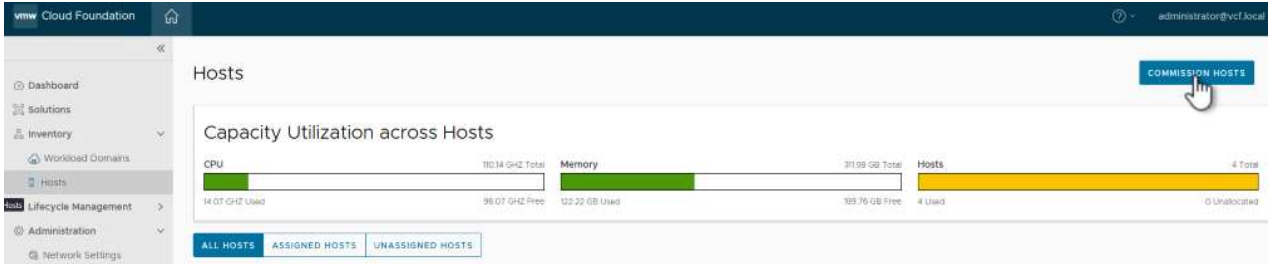
3. Cliquez sur le bouton **Enregistrer** pour terminer la création du pool réseau.

Hôtes de commission

Avant de pouvoir déployer les hôtes ESXi en tant que domaine de charge de travail, ils doivent être ajoutés à l'inventaire SDDC Manager. Cela implique de fournir les informations requises, de réussir la validation et de démarrer le processus de mise en service.

Pour plus d'informations, voir "[Hôtes de commission](#)" Dans le Guide d'administration VCF.

1. Dans l'interface du gestionnaire SDDC, naviguez jusqu'à **hosts** dans le menu de gauche et cliquez sur le bouton **Commission hosts**.



2. La première page est une liste de contrôle préalable. Cochez toutes les conditions préalables et cochez toutes les cases pour continuer.

Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- Select All**
- Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- Host is configured with DNS server for forward and reverse lookup and FQDN.
- Hostname should be same as the FQDN.
- Management IP is configured to first NIC port.
- Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- Host hardware health status is healthy without any errors.
- All disk partitions on HDD / SSD are deleted.
- Ensure required network pool is created and available before host commissioning.
- Ensure hosts to be used for vSAN workload domain are associated with vSAN enabled network pool.
- Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED

3. Dans la fenêtre **Ajout et validation d'hôte**, remplissez le champ **Nom de domaine hôte**, **Type de stockage**, le nom **Pool** qui inclut les adresses IP de stockage vMotion et NFS à utiliser pour le domaine de charge de travail, ainsi que les informations d'identification permettant d'accéder à l'hôte ESXi. Cliquez sur **Ajouter** pour ajouter l'hôte au groupe d'hôtes à valider.

1 Host Addition and Validation

2 Review

Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

Add new Import

Host FQDN

Storage Type vSAN NFS VMFS on FC vVol

Network Pool Name

User Name

Password

ADD

Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

REMOVE

Confirm all Finger Prints

VALIDATE ALL

| <input checked="" type="checkbox"/> | FQDN | Network Pool | IP Address | Confirm FingerPrint | Validation Status |
|-------------------------------------|--------------------------------|--------------|----------------|---|--|
| <input checked="" type="checkbox"/> | vcf-wkld-esx01.sddc.netapp.com | NFS_NP01 | 172.21.166.135 | <input checked="" type="checkbox"/> SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVdp6v EGM | <input type="checkbox"/> Not Validated |

1 hosts

CANCEL

NEXT

- Une fois que tous les hôtes à valider ont été ajoutés, cliquez sur le bouton **Valider tout** pour continuer.
- En supposant que tous les hôtes sont validés, cliquez sur **Suivant** pour continuer.

Hosts Added

✔ Host Validated Successfully. ✕

REMOVE Confirm all Finger Prints (i) VALIDATE ALL

| <input checked="" type="checkbox"/> | FGDN | Network Pool | IP Address | Confirm FingerPrint | Validation Status |
|-------------------------------------|--------------------------------|---|----------------|---|--|
| <input checked="" type="checkbox"/> | vcf-wkld-esx04.sddc.netapp.com | NFS_NP01 (i) | 172.21.166.138 | ✔ SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc | ✔ Valid |
| <input checked="" type="checkbox"/> | vcf-wkld-esx03.sddc.netapp.com | NFS_NP01 (i) | 172.21.166.137 | ✔ SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2IOWZDPFH+z0 | ✔ Valid |
| <input checked="" type="checkbox"/> | vcf-wkld-esx02.sddc.netapp.com | NFS_NP01 (i) | 172.21.166.136 | ✔ SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4IWY | ✔ Valid |
| <input checked="" type="checkbox"/> | vcf-wkld-esx01.sddc.netapp.com | NFS_NP01 (i) | 172.21.166.135 | ✔ SHA256:CKbsinfEOG+!+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM | ✔ Valid |

CANCEL NEXT

6. Passez en revue la liste des hôtes à mettre en service et cliquez sur le bouton **Commission** pour lancer le processus. Surveiller le processus de mise en service à partir du volet des tâches du gestionnaire SDDC.

Commission Hosts

1 Host Addition and Validation

2 **Review**

Review

Skip failed hosts during commissioning  On

| Validated Host(s) | |
|--------------------------------|--|
| vcf-wkld-esx04.sddc.netapp.com | Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS |
| vcf-wkld-esx03.sddc.netapp.com | Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS |
| vcf-wkld-esx02.sddc.netapp.com | Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS |
| vcf-wkld-esx01.sddc.netapp.com | Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS |

CANCEL

BACK

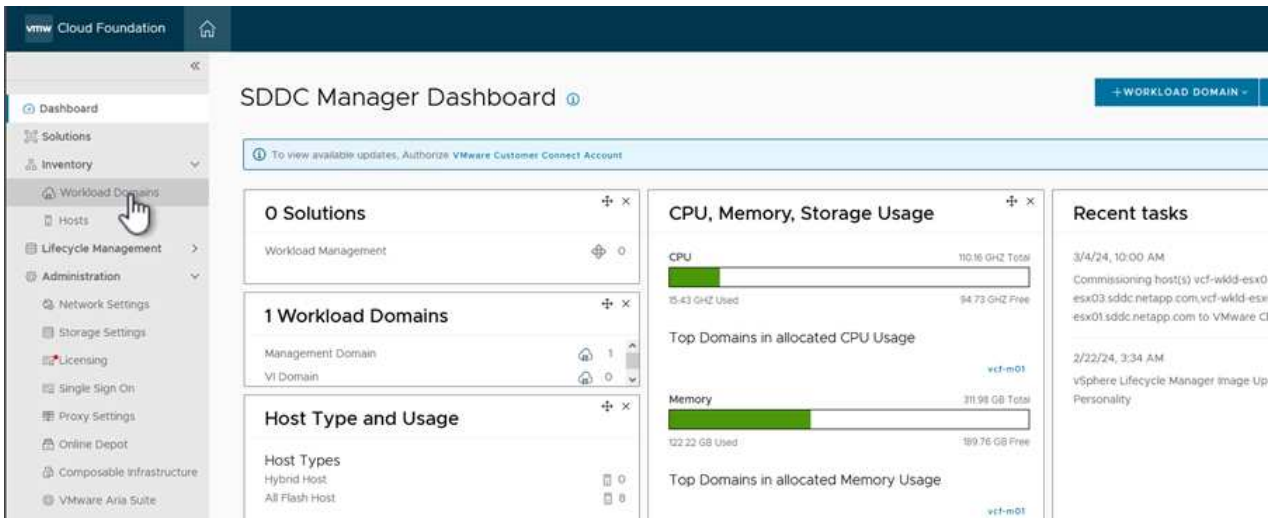
COMMISSION

Déployez VI Workload Domain

Le déploiement de domaines de workloads VI s'effectue à l'aide de l'interface VCF Cloud Manager. Seules les étapes liées à la configuration du stockage seront présentées ici.

Pour obtenir des instructions détaillées sur le déploiement d'un domaine de charge de travail VI, reportez-vous à la section "[Déployez un domaine de charge de travail VI à l'aide de l'interface utilisateur SDDC Manager](#)".

1. Dans le tableau de bord SDDC Manager, cliquez sur **+ Workload Domain** dans le coin supérieur droit pour créer un nouveau Workload Domain.



2. Dans l'assistant Configuration VI, remplissez les sections **informations générales**, **Cluster**, **calcul**, **mise en réseau** et **sélection d'hôte** selon les besoins.

Pour plus d'informations sur le remplissage des informations requises dans l'assistant de configuration VI, reportez-vous à la section "[Déployez un domaine de charge de travail VI à l'aide de l'interface utilisateur SDDC Manager](#)".

VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

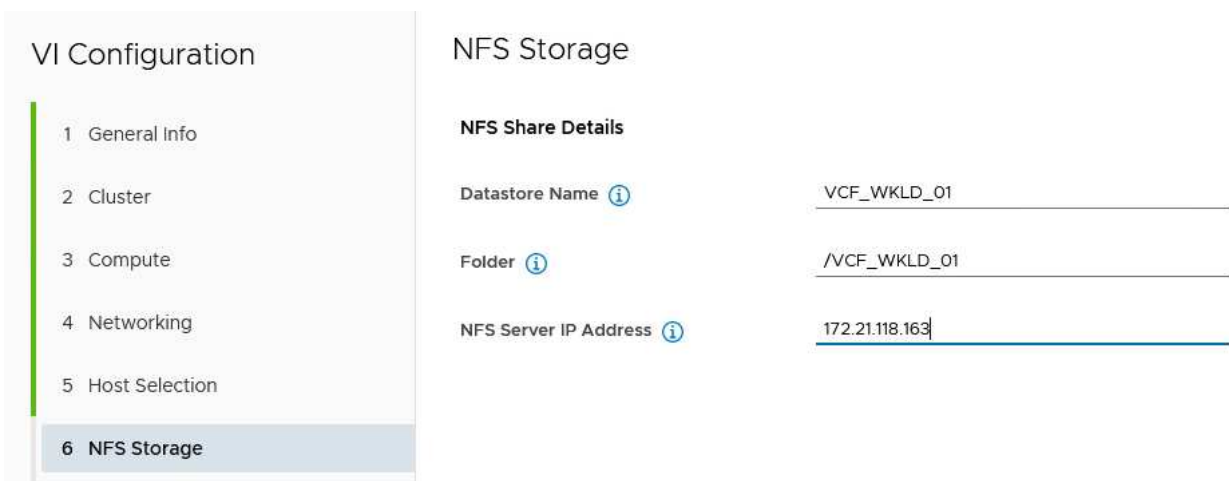
7 Switch Configuration

8 License

9 Review

+

1. Dans la section stockage NFS, indiquez le nom du datastore, le point de montage du dossier du volume NFS et l'adresse IP de la LIF de la machine virtuelle de stockage ONTAP NFS.



The screenshot shows the 'VI Configuration' interface with a sidebar on the left containing a list of steps: 1 General Info, 2 Cluster, 3 Compute, 4 Networking, 5 Host Selection, 6 NFS Storage (highlighted), 7 Switch Configuration, 8 License, and 9 Review. The main content area is titled 'NFS Storage' and contains a section for 'NFS Share Details' with three input fields:

| NFS Share Details | |
|-------------------------|----------------|
| Datastore Name ⓘ | VCF_WKLD_01 |
| Folder ⓘ | /VCF_WKLD_01 |
| NFS Server IP Address ⓘ | 172.21.118.163 |

2. Dans l'assistant de configuration VI, effectuez les étapes Configuration du commutateur et Licence, puis cliquez sur **Terminer** pour lancer le processus de création de domaine de charge de travail.

VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage
- 7 Switch Configuration
- 8 License
- 9 Review

Review

| General | |
|-----------------------------|--|
| Virtual Infrastructure Name | vcf-wkld-01 |
| Organization Name | it-inf |
| SSO Domain Option | Joining Management SSO Domain |
| Cluster | |
| Cluster Name | IT-INF-WKLD-01 |
| Compute | |
| vCenter IP Address | 172.21.166.143 |
| vCenter DNS Name | vcf-wkld-vc01.sddc.netapp.com |
| vCenter Subnet Mask | 255.255.255.0 |
| vCenter Default Gateway | 172.21.166.1 |
| Networking | |
| NSX Manager Instance Option | Creating new NSX instance |
| NSX Manager Cluster IP | 172.21.166.147 |
| NSX Manager Cluster FQDN | vcf-w01-nsxc101.sddc.netapp.com |
| NSX Manager IP Addresses | 172.21.166.144, 172.21.166.145, 172.21.166.146 |

CANCEL
BACK
FINISH

3. Surveiller le processus et résoudre tout problème de validation survenant au cours du processus.

Installation du plug-in NetApp NFS pour VMware VAAI

Le plug-in NetApp NFS pour VMware VAAI intègre les bibliothèques de disques virtuels VMware installées sur l'hôte VMware ESXi et assure des opérations de clonage plus performantes, plus rapides. Il s'agit d'une procédure recommandée lors de l'utilisation de systèmes de stockage ONTAP avec VMware vSphere.

Pour obtenir des instructions détaillées sur le déploiement du plug-in NetApp NFS pour VMware VAAI, suivez les instructions indiquées à l'adresse "[Installation du plug-in NetApp NFS pour VMware VAAI](#)".

Vidéo de démonstration de cette solution

[Datastores NFS en tant que stockage principal pour les domaines de charge de travail VCF](#)

Utilisez les outils ONTAP pour configurer le stockage supplémentaire (NFS et vVols) pour les domaines de charge de travail VCF

Dans ce scénario, nous allons montrer comment déployer et utiliser les outils ONTAP pour VMware vSphere pour configurer à la fois un datastore **NFS** et un datastore **vVols** pour un domaine de charge de travail VCF.

NFS est utilisé comme protocole de stockage pour le datastore vVols.

Auteur: Josh Powell, Ravi BCB

Présentation du scénario

Ce scénario couvre les étapes générales suivantes :

- Créez un SVM (Storage Virtual machine) avec des interfaces logiques (LIF) pour le trafic NFS.
- Créez un port group distribué pour le réseau NFS sur le domaine de charge de travail VI.
- Créez un adaptateur vmkernel pour NFS sur les hôtes ESXi pour le domaine de charge de travail VI.
- Déployez les outils ONTAP sur le domaine de charge de travail VI.
- Créez un datastore NFS sur le domaine de charge de travail VI.
- Créez un nouveau datastore vVols sur le domaine de la charge de travail VI.

Prérequis

Ce scénario nécessite les composants et configurations suivants :

- Un système de stockage ONTAP AFF doté de ports de données physiques sur des commutateurs ethernet dédiés au trafic de stockage.
- Le déploiement du domaine de gestion VCF est terminé et le client vSphere est accessible.
- Un domaine de charge de travail VI a déjà été déployé.

NetApp recommande un réseau redondant pour NFS, offrant une tolérance aux pannes pour les systèmes de stockage, les switches, les adaptateurs réseau et les systèmes hôtes. Il est courant de déployer NFS avec un ou plusieurs sous-réseaux, selon les exigences architecturales.

Reportez-vous à la section "[Meilleures pratiques pour l'exécution de NFS avec VMware vSphere](#)" Pour obtenir des informations détaillées spécifiques à VMware vSphere.

Pour obtenir des conseils réseau sur l'utilisation de ONTAP avec VMware vSphere, reportez-vous au "[Configuration réseau - NFS](#)" De la documentation des applications d'entreprise NetApp.

Cette documentation décrit le processus de création d'un SVM et de spécification des informations d'adresse IP pour créer plusieurs LIFs pour le trafic NFS. Pour ajouter de nouvelles LIFs à un SVM existant, voir "[Créer une LIF \(interface réseau\)](#)".

Étapes de déploiement

Pour déployer les outils ONTAP et les utiliser pour créer un datastore vVols et NFS sur le domaine de gestion VCF, effectuez les opérations suivantes :

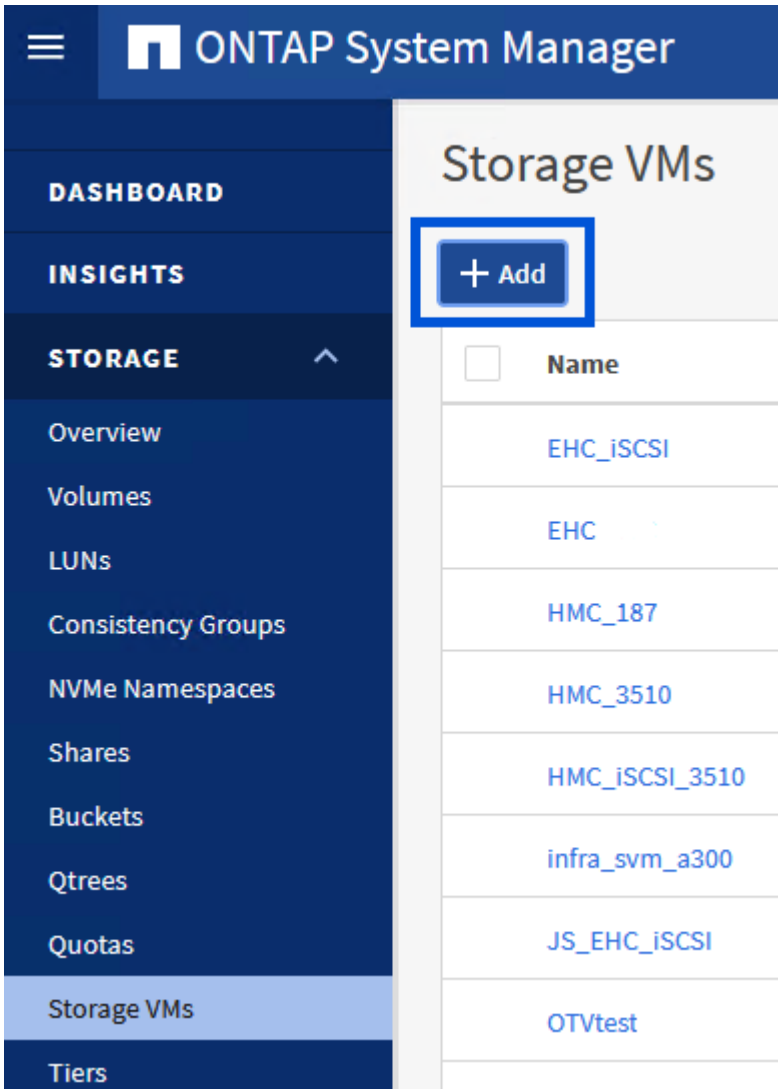
Créez un SVM et des LIF sur un système de stockage ONTAP

L'étape suivante s'effectue dans ONTAP System Manager.

Créez la VM de stockage et les LIF

Effectuer les étapes suivantes pour créer un SVM avec plusieurs LIF pour le trafic NFS.

1. Dans le Gestionnaire système ONTAP, accédez à **Storage VMs** dans le menu de gauche et cliquez sur **+ Add** pour démarrer.



2. Dans l'assistant **Add Storage VM**, indiquez un **Name** pour le SVM, sélectionnez **IP Space**, puis, sous **Access Protocol**, cliquez sur l'onglet **SMB/CIFS, NFS, S3** et cochez la case **Enable NFS**.

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default


Access Protocol

SMB/CIFS, NFS, S3 [iSCSI](#) [FC](#) [NVMe](#)

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



Il n'est pas nécessaire de cliquer ici sur le bouton **Autoriser l'accès client NFS** car les outils ONTAP pour VMware vSphere seront utilisés pour automatiser le processus de déploiement du datastore. Cela inclut l'accès client pour les hôtes ESXi. Et no 160 ;

3. Dans la section **interface réseau**, remplissez les champs **adresse IP**, **masque de sous-réseau** et **domaine de diffusion et Port** pour la première LIF. Pour les LIF suivantes, la case à cocher peut être activée pour utiliser des paramètres communs à toutes les LIF restantes ou pour utiliser des paramètres distincts.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

- Indiquez si vous souhaitez activer le compte Storage VM Administration (pour les environnements en colocation) et cliquez sur **Save** pour créer le SVM.

Storage VM Administration

Manage administrator account

Save

Cancel

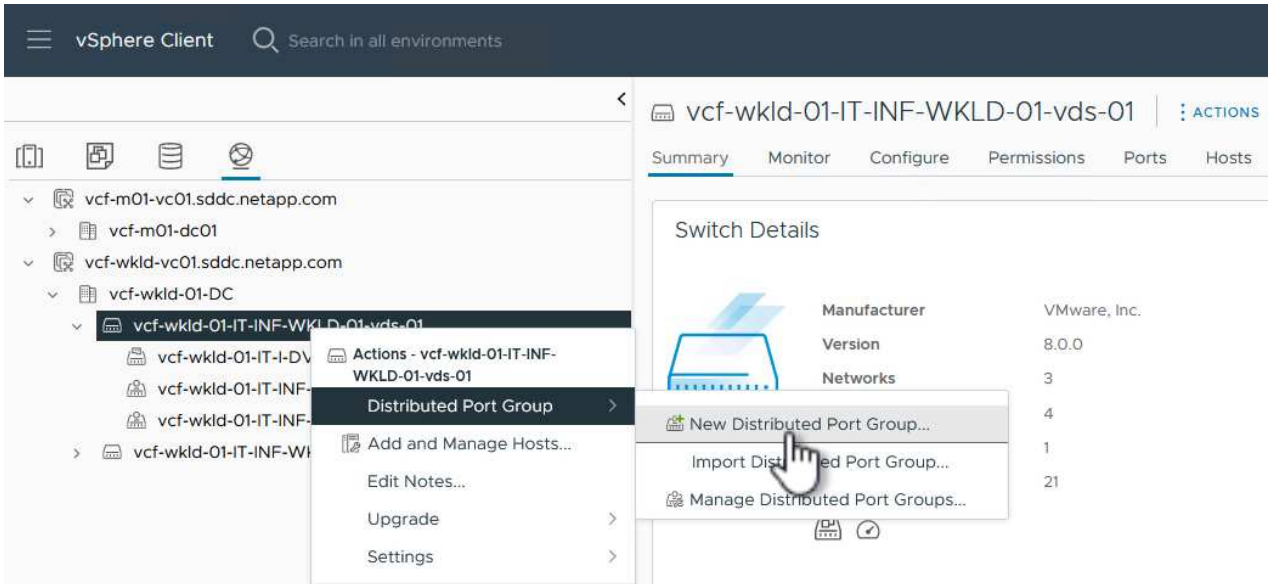
Configuration de la mise en réseau pour NFS sur les hôtes ESXi

Les étapes suivantes sont effectuées sur le cluster VI Workload Domain à l'aide du client vSphere. Dans ce cas, l'authentification unique vCenter est utilisée, de sorte que le client vSphere est commun aux domaines de gestion et de charge de travail.

Créez un Port Group distribué pour le trafic NFS

Pour créer un nouveau groupe de ports distribués pour le réseau qui transporte le trafic NFS, procédez comme suit :

1. Dans le client vSphere , accédez à **Inventory > Networking** pour le domaine de charge de travail. Naviguez jusqu'au commutateur distribué existant et choisissez l'action pour créer **Nouveau groupe de ports distribués....**



2. Dans l'assistant **Nouveau groupe de ports distribués**, entrez un nom pour le nouveau groupe de ports et cliquez sur **Suivant** pour continuer.
3. Sur la page **configurer les paramètres**, remplissez tous les paramètres. Si des VLAN sont utilisés, assurez-vous de fournir l'ID de VLAN correct. Cliquez sur **Suivant** pour continuer.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

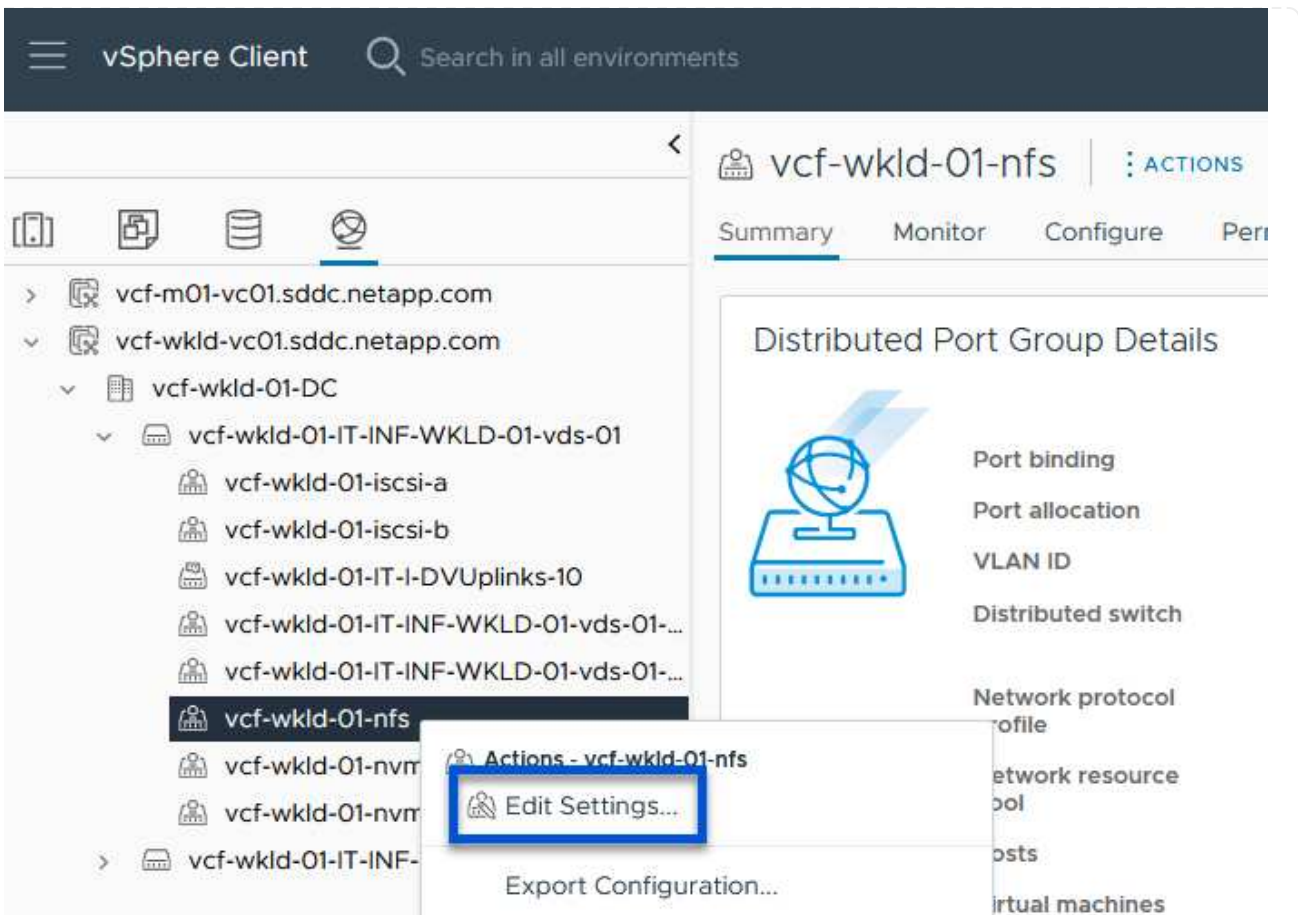
| | |
|---|------------------------|
| Port binding | Static binding |
| Port allocation | Elastic ? |
| Number of ports | 8 |
| Network resource pool | (default) |
| VLAN | |
| VLAN type | VLAN |
| VLAN ID | 3374 |
| Advanced | |
| <input type="checkbox"/> Customize default policies configuration | |

CANCEL

BACK

NEXT

4. Sur la page **prêt à terminer**, passez en revue les modifications et cliquez sur **Terminer** pour créer le nouveau groupe de ports distribués.
5. Une fois le groupe de ports créé, naviguez jusqu'au groupe de ports et sélectionnez l'action **Modifier les paramètres....**



6. Sur la page **Distributed Port Group - Edit Settings**, accédez à **Teaming and failover** dans le menu de gauche. Activez l'agrégation pour les liaisons montantes à utiliser pour le trafic NFS en vous assurant qu'elles sont regroupées dans la zone **Active uplinks**. Déplacez toutes les liaisons ascendantes inutilisées vers le bas jusqu'à **uplinks non utilisés**.

Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 

MOVE UP MOVE DOWN

Active uplinks

 uplink2

 uplink1

Standby uplinks

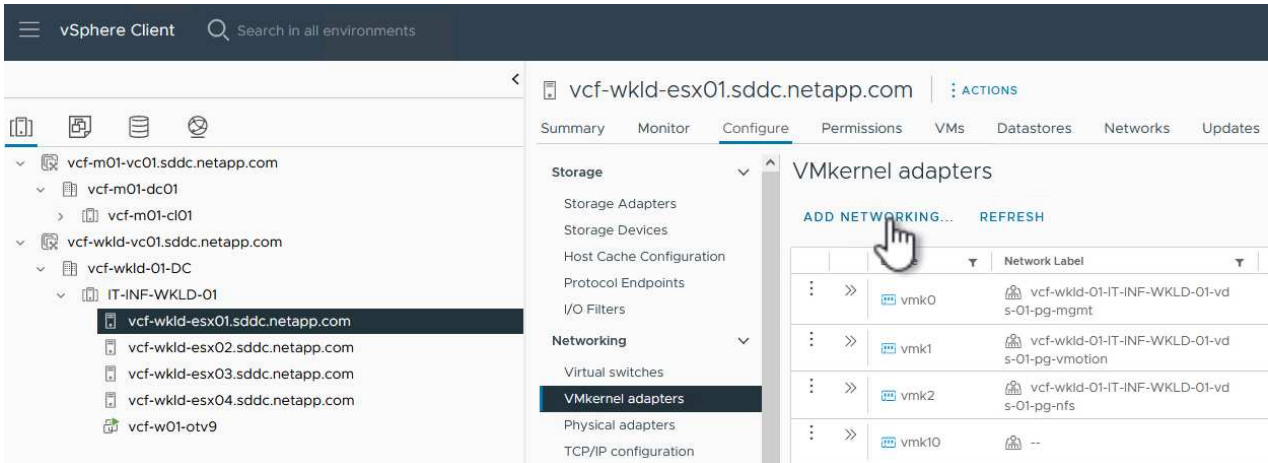
Unused uplinks

7. Répétez ce processus pour chaque hôte ESXi du cluster.

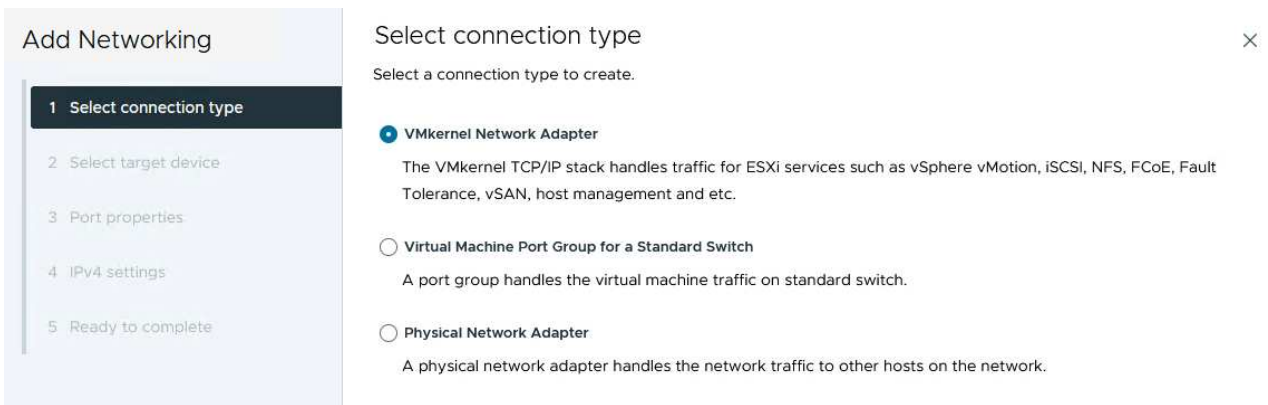
Créez un adaptateur VMkernel sur chaque hôte ESXi

Répétez ce processus sur chaque hôte ESXi du domaine de charge de travail.

1. À partir du client vSphere, accédez à l'un des hôtes ESXi de l'inventaire du domaine de charge de travail. Dans l'onglet **configurer**, sélectionnez **adaptateurs VMkernel** et cliquez sur **Ajouter réseau...** pour démarrer.



2. Dans la fenêtre **Select connection type**, choisissez **VMkernel Network adapter** et cliquez sur **Next** pour continuer.



3. Sur la page **Sélectionner le périphérique cible**, choisissez l'un des groupes de ports distribués pour NFS créés précédemment.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

| | Name | NSX Port Group ID | Distributed Switch |
|----------------------------------|--|-------------------|-----------------------------------|
| <input type="radio"/> | vcf-wkld-01-iscsi-a | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-iscsi-b | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-02 |
| <input type="radio"/> | vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input checked="" type="radio"/> | vcf-wkld-01-nfs | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-nvme-a | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |
| <input type="radio"/> | vcf-wkld-01-nvme-b | -- | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |

Manage Columns 8 items

CANCEL

BACK

NEXT

4. Sur la page **Port properties**, conservez les valeurs par défaut (aucun service activé) et cliquez sur **Next** pour continuer.
5. Sur la page **IPv4 settings**, remplissez **adresse IP**, **masque de sous-réseau** et fournissez une nouvelle adresse IP de passerelle (uniquement si nécessaire). Cliquez sur **Suivant** pour continuer.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address 172.21.118.145

Subnet mask 255.255.255.0

Default gateway Override default gateway for this adapter

172.21.166.1

DNS server addresses 10.61.185.231

CANCEL

BACK

NEXT

6. Consultez vos sélections sur la page **prêt à terminer** et cliquez sur **Terminer** pour créer l'adaptateur VMkernel.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete ✕

Review your selections before finishing the wizard

▼ **Select target device**

| | |
|------------------------|-----------------------------------|
| Distributed port group | vcf-wkld-01-nfs |
| Distributed switch | vcf-wkld-01-IT-INF-WKLD-01-vds-01 |

▼ **Port properties**

| | |
|-------------------------|---|
| New port group | vcf-wkld-01-nfs (vcf-wkld-01-IT-INF-WKLD-01-vds-01) |
| MTU | 9000 |
| vMotion | Disabled |
| Provisioning | Disabled |
| Fault Tolerance logging | Disabled |
| Management | Disabled |
| vSphere Replication | Disabled |
| vSphere Replication NFC | Disabled |
| vSAN | Disabled |
| vSAN Witness | Disabled |
| vSphere Backup NFC | Disabled |
| NVMe over TCP | Disabled |

CANCEL **BACK** **FINISH**

Déployer et utiliser les outils ONTAP pour configurer le stockage

Les étapes suivantes sont effectuées sur le cluster de domaine de gestion VCF à l'aide du client vSphere et impliquent le déploiement d'OTV, la création d'un datastore NFS vVols et la migration des machines virtuelles de gestion vers le nouveau datastore.

Pour les domaines de charge de travail VI, OTV est installé sur le cluster de gestion VCF, mais enregistré avec vCenter associé au domaine de charge de travail VI.

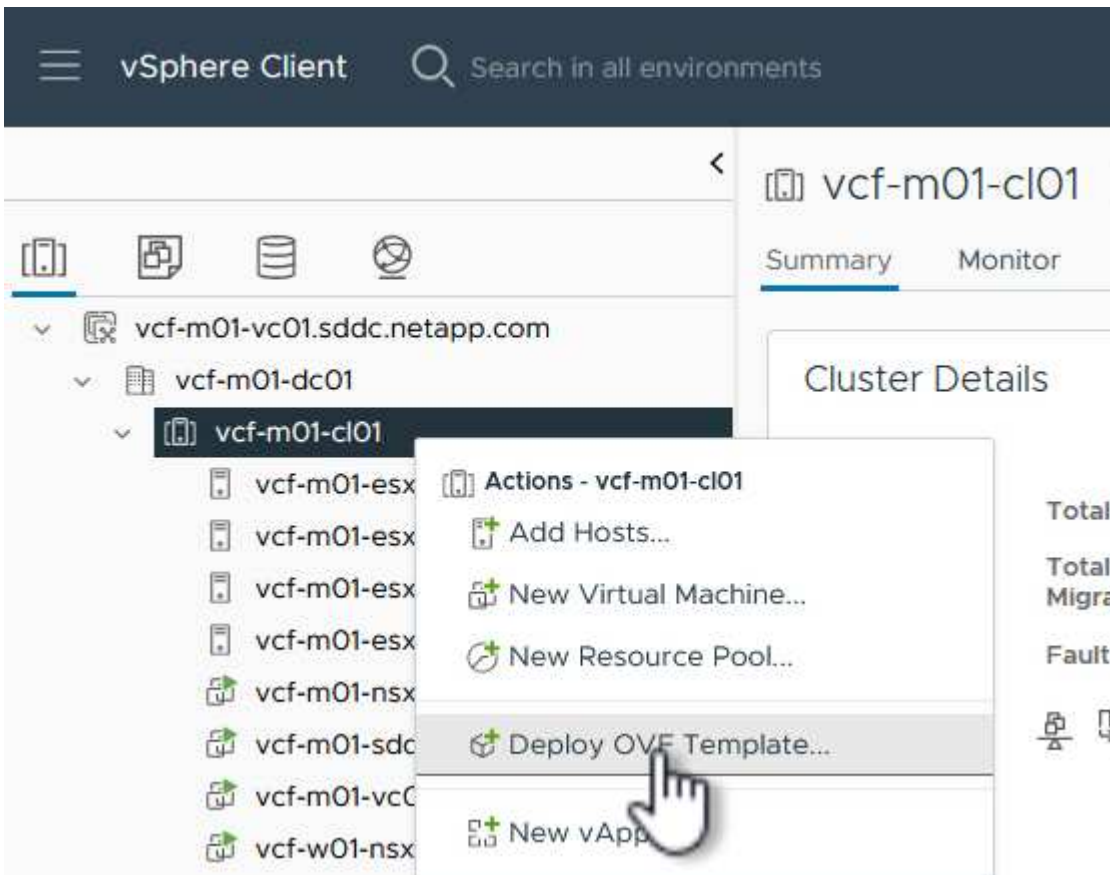
Pour plus d'informations sur le déploiement et l'utilisation des outils ONTAP dans un environnement à plusieurs serveurs vCenter, reportez-vous à la section ["Conditions requises pour l'enregistrement des outils ONTAP dans un environnement de plusieurs serveurs vCenter"](#).

Déployez les outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere (OTV) sont déployés en tant qu'appliance de machine virtuelle et fournissent une interface utilisateur vCenter intégrée pour la gestion du stockage ONTAP.

Procédez comme suit pour déployer les outils ONTAP pour VMware vSphere :

1. Obtenir l'image OVA des outils ONTAP à partir du "[Site de support NetApp](#)" et télécharger dans un dossier local.
2. Connectez-vous à l'appliance vCenter pour le domaine de gestion VCF.
3. Dans l'interface de l'appliance vCenter, cliquez avec le bouton droit de la souris sur le cluster de gestion et sélectionnez **déployer le modèle OVF...**



4. Dans l'assistant **déployer modèle OVF**, cliquez sur le bouton radio **fichier local** et sélectionnez le fichier OVA des outils ONTAP téléchargé à l'étape précédente.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Pour les étapes 2 à 5 de l'assistant, sélectionnez un nom et un dossier pour la machine virtuelle, sélectionnez la ressource de calcul, vérifiez les détails et acceptez le contrat de licence.
6. Pour l'emplacement de stockage des fichiers de configuration et des fichiers disque, sélectionnez le datastore VSAN du cluster du domaine de gestion VCF.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

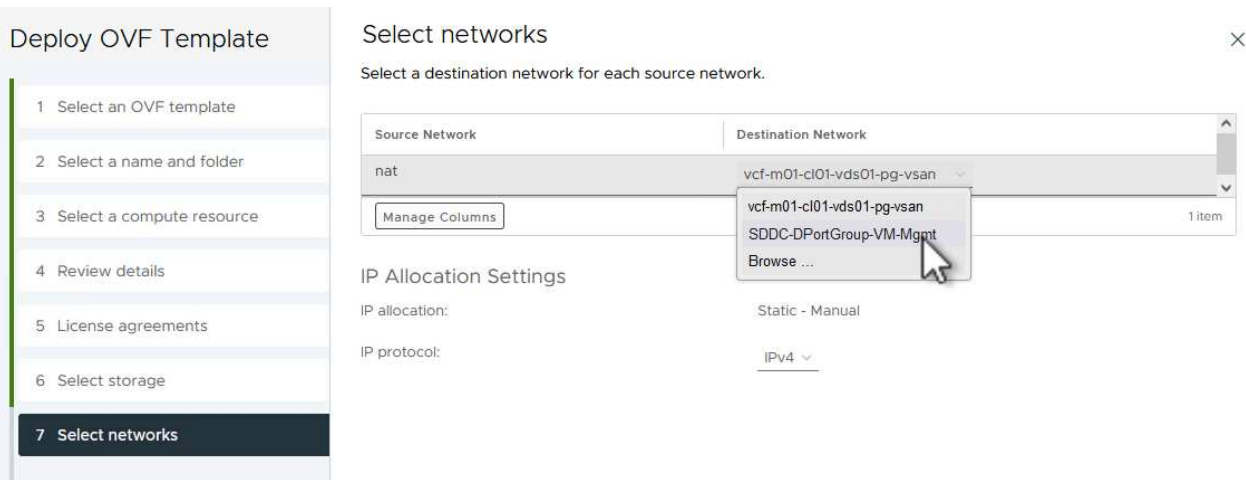
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

| | Name | Storage Compatibility | Capacity | Provisioned | Free | T |
|----------------------------------|-------------------------------------|-----------------------|-----------|-------------|-----------|---|
| <input checked="" type="radio"/> | vcf-m01-c01-ds-vsant01 | -- | 999.97 GB | 7.17 TB | 225.72 GB | v |
| <input type="radio"/> | vcf-m01-esx01-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx02-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx03-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |
| <input type="radio"/> | vcf-m01-esx04-esx-install-datastore | -- | 25.75 GB | 4.56 GB | 21.19 GB | v |

Manage Columns Items per page 10 5 items

7. Sur la page Sélectionner le réseau, sélectionnez le réseau utilisé pour le trafic de gestion.



8. Sur la page Personnaliser le modèle, remplissez toutes les informations requises :

- Mot de passe à utiliser pour l'accès administratif à OTV.
- Adresse IP du serveur NTP.
- Mot de passe du compte de maintenance OTV.
- Mot de passe OTV Derby DB.
- Ne cochez pas la case **Activer VMware Cloud Foundation (VCF)**. Le mode VCF n'est pas requis pour le déploiement de stockage supplémentaire.
- FQDN ou adresse IP de l'appliance vCenter pour le **VI Workload Domain**
- Informations d'identification pour l'appliance vCenter du **VI Workload Domain**
- Renseignez les champs de propriétés réseau requis.

Cliquez sur **Suivant** pour continuer.

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

! 2 properties have invalid values X

| System Configuration | | 4 settings |
|--------------------------------------|--|----------------------|
| Application User Password (*) | Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character. | |
| | Password | 👁 |
| | Confirm Password | 👁 |
| NTP Servers | A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1 | |
| Maintenance User Password (*) | Password to assign to maint user account. | |
| | Password | 👁 |
| | Confirm Password | 👁 |

Deploy OVF Template

- 1 Select an OVF template
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template**
- 9 Ready to complete

Customize template

! 2 properties have invalid values X

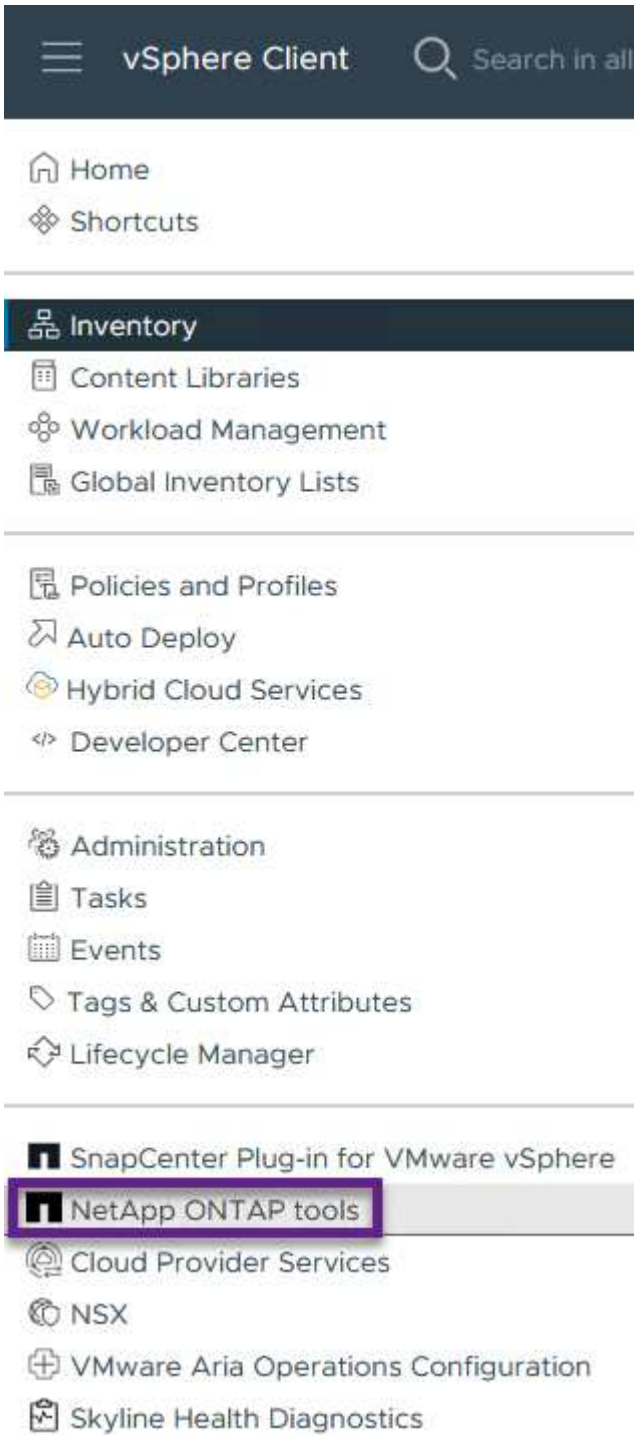
| Configure vCenter or Enable vCF | | 3 settings |
|---|--|----------------------|
| Enable VMware Cloud Foundation (VCF) | vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/> | |
| vCenter Server Address (*) | Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com | |
| Port (*) | Specify the HTTPS port of an existing vCenter to register to. 443 | |
| Username (*) | Specify the username of an existing vCenter to register to. administrator@vsphere.local | |
| Password (*) | Specify the password of an existing vCenter to register to. | |
| | Password | 👁 |
| | Confirm Password | 👁 |
| Network Properties | | 8 settings |
| Host Name | Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9 | |
| IP Address | Specify the IP address for the appliance. (Leave blank if DHCP is desired) | |

CANCEL BACK NEXT

9. Passez en revue toutes les informations de la page prêt à terminer et cliquez sur Terminer pour commencer à déployer l'appliance OTV.

Ajoutez un système de stockage aux outils ONTAP.

1. Accédez aux outils NetApp ONTAP en les sélectionnant dans le menu principal du client vSphere.



2. Dans le menu déroulant **INSTANCE** de l'interface de l'outil ONTAP, sélectionnez l'instance OTV associée au domaine de charge de travail à gérer.

NetApp ONTAP tools INSTANCE 172.21.166.139:8443 ▾

| Plugin Instance | Version | vCenter Server |
|---------------------|--------------|-------------------------------|
| 172.21.166.139:8443 | 9.13.0.36905 | vcf-m01-vc01.sddc.netapp.com |
| 172.21.166.149:8443 | 9.13.0.36905 | vcf-wkld-vc01.sddc.netapp.com |

3. Dans Outils ONTAP, sélectionnez **systèmes de stockage** dans le menu de gauche, puis appuyez sur **Ajouter**.


NetApp ONTAP tools INSTANCE 172.21.166.149:8443 ▾


Storage Systems

ADD **REDISCOVER ALL**

4. Indiquez l'adresse IP, les informations d'identification du système de stockage et le numéro de port. Cliquez sur **Ajouter** pour lancer le processus de découverte.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server vcf-m01-vc01.sddc.netapp.com 

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options 

ONTAP Cluster Certificate: Automatically fetch Manually upload

CANCEL

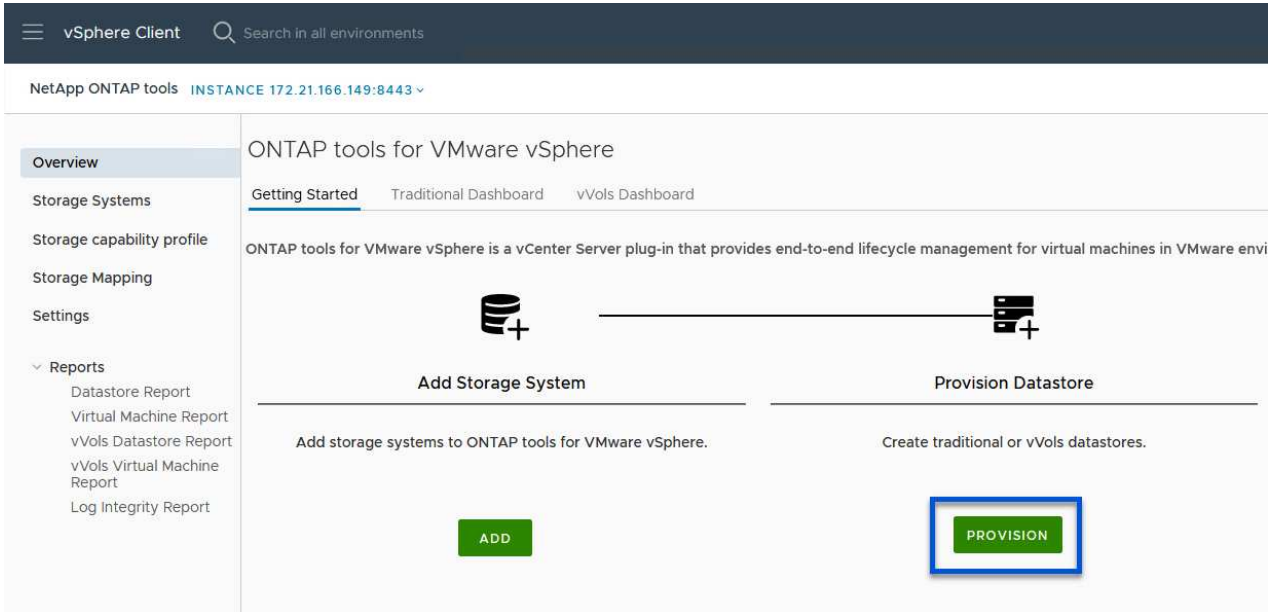
SAVE & ADD MORE

ADD

Créez un datastore NFS dans les outils ONTAP

Procédez comme suit pour déployer un datastore ONTAP, exécuté sur NFS, à l'aide des outils ONTAP.

1. Dans Outils ONTAP, sélectionnez **Présentation** et dans l'onglet **mise en route**, cliquez sur **Provision** pour démarrer l'assistant.



The screenshot shows the vSphere Client interface for ONTAP tools. The top navigation bar includes 'vSphere Client' and a search bar. Below the navigation bar, the instance name 'NetApp ONTAP tools' and 'INSTANCE 172.21.166.149:8443' are displayed. The main content area is titled 'ONTAP tools for VMware vSphere' and features a 'Getting Started' tab. A descriptive text states: 'ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi'. Two main actions are presented: 'Add Storage System' with an 'ADD' button, and 'Provision Datastore' with a 'PROVISION' button. The 'PROVISION' button is highlighted with a blue rectangular box.

2. Sur la page **général** de l'assistant Nouveau datastore, sélectionnez le centre de données vSphere ou la destination du cluster. Sélectionnez **NFS** comme type de datastore, indiquez un nom pour le datastore et sélectionnez le protocole. Vous pouvez choisir d'utiliser ou non les volumes FlexGroup et un fichier de capacité de stockage pour le provisionnement. Cliquez sur **Suivant** pour continuer.

Remarque : la sélection de **distribuer les données du datastore à travers le cluster** crée le volume sous-jacent en tant que volume FlexGroup qui empêche l'utilisation des profils de capacité de stockage. Reportez-vous à la section "[Configurations prises en charge et non prises en charge pour les volumes FlexGroup](#)" Pour en savoir plus sur l'utilisation de FlexGroup volumes.

New Datastore


1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision. 

Provisioning destination: [BROWSE](#)

Type: NFS VMFS vVols

Name:

Size:

Protocol: NFS 3 NFS 4.1

Distribute datastore data across the ONTAP cluster.

Use storage capability profile for provisioning

Advanced options >

CANCEL

NEXT

3. Sur la page **système de stockage**, sélectionner le profil de capacité de stockage, le système de stockage et le SVM. Cliquez sur **Suivant** pour continuer.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profile:

Storage system:

Storage VM:

4. Sur la page **attributs de stockage**, sélectionnez l'agrégat à utiliser, puis cliquez sur **Suivant** pour continuer.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Aggregate:

Volumes:

Advanced options >

5. Enfin, passez en revue le **Résumé** et cliquez sur Terminer pour commencer à créer le datastore NFS.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary**

Summary

General

| | |
|-----------------------------|-------------------------------|
| vCenter server: | vcf-wkld-vc01.sddc.netapp.com |
| Provisioning destination: | vcf-wkld-01-DC |
| Datastore name: | VCF_WKLD_05_NFS |
| Datastore size: | 2 TB |
| Datastore type: | NFS |
| Protocol: | NFS 3 |
| Datastore cluster: | None |
| Storage capability profile: | Platinum_AFF_A |

Storage system details

| | |
|-----------------|-------------------|
| Storage system: | ntaphci-a300e9u25 |
| SVM: | VCF_NFS |

Storage attributes

| | |
|------------|-----------|
| Aggregate: | FHC_Agr02 |
|------------|-----------|

CANCEL

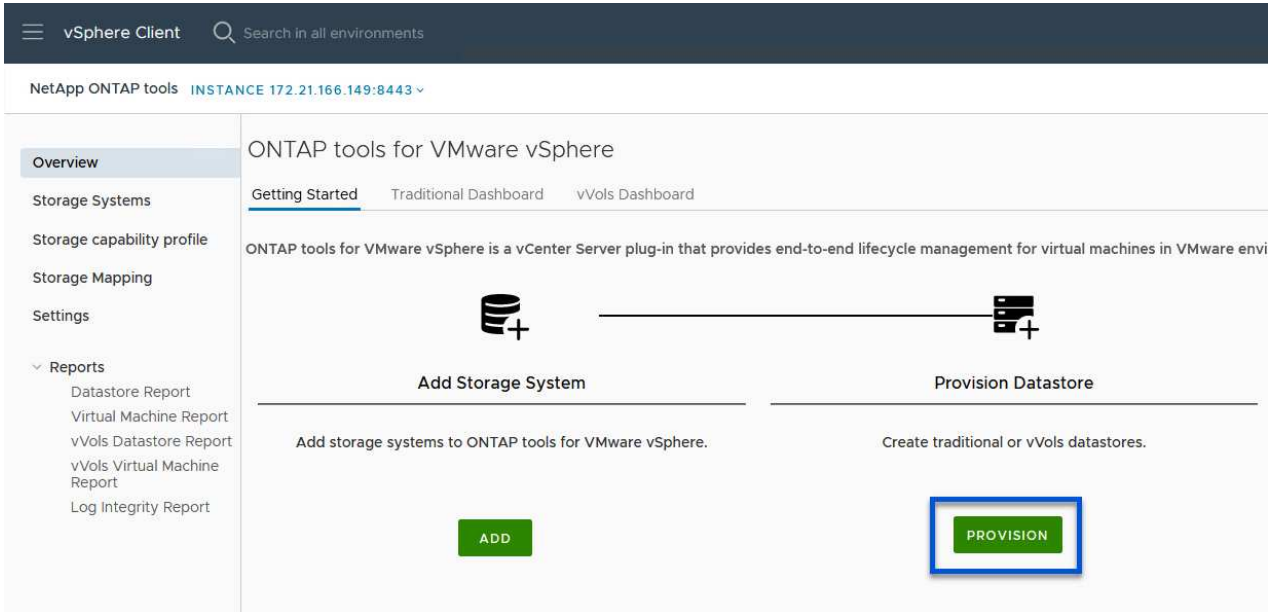
BACK

FINISH

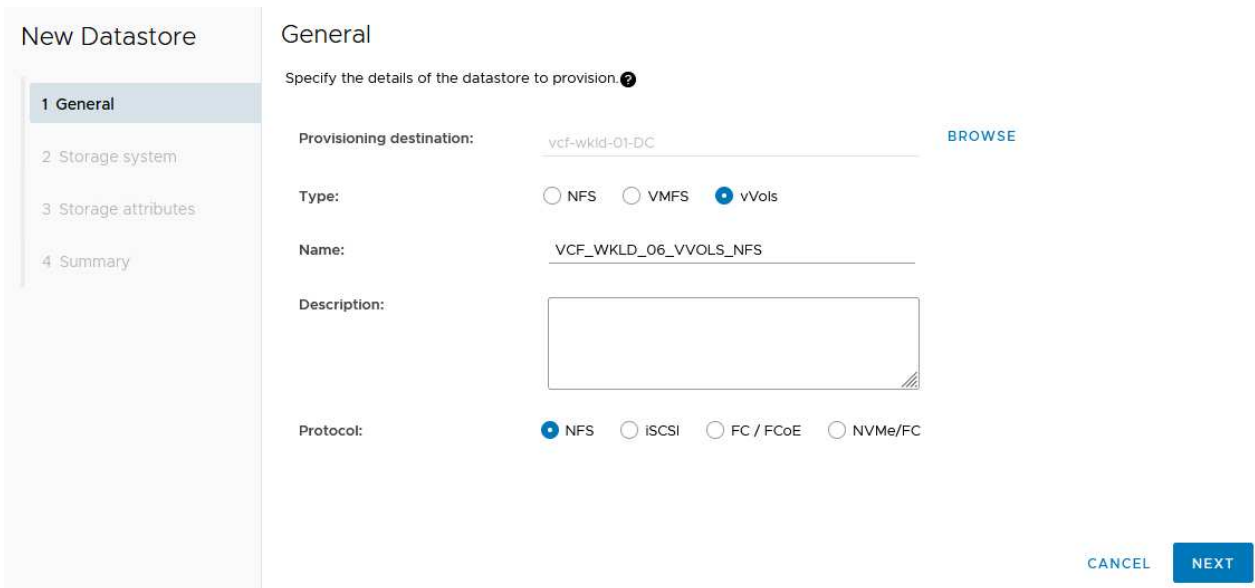
Créer un datastore vVols dans les outils ONTAP

Pour créer un datastore vVols dans les outils ONTAP, procédez comme suit :

1. Dans Outils ONTAP, sélectionnez **Présentation** et dans l'onglet **mise en route**, cliquez sur **Provision** pour démarrer l'assistant.



2. Sur la page **général** de l'assistant Nouveau datastore, sélectionnez le centre de données vSphere ou la destination du cluster. Sélectionnez **vVols** comme type de datastore, indiquez un nom pour le datastore et sélectionnez **NFS** comme protocole. Cliquez sur **Suivant** pour continuer.



3. Sur la page **système de stockage**, sélectionner le profil de capacité de stockage, le système de stockage et le SVM. Cliquez sur **Suivant** pour continuer.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

| | | |
|-----------------------------|---------------------------------|---|
| Storage capability profile: | Platinum_AFF_A | ▼ |
| Storage system: | ntaphci-a300e9u25 (172.16.9.25) | ▼ |
| Storage VM: | VCF_NFS | ▼ |

4. Sur la page **attributs de stockage**, sélectionnez pour créer un nouveau volume pour le datastore et remplissez les attributs de stockage du volume à créer. Cliquez sur **Ajouter** pour créer le volume, puis sur **Suivant** pour continuer.

| Name | Size(GB) ⓘ | Storage capability profile | Aggregates | Space reserve |
|------------------------|------------|----------------------------|-------------------------|---------------|
| <u>vcf_wkld_06_vvc</u> | 2000 | Platinum_AFF_A | EHCaggr02 - (25404 GB I | Thin |

ADD

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

| Name | Size | Storage Capability Profile | Aggregate |
|-------------------|---------|----------------------------|-----------|
| vcf_wkld_06_vvols | 2000 GB | Platinum_AFF_A | EHCaggr02 |

1 - 1 of 1 Item

| Name | Size(GB) ⓘ | Storage capability profile | Aggregates | Space reserve |
|------|------------|----------------------------|-------------------------|---------------|
| | | Platinum_AFF_A | EHCaggr02 - (25407.15 G | Thin |

ADD

Default storage capability profile: Platinum_AFF_A

CANCEL

BACK

NEXT

5. Enfin, passez en revue le **Résumé** et cliquez sur **Terminer** pour lancer le processus de création du datastore vVol.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

General

vCenter server: vcf-wkld-vc01.sddc.netapp.com

Provisioning destination: vcf-wkld-01-DC

Datastore name: VCF_WKLD_06_VVOLS_NFS

Datastore type: vVols

Protocol: NFS

Storage capability profile: Platinum_AFF_A

Storage system details

Storage system: ntaphci-a300e9u25

SVM: EHC_NFS

Storage attributes

| New FlexVol Name | New FlexVol Size | Aggregate | Storage Capability Profile |
|------------------|------------------|-----------|----------------------------|
| | | | |

CANCEL
BACK
FINISH

Informations supplémentaires

Pour plus d'informations sur la configuration des systèmes de stockage ONTAP, reportez-vous au ["Documentation ONTAP 9"](#) centre.

Pour plus d'informations sur la configuration de VCF, reportez-vous à la section ["Documentation de VMware Cloud Foundation"](#).

Migration de machines virtuelles

Migrez vos machines virtuelles vers les datastores ONTAP

Auteur: Suresh Thoppay

VMware vSphere by Broadcom prend en charge les datastores VMFS, NFS et vVol pour l'hébergement de machines virtuelles. Les clients ont la possibilité de créer ces datastores avec des infrastructures hyperconvergées ou avec des systèmes de stockage partagé centralisés. Les clients voient souvent les avantages de l'hébergement sur des systèmes de stockage ONTAP : snapshots et clones compacts des machines virtuelles, flexibilité de choisir différents modèles de déploiement dans les data centers et les clouds, efficacité opérationnelle grâce à des outils de surveillance et d'alerte, sécurité, gouvernance et outils de conformité facultatifs pour l'inspection des données des machines virtuelles. etc.

Les machines virtuelles hébergées sur des datastores ONTAP peuvent être protégées à l'aide du plug-in SnapCenter pour VMware vSphere (SCV). SCV crée des snapshots basés sur le stockage et effectue également des répliquions sur le système de stockage ONTAP distant. Les restaurations peuvent être réalisées à partir de systèmes de stockage primaires ou secondaires.

Les clients ont la possibilité de choisir les opérations Cloud Insights ou Aria, ou de combiner les deux outils ou d'autres outils tiers qui utilisent l'api ONTAP pour le dépannage, la surveillance des performances, le reporting et les fonctionnalités de notification d'alertes.

Les clients peuvent facilement provisionner un datastore à l'aide du plug-in vCenter Outils ONTAP ou de son API et de ses VM peuvent être migrés vers des datastores ONTAP, même lorsqu'il est sous tension.



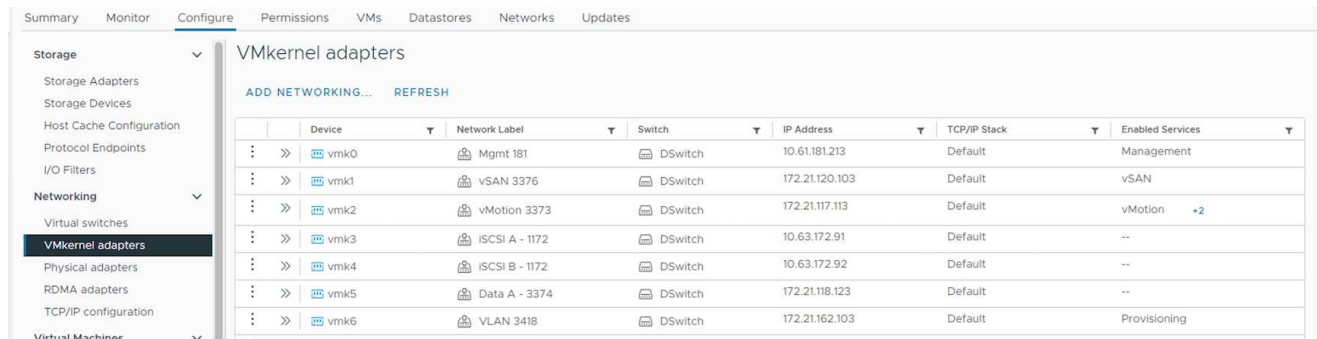
Certaines machines virtuelles déployées avec un outil de gestion externe tel qu'Aria Automation, Tanzu (ou toute autre version de Kubernetes) dépendent généralement des règles de stockage des machines virtuelles. Si la migration entre les datastores se fait au sein d'une même stratégie de stockage de machine virtuelle, son impact sur les applications devrait être moindre. Renseignez-vous auprès des propriétaires d'applications pour migrer correctement ces machines virtuelles vers le nouveau datastore. Introduction de vSphere 8 "[Notification VMotion](#)"
Pour préparer l'application pour vMotion.

Configuration réseau requise

Migration des machines virtuelles avec vMotion

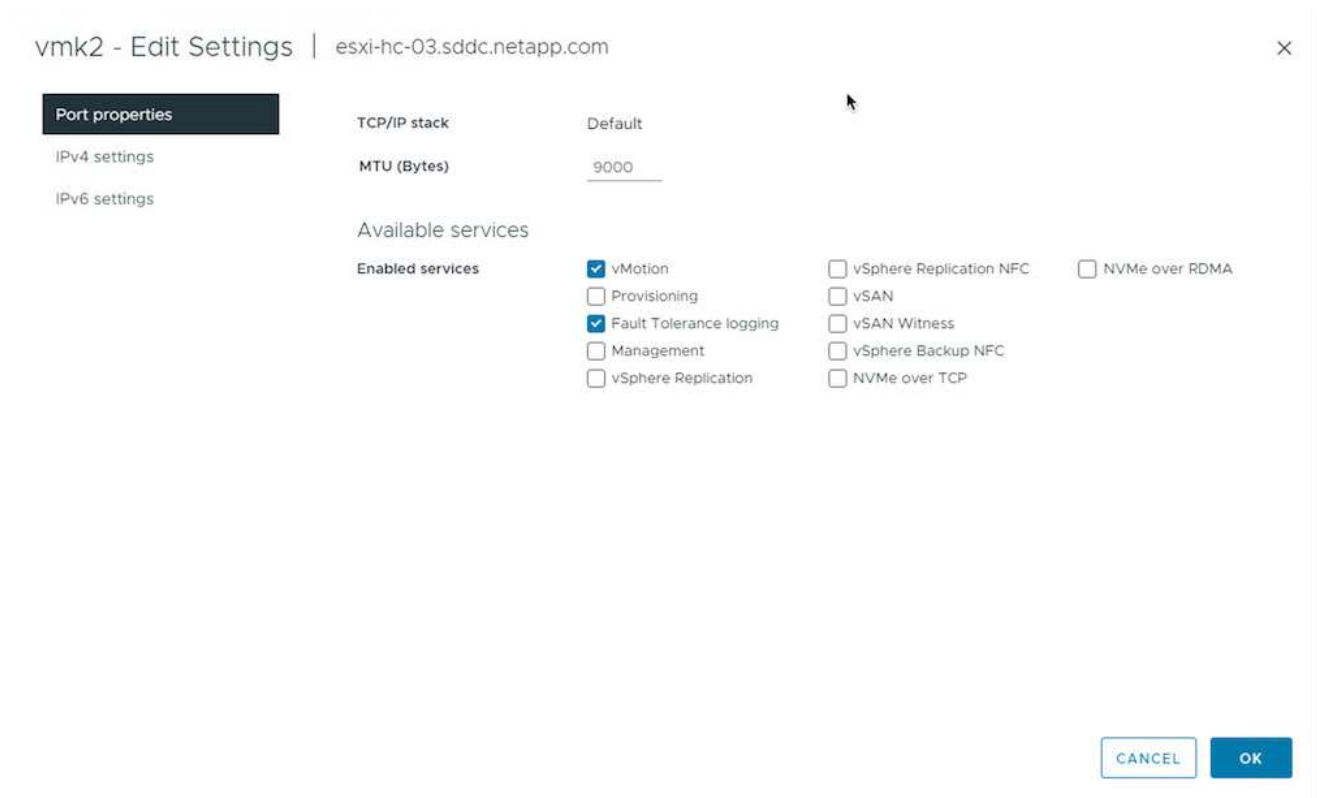
On suppose que le réseau de stockage double est déjà en place pour le datastore ONTAP afin d'assurer la connectivité, la tolérance aux pannes et l'optimisation des performances.

La migration des machines virtuelles sur les hôtes vSphere est également gérée par l'interface VMKernel de l'hôte vSphere. Pour la migration à chaud (optimisée sur des machines virtuelles), l'interface VMKernel avec le service compatible vMotion est utilisée et, pour la migration à froid (hors machines virtuelles), l'interface VMKernel avec le service de provisionnement activé est utilisée pour le déplacement des données. Si aucune interface valide n'a été trouvée, elle utilise l'interface de gestion pour déplacer les données qui peuvent ne pas être souhaitables pour certaines utilisations.



| Device | Network Label | Switch | IP Address | TCP/IP Stack | Enabled Services |
|--------|----------------|---------|----------------|--------------|------------------|
| vmk0 | Mgmt 181 | DSwitch | 10.61.181.213 | Default | Management |
| vmk1 | vSAN 3376 | DSwitch | 172.21.120.103 | Default | vSAN |
| vmk2 | vMotion 3373 | DSwitch | 172.21.117.113 | Default | vMotion +2 |
| vmk3 | iSCSI A - 1172 | DSwitch | 10.63.172.91 | Default | -- |
| vmk4 | iSCSI B - 1172 | DSwitch | 10.63.172.92 | Default | -- |
| vmk5 | Data A - 3374 | DSwitch | 172.21.118.123 | Default | -- |
| vmk6 | VLAN 3418 | DSwitch | 172.21.162.103 | Default | Provisioning |

Lorsque vous modifiez l'interface VMKernel, voici l'option permettant d'activer les services requis.



vmk2 - Edit Settings | esxi-hc-03.sddc.netapp.com

Port properties

IPv4 settings

IPv6 settings

TCP/IP stack: Default

MTU (Bytes): 9000

Available services

Enabled services

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN
- vSAN Witness
- vSphere Backup NFC
- NVMe over TCP
- NVMe over RDMA

CANCEL OK



Assurez-vous qu'au moins deux cartes réseau de liaison montante active haut débit sont disponibles pour le groupe de ports utilisé par les interfaces vMotion et VMkernel de provisionnement.

Scénarios de migration VM

VMotion est souvent utilisé pour migrer les machines virtuelles, quel que soit leur état d'alimentation. Vous trouverez ci-dessous d'autres considérations et une procédure de migration pour des scénarios spécifiques.



Comprendre "[Conditions des VM et limitations de vSphere vMotion](#)" Avant de procéder à toute option de migration de VM.

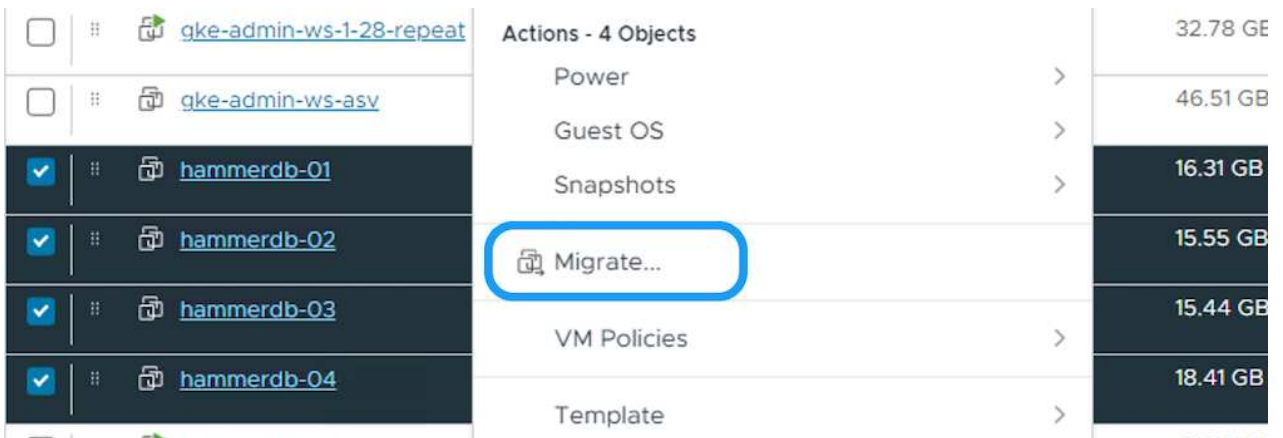
Migration des machines virtuelles à partir d'un datastore vSphere spécifique

Suivez la procédure ci-dessous pour migrer des machines virtuelles vers un nouveau datastore à l'aide de l'interface utilisateur.

1. Avec le client Web vSphere, sélectionnez le datastore dans l'inventaire du stockage et cliquez sur l'onglet VM.



2. Sélectionnez les machines virtuelles à migrer et cliquez avec le bouton droit de la souris pour sélectionner l'option migrer.



3. Choisissez l'option permettant de modifier uniquement le stockage, puis cliquez sur Suivant

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Sélectionnez la stratégie de stockage VM souhaitée et choisissez le datastore compatible. Cliquez sur Suivant.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NetApp Storage

Disable Storage DRS for this virtual machine

| Name | Storage Compatibility | Capacity | Provisioned | Free | T |
|--|-----------------------|----------|-------------|-----------|---|
| <input checked="" type="radio"/> ASA_VVOLS_1 | Compatible | 1.95 TB | 34.38 GB | 1.95 TB | |
| <input type="radio"/> DemoDS | Incompatible | 800 GB | 7.23 GB | 792.77 GB | N |
| <input type="radio"/> destination | Incompatible | 250 GB | 31.8 MB | 249.97 GB | N |
| <input type="radio"/> DRaaSTest | Incompatible | 1 TB | 201.13 GB | 880.86 GB | N |
| <input type="radio"/> E13A400_JCSI | Incompatible | 2 TB | 858.66 GB | 1.85 TB | \ |

Manage Columns Items per page 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Vérifiez et cliquez sur Terminer.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

×

Verify that the information is correct and click Finish to start the migration.

| | |
|-------------------|---|
| Migration Type | Change storage. Leave VM on the original compute resource |
| Virtual Machine | Migrating 4 VMs |
| Storage | ASA_VVOLS_1 |
| VM storage policy | NetApp Storage |
| Disk Format | Thin Provision |

CANCEL

BACK

FINISH

Pour migrer des machines virtuelles à l'aide de PowerCLI, voici l'exemple de script.


```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

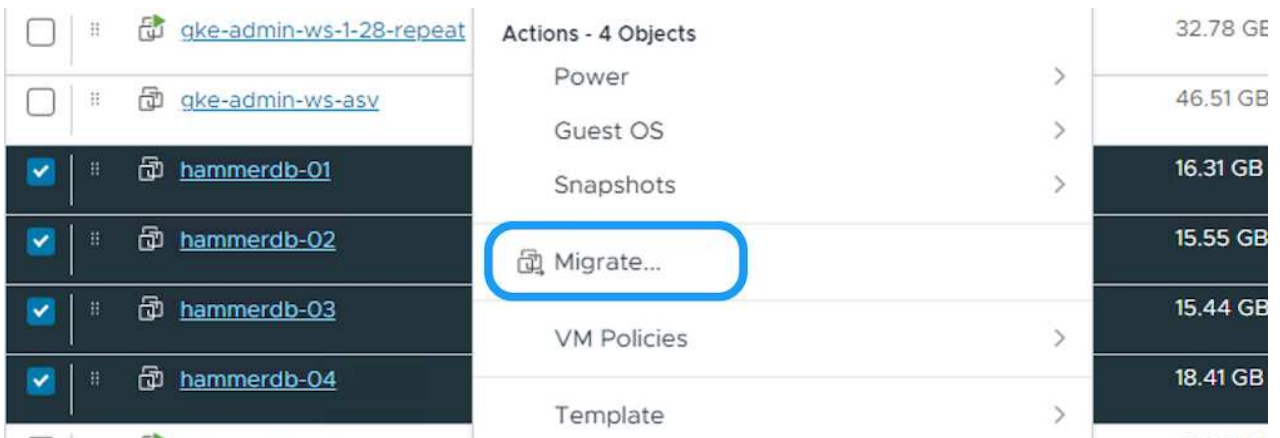
Migration de machines virtuelles dans le même cluster vSphere

Suivez la procédure ci-dessous pour migrer des machines virtuelles vers un nouveau datastore à l'aide de l'interface utilisateur.

1. Avec vSphere Web client, sélectionnez le cluster dans l'inventaire des hôtes et des clusters et cliquez sur l'onglet VM.



2. Sélectionnez les machines virtuelles à migrer et cliquez avec le bouton droit de la souris pour sélectionner l'option migrer.



3. Choisissez l'option permettant de modifier uniquement le stockage, puis cliquez sur Suivant

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Sélectionnez la stratégie de stockage VM souhaitée et choisissez le datastore compatible. Cliquez sur Suivant.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

[BATCH CONFIGURE](#) [CONFIGURE PER DISK](#)

Select virtual disk format

VM Storage Policy

Disable Storage DRS for this virtual machine

| | Name | Storage Compatibility | Capacity | Provisioned | Free | T |
|----------------------------------|--------------|-----------------------|----------|-------------|-----------|---|
| <input checked="" type="radio"/> | ASA_VVOLS_1 | Compatible | 1.95 TB | 34.38 GB | 1.95 TB | |
| <input type="radio"/> | DemoDS | Incompatible | 800 GB | 7.23 GB | 792.77 GB | N |
| <input type="radio"/> | destination | Incompatible | 250 GB | 31.8 MB | 249.97 GB | N |
| <input type="radio"/> | DRaaSTest | Incompatible | 1 TB | 201.13 GB | 880.86 GB | N |
| <input type="radio"/> | E13A400_JCSI | Incompatible | 2 TB | 858.66 GB | 1.85 TB | \ |

Manage Columns Items per page: 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Vérifiez et cliquez sur Terminer.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

×

Verify that the information is correct and click Finish to start the migration.

| | |
|-------------------|---|
| Migration Type | Change storage. Leave VM on the original compute resource |
| Virtual Machine | Migrating 4 VMs |
| Storage | ASA_VVOLS_1 |
| VM storage policy | NetApp Storage |
| Disk Format | Thin Provision |

CANCEL

BACK

FINISH

Pour migrer des machines virtuelles à l'aide de PowerCLI, voici l'exemple de script.

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```



Lorsque le cluster de datastores est utilisé avec DRS (Dynamic Resource Scheduling) de stockage entièrement automatisé et que les deux datastores (source et cible) sont du même type (VMFS/NFS/vVol), conservez les deux datastores dans le même cluster de stockage et migrez les VM depuis le datastore source en activant le mode de maintenance sur la source. L'expérience sera similaire au traitement des hôtes de calcul à des fins de maintenance.

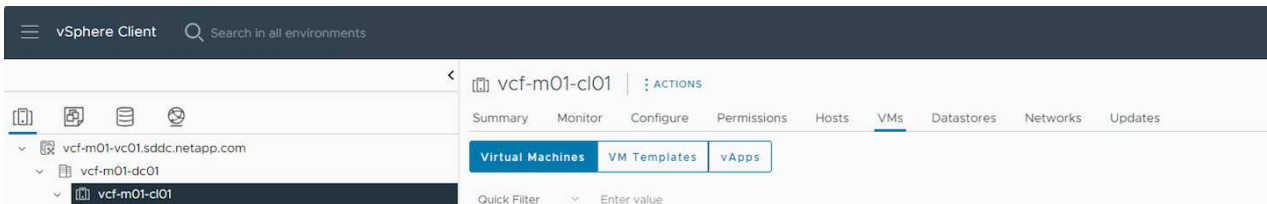
Migration des machines virtuelles sur plusieurs clusters vSphere



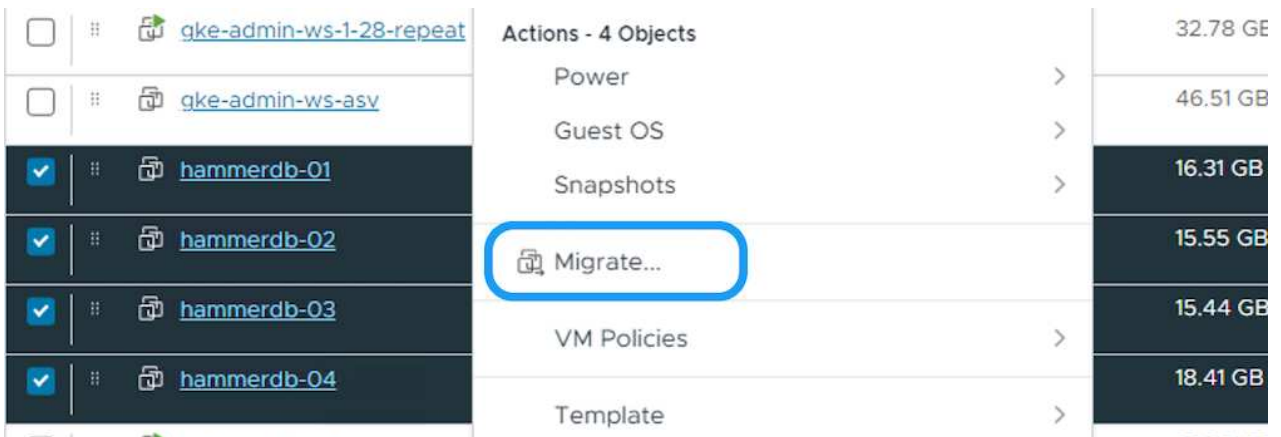
Reportez-vous à "[Compatibilité CPU et compatibilité vSphere Enhanced vMotion](#)" Lorsque les hôtes source et cible sont d'une famille ou d'un modèle de processeur différent.

Suivez la procédure ci-dessous pour migrer des machines virtuelles vers un nouveau datastore à l'aide de l'interface utilisateur.

1. Avec vSphere Web client, sélectionnez le cluster dans l'inventaire des hôtes et des clusters et cliquez sur l'onglet VM.



2. Sélectionnez les machines virtuelles à migrer et cliquez avec le bouton droit de la souris pour sélectionner l'option migrer.



3. Choisissez une option pour modifier les ressources de calcul et de stockage, puis cliquez sur Suivant

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Naviguez dans le cluster et choisissez celui qu'il vous faut pour migrer.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼  vcf-m01-vc01.sddc.netapp.com
 - >  vcf-m01-dc01
- ▼  vcf-wkld-vc01.sddc.netapp.com
 - ▼  vcf-wkld-01-DC
 - >  IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Sélectionnez la stratégie de stockage VM souhaitée et choisissez le datastore compatible. Cliquez sur Suivant.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage**
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision

VM Storage Policy NFS

| | Name | Storage Compatibility | Capacity | Provisioned | Free | |
|----------------------------------|--------------------------------------|-----------------------|----------|-------------|----------|--|
| <input checked="" type="radio"/> | VCF_WKLD_01 | Compatible | 5 TB | 5.91 GB | 5 TB | |
| <input type="radio"/> | VCF_WKLD_02_VVOLS | Incompatible | 2.93 TB | 18 MB | 2.93 TB | |
| <input type="radio"/> | VCF_WKLD_03_ISCSI | Incompatible | 3 TB | 858.61 GB | 2.85 TB | |
| <input type="radio"/> | vcf-wkld-esx01-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB | |
| <input type="radio"/> | vcf-wkld-esx02-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB | |
| <input type="radio"/> | vcf-wkld-esx03-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB | |

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Sélectionnez le dossier VM pour placer les VM cibles.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder**
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

vcf-wkld-01-DC

Discovered virtual machine

vCLS

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

7. Sélectionnez le groupe de ports cible.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks**
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

| Source Network | Used By | Destination Network |
|----------------------------|----------------------------|----------------------------------|
| >> SDDC-DPortGroup-VM-Mgmt | 4 VMs / 4 Network adapters | vcf-wkld-01-IT-INF-WKLD-01-vds-0 |

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Vérifiez et cliquez sur Terminer.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

| | |
|-------------------|---|
| Migration Type | Change storage. Leave VM on the original compute resource |
| Virtual Machine | Migrating 4 VMs |
| Storage | ASA_VVOLS_1 |
| VM storage policy | NetApp Storage |
| Disk Format | Thin Provision |

CANCEL

BACK

FINISH

Pour migrer des machines virtuelles à l'aide de PowerCLI, voici l'exemple de script.

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```

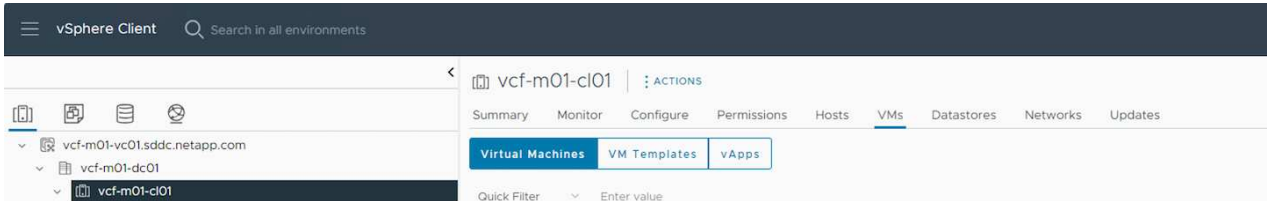
Migration des machines virtuelles sur les serveurs vCenter dans le même domaine SSO

Suivez la procédure ci-dessous pour migrer des machines virtuelles vers un nouveau serveur vCenter répertorié sur la même interface utilisateur du client vSphere.

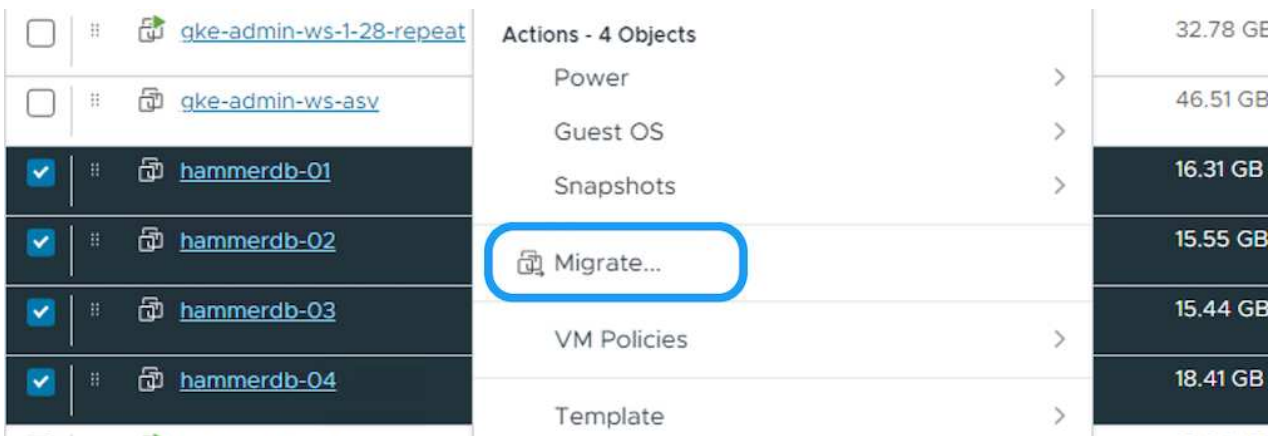


Pour connaître les exigences supplémentaires telles que les versions vCenter source et cible, etc., vérifiez "[Documentation vSphere sur les exigences relatives à vMotion entre instances de serveur vCenter](#)"

1. Avec vSphere Web client, sélectionnez le cluster dans l'inventaire des hôtes et des clusters et cliquez sur l'onglet VM.



2. Sélectionnez les machines virtuelles à migrer et cliquez avec le bouton droit de la souris pour sélectionner l'option migrer.



3. Choisissez une option pour modifier les ressources de calcul et de stockage, puis cliquez sur Suivant

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Sélectionnez le cluster cible dans le serveur vCenter cible.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ▼ vcf-wkld-vc01.sddc.netapp.com
 - ▼ vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Sélectionnez la stratégie de stockage VM souhaitée et choisissez le datastore compatible. Cliquez sur Suivant.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage**
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision

VM Storage Policy NFS

| | Name | Storage Compatibility | Capacity | Provisioned | Free | |
|----------------------------------|--------------------------------------|-----------------------|----------|-------------|----------|--|
| <input checked="" type="radio"/> | VCF_WKLD_01 | Compatible | 5 TB | 5.91 GB | 5 TB | |
| <input type="radio"/> | VCF_WKLD_02_VVOLS | Incompatible | 2.93 TB | 18 MB | 2.93 TB | |
| <input type="radio"/> | VCF_WKLD_03_ISCSI | Incompatible | 3 TB | 858.61 GB | 2.85 TB | |
| <input type="radio"/> | vcf-wkld-esx01-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB | |
| <input type="radio"/> | vcf-wkld-esx02-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB | |
| <input type="radio"/> | vcf-wkld-esx03-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB | |

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Sélectionnez le dossier VM pour placer les VM cibles.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder**
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

vcf-wkld-01-DC

Discovered virtual machine

vCLS

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

7. Sélectionnez le groupe de ports cible.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

| Source Network | Used By | Destination Network |
|---------------------------|----------------------------|----------------------------------|
| » SDDC-DPortGroup-VM-Mgmt | 4 VMs / 4 Network adapters | vcf-wkld-01-IT-INF-WKLD-01-vds-0 |

1 item

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Vérifiez les options de migration et cliquez sur Terminer.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

| | |
|-------------------|---|
| Migration Type | Change storage. Leave VM on the original compute resource |
| Virtual Machine | Migrating 4 VMs |
| Storage | ASA_VVOLS_1 |
| VM storage policy | NetApp Storage |
| Disk Format | Thin Provision |

CANCEL BACK FINISH

Pour migrer des machines virtuelles à l'aide de PowerCLI, voici l'exemple de script.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

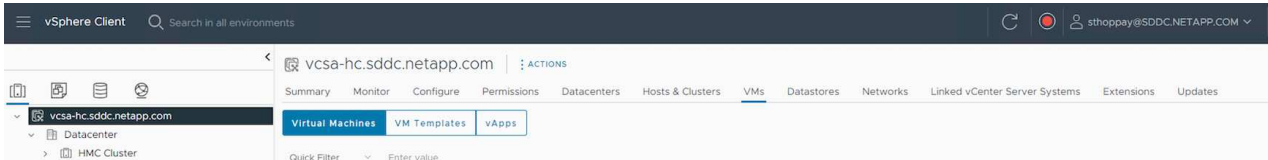
Migration des machines virtuelles entre les serveurs vCenter dans un domaine SSO différent



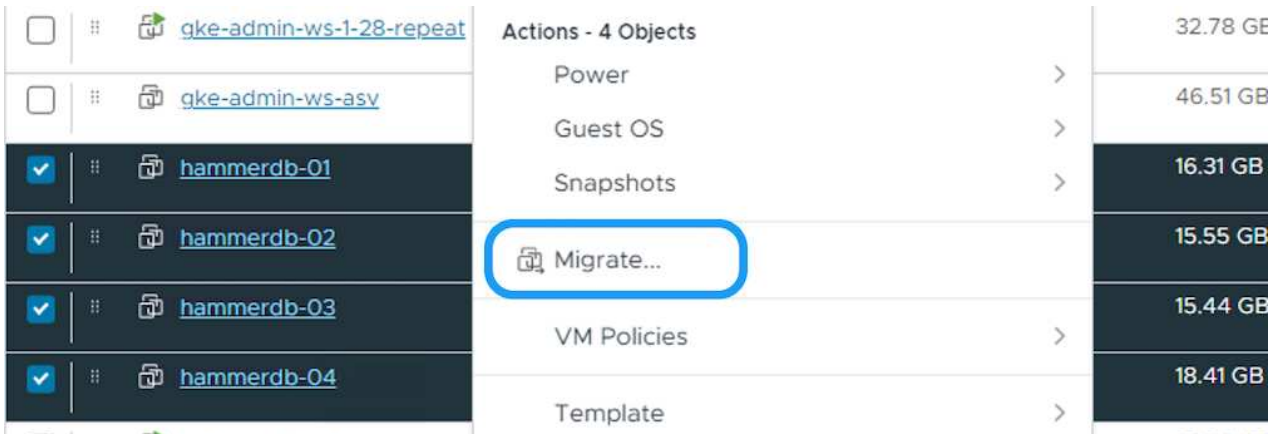
Ce scénario suppose que la communication existe entre les serveurs vCenter. Sinon, vérifiez le scénario d'emplacement de centre de données dans la liste ci-dessous. Pour connaître les conditions préalables, vérifiez "[Documentation vSphere sur Advanced Cross vCenter vMotion](#)"

Suivez la procédure ci-dessous pour migrer des machines virtuelles vers un serveur vCenter différent à l'aide de l'interface utilisateur.

1. Avec vSphere Web client, sélectionnez le serveur vCenter source et cliquez sur l'onglet VM.



2. Sélectionnez les machines virtuelles à migrer et cliquez avec le bouton droit de la souris pour sélectionner l'option migrer.



3. Choisissez l'option exportation Cross vCenter Server, puis cliquez sur Suivant

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only**
Migrate the virtual machines to another host or cluster.
- Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
 - Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL NEXT



La machine virtuelle peut également être importée depuis le serveur vCenter cible. Pour cette procédure, vérifiez "[Importation ou clonage d'une machine virtuelle avec Advanced Cross vCenter vMotion](#)"

4. Indiquez les informations d'identification vCenter et cliquez sur connexion.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

SAVED VCENTER SERVERS NEW VCENTER SERVER

vCenter Server address
vCenter Server FQDN or IP address

Username
example@domain.local

Password
Password

Save vCenter Server address ⓘ

LOGIN


CANCEL BACK NEXT

5. Confirmez et acceptez l'empreinte du certificat SSL du serveur vCenter

Security Alert ✕

Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:
17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

 Connect anyway?

Click Yes if you trust the vCenter Server.
Click No to cancel connecting to the vCenter Server.

6. Développez vCenter cible et sélectionnez le cluster de calcul cible.

Migrate | SQLSRV-05 ✕

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource**
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a compute resource ✕

Select a cluster, host, vApp or resource pool to run the virtual machines. VM ORIGIN ⓘ

- vcf-wkld-vc01.sddc.netapp.com
 - vcf-wkld-01-DC
 - IT-INF-WKLD-01**

Compatibility

✓ Compatibility checks succeeded.

7. Sélectionnez le datastore cible en fonction de la stratégie de stockage VM.

Migrate | SQLSRV-05

- Select a migration type
- Select a target vCenter Server
- Select a compute resource
- Select storage**
- Select folder
- Select networks
- Ready to complete

Select storage

Select the destination storage for the virtual machine migration. VM ORIGIN ⓘ

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

| | Name | Storage Compatibility | Capacity | Provisioned | Free |
|----------------------------------|--------------------------------------|-----------------------|----------|-------------|----------|
| <input checked="" type="radio"/> | VCF_WKLD_01 | Compatible | 5 TB | 5.93 GB | 5 TB |
| <input type="radio"/> | VCF_WKLD_02_VVOLS | Incompatible | 2.93 TB | 24 MB | 2.93 TB |
| <input type="radio"/> | VCF_WKLD_03_JSCSI | Incompatible | 3 TB | 1.35 TB | 2.59 TB |
| <input type="radio"/> | vcf-wkld-esx01-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB |
| <input type="radio"/> | vcf-wkld-esx02-esx-install-datastore | Incompatible | 25.75 GB | 3.68 GB | 22.07 GB |

Manage Columns | Items per page: 10 | 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

8. Sélectionnez le dossier VM cible.

Migrate | SQLSRV-05

- Select a migration type
- Select a target vCenter Server
- Select a compute resource
- Select storage
- Select folder**
- Select networks
- Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration. VM ORIGIN ⓘ

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - Discovered virtual machine
 - Oracle
 - SQL Server**
 - vCLS

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

9. Sélectionnez le groupe de ports VM pour chaque mappage de carte d'interface réseau.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration. VM ORIGIN ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

| Source Network | Used By | Destination Network |
|-----------------|----------------------------|-------------------------------------|
| » Mgmt 181 | 1 VMs / 1 Network adapters | vcf-wkld-01-IT-INF-WKLD-01-vds-01-p |
| » Data A - 3374 | 1 VMs / 1 Network adapters | vcf-wkld-01-iscsi-a |
| » Data B - 3375 | 1 VMs / 1 Network adapters | vcf-wkld-01-iscsi-b |

3 Items

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

10. Vérifiez et cliquez sur Terminer pour démarrer vMotion sur les serveurs vCenter.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration. VM ORIGIN ⓘ

| | |
|-------------------|---|
| Migration Type | Change compute resource and storage |
| Virtual Machine | SQLSRV-05 |
| vCenter | vcf-wkld-vc01.sddc.netapp.com |
| Folder | SQL Server |
| Cluster | IT-INF-WKLD-01 |
| Networks | Virtual network adapters from 3 networks will be reassigned to new destination networks |
| Storage | VCF_WKLD_01 |
| VM storage policy | NFS |
| Disk Format | Thin Provision |

CANCEL
BACK
FINISH

Pour migrer des machines virtuelles à l'aide de PowerCLI, voici l'exemple de script.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

Migration de machines virtuelles dans des data centers

- Lorsque le trafic de couche 2 est étendu entre les data centers à l'aide de la fédération NSX ou d'autres options, suivez la procédure de migration des machines virtuelles sur les serveurs vCenter.
- HCX fournit divers ["types de migration"](#) Y compris Replication Assisted vMotion dans les data centers pour déplacer les machines virtuelles sans temps d'indisponibilité.
- ["Site Recovery Manager \(SRM\)"](#) Est généralement destiné à la reprise sur incident et est souvent utilisé pour les migrations planifiées en utilisant la réplication basée sur des baies de stockage.
- Utilisation continue des produits de protection des données (CDP) ["vSphere API for IO \(VAIO\)"](#) Pour intercepter les données et envoyer une copie à un emplacement distant pour une solution RPO proche de zéro.
- Les produits de sauvegarde et de restauration peuvent également être utilisés. Mais elles entraînent souvent une durée de restauration plus longue.
- ["Reprise d'activité BlueXP en tant que service \(DRaaS\)"](#) Utilise la réplication basée sur les baies de stockage et automatise certaines tâches pour restaurer les VM sur le site cible.

Migration des machines virtuelles dans un environnement de cloud hybride

- ["Configurer le mode lié hybride"](#) et suivre la procédure de ["Migration des machines virtuelles sur les serveurs vCenter dans le même domaine SSO"](#)
- HCX fournit divers ["types de migration"](#) Y compris Replication Assisted vMotion dans les data centers pour déplacer la machine virtuelle lorsqu'elle est sous tension.
 - Lien [../ehc/aws-migrate-vmware-hcx.html](#) [TR 4942 : migration des workloads vers le datastore FSX ONTAP à l'aide de VMware HCX]
 - Lien [../ehc/azure-migrate-vmware-hcx.html](#) [TR-4940 : migration des workloads vers un datastore Azure NetApp Files à l'aide de VMware HCX - Guide de démarrage rapide]
 - Lien [../ehc/gcp-migrate-vmware-hcx.html](#) [migrer des workloads vers le datastore du service NetApp Cloud Volume sur Google Cloud VMware Engine à l'aide de VMware HCX - Guide de démarrage rapide]
- ["Reprise d'activité BlueXP en tant que service \(DRaaS\)"](#) Utilise la réplication basée sur les baies de stockage et automatise certaines tâches pour restaurer les VM sur le site cible.
- Avec les produits CDP (Continuous Data protection) pris en charge qui utilisent ["vSphere API for IO \(VAIO\)"](#) Pour intercepter les données et envoyer une copie à un emplacement distant pour une solution RPO proche de zéro.



Lorsque la VM source réside dans un datastore vVol bloc, elle peut être répliquée avec SnapMirror dans Amazon FSX pour NetApp ONTAP ou Cloud Volumes ONTAP (CVO) chez d'autres fournisseurs de cloud pris en charge et consommée en tant que volume iSCSI avec des VM cloud natives.

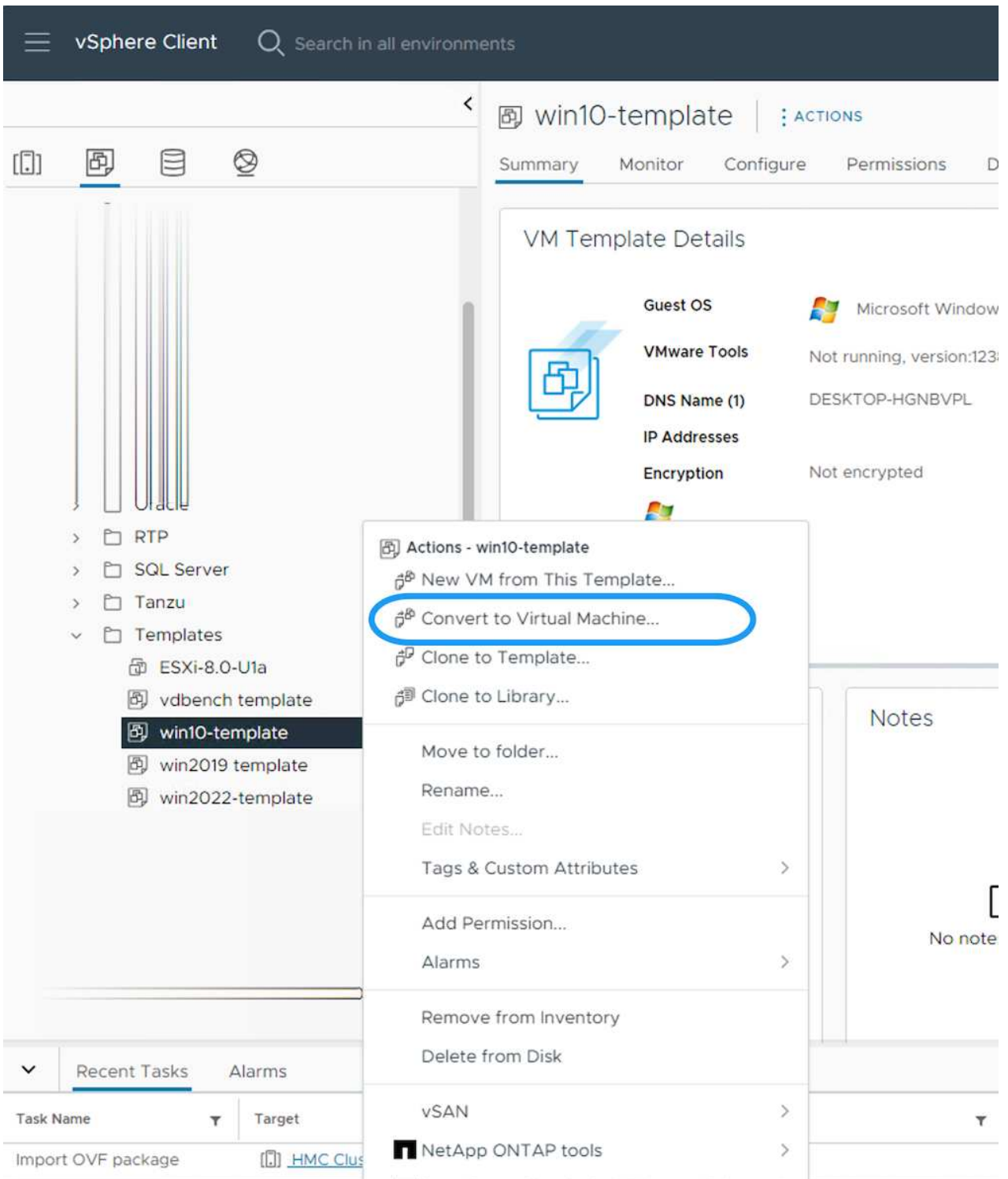
Scénarios de migration de modèles VM

Les modèles VM peuvent être gérés par vCenter Server ou par une bibliothèque de contenu. Distribution de modèles VM, de modèles OVF et OVA, d'autres types de fichiers sont gérés en les publiant dans une bibliothèque de contenu locale et les bibliothèques de contenu distantes peuvent s'y abonner.

- Les modèles de machine virtuelle stockés dans l'inventaire de vCenter peuvent être convertis en machine virtuelle et utiliser les options de migration de machine virtuelle.
- Les modèles OVF et OVA, les autres types de fichiers stockés dans la bibliothèque de contenu peuvent être clonés dans d'autres bibliothèques de contenu.
- Bibliothèque de contenu les modèles VM peuvent être hébergés sur n'importe quel datastore et doivent être ajoutés à la nouvelle bibliothèque de contenu.

Migration de modèles de machine virtuelle hébergés sur un datastore

1. Dans le client Web vSphere, cliquez avec le bouton droit de la souris sur le modèle de machine virtuelle dans la vue du dossier VM et Templates et sélectionnez l'option à convertir en machine virtuelle.



2. Une fois la conversion effectuée en tant que VM, suivez les options de migration VM.

Clonage d'éléments de la bibliothèque de contenu

1. Dans vSphere Web client, sélectionnez bibliothèques de contenu




 Home

 Shortcuts

 Inventory

 Content Libraries

 Workload Management

 Global Inventory Lists

 Policies and Profiles

 Auto Deploy

 Hybrid Cloud Services

 Developer Center

 Administration

 Tasks


 Events

 Tags & Custom Attributes

 Lifecycle Manager

 SnapCenter Plug-in for VMware vSphere

 NetApp ONTAP tools

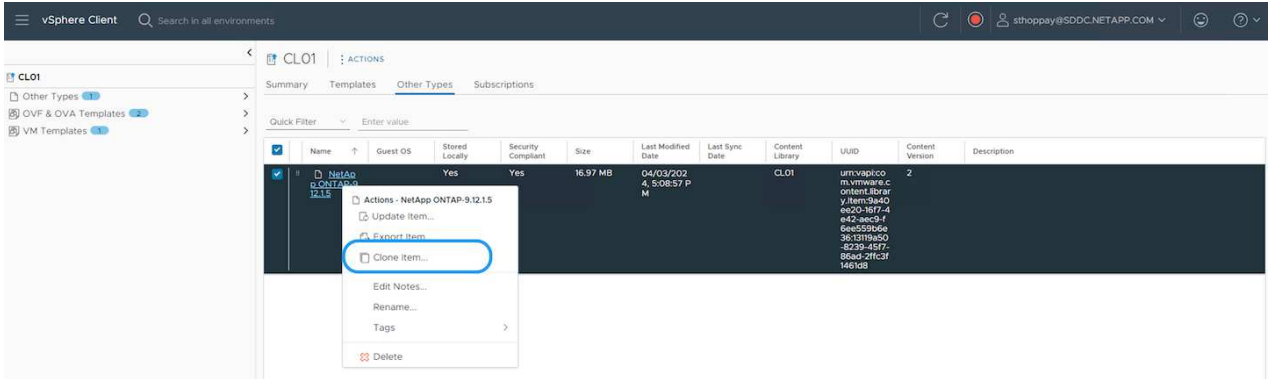
 Cloud Provider Services

 NSX

 VMware Aria Operations Configuration

 Skyline Health Diagnostics

2. Sélectionnez la bibliothèque de contenu dans laquelle vous souhaitez cloner l'élément
3. Cliquez avec le bouton droit de la souris sur l'élément et cliquez sur Cloner l'élément ..



Si vous utilisez le menu d'action, assurez-vous que l'objet cible correct est répertorié pour effectuer l'action.

4. Sélectionnez la bibliothèque de contenu cible et cliquez sur OK.

Clone Library Item | NetApp ONTAP-9.12.15 ✕

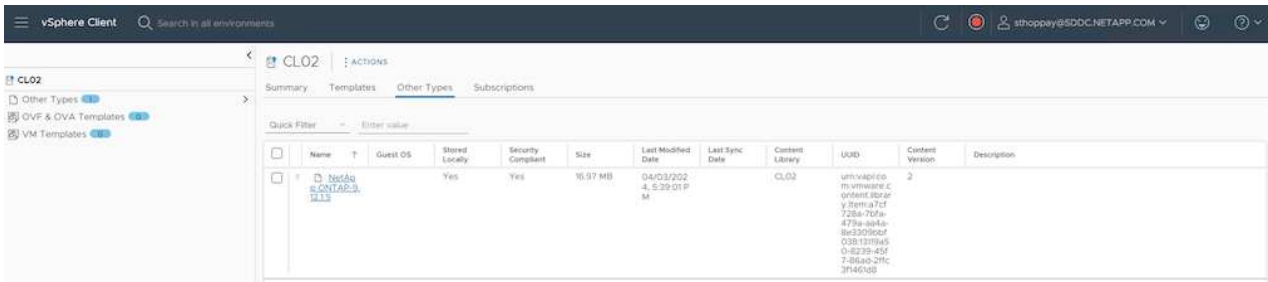
Name

Notes

Select a content library where to clone the library item.

| | Name | Notes | Creation Date |
|----------------------------------|------|-------|-----------------------|
| <input type="radio"/> | CL01 | | 9/26/2023, 5:02:03 PM |
| <input checked="" type="radio"/> | CL02 | | 4/1/2024, 12:37:51 PM |

5. Vérifiez que l'élément est disponible dans la bibliothèque de contenu cible.



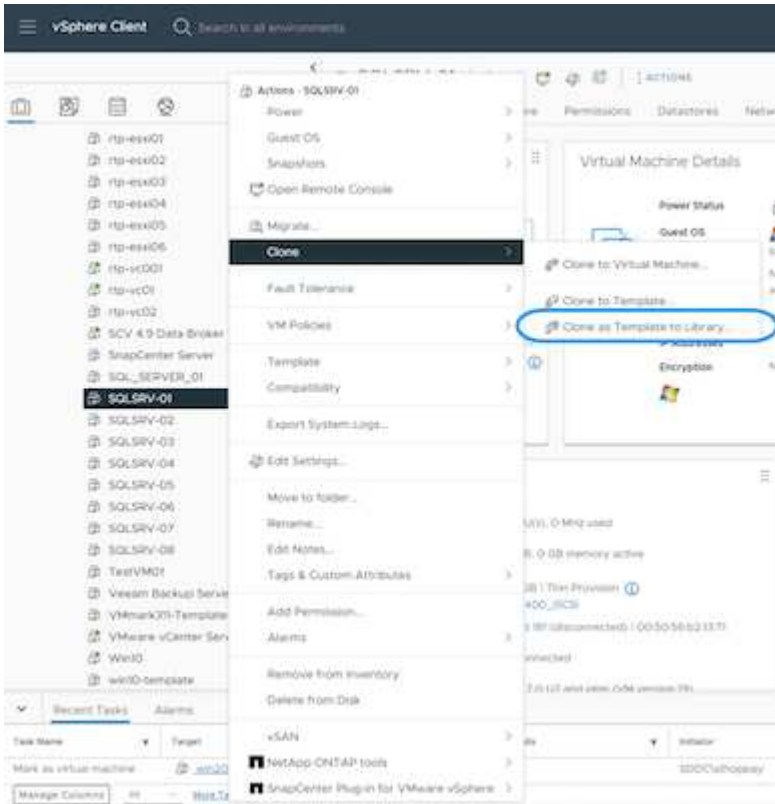
Voici l'exemple de script PowerCLI pour copier les éléments library de contenu de la bibliothèque de contenu CL01 vers CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL02' -Server
$targetvc)
```

Ajout d'une machine virtuelle en tant que modèles dans la bibliothèque de contenu

1. Dans le client Web vSphere, sélectionnez la machine virtuelle et cliquez avec le bouton droit de la souris pour choisir Cloner comme modèle dans la bibliothèque



Lorsque le modèle de machine virtuelle est sélectionné pour le clonage dans library, il peut uniquement le stocker comme modèle OVF & OVA et non comme modèle de machine virtuelle.

2. Confirmez que le type de modèle est sélectionné comme modèle VM et suivez les instructions de l'assistant pour terminer l'opération.

SQLSRV-01 - Clone Virtual Machine To Template

1 Basic information
2 Location
3 Select a compute resource
4 Select storage
5 Ready to complete

Basic information

Template type VM Template


Name SQLSRV-01

Notes

Select a folder for the template

- vcsa-hc.sddc.netapp.com
 - Datacenter

CANCEL NEXT

 Pour plus d'informations sur les modèles de machines virtuelles dans la bibliothèque de contenu, consultez ["Guide d'administration de vSphere VM"](#)

Cas d'utilisation

Migration à partir de systèmes de stockage tiers (y compris VSAN) vers des datastores ONTAP.

- En fonction de l'emplacement de provisionnement du datastore ONTAP, choisissez les options de migration de VM ci-dessus.

Migration de la version précédente vers la dernière version de vSphere.

- Si une mise à niveau sans déplacement des données n'est pas possible, peut créer un nouvel environnement et utiliser les options de migration ci-dessus.



Dans l'option de migration inter vCenter, importez depuis la cible si l'option d'exportation n'est pas disponible sur la source. Pour cette procédure, vérifiez ["Importation ou clonage d'une machine virtuelle avec Advanced Cross vCenter vMotion"](#)

Migration vers VCF Workload Domain.

- Migrer les machines virtuelles de chaque cluster vSphere vers un domaine de charge de travail cible.



Pour permettre la communication réseau avec les machines virtuelles existantes sur d'autres clusters du vCenter source, étendez le segment NSX en ajoutant les hôtes vcenter vSphere source à la zone de transport ou utilisez le pont L2 à la périphérie pour permettre la communication L2 dans le VLAN. Consultez la documentation NSX de ["Configurer une VM Edge pour le pontage"](#)

Ressources supplémentaires

- ["Migration des serveurs virtuels vSphere"](#)
- ["Nouveautés de vSphere 8 pour vMotion"](#)
- ["Ressources vSphere vMotion"](#)
- ["Configurations de passerelle de niveau 0 dans la fédération NSX"](#)
- ["Guide de l'utilisateur HCX 4.8"](#)
- ["Documentation VMware site Recovery Manager"](#)
- ["Reprise d'activité BlueXP pour VMware"](#)

Migration des serveurs virtuels vers Amazon EC2 à l'aide de FSxN

Migration des serveurs virtuels vers Amazon EC2 à l'aide de FSxN : présentation

Les entreprises accélèrent leurs migrations vers des solutions de cloud computing sur AWS, en profitant de services tels que les instances Amazon Elastic Compute Cloud (Amazon EC2) et Amazon FSX for NetApp ONTAP (FSX for ONTAP) pour moderniser leurs infrastructures IT, réaliser des économies et améliorer l'efficacité opérationnelle. Ces offres AWS permettent des migrations qui optimisent le TCO grâce à des modèles de tarification basés sur la consommation et à des fonctionnalités de stockage haute performance, offrant la flexibilité et l'évolutivité nécessaires pour répondre à l'évolution des besoins de l'entreprise à travers le monde.

Présentation

Pour les entreprises fortement investies dans VMware vSphere, la migration vers AWS est une option économique compte tenu des conditions actuelles du marché, qui représente une opportunité unique.

Lors de la transition vers AWS, ces entreprises cherchent à tirer parti de l'agilité et des économies du cloud, tout en préservant les fonctionnalités déjà en place, notamment en matière de stockage. Lors de la migration des workloads ou de la configuration de solutions de reprise après incident, il est essentiel de préserver la transparence des opérations grâce aux protocoles de stockage connus, en particulier iSCSI, les processus, les outils et les compétences.

En utilisant le service de stockage géré AWS FSX pour ONTAP pour conserver les fonctionnalités de stockage d'entreprise, telles que les solutions de stockage sur site proposées par des fournisseurs tiers, les entreprises peuvent exploiter toute la puissance d'AWS tout en minimisant les perturbations et en optimisant leurs

investissements futurs.

Ce rapport technique explique comment migrer des machines virtuelles VMware vSphere sur site vers une instance Amazon EC2 avec des disques de données placés sur des LUN iSCSI FSX pour ONTAP à l'aide de la fonctionnalité MigrateOps « mobilité des données en tant que code » de Cirrus Migrate Cloud (CMC).

De la solution

Les clients VMware cherchent actuellement à relever un certain nombre de défis. Ces entreprises souhaitent :

1. Valoriser les fonctionnalités de stockage, telles que le provisionnement fin, les technologies d'efficacité du stockage, les clones sans encombrement, les sauvegardes intégrées, la réplication de niveau bloc, et le tiering. Cela permet d'optimiser les efforts de migration et de pérenniser le déploiement sur AWS dès le premier jour.
2. Optimisez les déploiements de stockage sur AWS qui utilisent les instances Amazon EC2 en intégrant FSX pour ONTAP et les fonctionnalités d'optimisation des coûts qu'il fournit.
3. Réduisez le coût total de possession (TCO) de l'utilisation des instances Amazon EC2 avec des solutions de stockage bloc en redimensionnant correctement les instances Amazon EC2 pour répondre aux paramètres d'IOPS et de débit requis. Avec le stockage bloc, les opérations sur disque Amazon EC2 plafonner la bande passante et les débits d'E/S. Le stockage de fichiers avec FSX pour ONTAP utilise la bande passante réseau. En d'autres termes, FSX pour ONTAP n'a pas de limite d'E/S au niveau des VM.

Présentation des composants techniques

Concepts liés à FSX pour ONTAP

Amazon FSX pour NetApp ONTAP est un service de stockage AWS entièrement géré qui fournit aux systèmes de fichiers NetApp® ONTAP® toutes les fonctionnalités, performances et API de gestion des données ONTAP habituelles sur AWS. Son stockage haute performance prend en charge plusieurs protocoles (NFS, SMB, iSCSI), offrant un service unique pour les workloads utilisant des instances EC2 Windows, Linux et MacOS.

Étant donné que FSX for ONTAP est un système de fichiers ONTAP, il intègre une multitude de fonctionnalités et de services NetApp familiers, notamment la technologie de réplication des données SnapMirror®, les clones fins et les copies NetApp Snapshot™. En exploitant un Tier de capacité à faible coût par Tiering des données, FSX pour ONTAP offre une évolutivité pratiquement illimitée et est ainsi élastique. De plus, grâce à la technologie d'efficacité du stockage NetApp, les coûts de stockage sur AWS sont encore réduits. Pour plus d'informations, voir "[Commencez à utiliser Amazon FSX pour ONTAP](#)".

Système de fichiers

La ressource centrale de FSX pour ONTAP est son système de fichiers basé sur le stockage SSD. Lors du provisionnement d'un système de fichiers FSX pour ONTAP, l'utilisateur saisit le débit et la capacité de stockage souhaités, puis sélectionne un VPC Amazon dans lequel le système de fichiers doit résider.

Les utilisateurs ont également le choix entre deux modèles de déploiement haute disponibilité intégrés pour le système de fichiers : déploiement dans une zone de disponibilité multiple ou dans une zone de disponibilité unique. Chacune de ces options offre son propre niveau de durabilité et de disponibilité, que les clients peuvent sélectionner en fonction des exigences de continuité de l'activité de leur utilisation. Les déploiements multi-AZ consistent en deux nœuds qui répliquent de manière transparente dans deux zones de disponibilité. L'option de déploiement pour une disponibilité AZ plus économique structure le système de fichiers en deux nœuds répartis entre deux domaines de panne distincts qui résident tous deux dans une même zone de disponibilité AZ.

Ordinateurs virtuels de stockage

Les données du système de fichiers FSX for ONTAP sont accessibles via une partition de stockage logique

appelée SVM (Storage Virtual machine). Un SVM est en fait son propre serveur de fichiers équipé de ses propres données et de ses propres points d'accès admin. Lors de l'accès aux LUN iSCSI sur un système de fichiers FSX pour ONTAP, l'instance Amazon EC2 s'interface directement avec le SVM en utilisant l'adresse IP du terminal iSCSI du SVM.

Bien qu'il soit possible de maintenir un seul SVM dans un cluster, l'exécution de plusieurs SVM dans un cluster peut présenter de nombreux usages et avantages. Les clients peuvent déterminer le nombre optimal de SVM à configurer en tenant compte de leurs besoins, notamment de leurs exigences en matière d'isolation des charges de travail.

Volumes

Les données d'un SVM FSX for ONTAP sont stockées et organisées en structures appelées volumes, qui agissent comme des conteneurs virtuels. Un volume individuel peut être configuré avec une ou plusieurs LUN. Les données stockées dans chaque volume consomment de la capacité de stockage dans le système de fichiers. Toutefois, puisque FSX for ONTAP provisionne légèrement le volume, le volume ne prend en charge que la capacité de stockage correspondant à la quantité de données stockées.

Le concept de migration vers le cloud de Cirrus Migrate

CMC est une offre SaaS (Software-as-a-Service) transactable de Cirrus Data Solutions, Inc. Disponible sur AWS Marketplace. MigrateOps est une fonctionnalité d'automatisation de la mobilité des données en tant que code de CMC qui vous permet de gérer de manière déclarative vos opérations de mobilité des données à grande échelle à l'aide de configurations d'opérations simples dans YAML. Une configuration MigrateOps détermine la façon dont vous souhaitez exécuter vos tâches de mobilité des données. Pour en savoir plus sur MigrateOps, voir "[À propos de MigrateOps](#)".

MigrateOps utilise une approche axée sur l'automatisation, conçue spécialement pour rationaliser l'ensemble du processus, garantissant ainsi la mobilité des données d'entreprise à l'échelle du cloud sans interruption des opérations. Outre les fonctionnalités déjà riches en fonctionnalités offertes par CMC pour l'automatisation, MigrateOps ajoute d'autres automatisations souvent gérées en externe, telles que :

- Correction du système d'exploitation
- Planification de la mise en service et de l'approbation des applications
- Migration des clusters sans temps d'indisponibilité
- L'intégration d'une plateforme de cloud public/privé
- Intégration de la plateforme de virtualisation
- Intégration de la gestion du stockage d'entreprise
- Configuration SAN (iSCSI)

Les tâches ci-dessus étant entièrement automatisées, toutes les étapes fastidieuses de préparation de la machine virtuelle source sur site (par exemple, l'ajout d'agents et d'outils AWS), la création de LUN FSX de destination, la configuration d'iSCSI et de chemins d'accès multiples/MPIO sur l'instance de destination AWS, de plus, toutes les tâches d'arrêt/démarrage des services d'application sont éliminées en spécifiant simplement des paramètres dans un fichier YAML.

FSX pour ONTAP fournit les LUN de données et dimensionnez correctement le type d'instance Amazon EC2, tout en fournissant toutes les fonctionnalités disponibles précédemment dans leurs environnements sur site. La fonction MigrateOps de CMC sera utilisée pour automatiser toutes les étapes impliquées, y compris le provisionnement des LUN iSCSI mappés, ce qui en fait une opération déclarative prévisible.

Remarque : CMC nécessite l'installation d'un agent très léger sur les instances de machines virtuelles source

et de destination pour assurer le transfert sécurisé des données du stockage source vers FSX pour ONTAP.

Avantages de l'utilisation d'Amazon FSX pour NetApp ONTAP avec les instances EC2

Le stockage FSX pour ONTAP pour les instances Amazon EC2 offre plusieurs avantages :

- Un stockage à débit élevé et à faible latence qui fournit des performances élevées et prévisibles pour les charges de travail les plus exigeantes
- La mise en cache intelligente NVMe améliore les performances
- La capacité, le débit et les IOPS ajustables peuvent être modifiés à la volée et s'adapter rapidement à l'évolution des besoins de stockage
- Réplication des données basée sur les blocs depuis le stockage ONTAP sur site vers AWS
- L'accessibilité multiprotocole, y compris pour iSCSI, qui est largement utilisé dans les déploiements VMware sur site
- La technologie Snapshot™ de NetApp et la reprise sur incident orchestrée par SnapMirror empêchent la perte de données et accélèrent la restauration
- Fonctionnalités d'efficacité du stockage qui réduisent l'empreinte et les coûts du stockage, notamment l'allocation dynamique, la déduplication, la compression et la compaction des données
- La réplication efficace réduit le temps nécessaire à la création des sauvegardes, qui passe de plusieurs heures à quelques minutes, optimisant ainsi le RTO
- Options granulaires pour la sauvegarde et la restauration de fichiers à l'aide de NetApp SnapCenter®

Le déploiement des instances Amazon EC2 avec FSX ONTAP en tant que couche de stockage iSCSI offre des performances élevées, des fonctionnalités de gestion des données stratégiques et des fonctionnalités d'efficacité du stockage qui réduisent les coûts et transforment votre déploiement sur AWS.

Grâce à l'exécution d'un Flash cache, à plusieurs sessions iSCSI et à l'exploitation d'un jeu de travail de 5 %, FSX pour ONTAP peut fournir des IOPS d'environ 350 000, garantissant des niveaux de performances adaptés aux charges de travail les plus exigeantes.

Comme seules les limites de bande passante réseau sont appliquées à FSX pour ONTAP, pas les limites de bande passante du stockage bloc, les utilisateurs peuvent exploiter les petits types d'instances Amazon EC2 tout en obtenant les mêmes taux de performance que les types d'instances de plus grande taille. L'utilisation de tels types d'instances peu importants permet également de maîtriser les coûts de calcul et d'optimiser le TCO.

Autre avantage de FSX pour ONTAP : sa capacité à prendre en charge plusieurs protocoles permet de standardiser un service de stockage AWS pour répondre à un large éventail de besoins en services de fichiers et de données.

Pour les entreprises fortement investies dans VMware vSphere, la migration vers AWS est une option économique compte tenu des conditions actuelles du marché, qui représente une opportunité unique.

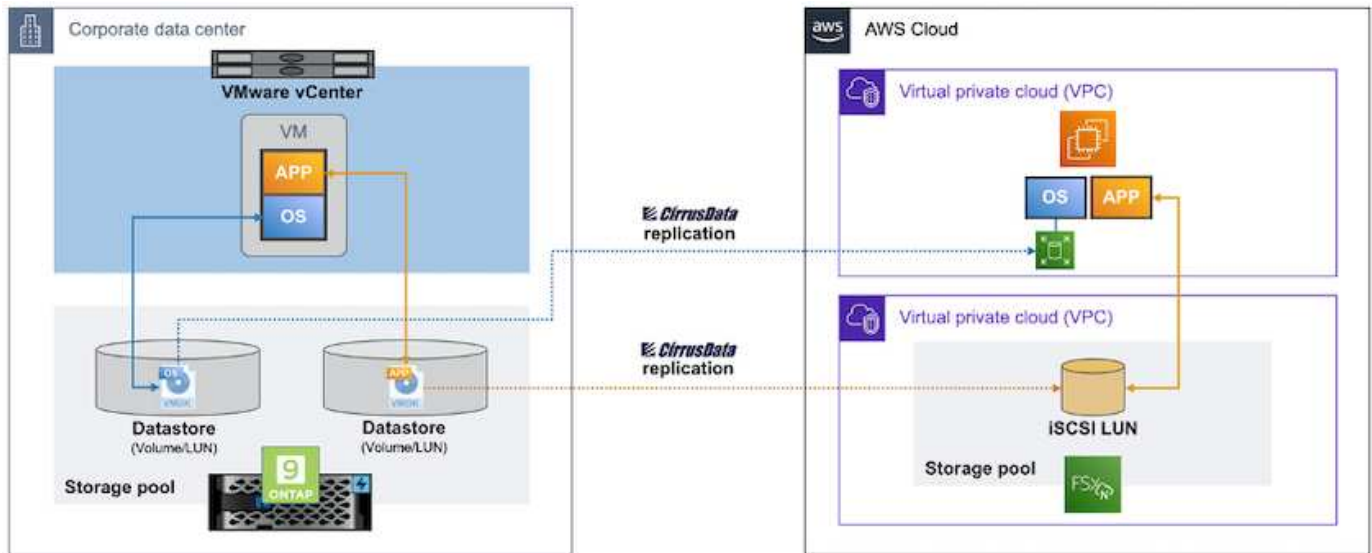
Migrer des machines virtuelles vers Amazon EC2 à l'aide de FSxN : architecture et conditions préalables

Cet article présente les critères généraux d'architecture et de déploiement requis pour effectuer la migration.

Architecture générale

Le diagramme ci-dessous illustre l'architecture générale de la migration des données VMDK (Virtual machine

Disk) sur VMware vers AWS à l'aide de CMC MigrateOps :



Comment migrer vos machines virtuelles VMware vers AWS à l'aide d'Amazon EC2 et FSX pour ONTAP iSCSI

Prérequis

Avant de commencer les étapes de présentation, assurez-vous que les conditions préalables suivantes sont remplies :

Sur AWS

- D'un compte AWS. Cela inclut les autorisations pour les sous-réseaux, la configuration VPC, les tables de routage, la migration des règles de sécurité, les groupes de sécurité, et d'autres exigences en matière de mise en réseau, telles que l'équilibrage de charge. Comme pour toute migration, la plupart des efforts et des considérations doivent être consacrés à la mise en réseau.
- Des rôles IAM appropriés qui vous permettent de provisionner à la fois les instances FSX pour ONTAP et Amazon EC2.
- Les tables de routage et les groupes de sécurité sont autorisés à communiquer avec FSX pour ONTAP.
- Ajoutez une règle entrante au groupe de sécurité approprié (voir ci-dessous pour plus de détails) pour sécuriser le transfert des données de votre data Center sur site vers AWS.
- Un DNS valide qui peut résoudre les noms de domaine Internet publics.
- Vérifiez que votre résolution DNS est fonctionnelle et vous permet de résoudre les noms d'hôte.
- Pour des performances optimales et un dimensionnement approprié, utilisez les données de performances de votre environnement source pour dimensionner correctement votre stockage FSX pour ONTAP.
- Chaque session MigrateOps utilise un EIP, de sorte que le quota pour EIP doit être augmenté pour plus de parallélisme. Gardez à l'esprit que le quota EIP par défaut est 5.
- (Si des charges de travail basées sur Active Directory sont en cours de migration) Un domaine Windows Active Directory sur Amazon EC2.

Pour Cirrus Migrate Cloud

- Un compte Cirrus Data Cloud sur "cloud.cirrusdata.com" doit être créé avant d'utiliser CMC. Les communications sortantes avec le CDN, les terminaux de données Cirrus et le référentiel logiciel via HTTPS doivent être autorisés.

- Permet la communication (sortante) avec les services Cirrus Data Cloud via le protocole HTTPS (Port 443).
- Pour qu'un hôte soit géré par le projet CMC, le logiciel CMC déployé doit initier une connexion TCP sortante unidirectionnelle vers Cirrus Data Cloud.
- Autoriser l'accès au protocole TCP, Port 443 à portal-gateway.cloud.cirrusdata.com, actuellement à 208.67.222.222.
- Autoriser les requêtes HTTP POST (via une connexion HTTPS) avec la charge de données binaire (application/flux d'octets). Ceci est similaire à un téléchargement de fichier.
- Assurez-vous que portal-gateway.cloud.cirrusdata.com peut être résolu par votre DNS (ou via le fichier hôte du système d'exploitation).
- Si vous disposez de règles strictes pour interdire aux instances de produit d'établir des connexions sortantes, la fonction « Relais de gestion » de CMC peut être utilisée lorsque la connexion 443 sortante provient d'un seul hôte sécurisé non productif.

Remarque : aucune donnée de stockage n'est jamais envoyée au noeud final Cirrus Data Cloud. Seules les métadonnées de gestion sont envoyées et peuvent être masquées de manière facultative, de sorte qu'aucun nom d'hôte, nom de volume ou IP réseau réel ne soit inclus.

MigrateOps automatise la gestion d'une connexion hôte à hôte (H2H) pour la migration des données à partir de référentiels de stockage sur site vers AWS. Il s'agit de connexions réseau TCP à sens unique optimisées que CMC utilise pour faciliter la migration à distance. Ce processus est doté de la compression et du chiffrement always-on, qui peuvent diviser par huit la quantité de trafic, selon la nature des données.

Remarque : CMC est conçu de sorte qu'aucune donnée de production / E/S ne quitte le réseau de production pendant toute la phase de migration. Par conséquent, une connectivité directe entre l'hôte source et l'hôte de destination est requise.

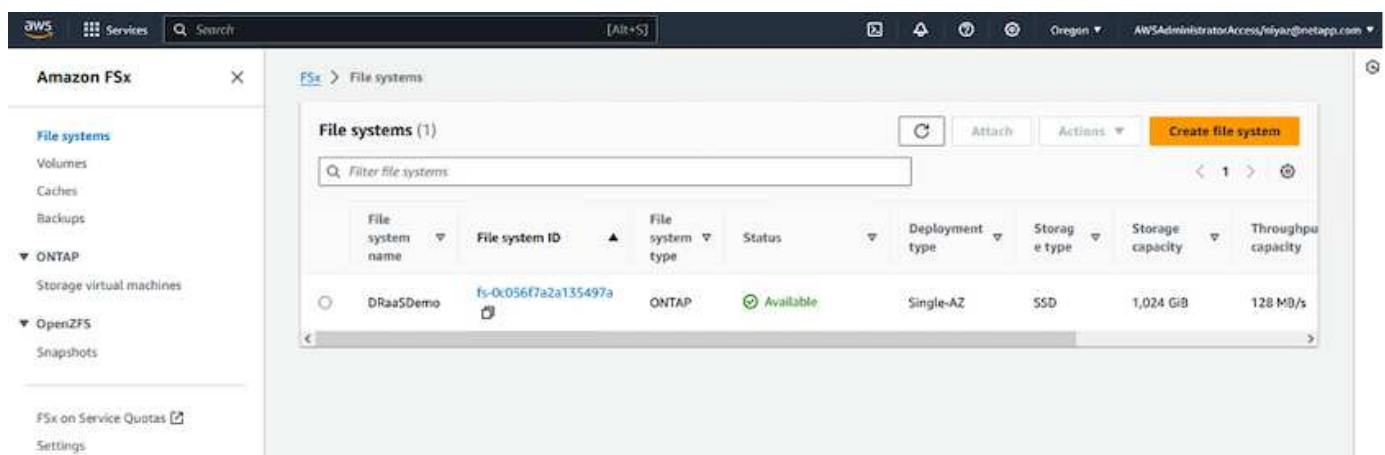
Migration des serveurs virtuels vers Amazon EC2 à l'aide de FSxN : guide de déploiement

Cet article décrit la procédure de déploiement pour ces solutions de migration.

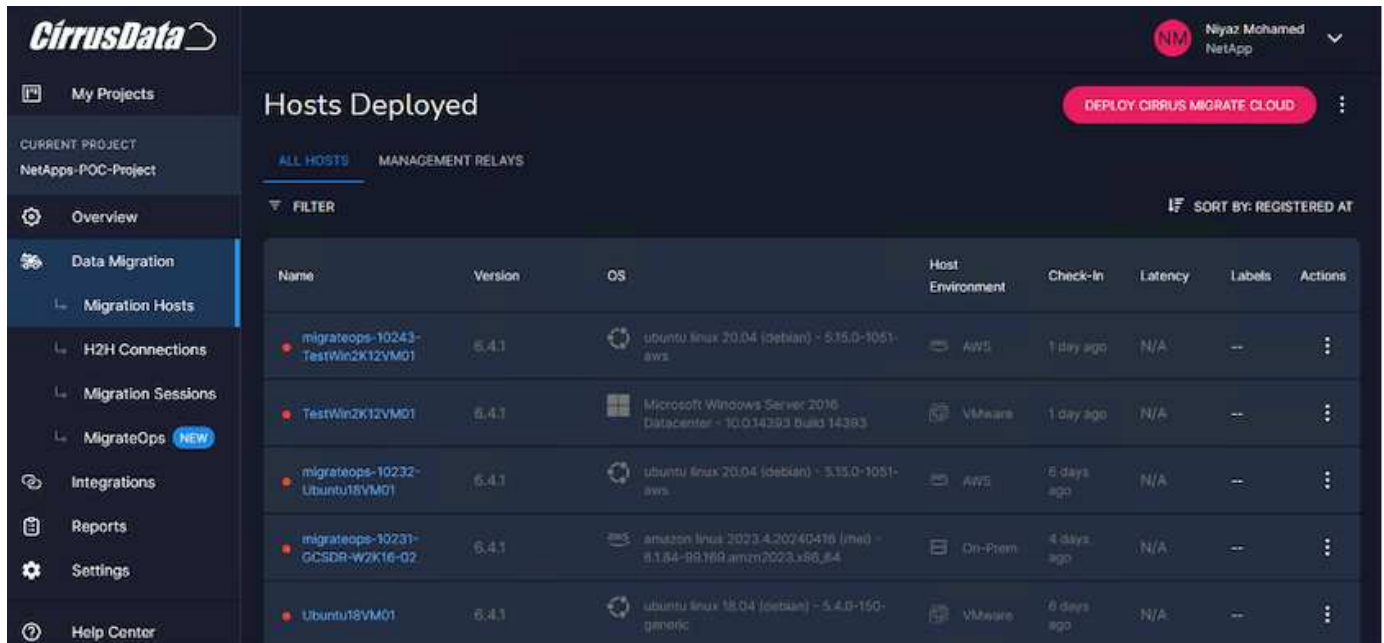
Configurez FSx pour ONTAP et Cirrus Data pour les opérations de migration

C'est ça "[guide de déploiement détaillé](#)" Montre comment ajouter un volume FSx pour ONTAP à un VPC. Étant donné que ces étapes sont de nature séquentielle, assurez-vous qu'elles sont couvertes dans l'ordre.

Pour les besoins de cette démonstration, "DRaaS Demo" est le nom du système de fichiers créé.



Une fois que votre VPC AWS est configuré et que FSX pour ONTAP est provisionné en fonction de vos besoins en termes de performances, connectez-vous à "cloud.cirrusdata.com" et "[créer un nouveau projet](#)" ou accéder à un projet existant.



Avant de créer la recette du MigrationOps, vous devez ajouter AWS Cloud en tant qu'intégration. CMC offre une intégration intégrée à FSX pour ONTAP et AWS. L'intégration de FSX for ONTAP fournit les fonctionnalités automatisées suivantes :

Préparez votre système de fichiers FSX pour ONTAP :

- Créez des volumes et des LUN correspondant aux volumes source

Remarque : un disque de destination dans le modèle FSX for ONTAP FS est un « LUN » créé sur un « volume » qui a suffisamment de capacité pour contenir le LUN et une quantité raisonnable de surcharge pour faciliter les snapshots et les métadonnées. L'automatisation CMC prend en charge tous ces détails pour créer le volume approprié et le LUN avec des paramètres facultatifs définis par l'utilisateur.

- Créez l'entité hôte (appelée iGroups dans FSX) avec l'IQN de l'initiateur hôte
- Mappez les nouveaux volumes créés vers les entités hôtes appropriées à l'aide de mappages
- Créer toutes les autres configurations nécessaires

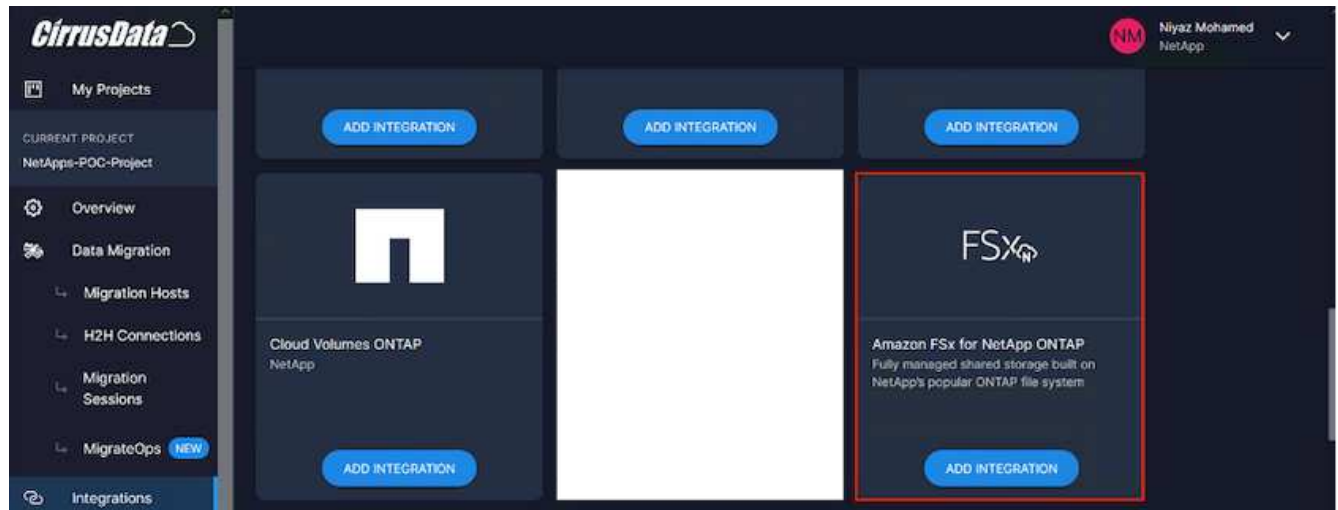
Préparer l'hôte de production pour la connexion iSCSI :

- Si nécessaire, installez et configurez la fonction iSCSI et configurez l'initiateur.
- Si nécessaire, installez et configurez le multipath (MPIO pour Windows) avec les identifiants de fournisseur appropriés.
- Ajustez les paramètres système, si nécessaire, en fonction des meilleures pratiques du fournisseur, par exemple avec les paramètres udev sur Linux.
- Créez et gérez des connexions iSCSI telles que des cibles iSCSI persistantes/favorites sous Windows.

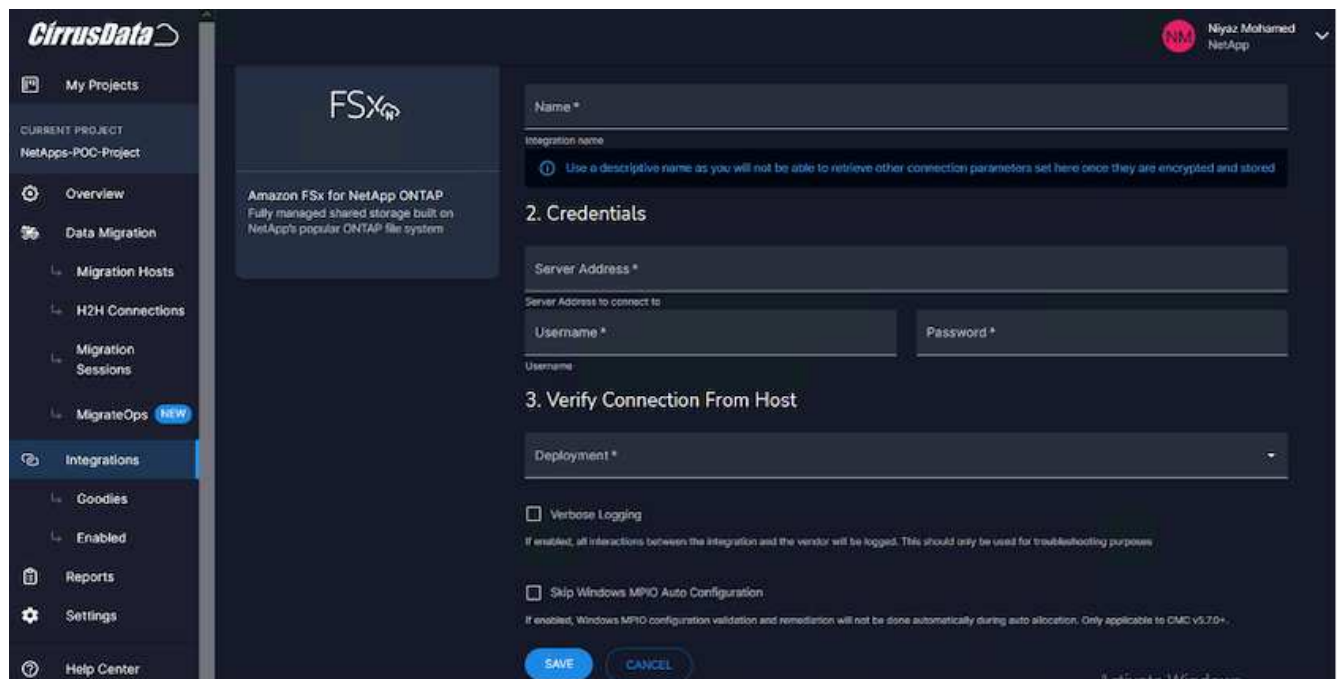
Pour configurer l'intégration de CMC pour FSX for ONTAP et AWS, effectuez les opérations suivantes :

1. Connectez-vous au portail Cirrus Data Cloud.

2. Accédez au projet pour lequel vous souhaitez activer l'intégration.
3. Accédez à intégrations → Goodies.
4. Faites défiler l'écran pour trouver FSX pour NetApp ONTAP et cliquez sur ADD INTEGRATION.



5. Indiquez un nom descriptif (strictement à des fins d'affichage) et ajoutez les informations d'identification appropriées.



6. Une fois l'intégration créée, lors de la création d'une nouvelle session de migration, sélectionnez allouer automatiquement les volumes de destination pour allouer automatiquement de nouveaux volumes sur FSX pour ONTAP.

Remarque : les nouveaux LUN seront créés avec la même taille que le volume source, sauf si « migrer vers des volumes plus petits » est activé pour la migration.

Remarque : si une entité hôte (iGroup) n'existe pas déjà, une nouvelle entité sera créée. Tous les IQN de l'initiateur iSCSI de l'hôte seront ajoutés à cette nouvelle entité hôte.

Remarque : si une entité hôte existante avec l'un des initiateurs iSCSI existe déjà, elle sera réutilisée.

7. Ensuite, ajoutez l'intégration pour AWS en suivant les étapes à l'écran.

Remarque : cette intégration est utilisée lors de la migration des machines virtuelles du stockage sur site vers AWS, en association avec l'intégration de FSX pour ONTAP.

Remarque : utilisez des relais de gestion pour communiquer avec Cirrus Data Cloud s'il n'y a pas de connexion sortante directe pour les instances de production à migrer.

Lorsque des intégrations sont ajoutées, il est temps d'enregistrer des hôtes dans le projet. Prenons un exemple de scénario.

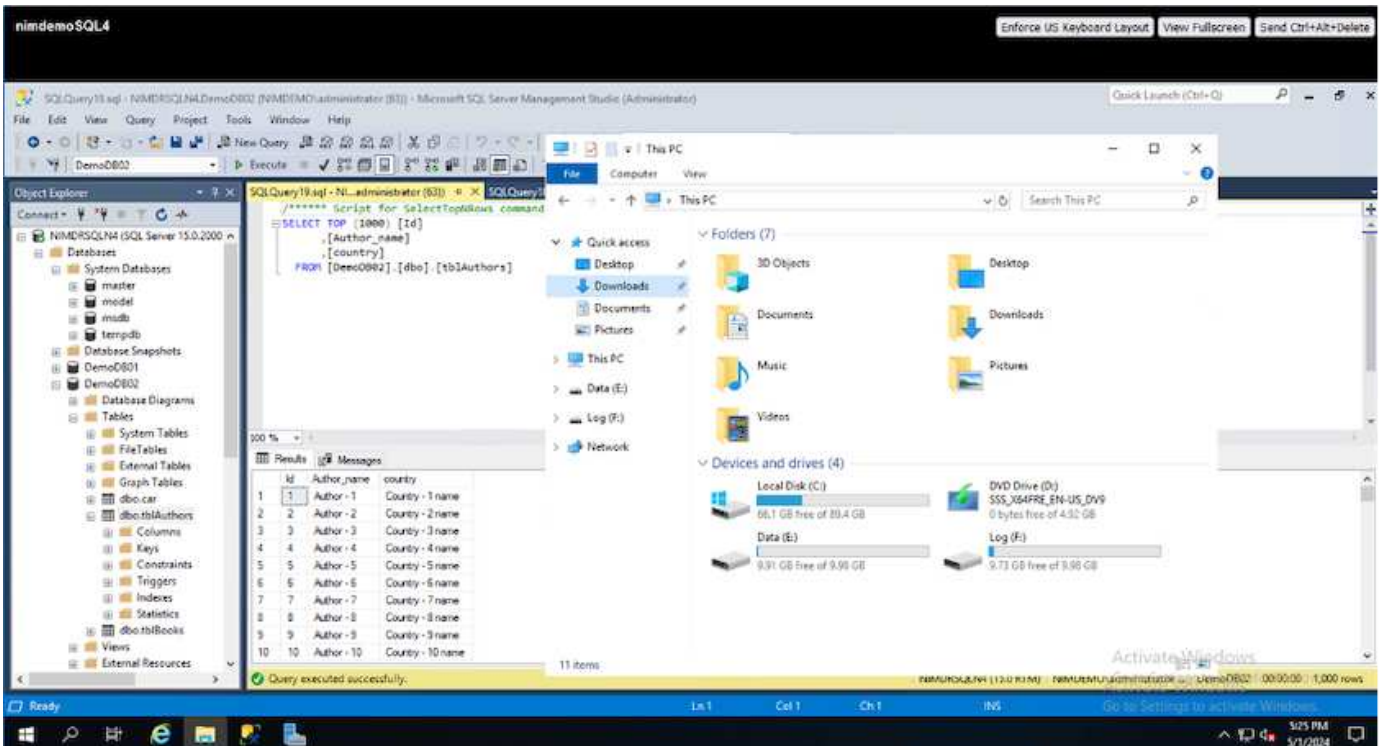
Scénario d'enregistrement d'hôte

Machines virtuelles VMware invitées résidant sur vCenter dans un data Center sur site :

- Windows 2016 s'exécutant avec SQL Server avec trois VMDK incluant des systèmes d'exploitation et des disques de données. Il exécute une base de données active. La base de données se trouve sur un volume de données sauvegardé par deux VMDK.

Remarque : étant donné que la source est un environnement VMware et que des VMDK sont utilisés, le logiciel Windows iSCSI Initiator n'est pas actuellement configuré sur cette machine virtuelle invitée. Pour se connecter à notre stockage de destination via iSCSI, iSCSI et MPIO devront être installés et configurés. L'intégration de Cirrus Data Cloud effectuera cette installation automatiquement au cours du processus.

Remarque : l'intégration configurée dans la section précédente automatise la configuration du nouveau stockage de destination lors de la création des nouveaux disques, de la configuration des entités hôtes et de leurs IQN, et même de la correction de la machine virtuelle (hôte) de l'application pour les configurations iSCSI et multipathing.



Dans cette démonstration, nous migrerons les VMDK d'application de chaque machine virtuelle vers un volume iSCSI provisionné et mappé automatiquement à partir de FSX pour ONTAP. Dans ce cas, le VMDK du système d'exploitation sera migré vers un volume Amazon EBS, car les instances Amazon EC2 prennent en charge cette plateforme Amazon EBS uniquement en tant que disque de démarrage.

Remarque : le facteur d'échelle associé à cette approche de migration est la bande passante réseau et le canal reliant les installations sur site au VPC AWS. Étant donné que chaque machine virtuelle possède une session hôte 1:1 configurée, la performance globale de la migration dépend de deux facteurs :

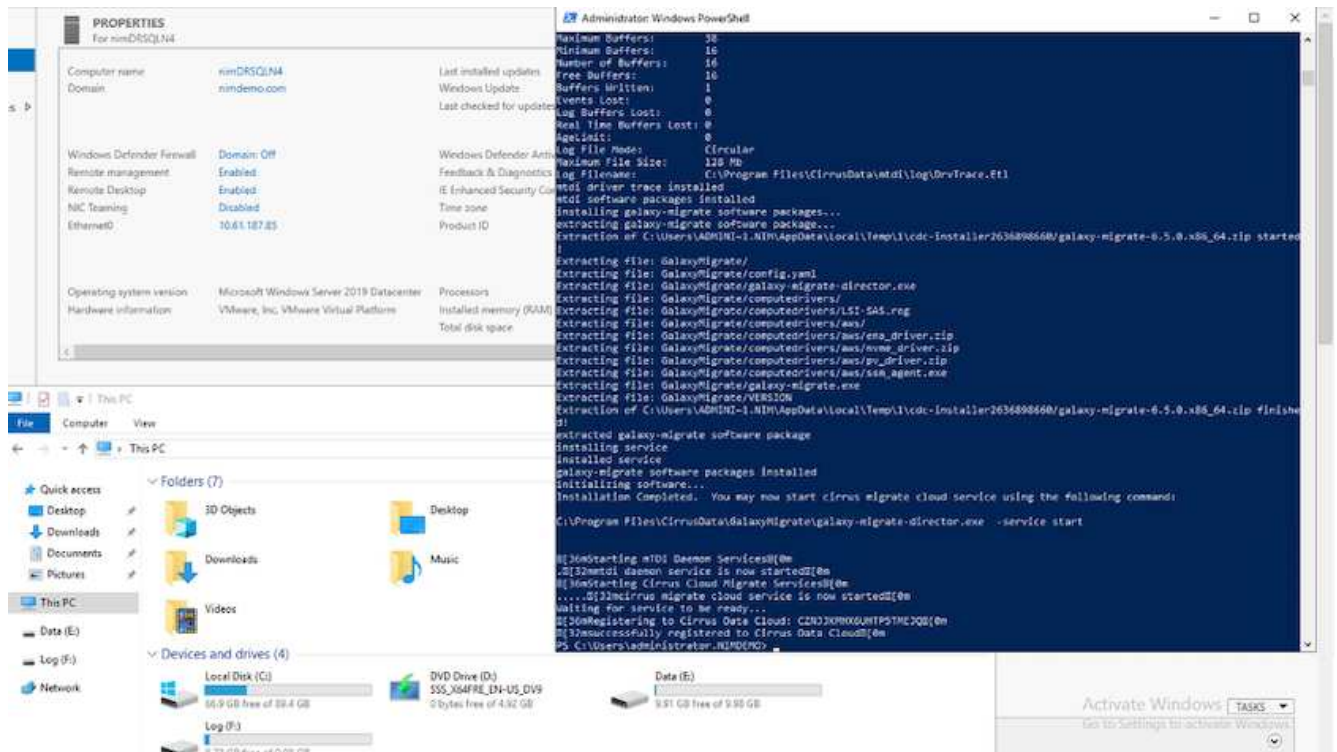
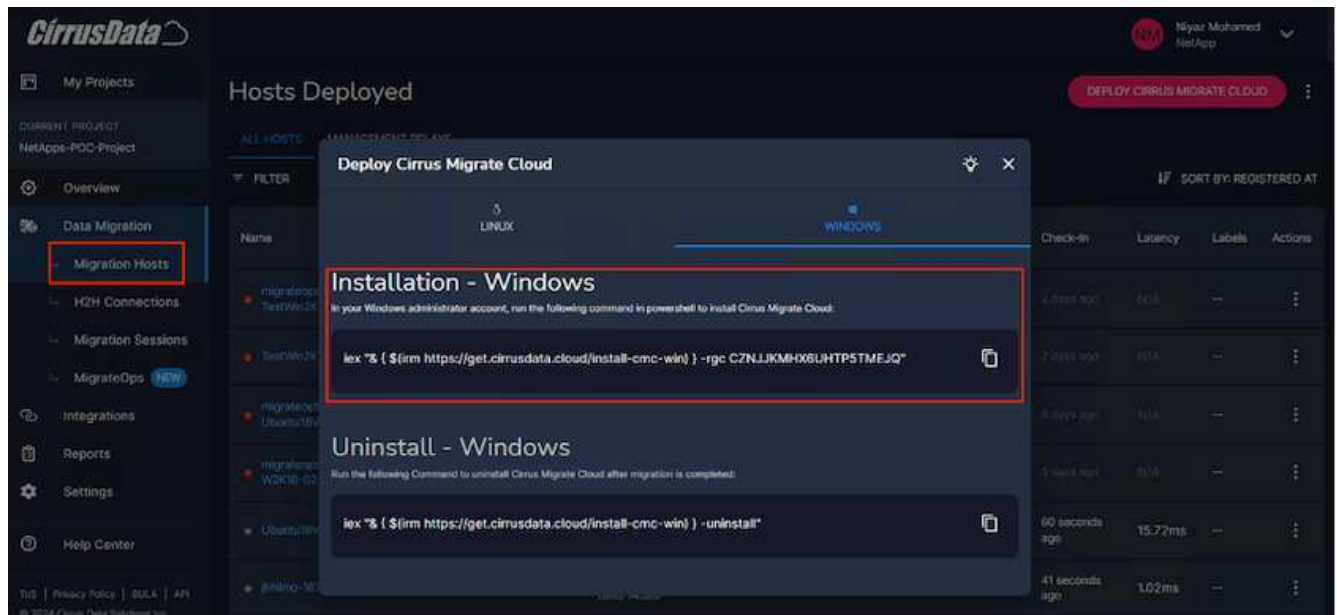
- La bande passante du réseau
- Type d'instance cible et bande passante ENI

La procédure de migration est la suivante :

1. Installez l'agent CMC sur chaque hôte (Windows et Linux) désigné pour la vague de migration. Ceci peut être effectué en exécutant une commande d'installation à une ligne.

Pour ce faire, accédez à migration des données > hôtes de migration > cliquez sur « déployer Cirrus Migrate Cloud » et sélectionnez « Windows ».

Ensuite, copiez le `ix` Pour l'hôte et l'exécuter à l'aide de PowerShell. Une fois le déploiement de l'agent réussi, l'hôte est ajouté au projet sous « hôtes de migration ».



2. Préparez le YAML pour chaque machine virtuelle.

Remarque : il s'agit d'une étape essentielle pour avoir un YAML pour chaque VM qui spécifie la recette ou le modèle nécessaire pour la tâche de migration.

Le YAML fournit le nom de l'opération, des notes (description) ainsi que le nom de la recette `MIGRATEOPS_AWS_COMPUTE`, le nom d'hôte (`system_name`) et le nom de l'intégration (`integration_name`) et la configuration source et destination. Des scripts personnalisés peuvent être spécifiés avant et après la mise en service.

```
operations:
  - name: Win2016 SQL server to AWS
```

```

notes: Migrate OS to AWS with EBS and Data to FSx for ONTAP
recipe: MIGRATEOPS_AWS_COMPUTE
config:
  system_name: Win2016-123
  integration_name: NimAWSHybrid
  migrateops_aws_compute:
    region: us-west-2
    compute:
      instance_type: t3.medium
      availability_zone: us-west-2b
    network:
      vpc_id: vpc-05596abe79cb653b7
      subnet_id: subnet-070aeb9d6b1b804dd
      security_group_names:
        - default
    destination:
      default_volume_params:
        volume_type: GP2
      iscsi_data_storage:
        integration_name: DemoDRaaS
      default_volume_params:
        netapp:
          qos_policy_name: ""
    migration:
      session_description: Migrate OS to AWS with EBS and
Data to FSx for ONTAP
      qos_level: MODERATE
    cutover:
      stop_applications:
        - os_shell:
            script:
              - stop-service -name 'MSSQLSERVER'
-Force
              - Start-Sleep -Seconds 5
              - Set-Service -Name 'MSSQLSERVER'
-StartupType Disabled
              - write-output "SQL service stopped
and disabled"
        - storage_unmount:
            mountpoint: e
        - storage_unmount:
            mountpoint: f
      after_cutover:
        - os_shell:
            script:

```

```

-Force
mount disks..." > log.txt
E and F for SQL..." >>log.txt
  - storage_unmount:
    mountpoint: e
  - storage_unmount:
    mountpoint: f
  - storage_mount_all: {}
  - os_shell:
    script:
      - write-output "Waiting 60 seconds to
restart SQL Services..." >>log.txt
      - Start-Sleep -Seconds 60
      - stop-service -name 'MSSQLSERVER'
-Force
      - Start-Sleep -Seconds 3
      - write-output "Start SQL Services..."
>>log.txt
-StartupType Automatic
      - Set-Service -Name 'MSSQLSERVER'
      - start-service -name 'MSSQLSERVER'
      - write-output "SQL started" >>log.txt

```

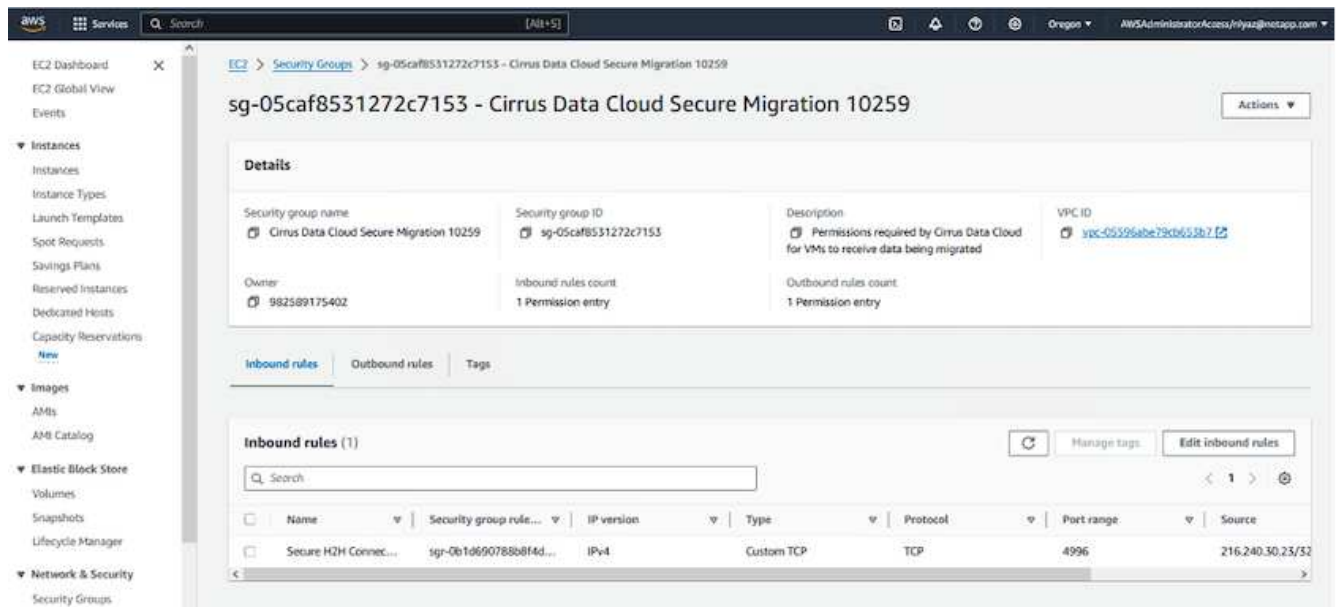
3. Une fois les YAML en place, créez la configuration MigrateOps. Pour ce faire, accédez à Data migration > MigrateOps, cliquez sur Start New Operation et entrez la configuration dans un format YAML valide.
4. Cliquez sur "Créer une opération".

Note: Pour obtenir le parallélisme, chaque hôte doit avoir un fichier YAML spécifié et configuré.

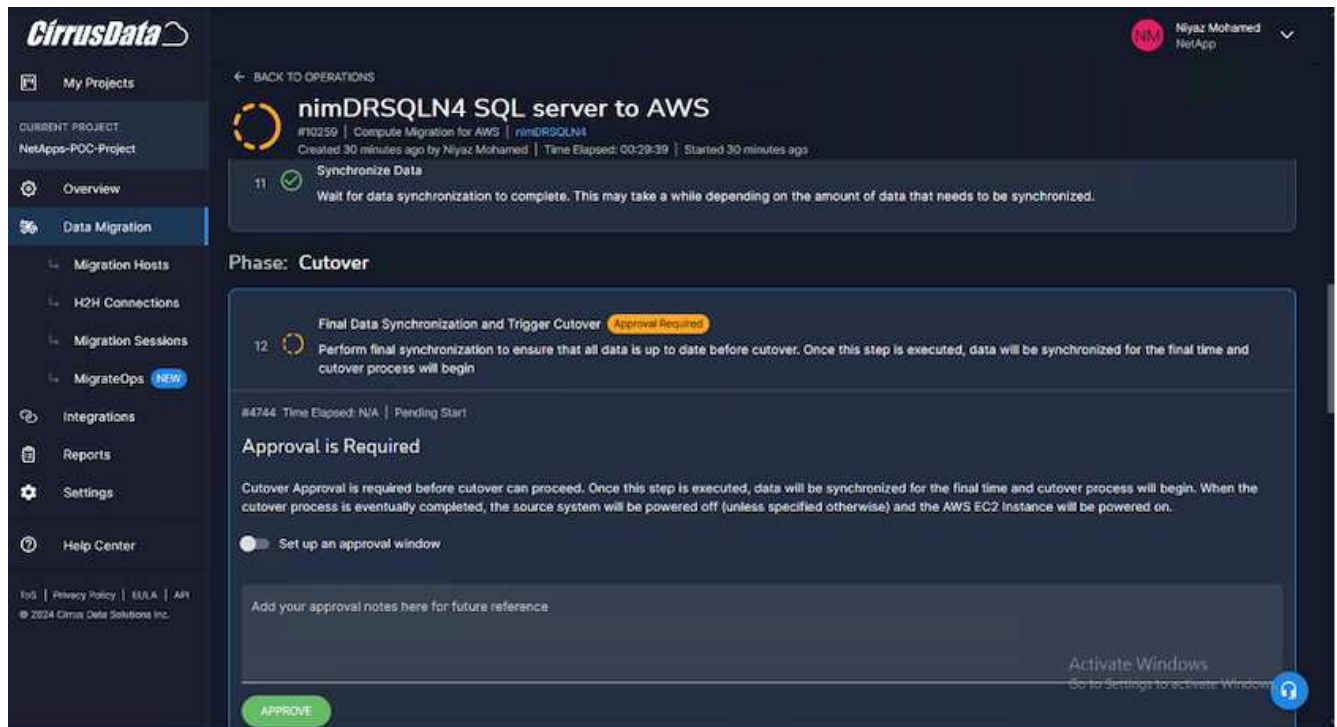
5. À moins que le `scheduled_start_time` le champ est spécifié dans la configuration, l'opération démarre immédiatement.
6. L'opération va maintenant s'exécuter et se poursuivre. À partir de l'interface utilisateur de Cirrus Data Cloud, vous pouvez surveiller la progression avec des messages détaillés. Ces étapes incluent automatiquement les tâches normalement effectuées manuellement, telles que l'allocation automatique et la création de sessions de migration.



Remarque : pendant la migration hôte à hôte, un groupe de sécurité supplémentaire avec une règle autorisant le port entrant 4996 sera créé, ce qui permettra au port requis de communiquer et il sera automatiquement supprimé une fois la synchronisation terminée.



7. Pendant la synchronisation de cette session de migration, il existe une étape future de la phase 3 (mise en service) avec le libellé « approbation requise ». Dans une formule MigrateOps, les tâches stratégiques (telles que les conversions de migration) requièrent l'approbation de l'utilisateur avant de pouvoir être exécutées. Les opérateurs de projet ou les administrateurs peuvent approuver ces tâches à partir de l'interface utilisateur. Une fenêtre d'approbation future peut également être créée.



8. Après approbation, l'opération MigrateOps se poursuit avec la mise en service.
9. Après un bref instant, l'opération est terminée.



Note: Avec l'aide de la technologie Cirrus Data cMotion™, le stockage de destination a été mis à jour avec tous les changements les plus récents. Par conséquent, après approbation, l'intégralité du processus de mise en service finale prendra moins d'une minute.

Vérification après migration

Examinons l'instance Amazon EC2 migrée exécutant le système d'exploitation Windows Server et les étapes suivantes qui ont abouti :

1. Windows SQL Services est maintenant lancé.

2. La base de données est de nouveau en ligne et utilise le stockage à partir du périphérique iSCSI Multipath.
3. Tous les nouveaux enregistrements de base de données ajoutés lors de la migration se trouvent dans la base de données nouvellement migrée.
4. L'ancien stockage est maintenant hors ligne.

Remarque : d'un simple clic pour soumettre l'opération de mobilité des données sous forme de code, et d'un clic pour approuver la mise en service, le serveur virtuel a migré avec succès de VMware sur site vers une instance Amazon EC2 à l'aide de FSX pour ONTAP et de ses fonctionnalités iSCSI.

Remarque : en raison de la limitation de l'API AWS, les machines virtuelles converties s'affichent sous la forme « Ubuntu ». Il s'agit strictement d'un problème d'affichage et n'affecte pas la fonctionnalité de l'instance migrée. Une version à venir permettra de résoudre ce problème.

Remarque : les instances Amazon EC2 migrées sont accessibles à l'aide des informations d'identification utilisées côté site.

Migration des machines virtuelles vers Amazon EC2 à l'aide de FSxN : d'autres possibilités et conclusion

Cet article présente d'autres possibilités pour cette solution de migration et conclut le sujet.

Autres possibilités

La même approche peut être étendue pour migrer des machines virtuelles à l'aide du stockage invité sur des machines virtuelles sur site. Le VMDK du système d'exploitation peut être migré à l'aide de CMC et les LUN iSCSI invités peuvent être répliqués à l'aide de SnapMirror. Ce processus nécessite de briser le miroir et de connecter le LUN à l'instance Amazon EC2 qui vient d'être migrée, comme illustré dans le schéma ci-dessous.



Conclusion

Ce document fournit une présentation complète de l'utilisation de la fonctionnalité MigrateOps de CMC pour migrer les données stockées dans des référentiels VMware sur site vers AWS à l'aide d'instances Amazon EC2 et de FSX pour ONTAP.

La vidéo suivante présente le processus de migration du début à la fin :

[Migrez les machines virtuelles VMware vers Amazon EC2](#)

Pour consulter l'interface graphique et la migration locale de base d'Amazon EBS vers FSX pour ONTAP, regardez cette vidéo de démonstration de cinq minutes :



Migration vers n'importe quel stockage évolutif avec Cirrus Migrate Cloud

Multicloud hybride NetApp avec les solutions VMware

Cas d'usage du multicloud hybride VMware

Cas d'utilisation de l'environnement multicloud hybride NetApp avec VMware

Présentation des cas d'utilisation importants pour les ÉQUIPES IT lors de la planification de déploiements de cloud hybride ou premier cloud.

Cas d'utilisation populaires

Cas d'utilisation :

- Reprise sur incident,
- Hébergement de charges de travail pendant la maintenance du data Center, * rafale rapide dans laquelle des ressources supplémentaires sont requises au-delà de ce qui est provisionné dans le data Center local,
- L'extension de site VMware,
- Migration rapide vers le cloud,
- Développement/test et

- La modernisation des applications en tirant parti de technologies complémentaires du cloud.

Dans cette documentation, les références aux charges de travail cloud seront détaillées dans les cas d'utilisation de VMware. Ces utilisations sont les suivantes :

- Protection (inclut la reprise après incident et la sauvegarde/restauration)
- Migrer
- Extension

Inside ® le parcours DE L'IT

La plupart des entreprises sont en voie de transformation et de modernisation. Dans le cadre de ce processus, les entreprises tentent d'utiliser leurs investissements VMware existants, tout en tirant parti des avantages du cloud et en explorant les façons de rendre le processus de migration aussi transparent que possible. Cette approche facilite grandement la tâche de modernisation, car les données sont déjà dans le cloud.

La réponse la plus simple à ce scénario est d'utiliser des offres VMware pour chaque hyperscaler. Comme NetApp® Cloud volumes, VMware offre un moyen de déplacer ou d'étendre les environnements VMware sur site vers n'importe quel cloud. Vous pouvez ainsi conserver vos ressources, compétences et outils sur site existants tout en exécutant les charges de travail de façon native dans le cloud. Les risques sont réduits, car aucun service n'est disponible ni modifié IP. De plus, l'équipe INFORMATIQUE est en mesure de gérer ses pratiques sur site à l'aide des compétences et des outils existants. Cela permet d'accélérer les migrations vers le cloud et de faciliter la transition vers une architecture multicloud hybride.

Comprendre l'importance d'autres options de stockage NFS

Même si VMware quel que soit le cloud offre des fonctionnalités hybrides uniques à chaque client, les options de stockage NFS supplémentaires limitées ne sont pas utiles pour les entreprises qui traitent de charges de travail très exigeantes en termes de stockage. Comme le stockage est directement lié aux hôtes, le seul moyen de faire évoluer le stockage consiste à ajouter d'autres hôtes, ce qui représente une augmentation des coûts de 35 à 40 % ou plus pour les charges de travail consommatrices de stockage. Ces charges de travail ont simplement besoin d'espace de stockage supplémentaire et ne sont pas de puissance supplémentaire. Mais cela signifie que les hôtes supplémentaires sont payants.

Examinons ce scénario :

Un client ne requiert que cinq hôtes pour le processeur et la mémoire, mais ses besoins en stockage sont nombreux et doit disposer de 12 hôtes pour répondre aux besoins en stockage. En fin de compte, il est indispensable de faire évoluer l'infrastructure financière en achetant de la puissance supplémentaire si nécessaire.

Lorsque vous planifiez l'adoption et les migrations du Cloud, il est toujours important d'évaluer la meilleure approche et de prendre le chemin le plus simple qui réduit les investissements totaux. L'approche la plus courante et la plus simple pour toute migration d'applications est le réhébergement (aussi appelé lift and shift) où il n'existe pas de machine virtuelle (VM) ou de conversion des données. L'utilisation de NetApp Cloud volumes avec le Software-Defined Data Center VMware (SDDC), tout en complétant VSAN, offre une option facile à déplacer.

Automatisation VMware vSphere

Introduction à l'automatisation pour ONTAP et vSphere

Cette page décrit les avantages de l'automatisation de la fonctionnalité ONTAP de base

dans un environnement VMware vSphere.

Automatisation avec VMware

Depuis les premiers jours de VMware ESX, l'automatisation fait partie intégrante de la gestion des environnements VMware. La possibilité de déployer une infrastructure en tant que code et d'étendre les pratiques aux opérations de cloud privé permet de réduire les problèmes liés à l'évolutivité, à la flexibilité, au provisionnement automatique et à l'efficacité.

L'automatisation peut être organisée selon les catégories suivantes :

- **Déploiement d'infrastructure virtuelle**
- **Fonctionnement de la machine invitée**
- **Opérations dans le cloud**

Les administrateurs disposent de nombreuses options pour automatiser leur infrastructure. Qu'il s'agisse d'utiliser des fonctionnalités vSphere natives, telles que des profils d'hôtes ou des spécifications de personnalisation des machines virtuelles vers des API disponibles sur les composants logiciels VMware, les systèmes d'exploitation et les systèmes de stockage NetApp, la documentation et les conseils fournis sont considérables.

Data ONTAP 8.0.1 et versions ultérieures prennent en charge certaines API VMware vSphere pour l'intégration de baies (VAAI) lorsque l'hôte ESX exécute ESX 4.1 ou une version ultérieure. VAAI est un ensemble d'API qui permettent la communication entre les hôtes VMware vSphere ESXi et les périphériques de stockage. Ces fonctionnalités permettent de décharger l'hôte ESX vers le système de stockage et d'augmenter le débit du réseau. L'hôte ESX active ces fonctionnalités automatiquement dans l'environnement adéquat. Vous pouvez déterminer dans quelle mesure votre système utilise des fonctions VAAI en consultant les statistiques contenues dans les compteurs VAAI.

Le point de départ le plus courant pour l'automatisation du déploiement d'un environnement VMware consiste à provisionner des datastores basés sur des blocs ou des fichiers. Il est important de définir les exigences des tâches réelles avant de développer l'automatisation correspondante.

Pour plus d'informations sur l'automatisation des environnements VMware, consultez les ressources suivantes :

- ["NetApp Pub"](#). Gestion et automatisation de la configuration NetApp.
- ["Communauté Ansible Galaxy pour VMware"](#). Ensemble de ressources Ansible pour VMware.
- ["Ressources VMware {code}"](#). Ressources nécessaires à la conception de solutions pour le Software-Defined Data Center, y compris des forums, des normes de conception, des exemples de code et des outils de développement.

Provisionnement classique du stockage bloc

Provisionnement traditionnel du stockage bloc vSphere avec ONTAP

VMware vSphere prend en charge les options de datastore VMFS suivantes avec la prise en charge du protocole SAN ONTAP indiquée.

| Options de datastore VMFS | Prise en charge du protocole SAN ONTAP |
|--|--|
| "Fibre Channel (FC)" | oui |
| "FCoE (Fibre Channel over Ethernet)" | oui |
| "iSCSI" | oui |
| Extensions iSCSI pour RDMA (iser) | non |
| "NVMe over Fabric avec FC (NVMe/FC)" | oui |
| NVMe over Fabric avec RDMA over Converged Ethernet (NVMe/RoCE) | non |



Si iser ou NVMe/RoCE VMFS est requis, vérifiez les systèmes de stockage SANtricity.

Datastore VMFS vSphere - stockage Fibre Channel back-end avec ONTAP

Cette section décrit la création d'un datastore VMFS avec un stockage ONTAP Fibre Channel (FC).

Ce dont vous avez besoin

- Les compétences de base nécessaires à la gestion d'un environnement vSphere et d'ONTAP
- Un système de stockage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) exécutant {ontap_version}
- Identifiants ONTAP (nom du SVM, ID d'utilisateur et mot de passe)
- WWPN ONTAP des informations relatives à l'hôte, à la cible et aux SVM et aux LUN
- ["La fiche de configuration FC remplie"](#)
- Informations d'identification du serveur vCenter
- Informations sur les hôtes vSphere
 - {vsphere_version}
- Commutateur(s) de structure
 - Avec ports de données FC ONTAP connectés et hôtes vSphere
 - Avec la fonctionnalité NPIV (N_port ID Virtualization) activée
 - Créer une seule zone cible d'initiateur.
 - Créer une zone pour chaque initiateur (zone initiateur unique).
 - Pour chaque zone, inclure une cible faisant l'interface logique (WWPN) FC ONTAP pour les SVM. Il devrait y avoir au minimum deux interfaces logiques par nœud et par SVM. N'utilisez pas le WWPN des ports physiques.
- Un outil ONTAP pour VMware vSphere est déployé, configuré et prêt à l'emploi.

Provisionnement d'un datastore VMFS

Pour provisionner un datastore VMFS, procédez comme suit :

1. Vérifier la compatibilité avec le ["Matrice d'interopérabilité \(IMT\)"](#)
2. Vérifiez que le ["La configuration FCP est prise en charge"](#).

Tâches ONTAP

1. ["Vérifiez que vous disposez d'une licence ONTAP pour FCP."](#)
 - a. Utilisez le `system license show` Commande permettant de vérifier que FCP est répertorié.
 - b. Utiliser `licen se add -license-code <license code>` pour ajouter la licence.
2. S'assurer que le protocole FCP est activé sur le SVM
 - a. ["Vérifier le FCP sur un SVM existant."](#)
 - b. ["Configurer FCP sur un SVM existant."](#)
 - c. ["Créer s nouveau SVM avec le FCP"](#)
3. Vérifier que les interfaces logiques FCP sont disponibles sur un SVM.
 - a. Utiliser `Network Interface show` Pour vérifier l'adaptateur FCP.
 - b. Lorsqu'un SVM est créé avec l'interface utilisateur graphique, les interfaces logiques font partie de ce processus.
 - c. Pour renommer les interfaces réseau, utilisez `Network Interface modify`.
4. ["Créer et mapper une LUN."](#) Ignorez cette étape si vous utilisez les outils ONTAP pour VMware vSphere.

Tâches VMware vSphere

1. Vérifiez que les pilotes HBA sont installés. Les adaptateurs HBA pris en charge par VMware disposent de pilotes déployés clé en main et doivent être visibles dans ["Informations sur l'adaptateur de stockage"](#).
2. ["Provisionnement d'un datastore VMFS avec les outils ONTAP"](#).

Datastore VMFS vSphere - protocole de stockage Fibre Channel over Ethernet avec ONTAP

Cette section aborde la création d'un datastore VMFS avec le protocole de transport Fibre Channel over Ethernet (FCoE) vers le stockage ONTAP.

Ce dont vous avez besoin

- Les compétences de base nécessaires à la gestion d'un environnement vSphere et d'ONTAP
- Un système de stockage ONTAP (FAS/AFF/CVO/ONTAP Select) exécutant {ontap_version}
- Identifiants ONTAP (nom du SVM, ID d'utilisateur et mot de passe)
- ["Une combinaison FCoE prise en charge"](#)
- ["Une fiche de configuration remplie"](#)
- Informations d'identification du serveur vCenter
- Informations sur les hôtes vSphere
 - {vsphere_version}
- Commutateur(s) de structure
 - Avec des ports de données FC ONTAP ou des hôtes vSphere connectés

- Avec la fonctionnalité NPIV (N_port ID Virtualization) activée
- Créer une seule zone cible d'initiateur.
- ["Segmentation FC/FCoE configurée"](#)
- Commutateur(s) réseau
 - Prise en charge de FCoE
 - Prise en charge de DCB
 - ["Trames Jumbo pour FCoE"](#)
- L'outil ONTAP pour VMware vSphere est déployé, configuré et prêt à l'emploi

Provisionnement d'un datastore VMFS

- Vérifiez la compatibilité avec le ["Matrice d'interopérabilité \(IMT\)"](#).
- ["Vérifiez que la configuration FCoE est prise en charge"](#).

Tâches ONTAP

1. ["Vérifiez la licence ONTAP pour FCP."](#)
 - a. Utilisez le `system license show` Commande pour vérifier que le FCP est répertorié.
 - b. Utiliser `license add -license-code <license code>` pour ajouter une licence.
2. Vérifier que le protocole FCP est activé sur le SVM
 - a. ["Vérifier le FCP sur un SVM existant."](#)
 - b. ["Configurer FCP sur un SVM existant."](#)
 - c. ["Créer un nouveau SVM avec le FCP"](#)
3. Vérifier que les interfaces logiques FCP sont disponibles sur le SVM.
 - a. Utiliser `Network Interface show` Pour vérifier l'adaptateur FCP.
 - b. Lorsque le SVM est créé avec l'interface utilisateur graphique, les interfaces logiques font partie de ce processus.
 - c. Pour renommer l'interface réseau, utilisez `Network Interface modify`.
4. ["Créer et mapper une LUN"](#); Ignorez cette étape si vous utilisez les outils ONTAP pour VMware vSphere.

Tâches VMware vSphere

1. Vérifiez que les pilotes HBA sont installés. Les pilotes déployés clé en main sur les HBA pris en charge par VMware doivent être visibles dans ["informations sur l'adaptateur de stockage"](#).
2. ["Provisionnement d'un datastore VMFS avec les outils ONTAP"](#).

Datastore VMFS vSphere - stockage iSCSI back-end avec ONTAP

Cette section décrit la création d'un datastore VMFS avec un stockage iSCSI ONTAP.

Pour le provisionnement automatisé, utilisez le script suivant : [\[Ansible\]](#).

Ce dont vous avez besoin

- Les compétences de base nécessaires à la gestion d'un environnement vSphere et d'ONTAP.
- Un système de stockage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) exécutant {ontap_version}
- Identifiants ONTAP (nom du SVM, ID d'utilisateur et mot de passe)
- Informations relatives au port réseau ONTAP, au SVM et aux LUN pour iSCSI
- ["Une fiche de configuration iSCSI remplie"](#)
- Informations d'identification du serveur vCenter
- Informations sur les hôtes vSphere
 - {vsphere_version}
- Informations IP de l'adaptateur VMKernel iSCSI
- Commutateur(s) réseau
 - Grâce aux ports de données du système ONTAP et aux hôtes vSphere connectés
 - VLAN(s) configurés(s) pour iSCSI
 - (Facultatif) agrégation de liens configurée pour les ports de données réseau ONTAP
- L'outil ONTAP pour VMware vSphere est déployé, configuré et prêt à l'emploi

Étapes

1. Vérifiez la compatibilité avec le ["Matrice d'interopérabilité \(IMT\)"](#).
2. ["Vérifiez que la configuration iSCSI est prise en charge."](#)
3. Effectuez les tâches ONTAP et vSphere suivantes.

Tâches ONTAP

1. ["Vérifiez la licence ONTAP pour iSCSI"](#).
 - a. Utilisez le `system license show` Commande pour vérifier si iSCSI est répertorié.
 - b. Utiliser `license add -license-code <license code>` pour ajouter la licence.
2. ["Vérifier que le protocole iSCSI est activé sur le SVM"](#)
3. Vérifier que les interfaces logiques réseau iSCSI sont disponibles sur le SVM.



Lorsqu'un SVM est créé via l'interface utilisateur graphique, les interfaces réseau iSCSI sont également créées.

4. Utilisez le `Network interface` commande pour afficher ou apporter des modifications à l'interface réseau.



Deux interfaces réseau iSCSI par nœud sont recommandées.

5. ["Créez une interface réseau iSCSI."](#) Vous pouvez utiliser la stratégie de service blocs de données par défaut.
6. ["Vérifiez que le service Data-iscsi est inclus dans la stratégie de service."](#) Vous pouvez utiliser `network interface service-policy show` à vérifier.

7. "Vérifiez que les trames Jumbo sont activées."
8. "Créer et mapper la LUN." Ignorez cette étape si vous utilisez les outils ONTAP pour VMware vSphere. Répétez cette procédure pour chaque LUN.

Tâches VMware vSphere

1. Vérifiez qu'au moins une carte réseau est disponible pour le VLAN iSCSI. Deux cartes réseau sont à privilégier pour de meilleures performances et une meilleure tolérance aux pannes.
2. "Identifier le nombre de cartes réseau physiques disponibles sur l'hôte vSphere."
3. "Configurez l'initiateur iSCSI." Un cas d'utilisation typique est un initiateur iSCSI logiciel.
4. "Vérifiez que la pile TCP/IP pour iSCSI est disponible".
5. "Vérifiez que les groupes de ports iSCSI sont disponibles".
 - Nous utilisons généralement un seul commutateur virtuel avec plusieurs ports de liaison ascendante.
 - Utilisez le mappage de carte 1:1.
6. Vérifiez que les adaptateurs iSCSI VMKernel sont activés pour correspondre au nombre de cartes réseau et que les adresses IP sont attribuées.
7. "Reliez la carte logicielle iSCSI aux adaptateurs VMKernel iSCSI."
8. "Provisionnement du datastore VMFS avec les outils ONTAP". Répétez cette étape pour tous les datastores.
9. "Vérifier la prise en charge de l'accélération matérielle."

Et la suite ?

Une fois ces tâches terminées, le datastore VMFS est prêt à utiliser pour le provisionnement des machines virtuelles.

PlayBook Ansible

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
        password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin
```

```

# Generate Session ID for ONTAP tools with vCenter
- name: Generate a Session ID for ONTAP tools with vCenter
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/security/user/login"
    validate_certs: false
    method: POST
    return_content: yes
    body_format: json
    body:
      vcenterUserName: "{{ vcenter_username }}"
      vcenterPassword: "{{ vcenter_password }}"
  register: login

# Get existing registered ONTAP Cluster info with ONTAP tools
- name: Get ONTAP Cluster info from ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
    validate_certs: false
    method: Get
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"

```

```

    validate_certs: false
    method: GET
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      cluster-id: "{{ ontap_svm_id }}"
  when: ontap_svm_id != ''
  register: aggrinfo

- name: Select Aggregate with max free capacity
  set_fact:
    aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
  vars:
    aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB
  set_fact:
    datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

- name: Get vSphere Cluster Info
  uri:
    url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
    validate_certs: false
    method: GET
    return_content: yes
    body_format: json
    headers:
      vmware-api-session-id: "{{ vclogin.json.value }}"
  when: vsphere_cluster != ''
  register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
    validate_certs: false
    method: POST
    return_content: yes
    status_code: [200]
    body_format: json
    body:
      traditionalDatastoreRequest:
        name: "{{ iscsi_datastore_name }}"
        datastoreType: VMFS

```



```

    protocol: ISCSI
    spaceReserve: Thin
    clusterID: "{{ ontap_cluster_id }}"
    svmID: "{{ ontap_svm_id }}"
    targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
    datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
    vmfsFileSystem: VMFS6
    aggrName: "{{ aggr_name }}"
    existingFlexVolName: ""
    volumeStyle: FLEXVOL
    datastoreClusterMoref: ""
  headers:
    vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
  register: result
  changed_when: result.status == 200

```

Datstore VMFS vSphere - NVMe/FC avec ONTAP

Cette section décrit la création d'un datastore VMFS avec un stockage ONTAP utilisant NVMe/FC.

Ce dont vous avez besoin

- Compétences de base requises pour gérer un environnement vSphere et ONTAP.
- ["Présentation de base du protocole NVMe/FC"](#).
- Un système de stockage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) exécutant {ontap_version}
- Identifiants ONTAP (nom du SVM, ID d'utilisateur et mot de passe)
- WWPN ONTAP pour l'hôte, la cible et les SVM et informations relatives aux LUN
- ["Une fiche de configuration FC remplie"](#)
- Serveur vCenter
- Informations sur les hôtes vSphere ({vsphere_version})
- Commutateur(s) de structure
 - Avec des ports de données FC ONTAP et des hôtes vSphere connectés.
 - Avec la fonctionnalité NPIV (N_port ID Virtualization) activée.
 - Créer une seule zone cible d'initiateur.
 - Créer une zone pour chaque initiateur (zone initiateur unique).
 - Pour chaque zone, inclure une cible faisant l'interface logique (WWPN) FC ONTAP pour les SVM. Il devrait y avoir au minimum deux interfaces logiques par nœud et par SVM. N'utilisez pas le WWPN des ports physiques.

Provisionner le datastore VMFS

1. Vérifiez la compatibilité avec le ["Matrice d'interopérabilité \(IMT\)"](#).
2. ["Vérifiez que la configuration NVMe/FC est prise en charge."](#)

Tâches ONTAP

1. ["Vérifiez la licence ONTAP pour FCP."](#) Utilisez le `system license show` Commande et vérifiez si NVMe_of est répertorié. Utiliser `license add -license-code <license code>` pour ajouter une licence.
2. Vérifier que le protocole NVMe est activé sur le SVM
 - a. ["Configuration des SVM pour NVMe"](#)
3. Vérifier que les interfaces logiques NVMe/FC sont disponibles sur les SVM.
 - a. Utiliser `Network Interface show` Pour vérifier l'adaptateur FCP.
 - b. Lorsqu'un SVM est créé avec l'interface utilisateur graphique, les interfaces logiques font partie de ce processus.
 - c. Pour renommer l'interface réseau, utilisez la commande `Network Interface modify`.
4. ["Créez un espace de noms et un sous-système NVMe"](#)

Tâches VMware vSphere

1. Vérifiez que les pilotes HBA sont installés. Les pilotes déployés sont prêts à l'emploi pour les HBA pris en charge par VMware. Ils doivent être visibles à l'adresse ["Informations sur l'adaptateur de stockage"](#)
2. ["Effectuez les tâches d'installation et de validation du pilote NVMe hôte vSphere"](#)
3. ["Créer un datastore VMFS"](#)

Provisionnement traditionnel du stockage de fichiers

Provisionnement traditionnel du stockage de fichiers vSphere avec ONTAP

VMware vSphere prend en charge les protocoles NFS suivants, tous deux prenant en charge ONTAP.

- ["NFS version 3"](#)
- ["NFS version 4.1"](#)

Si vous avez besoin d'aide pour sélectionner la version NFS appropriée pour vSphere, vérifiez ["Cette comparaison des versions client NFS"](#).

Référence

["Fonctionnalités du datastore et du protocole vSphere : NFS"](#)

Datastore vSphere NFS - version 3 avec ONTAP

Création du datastore NFS version 3 avec stockage NAS ONTAP.

Ce dont vous avez besoin

- Les compétences de base nécessaires à la gestion d'un environnement vSphere et d'ONTAP.
- Un système de stockage ONTAP (FAS/AFF/CVO/ONTAP Select/Service de volume cloud/Azure NetApp Files) exécutant {ONTAP_version}
- Identifiants ONTAP (nom du SVM, ID utilisateur, mot de passe)
- Informations sur le port réseau ONTAP, le SVM et le LUN pour NFS
 - ["Une fiche de configuration NFS remplie"](#)
- Informations d'identification du serveur vCenter
- Informations sur le ou les hôtes vsphere pour {vsphere_version}
- Informations IP de l'adaptateur NFS VMKernel
- Commutateur(s) réseau
 - Grâce aux ports de données du système ONTAP et aux hôtes vSphere connectés
 - VLAN(s) configurés(s) pour NFS
 - (Facultatif) agrégation de liens configurée pour les ports de données réseau ONTAP
- L'outil ONTAP pour VMware vSphere est déployé, configuré et prêt à l'emploi

Étapes

- Vérifiez la compatibilité avec le ["Matrice d'interopérabilité \(IMT\)"](#)
 - ["Vérifiez que la configuration NFS est prise en charge."](#)
- Effectuez les tâches ONTAP et vSphere suivantes.

Tâches ONTAP

1. ["Vérifiez la licence ONTAP pour NFS."](#)
 - a. Utilisez le `system license show` Commande et vérifiez que NFS est répertorié.
 - b. Utiliser `license add -license-code <license code>` pour ajouter une licence.
2. ["Suivez le workflow de configuration NFS."](#)

Tâches VMware vSphere

["Suivre le workflow de la configuration client NFS pour vSphere."](#)

Référence

["Fonctionnalités du datastore et du protocole vSphere : NFS"](#)

Et la suite ?

Une fois ces tâches effectuées, le datastore NFS est prêt à consommer pour le provisionnement des machines virtuelles.

Datastore vSphere NFS - version 4.1 avec ONTAP

Cette section décrit la création d'un datastore NFS version 4.1 avec stockage NAS ONTAP.

Ce dont vous avez besoin

- Les compétences de base nécessaires à la gestion d'un environnement vSphere et d'ONTAP
- Système de stockage ONTAP (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) exécutant {ontap_version}
- Identifiants ONTAP (nom du SVM, ID utilisateur, mot de passe)
- Informations sur le port réseau ONTAP, le SVM et le LUN pour NFS
- ["Une fiche de configuration NFS remplie"](#)
- Informations d'identification du serveur vCenter
- Informations sur l'hôte(s) vSphere {vsphere_version}
- Informations IP de l'adaptateur NFS VMKernel
- Commutateur(s) réseau
 - Grâce aux ports de données réseau du système ONTAP, aux hôtes vSphere et aux connexions
 - VLAN(s) configurés(s) pour NFS
 - (Facultatif) agrégation de liens configurée pour les ports de données réseau ONTAP
- Outils ONTAP pour VMware vSphere déployés, configurés et prêts à l'emploi

Étapes

- Vérifier la compatibilité avec le ["Matrice d'interopérabilité \(IMT\)."](#)
 - ["Vérifiez que la configuration NFS est prise en charge."](#)
- Effectuez les tâches ONTAP et vSphere ci-dessous.

Tâches ONTAP

1. ["Vérifier la licence ONTAP pour NFS"](#)
 - a. Utilisez `system license show` Commande pour vérifier si NFS est répertorié.
 - b. Utilisez `license add -license-code <license code>` pour ajouter une licence.
2. ["Suivez le workflow de configuration NFS"](#)

Tâches VMware vSphere

["Suivez le workflow NFS client Configuration for vSphere."](#)

Et la suite ?

Une fois ces tâches effectuées, le datastore NFS est prêt à consommer pour le provisionnement des machines virtuelles.

Postes de travail virtuels

Services de postes de travail virtuels (VDS)

VDI cloud hybride avec NetApp Virtual Desktop Service

Tr-4861 : VDI dans le cloud hybride avec service de postes de travail virtuels

Technologiques Suresh, NetApp

VDS (Virtual Desktop Service) NetApp orchestre les services RDS (Remote Desktop Services) dans les principaux clouds publics et privés. VDS prend en charge Windows Virtual Desktop (WVD) sur Microsoft Azure. VDS automatise de nombreuses tâches à effectuer après le déploiement de WVD ou RDS, notamment la configuration des partages de fichiers SMB (pour les profils d'utilisateurs, les données partagées et le disque dur domestique des utilisateurs), l'activation des fonctionnalités Windows, de l'installation des applications et des agents, du pare-feu et des règles, etc.

Les utilisateurs consomment VDS pour les postes de travail dédiés, les postes de travail partagés et les applications distantes. VDS fournit des événements utilisant des scripts pour automatiser la gestion des applications des bureaux et réduit le nombre d'images à gérer.

VDS fournit un portail de gestion unique pour la gestion des déploiements dans des environnements clouds publics et privés.

En valeur pour le client

Avec l'explosion de 2020 000 employés, les exigences de continuité de l'activité ont changé. Les départements INFORMATIQUES sont confrontés à de nouveaux challenges qui doivent provisionner rapidement les postes de travail virtuels. Par conséquent, ils nécessitent une agilité du provisionnement, une gestion à distance et les avantages en termes de coût total de possession d'un cloud hybride qui simplifie le provisionnement des ressources sur site et dans le cloud. Ils ont besoin d'une solution de cloud hybride qui :

- Répond à la réalité de l'espace de travail post-COVID pour mettre en place des modèles de travail flexibles dotés de dynamiques mondiales
- Favorise le travail par équipe en simplifiant et en accélérant le déploiement d'environnements de travail pour tous les employés, des travailleurs chargés de tâches aux utilisateurs intensifs
- Mobilise vos équipes en fournissant des ressources VDI riches et sécurisées, quel que soit l'emplacement physique
- Simplifie le déploiement du cloud hybride
- Automatise et simplifie la gestion de la réduction des risques

Cas d'utilisation

La VDI hybride avec NetApp VDS permet aux fournisseurs de services et aux administrateurs des postes de travail virtuels d'étendre facilement les ressources à d'autres environnements clouds sans affecter les utilisateurs. La présence de ressources sur site offre un meilleur contrôle des ressources et un large choix de solutions (calcul, GPU, stockage et réseau) pour répondre à la demande.

Cette solution s'applique aux cas d'utilisation suivants :

- Le cloud bursting permet aux postes de travail et aux applications distants de bénéficier de plus de demande croissante

- En réduisant le TCO des postes de travail et applications distants à longue durée d'exécution, et en les hébergeant sur site avec des ressources de processeurs graphiques et de stockage Flash
- Facilité de gestion des postes de travail et des applications distants dans les environnements clouds
- Bénéficiez de postes de travail et d'applications à distance en utilisant un modèle de logiciel en tant que service avec des ressources sur site

Public visé

La solution cible plusieurs groupes d'utilisateurs :

- Les architectes EUC/VDI qui souhaitent comprendre les exigences d'un VDS hybride
- Partenaires NetApp qui voudraient aider les clients en termes de besoins en termes d'applications et de postes de travail distants
- Clients NetApp HCI existants qui souhaitent répondre aux besoins des applications et des postes de travail à distance

Présentation du service NetApp Virtual Desktop Service

NetApp propose de nombreux services clouds, dont le provisionnement rapide du poste de travail virtuel avec des applications WVD ou distantes et l'intégration rapide à Azure NetApp Files.

Généralement, il faut plusieurs semaines pour provisionner et fournir des services de postes de travail distants aux clients. Outre le provisionnement, il peut être difficile de gérer les applications, les profils d'utilisateurs, les données partagées et les objets de stratégie de groupe pour appliquer les règles. Les règles de pare-feu peuvent augmenter la complexité et nécessiter des compétences et des outils séparés.

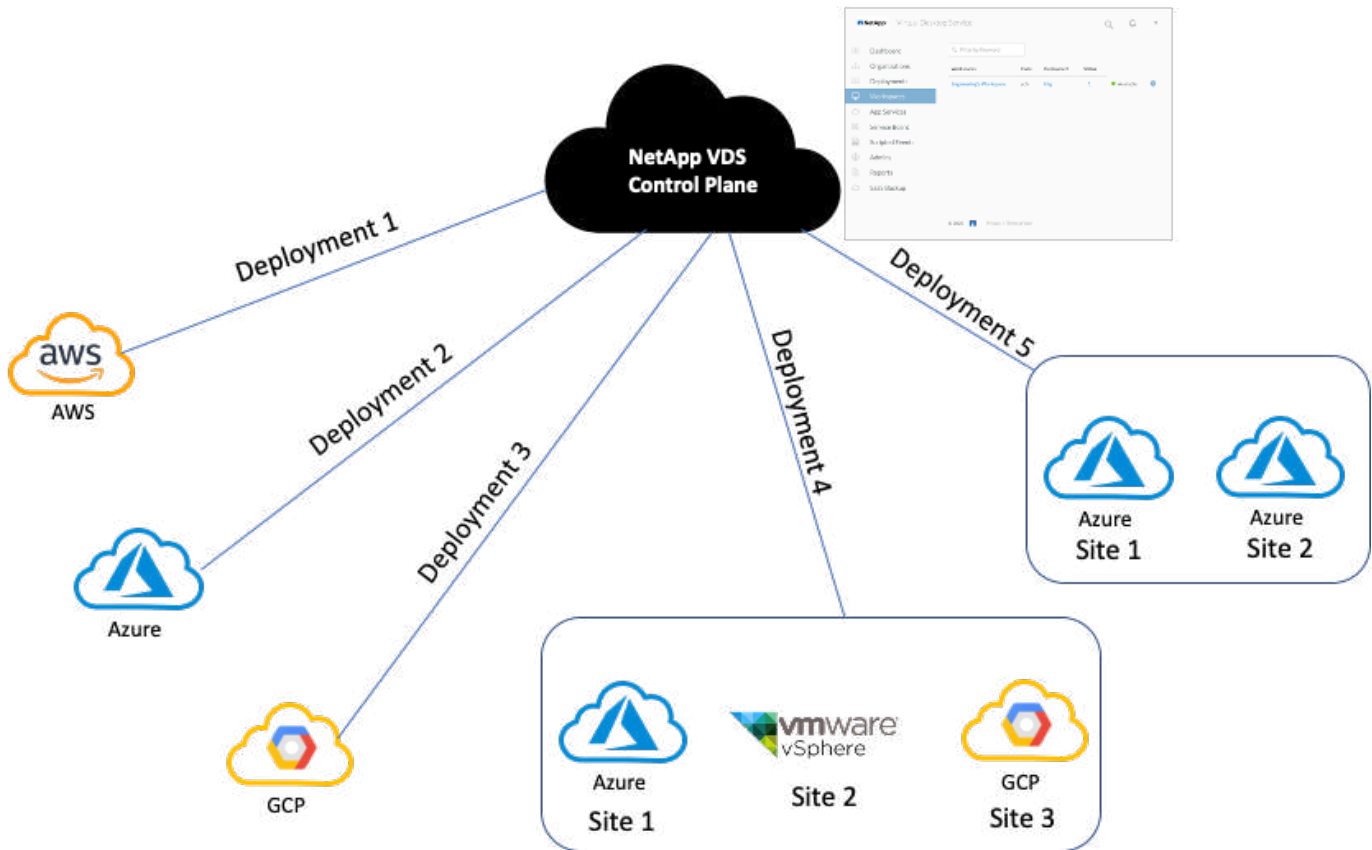
Avec le service Microsoft Azure Windows Virtual Desktop, Microsoft assure la maintenance des composants des services de poste de travail à distance. Ainsi, les clients peuvent se concentrer sur le provisionnement d'espaces de travail dans le cloud. Les clients doivent provisionner et gérer l'ensemble de la pile, ce qui nécessite des compétences particulières pour gérer leurs environnements VDI.

Avec NetApp VDS, les clients peuvent déployer rapidement des postes de travail virtuels sans se soucier de l'emplacement des composants de l'architecture tels que les courtiers, les passerelles, les agents, etc. Les clients qui ont besoin d'un contrôle total de leur environnement peuvent travailler avec une équipe de services professionnels pour atteindre leurs objectifs. Les clients consomment VDS en tant que service et peuvent ainsi se concentrer sur leurs principaux défis commerciaux.

NetApp VDS est une offre SaaS qui permet de gérer de manière centralisée de multiples déploiements dans des environnements AWS, Azure, GCP et clouds privés. Microsoft Windows Virtual Desktop est uniquement disponible sur Microsoft Azure. NetApp VDS orchestre les services Microsoft Remote Desktop Services dans d'autres environnements.

Microsoft propose plusieurs sessions sur Windows 10 exclusivement pour les environnements Windows Virtual Desktop sur Azure. L'authentification et l'identité sont gérées par la technologie de poste de travail virtuel ; WVD requiert la synchronisation d'Azure Active Directory (avec AD Connect) avec Active Directory et les VM de session joints à Active Directory. RDS requiert Active Directory pour l'identité et l'authentification des utilisateurs, ainsi que pour la jointure et la gestion du domaine de VM.

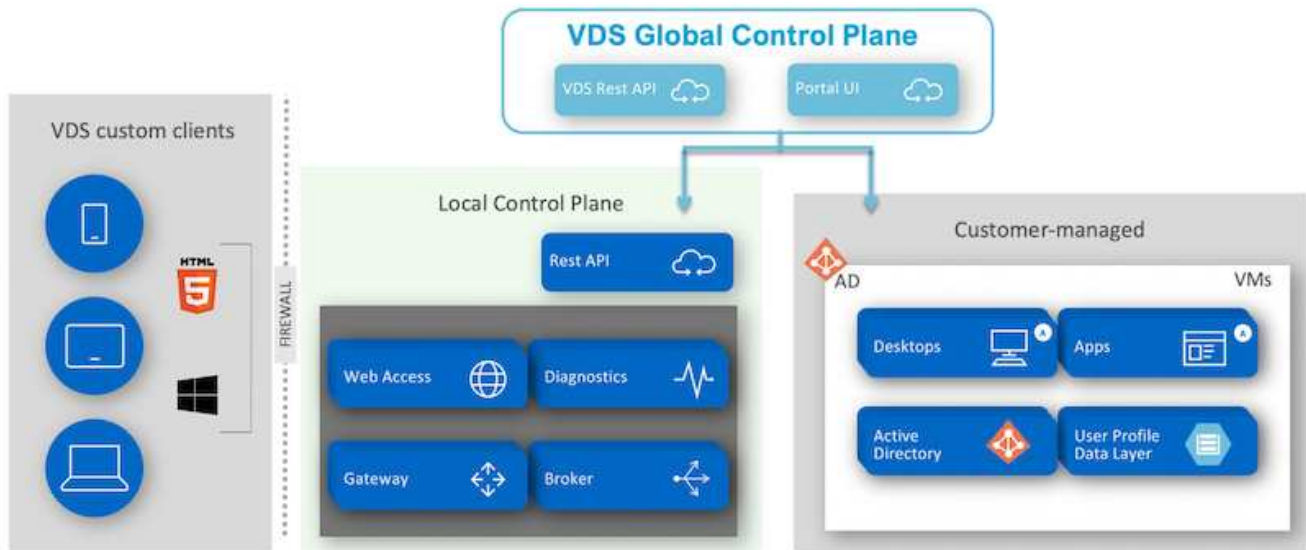
La figure suivante présente un exemple de topologie de déploiement.



Chaque déploiement est associé à un domaine Active Directory et fournit aux clients un point d'entrée d'accès pour les espaces de travail et les applications. Un fournisseur de services ou une entreprise qui possède plusieurs domaines Active Directory a généralement plus de déploiements. Un seul domaine Active Directory qui couvre plusieurs régions a généralement un déploiement unique avec plusieurs sites.

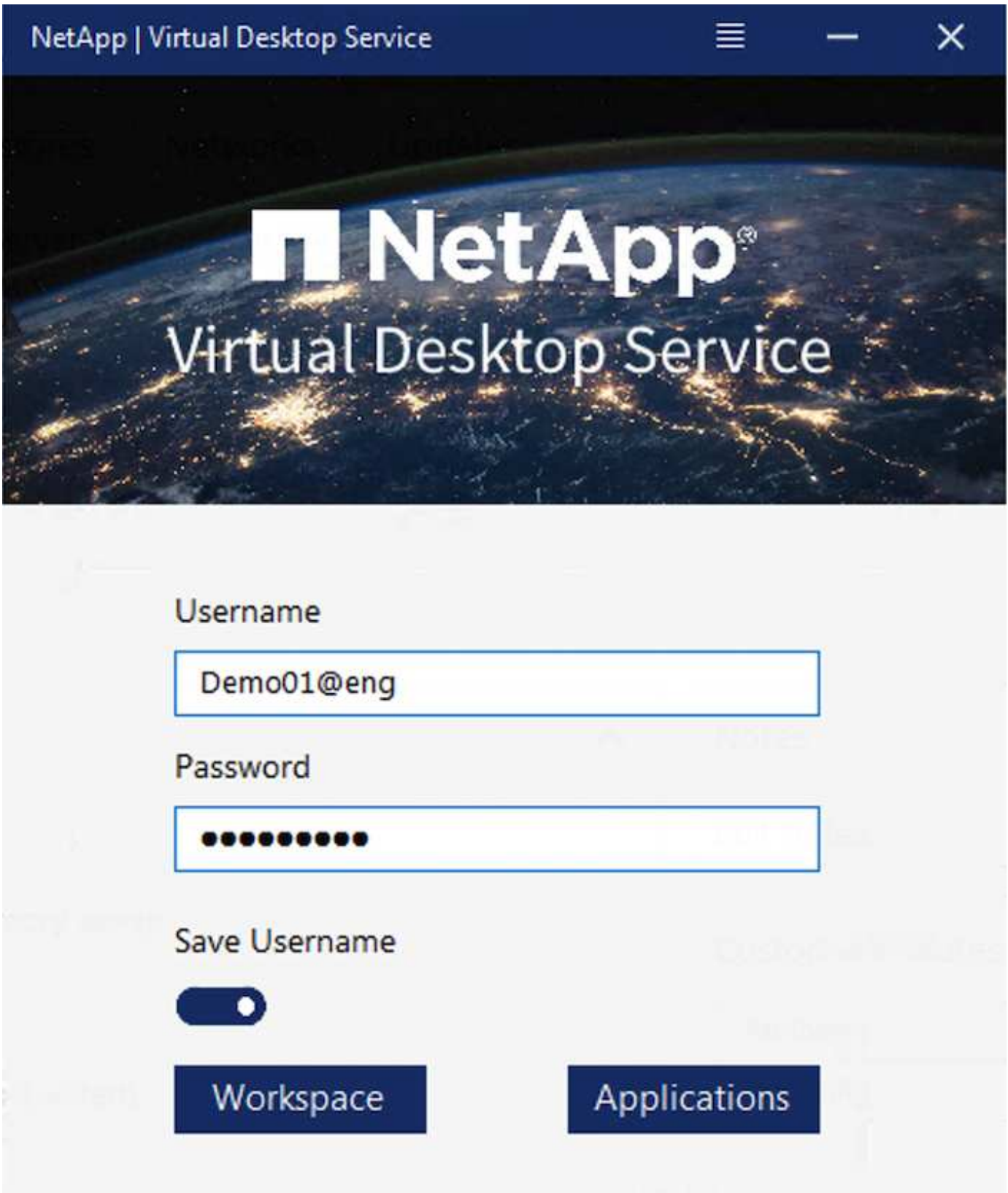
Pour WVD dans Azure, Microsoft propose une plateforme à la demande consommée par les systèmes NetApp VDS. Pour les autres environnements, NetApp VDS orchestre le déploiement et la configuration des services Microsoft Remote Desktop Services. Les systèmes VDS NetApp prennent en charge les ARM WVD Classic et WVD et ils peuvent également être utilisés pour mettre à niveau les versions existantes.

Chaque déploiement dispose de ses propres services de plateforme, qui comprennent Cloud Workspace Manager (terminal d'API REST), une passerelle HTML 5 (connexion aux VM à partir d'un portail de gestion VDS), des passerelles RDS (point d'accès pour les clients) et un contrôleur de domaine. La figure suivante décrit l'architecture du plan de contrôle VDS pour la mise en œuvre RDS.



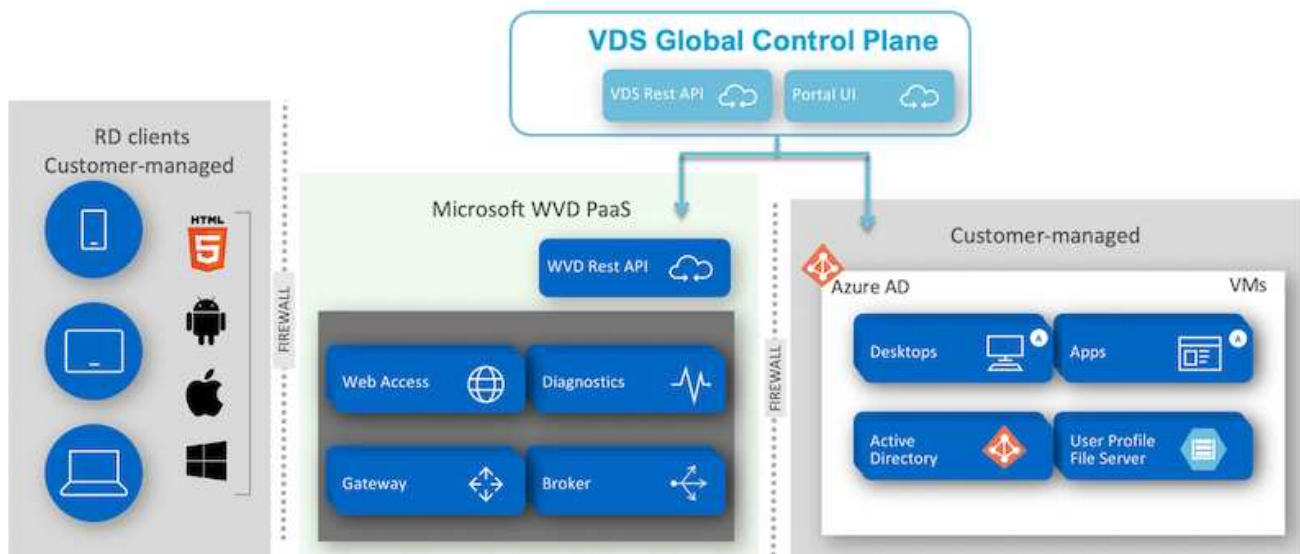
Pour les implémentations RDS, NetApp VDS peut être facilement accessible depuis Windows et les navigateurs à l'aide d'un logiciel client personnalisable afin d'inclure le logo du client et les images. En fonction des informations d'identification de l'utilisateur, il permet à l'utilisateur d'accéder aux espaces de travail et aux applications approuvés. Il n'est pas nécessaire de configurer les détails de la passerelle.

La figure suivante présente le client VDS NetApp.



Dans l'implémentation Azure WVD, Microsoft gère le point d'entrée d'accès pour les clients et peut être utilisé par un client Microsoft WVD disponible de manière native pour divers systèmes d'exploitation. Il est également accessible via un portail en ligne. La configuration du logiciel client doit être gérée par l'objet de stratégie de groupe (GPO, Group Policy Object) ou par d'autres méthodes que les clients préfèrent.

La figure suivante décrit l'architecture du plan de contrôle VDS pour les implémentations Azure WVD.



Outre le déploiement et la configuration des composants requis, NetApp VDS prend également en charge la gestion des utilisateurs, la gestion des applications, l'évolutivité des ressources et l'optimisation.

Les systèmes VDS NetApp peuvent créer des utilisateurs ou octroyer l'accès aux comptes utilisateurs existants aux services d'espace de travail cloud ou d'application. Le portail peut également être utilisé pour les réinitialisations de mot de passe et la délégation de l'administration d'un sous-ensemble de composants. Les administrateurs du service d'assistance ou les techniciens de niveau 3 peuvent créer des clichés instantanés des sessions utilisateur pour le dépannage ou se connecter aux serveurs à partir du portail.

NetApp VDS peut utiliser des modèles d'images que vous créez ou utiliser des modèles existants depuis le Marketplace pour un provisionnement basé sur le cloud. Pour réduire le nombre d'images à gérer, vous pouvez utiliser une image de base et toutes les applications supplémentaires dont vous avez besoin peuvent être provisionnées à l'aide du framework fourni afin d'inclure tous les outils de ligne de commande tels que Chocolatey, MSIX app Attach, PowerShell, etc. Même les scripts personnalisés peuvent être utilisés dans le cadre des événements de cycle de vie de la machine.

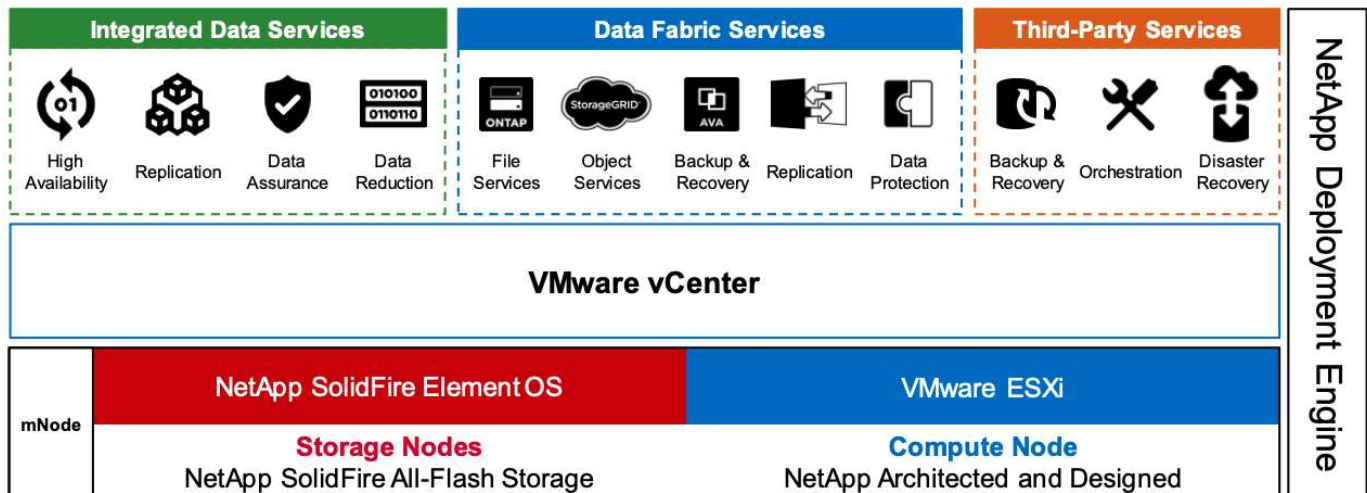
Présentation de NetApp HCI

NetApp HCI est une infrastructure de cloud hybride constituée d'un ensemble de nœuds de stockage et de nœuds de calcul. Elle est disponible en tant qu'unité à deux racks ou en 1 unité, selon le modèle. L'installation et la configuration requises pour déployer les machines virtuelles sont automatisées avec le moteur de déploiement NetApp. Les clusters de calcul sont gérés avec VMware vCenter, et les clusters de stockage sont gérés à l'aide du plug-in vCenter déployé avec NDE. Une VM de gestion appelée le nœud M est déployée dans le cadre du moteur de déploiement NetApp.

NetApp HCI prend en charge les fonctions suivantes :

- Mises à niveau des versions
- Envoi d'événements vers vCenter
- Gestion du plug-in vCenter
- Un tunnel VPN pour la prise en charge
- Le collecteur du conseiller numérique NetApp Active IQ (également appelé conseiller numérique)

- L'extension des services cloud de NetApp sur site, ce qui donne la possibilité d'une infrastructure de cloud hybride. La figure suivante décrit les composants d'HCI.



Nœuds de stockage

Les nœuds de stockage sont disponibles en unité de rack demi-largeur ou pleine largeur. Dans un premier temps, quatre nœuds de stockage au moins sont nécessaires et un cluster peut évoluer jusqu'à 40 nœuds. Un cluster de stockage peut être partagé entre plusieurs clusters de calcul. Tous les nœuds de stockage disposent d'un contrôleur de cache afin d'améliorer les performances en écriture. Un seul nœud fournit 50 000 ou 100 000 IOPS à une taille de bloc de 4 Ko.

Les nœuds de stockage NetApp HCI exécutent le logiciel NetApp Element qui permet d'atteindre des limites de QoS minimales, maximales ou en rafale. Le cluster de stockage prend en charge plusieurs nœuds de stockage, bien qu'un nœud de stockage ne puisse pas dépasser un tiers de la capacité totale.

Nœuds de calcul



NetApp prend en charge son stockage connecté à n'importe quel serveur de calcul répertorié dans le "[Guide de compatibilité avec VMware](#)".

Les nœuds de calcul sont disponibles en demi-largeur, pleine largeur et en deux tailles d'unité de rack. Les nœuds NetApp HCI H410C et H610C sont basés sur des processeurs Intel Skylake évolutifs. La technologie H615C est basée sur des processeurs Intel Cascade Lake évolutifs de deuxième génération. Il existe deux modèles de calcul qui contiennent des GPU : ce dernier contient deux cartes NVIDIA M10 et la H615C contient trois cartes NVIDIA T4.



La NVIDIA T4 dispose de 40 cœurs RT qui fournissent la puissance de calcul nécessaire pour réaliser le traçage des rayons en temps réel. Le même modèle de serveur utilisé par les concepteurs et les ingénieurs peut désormais être utilisé par les artistes pour créer des images photoréalistes qui offrent des rebondissements de lumière sur les surfaces comme dans la vie réelle. Ce processeur graphique compatible RTX permet de tracer en temps réel jusqu'à cinq rayons Giga par seconde. Combiné au logiciel Quadro Virtual Data Center Workstation (Quadro VDWS), le NVIDIA T4 permet aux artistes de créer des conceptions photoréalistes avec des ombres, des reflets et des réfractions précis sur n'importe quel appareil, où.

Les cœurs Tensor vous permettent d'exécuter des workloads d'inférence d'apprentissage profond. Lors de l'exécution de ces charges de travail, une NVIDIA T4 optimisée avec Quadro VDWS peut assurer des performances jusqu'à 25 fois plus rapides qu'une machine virtuelle basée sur un serveur à processeur uniquement. Un système NetApp H615C équipé de trois cartes NVIDIA T4 dans une unité de rack est une solution idéale pour les workloads graphiques et gourmands en ressources de calcul.

La figure suivante répertorie les cartes graphiques NVIDIA et compare leurs fonctionnalités.

| NVIDIA GPUs Recommended for Virtualization | | | | Available on NetApp HCI H615C | Available on NetApp HCI H610C | |
|--|---|---|--|---|---|---|
| | V100S | RTX 8000 | RTX 6000 | T4 | M10 | P6 |
| GPU | 1 NVIDIA Volta | 1 NVIDIA Turing | 1 NVIDIA Turing | 1 NVIDIA Turing | 4 NVIDIA Maxwell | 1 NVIDIA Pascal |
| CUDA Cores | 5,120 | 4,608 | 4,608 | 2,560 | 2,560 (640 per GPU) | 2,048 |
| Tensor Cores | 640 | 576 | 576 | 320 | — | — |
| RT Cores | — | 72 | 72 | 40 | — | — |
| Guaranteed QoS (GPU Scheduler) | ✓ | ✓ | ✓ | ✓ | — | ✓ |
| Live Migration | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Multi-vGPU | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Memory Size | 32/16 GB HBM2 | 48 GB GDDR6 | 24 GB GDDR6 | 16 GB GDDR6 | 32 GB GDDR5 (8 GB per GPU) | 16 GB GDDR5 |
| vGPU Profiles | 1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB | 1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB | 1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB | 1 GB, 2 GB, 4 GB, 8 GB, 16 GB | 0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB | 1 GB, 2 GB, 4 GB, 8 GB, 16 GB |
| Form Factor | PCIe 3.0 dual slot and SXM2 | PCIe 3.0 dual slot | PCIe 3.0 dual slot | PCIe 3.0 single slot | PCIe 3.0 dual slot | MXM (blade servers) |
| Power | 250 W /300 W (SXM2) | 250 W | 250 W | 70 W | 225 W | 90 W |
| Thermal | passive | passive | passive | passive | passive | bare board |
| vGPU Software Support | Quadro vDWS, GRID vPC, GRID vApps, vComputeServer | Quadro vDWS, GRID vPC, GRID vApps, vComputeServer | Quadro vDWS, GRID vPC, GRID vApps, vComputeServer | Quadro vDWS, GRID vPC, GRID vApps, vComputeServer | Quadro vDWS, GRID vPC, GRID vApps | Quadro vDWS, GRID vPC, GRID vApps, vComputeServer |
| Use Case | Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100 | High-end rendering, 3D design and creative workflows with Quadro vDWS | Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS | Entry-level to high-end 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software. | Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multimonitor support with NVIDIA GRID vPC/vApps | For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6 |

Le processeur graphique M10 reste la solution de coût total de possession la plus adaptée aux cas d'utilisation des travailleurs du savoir. Toutefois, le T4 constitue une excellente alternative pour standardiser les GPU sur plusieurs cas d'utilisation, comme les postes de travail virtuels, la performance graphique, le rendu interactif en temps réel et l'inférence. Grâce au T4, le DÉPARTEMENT INFORMATIQUE peut exploiter les mêmes ressources GPU pour exécuter des charges de travail mixtes—, par exemple, exécuter une infrastructure VDI pendant la journée, puis requalifier les ressources pour exécuter des charges de travail de calcul le soir.

Le nœud de calcul H610C est une taille de rack ; il s'agit d'une unité de rack qui consomme moins d'énergie. L' H615C prend en charge le codage et le décodage H.264 et H.265 (vidéo haute efficacité [HEVC]) 4:4:4. Il prend également en charge le décodeur VP9 de plus en plus intégré ; même le paquet de conteneurs WebM servi par YouTube utilise le codec VP9 pour la vidéo.

Le nombre de nœuds d'un cluster de calcul est dicté par VMware ; actuellement, il est 96 avec VMware vSphere 7.0 Update 1. L'association de différents modèles de nœuds de calcul dans un cluster est prise en charge lorsque la compatibilité vMotion améliorée (EVC) est activée.

Les licences NVIDIA

Lors de l'utilisation d'un H610C ou d'une technologie H615C, la licence du GPU doit être obtenue auprès des partenaires NVIDIA autorisés à revendre les licences. Vous pouvez trouver des partenaires NVIDIA avec le "[outil de recherche de partenaires](#)". Recherchez des compétences telles que Virtual GPU (vGPU) ou Tesla.

Le logiciel NVIDIA vGPU est disponible en quatre éditions :

- NVIDIA GRID Virtual PC (GRID VPC)
- NVIDIA GRID Virtual applications (vApps)
- Station de travail NVIDIA Quadro Virtual Data Center (Quadro VDWS)
- NVIDIA Virtual ComputeServer (vComputeServer)

PC virtuel GRID

Ce produit est idéal pour les utilisateurs qui recherchent un poste de travail virtuel offrant une expérience utilisateur exceptionnelle pour les applications Microsoft Windows, les navigateurs, la vidéo haute définition et la prise en charge multi-moniteurs. La solution NVIDIA GRID Virtual PC offre une expérience native dans un environnement virtualisé, ce qui vous permet d'exécuter toutes les applications de votre PC à des performances optimales.

APPLICATIONS virtuelles DE GRID

Les vApps DU GRID sont destinées aux entreprises qui déploient un hôte de session de bureau à distance (RDSH) ou d'autres solutions de streaming au niveau des applications ou des sessions. Conçus pour fournir des applications Microsoft Windows à des performances maximales, les postes de travail RDSH hébergés par Windows Server sont également pris en charge par les vApps DU GRID.

Station de travail Quadro Virtual Data Center

Cette édition est idéale pour les concepteurs grand public et haut de gamme qui utilisent de puissantes applications de création de contenu 3D comme Dassault CATIA, SOLIDWORKS, 3Dexcite, Siemens NX, PTC, Creo Schlumberger Petrel ou Autodesk Maya. La carte NVIDIA Quadro VDWS permet aux utilisateurs d'accéder à leurs applications graphiques professionnelles, avec des fonctionnalités et des performances complètes, partout sur n'importe quel périphérique.

NVIDIA Virtual ComputeServer

De nombreuses entreprises exécutent des charges de travail serveur gourmandes en ressources système, telles que l'intelligence artificielle (IA), l'apprentissage profond (AP) et la data science. Pour ces cas d'utilisation, le logiciel NVIDIA vComputeServer virtualise le processeur graphique NVIDIA, qui accélère les charges de travail serveur intensives en ressources de calcul grâce à des fonctionnalités telles que le code de correction d'erreur, le retrait de page, la liaison peer-to-peer sur NVLink et le multivGPU.



Une licence Quadro VDWS vous permet d'utiliser GRID VPC et NVIDIA vComputeServer.

Déploiement

Vous pouvez déployer NetApp VDS sur Microsoft Azure à l'aide d'une application de configuration disponible en fonction de la base de code requise. La version actuelle est disponible ["ici"](#) la version de présentation du produit à venir est également disponible ["ici"](#).

Voir ["vidéo"](#) pour des instructions de déploiement.



NetApp Virtual Desktop Service

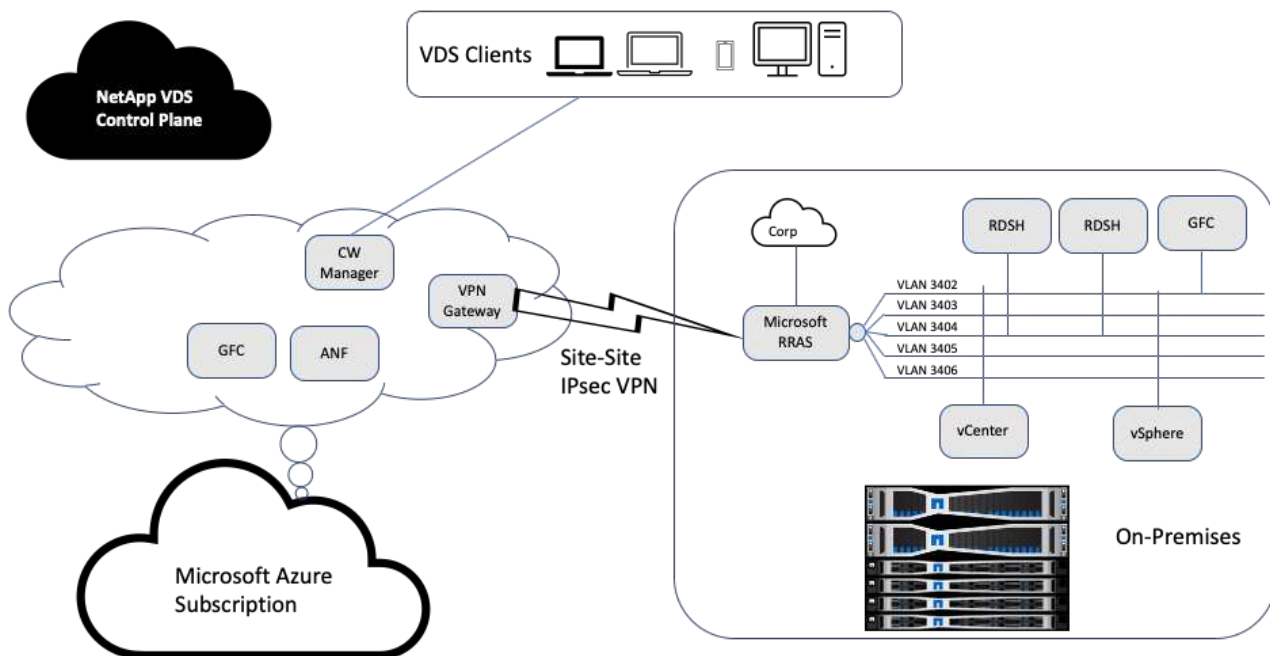
Deployment & AD Connect

Toby vanRoojen
Product Marketing Manager
June, 2020

Environnement cloud hybride

Le service NetApp Virtual Desktop peut être étendu aux environnements sur site lorsque la connectivité entre les ressources sur site et les ressources clouds. Les entreprises peuvent établir le lien vers Microsoft Azure à l'aide d'Express route ou d'une connexion VPN IPsec de site à site. Vous pouvez également créer des liens vers d'autres clouds de la même manière, soit à l'aide d'une liaison dédiée, soit avec un tunnel VPN IPsec.

Pour la validation de la solution, nous avons utilisé l'environnement décrit dans la figure suivante.



Sur site, nous disposons de plusieurs VLAN pour la gestion, des hôtes de session de postes de travail distants, etc. Ils se trouvaient sur le sous-réseau 172.21.146-150.0/24 et étaient acheminés vers le réseau d'entreprise à l'aide du service d'accès de routage à distance de Microsoft. Nous avons également effectué les tâches suivantes :

1. Nous avons noté l'adresse IP publique de Microsoft Routing and Remote Access Server (RRAS, identifié par IPchicken.com).
2. Nous avons créé une ressource de passerelle réseau virtuel (VPN par route) pour l'abonnement Azure.
3. Nous avons créé la connexion fournissant l'adresse de passerelle réseau locale pour l'adresse IP publique du serveur Microsoft RRAS.
4. Nous avons effectué la configuration VPN sur RRAS pour créer une interface virtuelle à l'aide de l'authentification pré-partagée fournie lors de la création de la passerelle VPN. S'il est configuré correctement, le VPN doit être à l'état connecté. Au lieu de Microsoft RRAS, vous pouvez également utiliser pfSense ou d'autres outils pertinents pour créer le tunnel VPN IPsec site à site. Étant donné qu'il est basé sur l'itinéraire, le tunnel redirige le trafic en fonction des sous-réseaux spécifiques configurés.

Microsoft Azure Active Directory fournit une authentification d'identité basée sur OAuth. Les authentifications de clients d'entreprise nécessitent généralement une authentification NTLM ou Kerberos. Les services de domaine Microsoft Azure Active Directory effectuent une synchronisation de hachage de mot de passe entre Azure Active Directory et les contrôleurs de domaine sur site à l'aide d'ADConnect.

Pour la validation de cette solution VDS hybride, nous avons initialement déployé sur Microsoft Azure et avons ajouté un site supplémentaire avec vSphere. L'avantage de cette approche est que les services de plateforme ont été déployés sur Microsoft Azure et ont ensuite été sauvegardés à l'aide du portail. Les services peuvent alors être facilement accessibles depuis n'importe où, même si la liaison VPN du site est indisponible.

Pour ajouter un autre site, nous avons utilisé un outil appelé DCConfig. Le raccourci vers cette application est disponible sur le bureau de la VM du gestionnaire d'espace de travail du cloud (CWMgr). Une fois cette application lancée, accédez à l'onglet sites de datacenter, ajoutez le nouveau site de datacenter et remplissez

les informations requises comme indiqué ci-dessous. L'URL pointe vers l'adresse IP vCenter. Assurez-vous que la VM CWMgr peut communiquer avec vCenter avant d'ajouter la configuration.



Assurez-vous que vSphere PowerCLI 5.1 sur CloudWorkspace Manager est installé pour permettre la communication avec l'environnement VMware vSphere.

La figure suivante décrit la configuration du site d'un data Center sur site.

The screenshot shows the 'Configuration' window with the 'DataCenter Sites' tab selected. On the left, a table lists two sites:

| DataCenter Site | Type | Is Primary | DataCenter Site Detail |
|-----------------|---------|-------------------------------------|------------------------|
| Site 1 | AzureRM | <input checked="" type="checkbox"/> | |
| Site 2 | vSphere | <input type="checkbox"/> | |

Below the table is a red instruction: "To delete DataCenter Site(s), Select it and right click to delete".

The right side of the interface shows the configuration for 'Site 2' (vSphere):

- DataCenter Site:** Site 2
- Hypervisor:** vSphere
- General Settings:**
 - Local VM Account:** Username: Administrator, Password: [masked]
 - Hypervisor Account:** Username: Administrator@vsphere, Password: [masked]
 - URL:** https://172.21.146.150/sdk/
 - VM Name Prefix:** [empty]
 - Max Concurrent Create Server:** 20
 - Subnet Mask:** 255.255.255.0
 - Default Gateway:** 172.21.148.250
 - Is Primary Hypervisor?:** Yes No
 - Must Set IpAddress Of VM:** Yes No
- DNS:**
 - Primary DNS:** 10.67.78.11
 - Secondary DNS:** [empty]
 - Set DNS Address:** Yes No
- vSphere:**
 - Data Center:** NetApp-HCI-Datacenter
 - Cluster:** [empty]
 - Resource Pool:** [empty]
 - Host Name:** [empty]
 - VM Folder:** VDS
 - Max VMs In Datastore:** -1
 - Min HD Free Space In Datastore GB:** -1
 - Min Ram Free GB:** -1

At the bottom, there are two checkboxes: 'Exclude vSphere DataStore' and 'Exclude vSphere ResourcePools', both currently unchecked.

Notez que des options de filtrage sont disponibles pour la ressource de calcul en fonction du cluster, du nom d'hôte ou de l'espace RAM disponible. Les options de filtrage de la ressource de stockage incluent l'espace libre minimal sur les datastores ou le nombre maximal de machines virtuelles par datastore. Les datastores peuvent être exclus à l'aide d'expressions régulières. Cliquez sur le bouton Enregistrer pour enregistrer la configuration.

Pour valider la configuration, cliquez sur le bouton Test ou cliquez sur Charger l'hyperviseur et cochez une liste déroulante sous la section vSphere. Il doit être rempli avec les valeurs appropriées. Il est recommandé de conserver l'hyperviseur principal sur yes pour le site de provisionnement par défaut.

Les modèles de machine virtuelle créés sur VMware vSphere sont utilisés en tant que collections de provisionnement sur VDS. Les collections de provisionnement sont disponibles sous deux formes : partagées et VDI. Le type de collecte de provisionnement partagé est utilisé pour les services de bureau à distance pour

lesquels une stratégie de ressources unique est appliquée à tous les serveurs. Le type VDI est utilisé pour les instances WVD pour lesquelles la stratégie de ressources est attribuée individuellement. Les serveurs d'une collection de provisionnement peuvent être affectés à l'un des trois rôles suivants :

- **TSDATA.** combinaison de services terminal Server et de rôle de serveur de données.
- **TS.** terminal Services (hôte de session).
- **DONNÉES.** serveur de fichiers ou serveur de bases de données. Lorsque vous définissez le rôle de serveur, vous devez choisir le modèle de machine virtuelle et le stockage (datastore). Le datastore choisi peut être réservé à un datastore spécifique ou vous pouvez utiliser l'option la moins utilisée dans laquelle le datastore est sélectionné en fonction de l'utilisation des données.

Chaque déploiement dispose des valeurs par défaut des ressources des machines virtuelles pour l'allocation des ressources cloud en fonction des utilisateurs actifs, du nombre fixe, de la charge des serveurs ou du nombre d'utilisateurs.

Test de charge d'un serveur unique avec VSI à la connexion

NetApp Virtual Desktop Service utilise le protocole Microsoft Remote Desktop Protocol pour accéder aux applications et aux sessions des postes de travail virtuels. L'outil Login VSI détermine le nombre maximal d'utilisateurs pouvant être hébergés sur un modèle de serveur spécifique. Connexion VSI simule la connexion utilisateur à des intervalles spécifiques et effectue des opérations utilisateur telles que l'ouverture de documents, la lecture et la rédaction de messages, l'utilisation d'Excel et PowerPoint, l'impression de documents, la compression de fichiers et la prise de pauses aléatoires. Il mesure alors les temps de réponse. Le temps de réponse des utilisateurs est faible lorsque l'utilisation des serveurs est faible et augmente lors de l'ajout de sessions utilisateur supplémentaires. Login VSI détermine la base en fonction des sessions de connexion de l'utilisateur initiales et indique la session utilisateur maximale lorsque la réponse de l'utilisateur dépasse 2 secondes de la ligne de base.

NetApp Virtual Desktop Service utilise le protocole Microsoft Remote Desktop Protocol pour accéder aux applications et sessions de postes de travail virtuels. Pour déterminer le nombre maximal d'utilisateurs pouvant être hébergés sur un modèle de serveur spécifique, nous avons utilisé l'outil Login VSI. Connectez-vous à VSI simule la connexion utilisateur à des intervalles spécifiques et effectue des opérations utilisateur telles que l'ouverture de documents, la lecture et la rédaction de messages, l'utilisation d'Excel et PowerPoint, l'impression de documents, la compression de fichiers, la prise de pauses aléatoires, etc. Il mesure également les temps de réponse. Le temps de réponse des utilisateurs est faible lorsque l'utilisation des serveurs est faible et augmente lors de l'ajout de sessions utilisateur supplémentaires. L'ISBC de connexion détermine la base en fonction des sessions de connexion utilisateur initiales et indique le nombre maximal de sessions utilisateur lorsque la réponse utilisateur dépasse 2 secondes de la ligne de base.

Le tableau suivant contient le matériel utilisé pour cette validation.

| Modèle | Nombre | Description |
|------------------|--------|--|
| NetApp HCI H610C | 4 | Trois dans un cluster pour les lanceurs, AD, DHCP, etc. Un serveur pour le test de charge. |
| NetApp HCI H615C | 1 | 2 x 24C Intel Xeon Gold 6282 @2,1 GHz. 1,5 TO DE RAM. |

Le tableau suivant contient le logiciel utilisé pour cette validation.

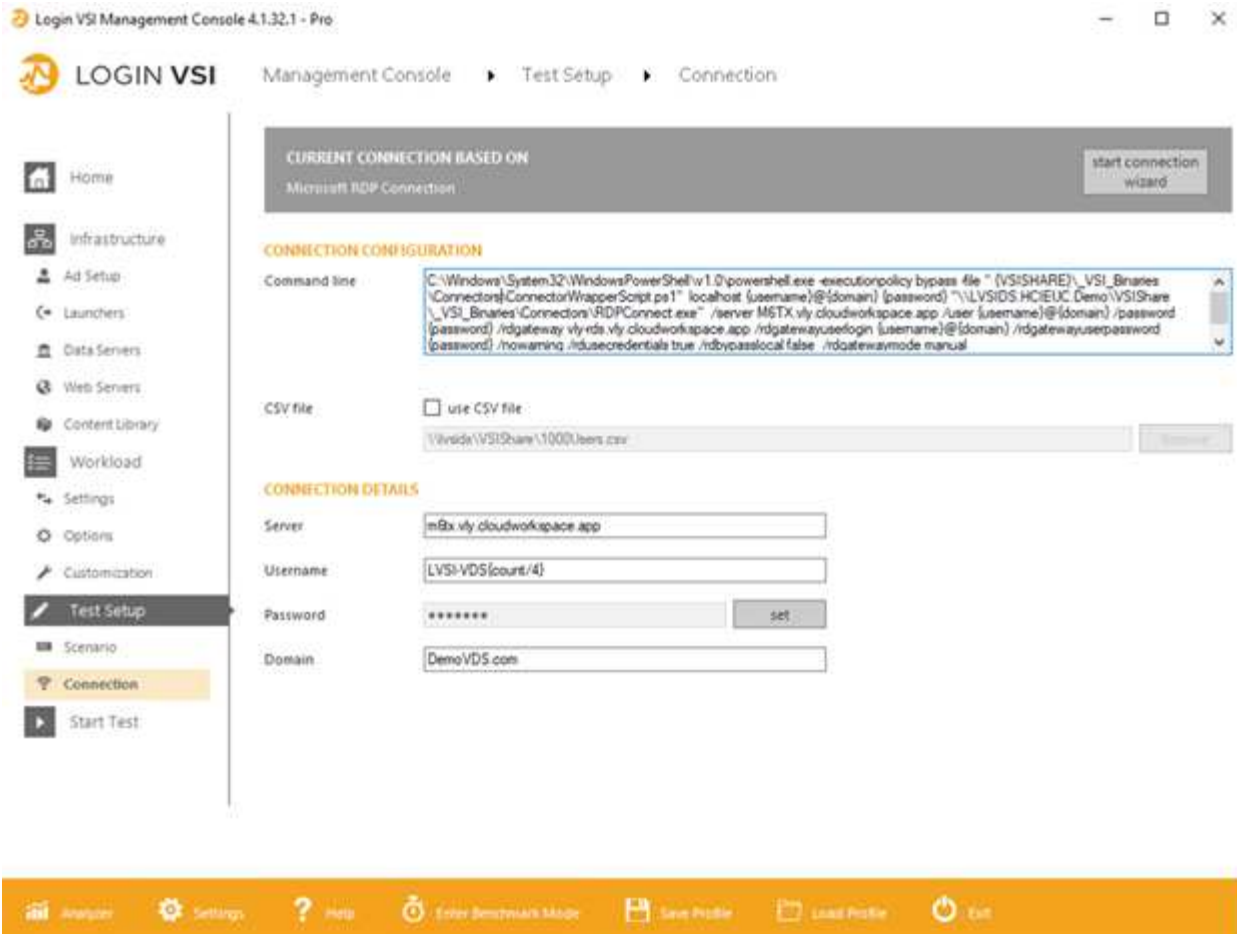
| Solution NetApp | Description |
|---|-------------------------|
| NetApp VDS 5.4 | Orchestration |
| Modèle de machine virtuelle Windows 2019 1809 | OS serveur pour RDSH |
| Connexion VSI | 4.1.32.1 |
| Mise à jour 3 de VMware vSphere 6.7 | Hyperviseur |
| Mise à jour 6.7 de VMware vCenter 3f | Outil de gestion VMware |

Les résultats du test Login VSI sont les suivants :

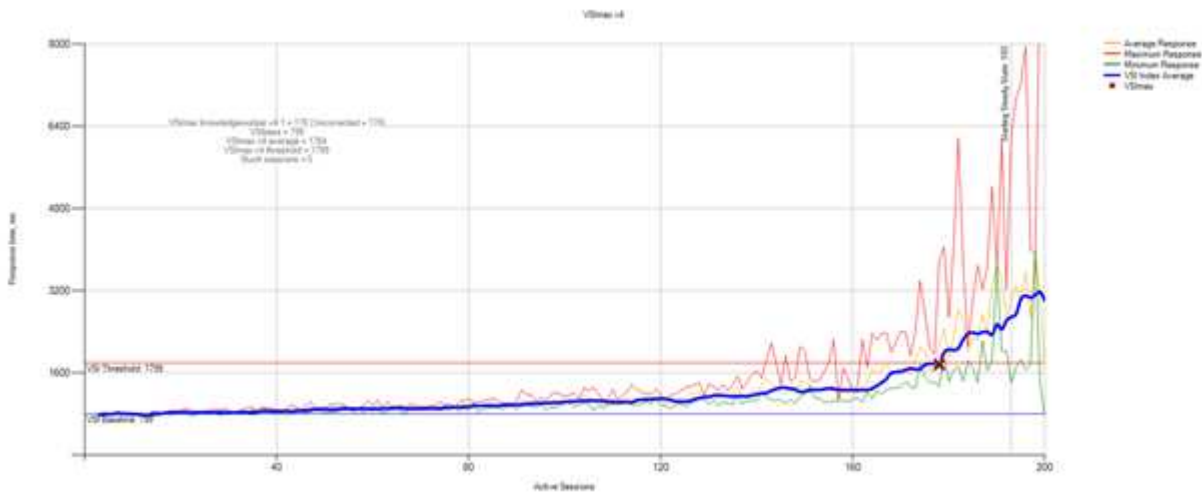
| Modèle | Configuration de machines virtuelles | Connexion de base VSI | Connexion VSI max |
|---------------|---|------------------------------|--------------------------|
| H610C | 8 vCPU, 48 Go de RAM, 75 Go de disque, profil 8Q vGPU | 799 | 178 |
| H615C | 12 vCPU, 128 Go de RAM, 75 Go de disque | 763 | 272 |

Si l'on tient compte des frontières de la sous-NUMA et de l'hyperthreading, les huit machines virtuelles choisies pour le test et la configuration des machines virtuelles dépendent des cœurs disponibles sur l'hôte.

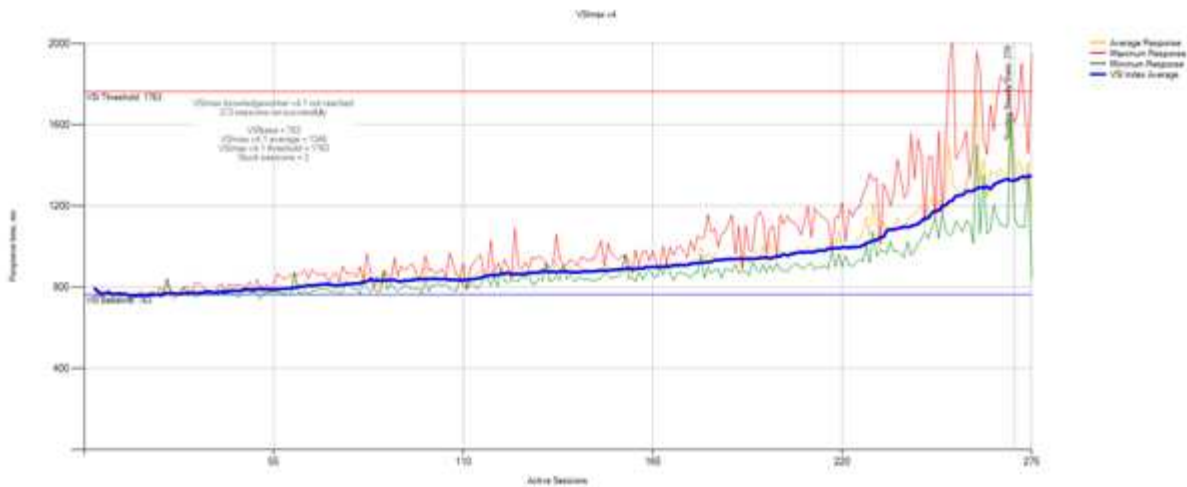
Nous avons utilisé 10 machines virtuelles de lancement sur H610C, qui ont utilisé le protocole RDP pour se connecter à la session utilisateur. La figure suivante illustre les informations de connexion VSI.



La figure suivante affiche le temps de réponse de Login VSI par rapport aux sessions actives du H610C.



La figure suivante affiche le temps de réponse de Login VSI par rapport aux sessions actives de l' H615C.



Les mesures de performances de Cloud Insights lors des tests VSI de connexion H615C pour l'hôte vSphere et les machines virtuelles sont présentées dans la figure suivante.



Portail de gestion

Le portail NetApp VDS Cloud Workspace Management Suite est disponible ["ici"](#) la version à venir est également disponible ["ici"](#).

Le portail permet une gestion centralisée de différents déploiements VDS, y compris un site défini pour les utilisateurs sur site, les utilisateurs administratifs, le catalogue d'applications et les événements avec script. Le portail est également utilisé par les utilisateurs administratifs pour le provisionnement manuel des applications si nécessaire et pour se connecter à n'importe quel ordinateur pour le dépannage.

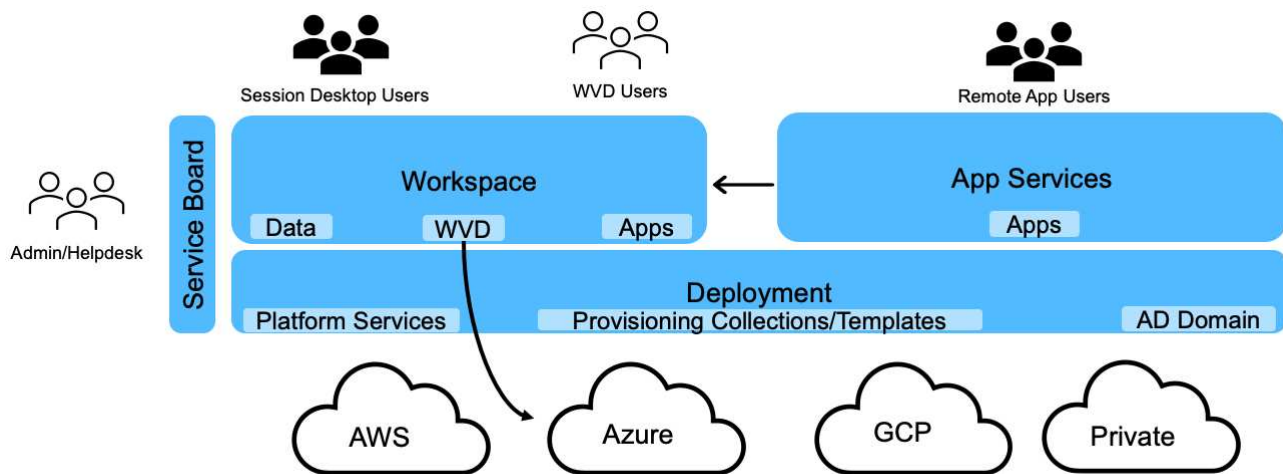
Les prestataires de services peuvent utiliser ce portail pour ajouter leurs propres partenaires de distribution et leur permettre de gérer leurs propres clients.

Gestion des utilisateurs

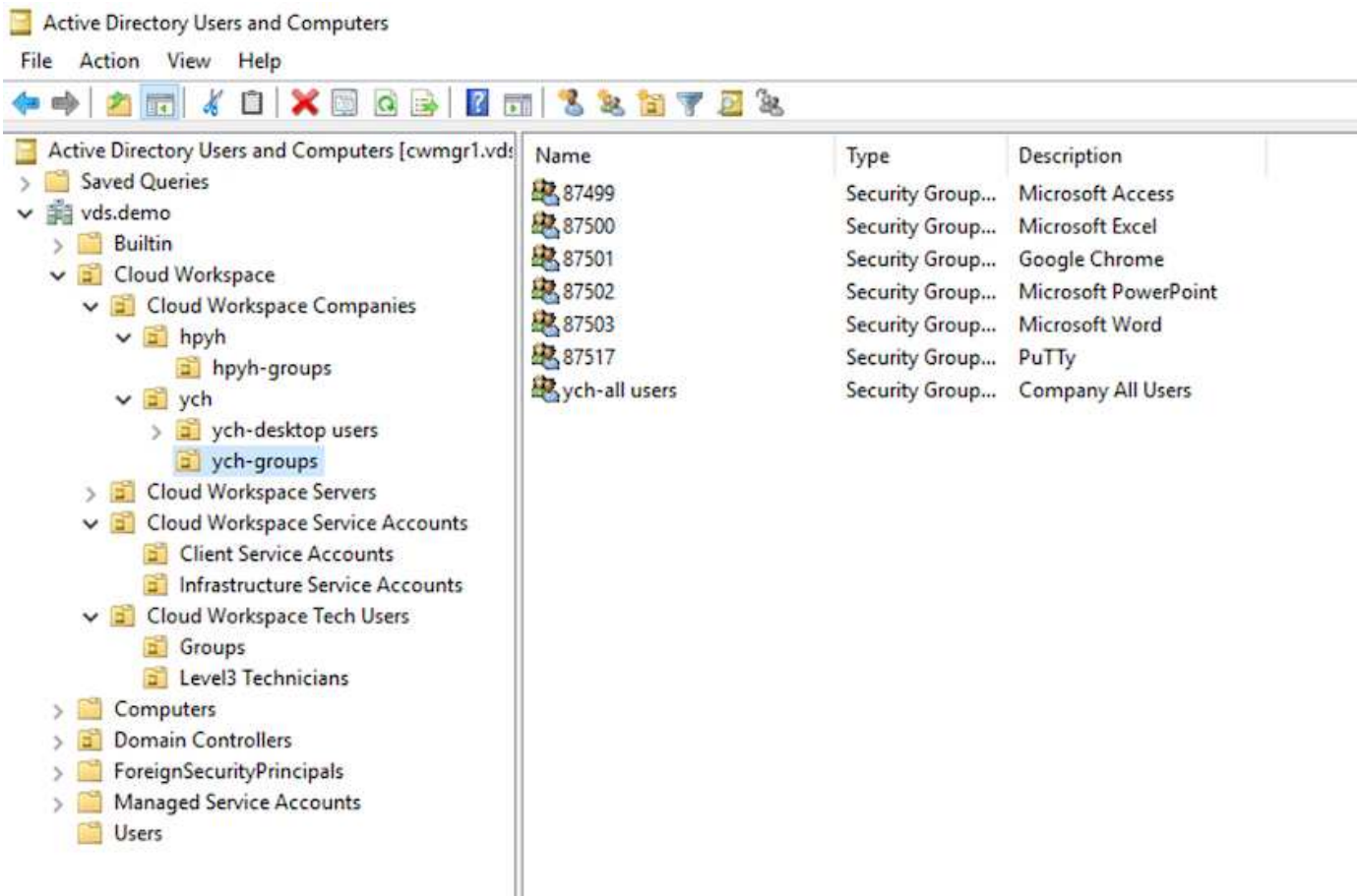
NetApp VDS utilise Azure Active Directory pour l'authentification des identités et les services de domaine Azure Active Directory pour l'authentification NTLM/Kerberos. L'outil ADConnect permet de synchroniser un domaine Active Directory sur site avec Azure Active Directory.

Vous pouvez ajouter de nouveaux utilisateurs à partir du portail ou activer l'espace de travail cloud pour les utilisateurs existants. Les autorisations pour les espaces de travail et les services d'application peuvent être contrôlées par des utilisateurs individuels ou par des groupes. À partir du portail de gestion, les utilisateurs administratifs peuvent être définis pour contrôler les autorisations du portail, des espaces de travail, etc.

La figure suivante décrit la gestion des utilisateurs dans NetApp VDS.



Chaque espace de travail réside dans sa propre unité d'organisation Active Directory (ou) sous l'unité d'organisation Cloud Workspace, comme illustré dans la figure suivante.



Pour plus d'informations, voir "[vidéo](#)" Sur les autorisations des utilisateurs et la gestion des utilisateurs dans NetApp VDS.

Lorsqu'un groupe Active Directory est défini comme un groupe CRAUserGroup à l'aide d'un appel API pour le centre de données, tous les utilisateurs de ce groupe sont importés dans CloudWorkspace pour la gestion à l'aide de l'interface utilisateur. Lorsque l'espace de travail Cloud est activé pour l'utilisateur, VDS crée des dossiers d'accueil utilisateur, des autorisations de paramètres, des mises à jour des propriétés utilisateur, etc.

Si l'option utilisateur VDI activé est cochée, VDS crée une machine RDS d'une session dédiée à cet utilisateur. Elle demande le modèle et le datastore à provisionner.

Security Settings

VDI User Enabled Mobile Drive Enabled

Hypervisor Template
Windows20192899ver1

Storage Type
DS02

Account Expiration Enabled Local Drive Access Enabled

Force Password Reset at Next Login Wake On Demand Enabled

Multi-factor Auth Enabled

Update

Gestion de l'espace de travail

Un espace de travail est constitué d'un environnement de postes de travail. Il peut s'agir de sessions de postes de travail distants partagées hébergées sur site ou dans tout environnement cloud pris en charge. Avec Microsoft Azure, l'environnement de postes de travail peut être persistant avec les postes de travail virtuels Windows. Chaque espace de travail est associé à une organisation ou à un client spécifique. Les options disponibles lors de la création d'un nouvel espace de travail sont visibles dans la figure suivante.

New Workspace

Client & Settings
Choose Applications
Add Users
Review & Provision

Select a Client [Add](#)

No Clients Added.

Workspace Settings

Company Name

Primary Notification Email

Application Settings

Enable Remote App

Enable App Locker

Enable Application Usage Tracking

Device Settings

Disable Printing Access

Enable Workspace User Data Storage

Security Settings

Require Complex User Password

Enable MFA for All Users

Permit Access To Task Manager

Cancel
Continue



Chaque espace de travail est associé à un déploiement spécifique.

Les espaces de travail contiennent des applications et des services d'application associés, des dossiers de données partagés, des serveurs et une instance WVD. Chaque espace de travail peut contrôler des options de sécurité telles que l'application de la complexité des mots de passe, l'authentification multifactorielle, l'audit des fichiers, etc.

Les espaces de travail peuvent contrôler la planification des charges de travail pour mettre sous tension des serveurs supplémentaires, limiter le nombre d'utilisateurs par serveur ou définir la planification des ressources disponibles pour une période donnée (toujours activé/désactivé). Les ressources peuvent également être configurées pour être réveillés à la demande.

L'espace de travail peut remplacer les valeurs par défaut des ressources de la machine virtuelle de déploiement, si nécessaire. Pour WVD, les pools d'hôtes WVD (qui contiennent des hôtes de session et des groupes d'applications) et les espaces de travail WVD peuvent également être gérés à partir du portail de la suite de gestion d'espace de travail cloud. Pour plus d'informations sur le pool hôte WVD, consultez ce document ["vidéo"](#).

Gestion des applications

Les employés chargés de tâches peuvent rapidement lancer une application à partir de la liste des applications mises à leur disposition. Les services d'application publient des applications à partir des hôtes de session Remote Desktop Services. Avec WVD, les groupes d'applications offrent des fonctionnalités similaires à partir de pools d'hôtes

Windows 10 multi-session.

Pour les employés du bureau qui souhaitent pouvoir alimenter les utilisateurs, les applications dont ils ont besoin peuvent être provisionnées manuellement via un tableau de services ou provisionnées automatiquement à l'aide de la fonctionnalité d'événements scripts dans NetApp VDS.

Pour plus d'informations, reportez-vous à la section "[Droits des applications NetApp](#)".

Fonctionnalités de ONTAP pour le service de postes de travail virtuels

Les fonctionnalités ONTAP suivantes font du choix une solution intéressante pour un service de poste de travail virtuel.

- **Système de fichiers scale-out.** les volumes ONTAP FlexGroup peuvent atteindre une taille de plus de 20 po et contenir plus de 400 milliards de fichiers dans un seul espace de noms. Le cluster peut contenir jusqu'à 24 nœuds de stockage, chacun disposant d'un nombre flexible de cartes d'interface réseau en fonction du modèle utilisé.

Les postes de travail virtuels, les dossiers locaux et les conteneurs de profil utilisateur, les données partagées, etc. Peuvent croître à la demande sans craindre les limitations du système de fichiers.

- **Analyse du système de fichiers.** vous pouvez utiliser l'outil XCP pour obtenir des informations sur les données partagées. Avec ONTAP 9.8+ et ActiveIQ Unified Manager, vous pouvez facilement interroger et récupérer les informations de métadonnées de fichier et identifier les données inactives.
- **Cloud Tiering.** vous pouvez migrer des données inactives vers un magasin d'objets dans le cloud ou vers tout stockage compatible S3 de votre datacenter.
- **Les versions de fichiers.** Les utilisateurs peuvent restaurer des fichiers protégés par les copies Snapshot NetApp ONTAP. Les copies Snapshot de ONTAP sont très peu gourmandes en espace car elles n'enregistrent que les blocs modifiés.
- **Espace de noms global.** la technologie ONTAP FlexCache permet la mise en cache à distance du stockage de fichiers, ce qui facilite la gestion des données partagées à travers des emplacements contenant des systèmes de stockage ONTAP.
- **Prise en charge de la colocation sécurisée.** Un cluster de stockage physique unique peut être présenté sous forme de plusieurs baies de stockage virtuelles chacune avec ses propres volumes, protocoles de stockage, interfaces réseau logiques, domaine d'authentification et d'identité, utilisateurs de gestion, etc. C'est pourquoi vous pouvez partager la baie de stockage entre plusieurs unités commerciales ou environnements, comme le test, le développement et la production.

Pour garantir les performances, vous pouvez utiliser la QoS adaptative pour définir des niveaux de performance en fonction de l'espace utilisé ou alloué. Vous pouvez également contrôler la capacité de stockage à l'aide de quotas.

- **Intégration VMware.** les outils ONTAP pour VMware vSphere fournissent un plug-in vCenter pour le provisionnement des datastores, la mise en œuvre des meilleures pratiques de l'hôte vSphere et la surveillance des ressources ONTAP.

ONTAP prend en charge les API vStorage pour l'intégration de baies (VAAI) pour transférer les opérations SCSI/fichiers vers la baie de stockage. ONTAP prend également en charge les API vStorage pour Storage Awareness (VASA) et les volumes virtuels pour les protocoles de niveau bloc et fichier.

Le plug-in SnapCenter pour VMware vSphere constitue un moyen simple de sauvegarder et restaurer les machines virtuelles à l'aide de la fonctionnalité Snapshot sur une baie de stockage.

ActiveIQ Unified Manager offre une visibilité complète sur le réseau de stockage, dans un environnement vSphere. Les administrateurs peuvent facilement identifier les problèmes de latence susceptibles de survenir dans les environnements de postes de travail virtuels hébergés sur ONTAP.

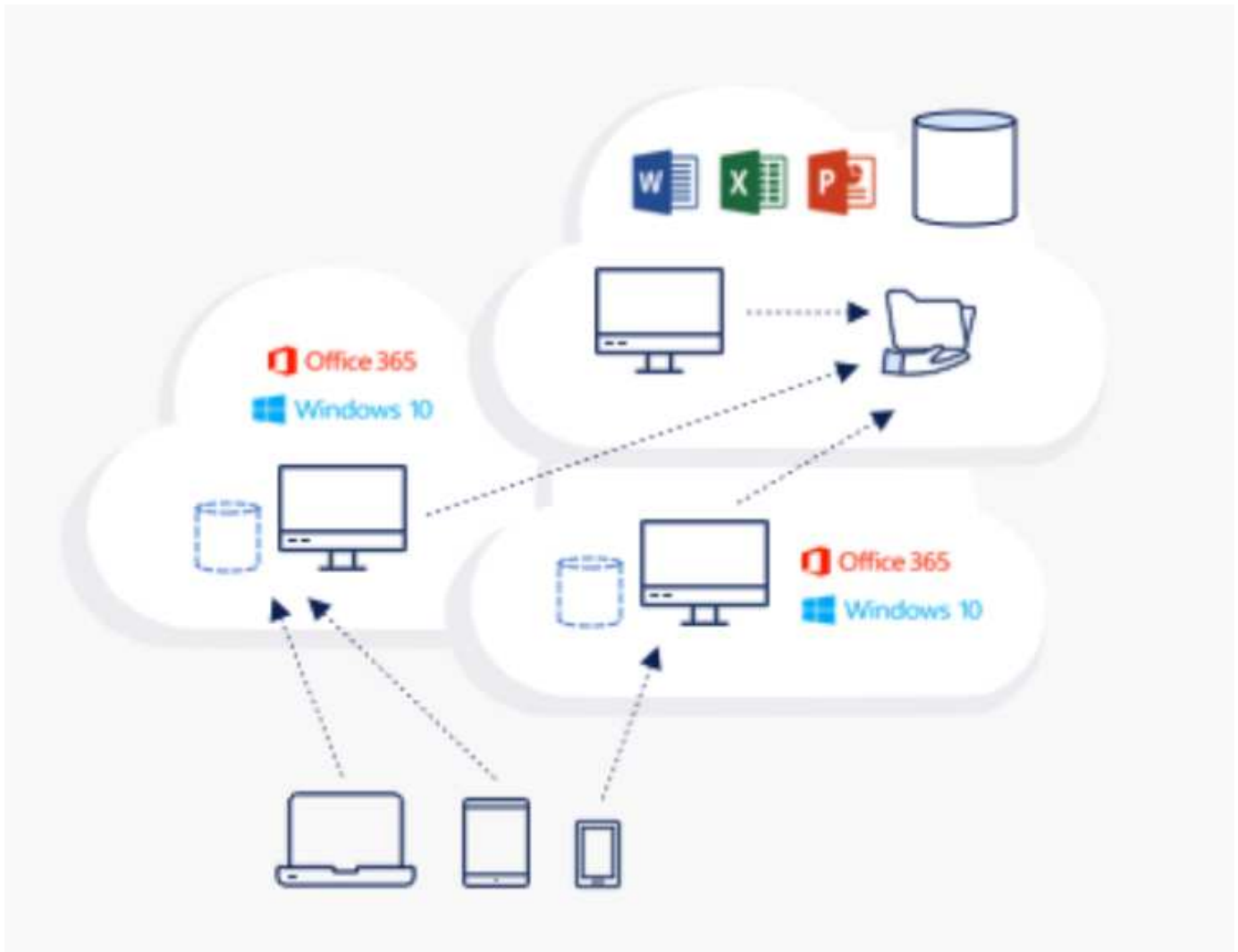
- **Conformité à la sécurité.** avec Active IQ Unified Manager, vous pouvez surveiller plusieurs systèmes ONTAP avec des alertes pour toute violation de stratégie.
- **Prise en charge multiprotocole.** ONTAP prend en charge les blocs (iSCSI, FC, FCoE et NVMe/FC), les fichiers (NFSv3, Protocoles de stockage NFSv4.1, SMB2.x et SMB3.x) et objet (S3).
- **Prise en charge de l'automatisation.** ONTAP fournit des modules API REST, Ansible et PowerShell pour automatiser les tâches avec le portail de gestion VDS.

Gestion des données

Dans le cadre du déploiement, vous pouvez choisir la méthode des services de fichiers pour héberger le profil utilisateur, les données partagées et le dossier du lecteur de base. Les options disponibles sont serveur de fichiers, Azure Files ou Azure NetApp Files. Toutefois, après le déploiement, vous pouvez modifier ce choix à l'aide de l'outil Command Center pour pointer vers n'importe quel partage SMB. "[L'hébergement avec NetApp ONTAP présente divers avantages](#)". Pour savoir comment modifier le partage SMB, reportez-vous à la section "[Changer la couche de données](#)".

Cache global de fichiers

Lorsque les utilisateurs sont répartis sur plusieurs sites au sein d'un espace de noms global, Global File cache permet de réduire la latence des données fréquemment utilisées. Le déploiement du cache de fichiers global peut être automatisé à l'aide d'un ensemble de provisionnement et d'événements avec script. Global File cache gère les caches de lecture et d'écriture localement et conserve les verrous de fichiers entre les emplacements. Le cache de fichiers global peut fonctionner avec tous les serveurs de fichiers SMB, y compris Azure NetApp Files.



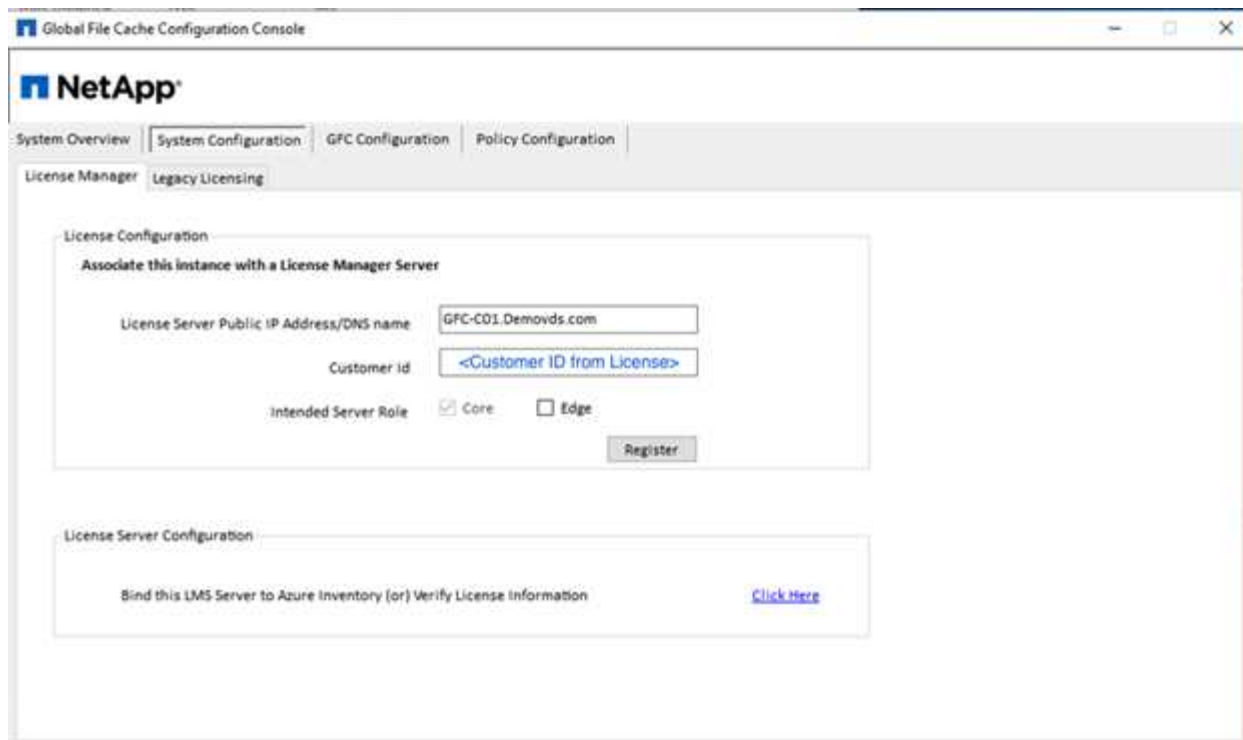
Le cache de fichiers global nécessite les éléments suivants :

- Serveur de gestion (serveur de gestion des licences)
- Cœur
- Bord avec une capacité de disque suffisante pour mettre les données en cache

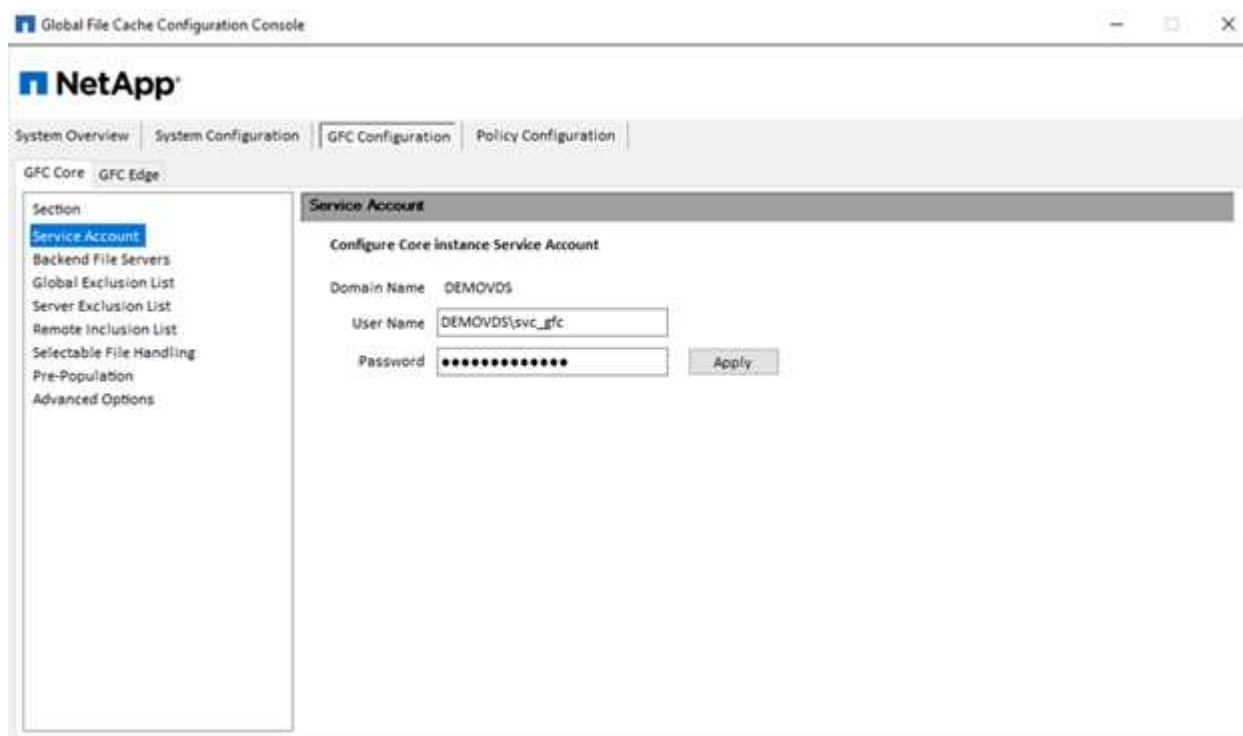
Pour télécharger le logiciel et calculer la capacité du cache de disque pour Edge, reportez-vous à la section ["Documentation Fibre Channel"](#).

À des fins de validation, nous avons déployé les ressources centrales et de gestion sur la même machine virtuelle dans Azure et les ressources Edge sur NetApp HCI. Notez que le cœur requiert l'accès aux données à volume élevé et que la périphérie fait partie du cœur. Une fois le logiciel installé, vous devez activer la licence activée avant utilisation. Pour ce faire, procédez comme suit :

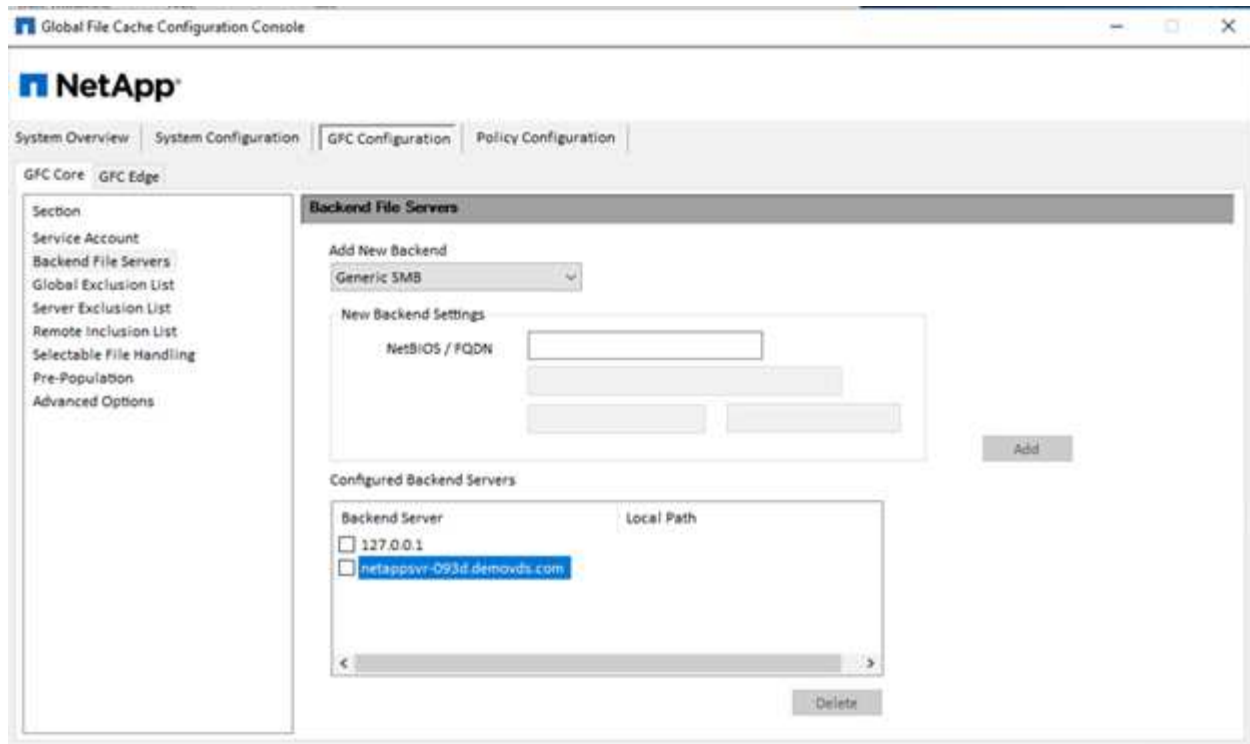
1. Dans la section Configuration de la licence, cliquez [ici](#) pour terminer l'activation de la licence. Enregistrez ensuite le fichier « core ».



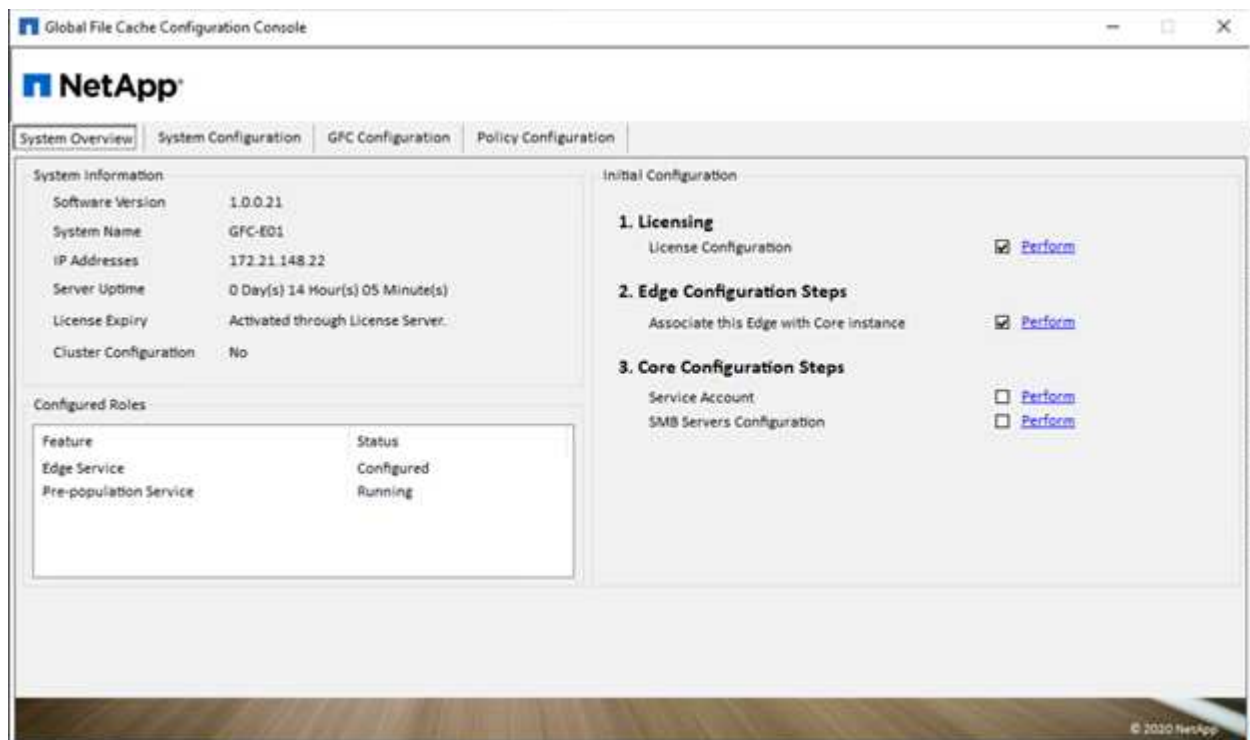
2. Fournissez le compte de service à utiliser pour le cache de fichiers global. Pour connaître les autorisations requises pour ce compte, reportez-vous à la section "[Documentation Fibre Channel](#)".



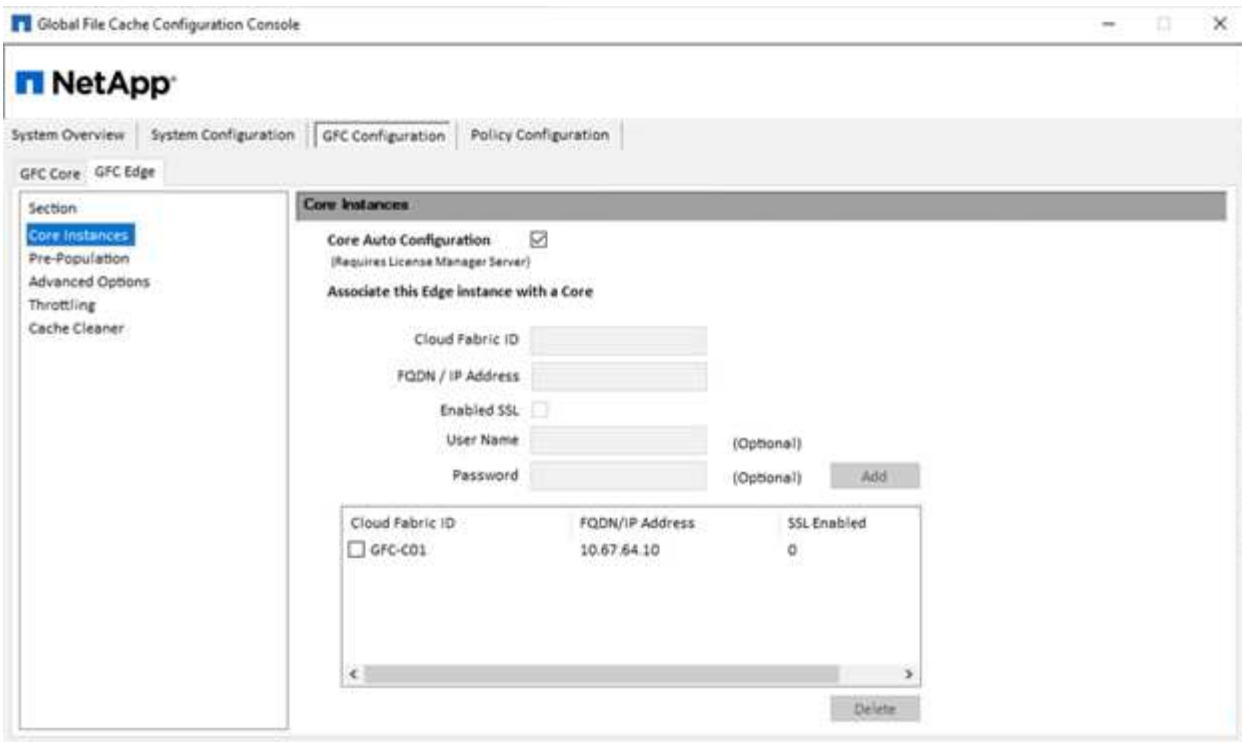
3. Ajoutez un nouveau serveur de fichiers backend et fournissez le nom du serveur de fichiers ou l'adresse IP.



4. Sur le bord, le lecteur de cache doit avoir la lettre D. Si ce n'est pas le cas, utilisez diskpart.exe pour sélectionner le volume et modifier la lettre du lecteur. Enregistrez-vous avec le serveur de licences en tant que périphérie.

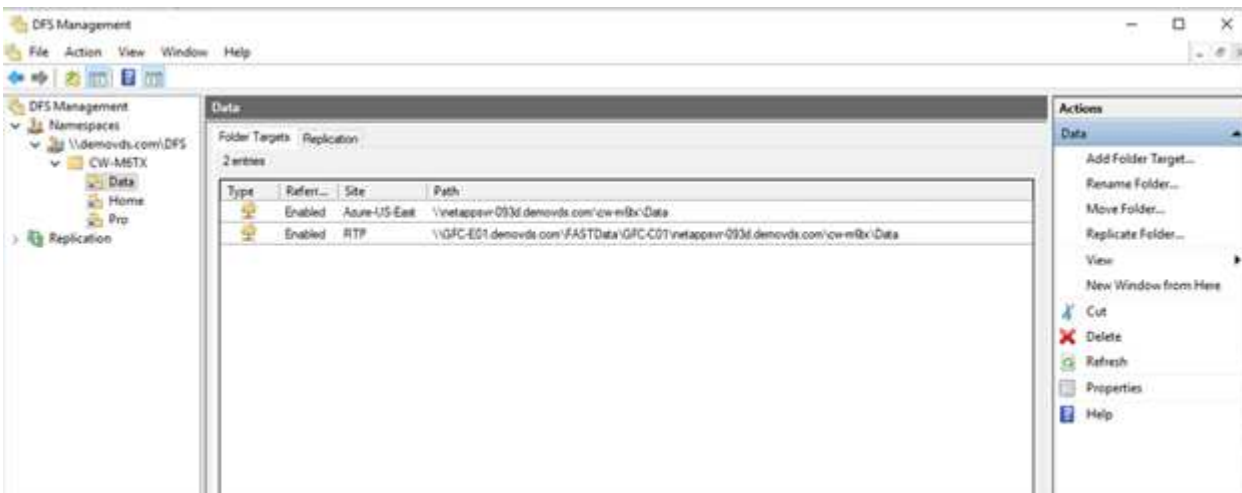


Si la configuration automatique des cœurs est activée, les informations de base sont extraites automatiquement du serveur de gestion des licences.

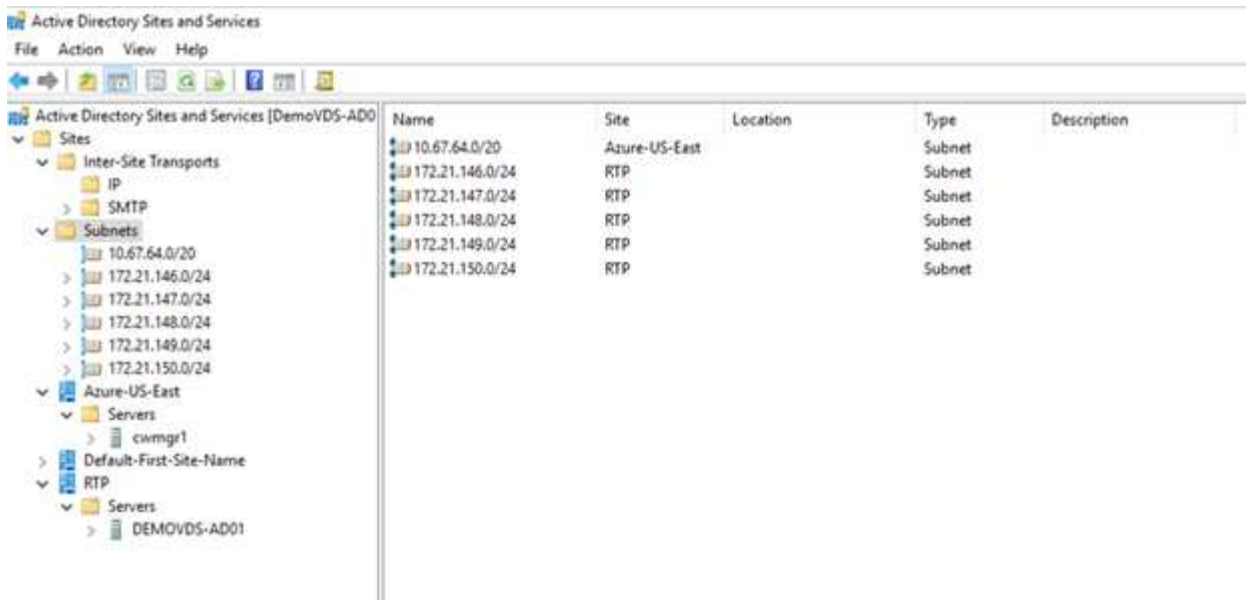


À partir de n'importe quel ordinateur client, les administrateurs qui ont utilisé pour accéder au partage sur le serveur de fichiers peuvent y accéder avec Fibre Channel Edge à l'aide du chemin UNC `\\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>`. Les administrateurs peuvent inclure ce chemin dans le logonscript utilisateur ou GPO pour les utilisateurs mappage de lecteurs à l'emplacement en périphérie.

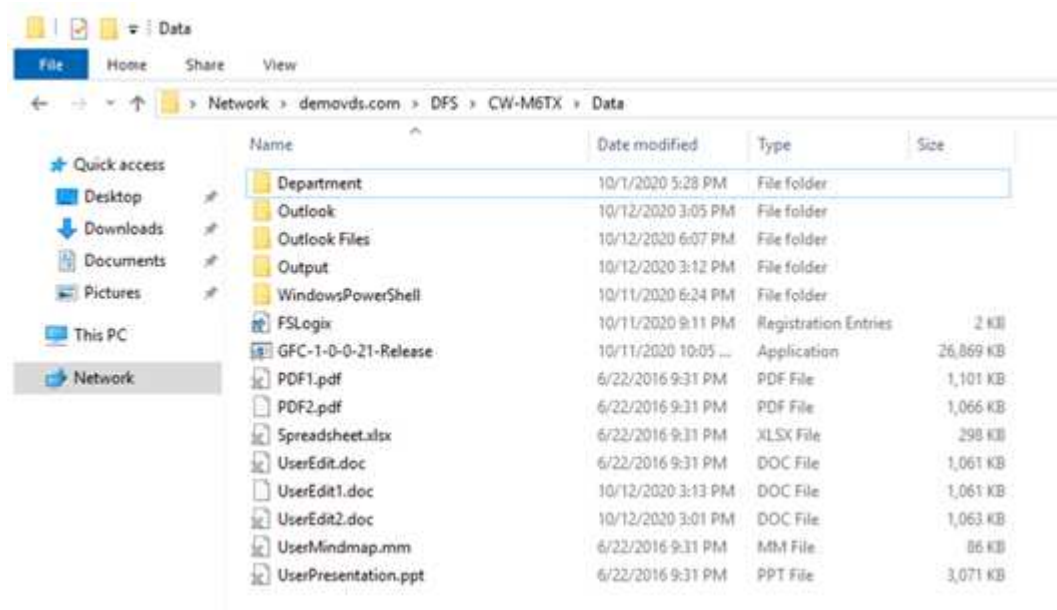
Pour fournir un accès transparent aux utilisateurs du monde entier, un administrateur peut configurer Microsoft Distributed Filesystem (DFS) avec des liens pointant vers des partages de serveurs de fichiers et vers des emplacements en périphérie.



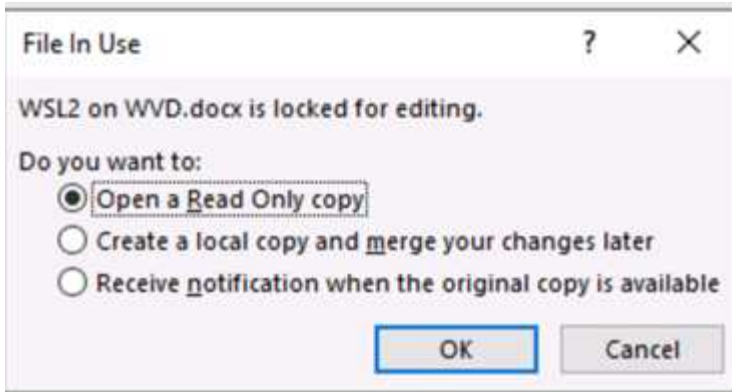
Lorsque les utilisateurs se connectent à l'aide des identifiants Active Directory en fonction des sous-réseaux associés au site, le lien approprié est utilisé par le client DFS pour accéder aux données.



Les icônes de fichier changent selon qu'un fichier est mis en cache ; les fichiers qui ne sont pas mis en cache ont un X gris dans le coin inférieur gauche de l'icône. Lorsqu'un utilisateur situé à l'emplacement d'une arête accède à un fichier, ce fichier est mis en cache et l'icône change.



Lorsqu'un fichier est ouvert et qu'un autre utilisateur tente d'ouvrir le même fichier à partir d'un emplacement de bord, l'utilisateur est invité à sélectionner la commande suivante :



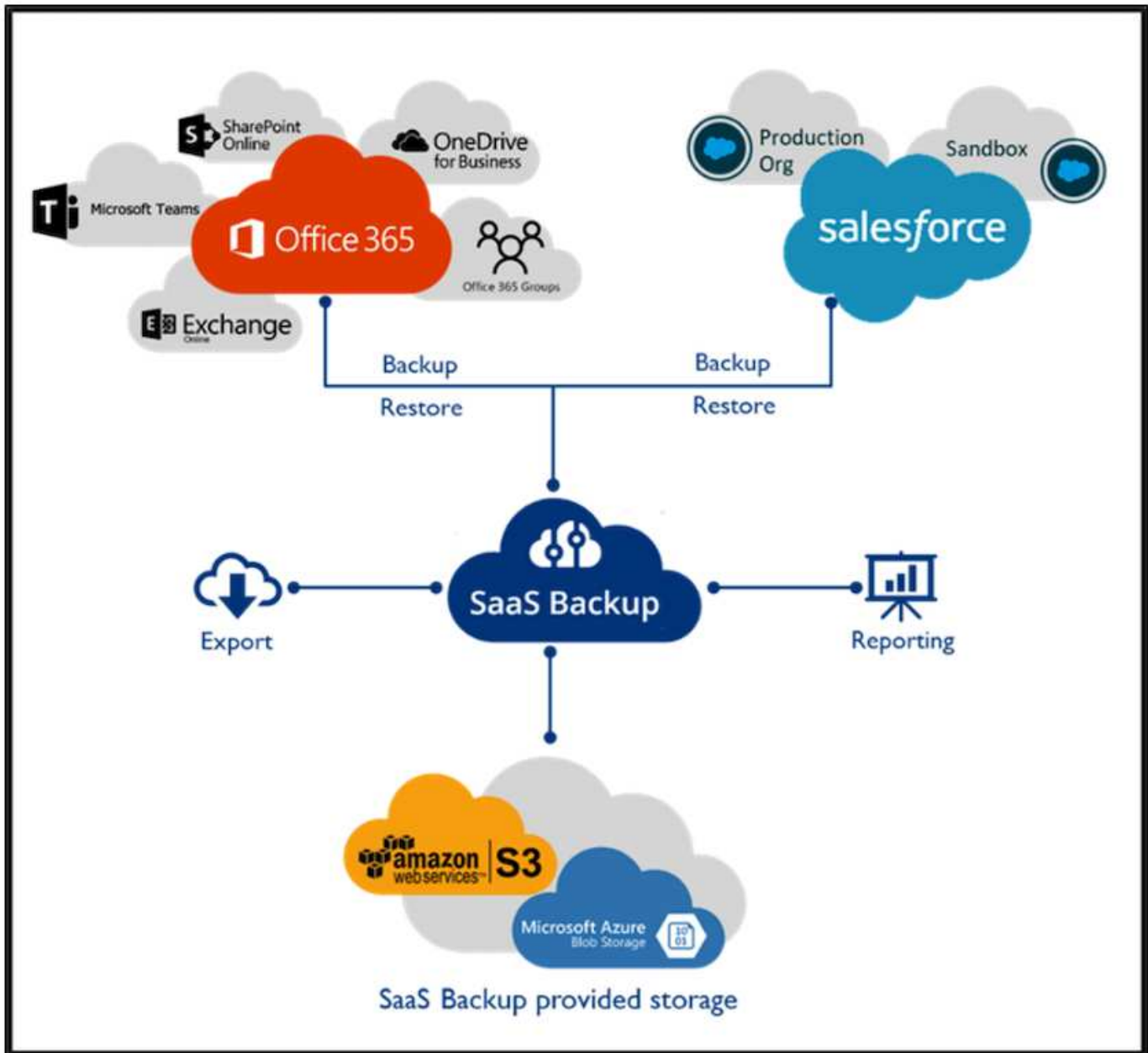
Si l'utilisateur sélectionne l'option de réception d'une notification lorsque la copie d'origine est disponible, l'utilisateur en est averti comme suit :



Pour plus d'informations, reportez-vous à ce document "[Vidéo sur talon et Azure NetApp Files Deployment](#)".

NetApp SaaS Backup

NetApp VDS fournit une protection des données Salesforce et Microsoft Office 365, notamment Exchange, SharePoint et Microsoft OneDrive. La figure suivante montre comment NetApp VDS fournit SaaS Backup pour ces services de données.



Pour découvrir les fonctionnalités de protection des données Microsoft Office 365, consultez ["vidéo"](#).

Pour une démonstration de la protection des données Salesforce, consultez ["vidéo"](#).

Gestion des opérations

Grâce à NetApp VDS, les administrateurs peuvent déléguer des tâches à d'autres personnes. Ils peuvent se connecter aux serveurs déployés pour résoudre les problèmes, afficher les journaux et exécuter des rapports d'audit. Tout en aidant les clients, le service d'assistance ou les techniciens de niveau 3 peuvent créer des clichés instantanés des sessions utilisateur, consulter les listes de processus et arrêter les processus si nécessaire.

Pour plus d'informations sur les fichiers journaux VDS, reportez-vous au ["Dépannage de la page actions VDA ayant échoué"](#).

Pour plus d'informations sur les autorisations minimales requises, reportez-vous à la section "[Page composants et autorisations VDA](#)".

Pour cloner manuellement un serveur, reportez-vous à la section "[Page clonage de machines virtuelles](#)".

Pour augmenter automatiquement la taille des disques de l'ordinateur virtuel, consultez la "[Augmenter automatiquement l'espace disque](#)".

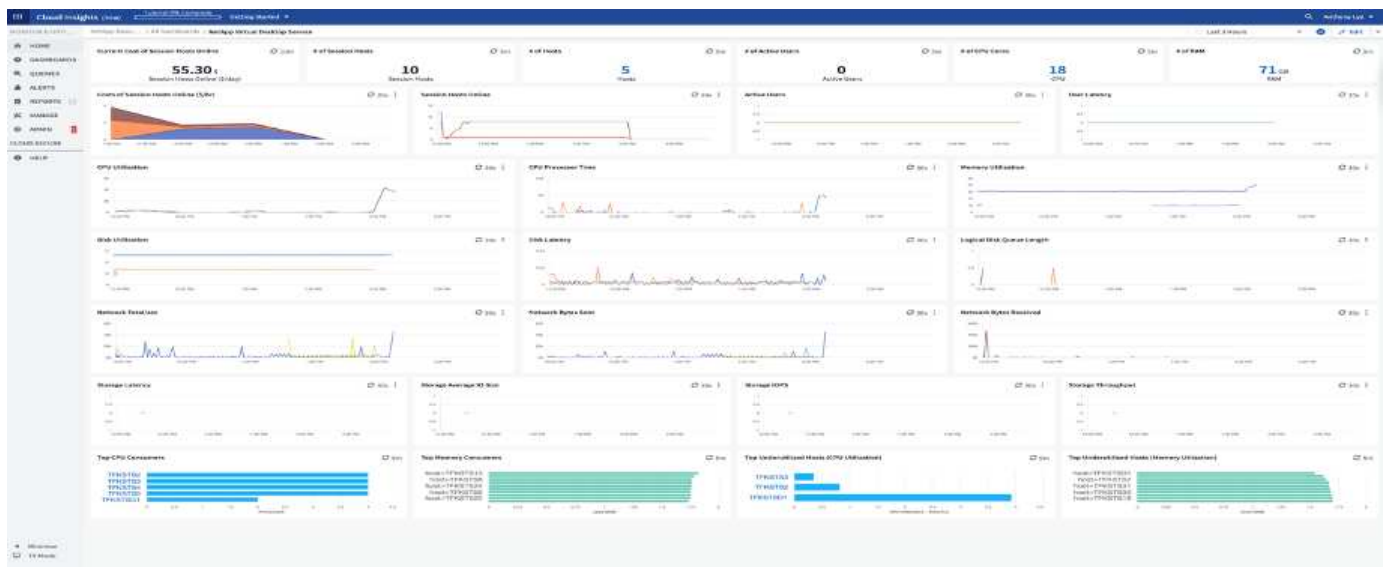
Pour identifier l'adresse de passerelle permettant de configurer manuellement le client, reportez-vous à la section "[Exigences de l'utilisateur final](#)".

Cloud Insights

NetApp Cloud Insights est un outil de surveillance web qui offre une visibilité complète sur l'infrastructure et les applications exécutées sur NetApp et d'autres composants de l'infrastructure tiers. Cloud Insights prend en charge les clouds privés et publics pour surveiller, dépanner et optimiser les ressources.

Seule la machine virtuelle de l'unité d'acquisition (peut être Windows ou Linux) doit être installée sur un cloud privé pour collecter des metrics à partir de collecteurs de données sans nécessiter d'agents. Les collecteurs de données basés sur un agent vous permettent d'extraire des mesures personnalisées à partir du moniteur de performances Windows ou de tout agent d'entrée pris en charge par Telegraf.

La figure suivante représente le tableau de bord VDS Cloud Insights.



Pour plus d'informations sur NetApp Cloud Insights, rendez-vous sur "[vidéo](#)".

Outils et journaux

Cette page présente l'outil DCCconfig, les outils TestVcc et les fichiers journaux.

Outil DCCconfig

L'outil DCCconfig prend en charge les options d'hyperviseur suivantes pour l'ajout d'un site :

DataCenter Site

DataCenter Site

Hypervisor

Cancel New Save

Load Hypervisor Test

Select Hypervisor

- Aws
- AzureClassic
- AzureRM
- ComputeEngine
- HyperV
- ProfitBricks
- vCloud
- vCloudRest
- vSphere
- XenServer

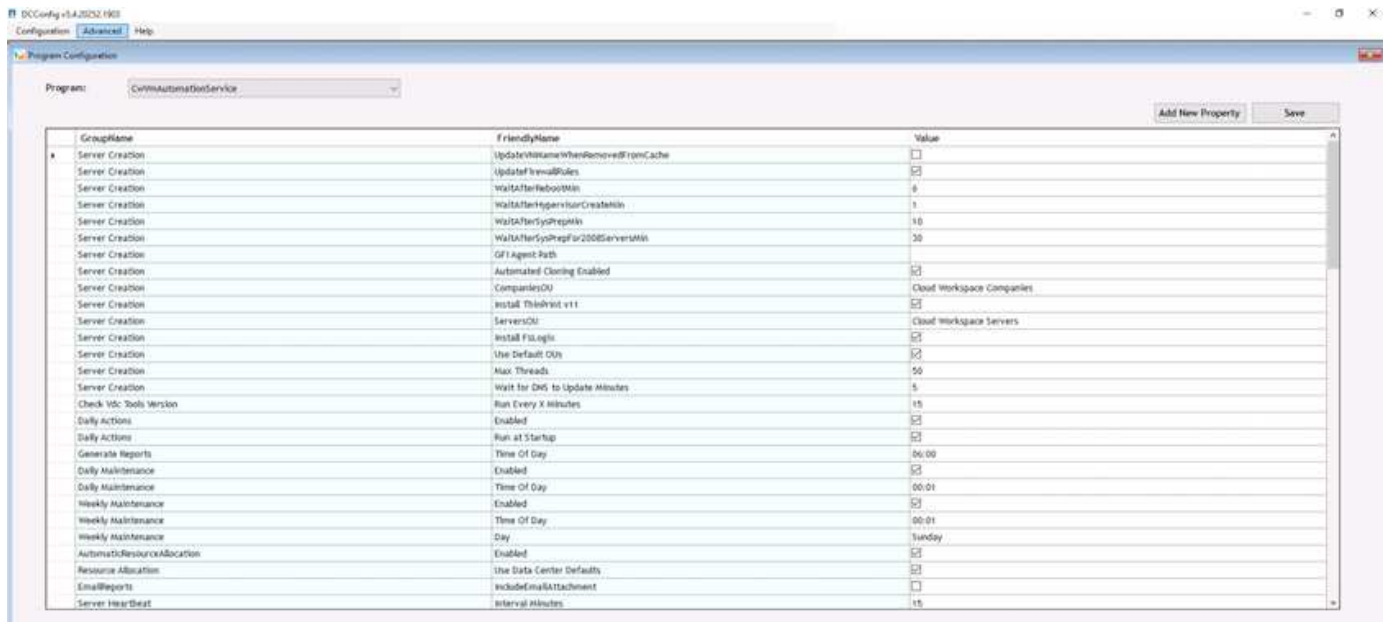
Configuration

DataCenter Accounts Email DatabaseConnection Exclude DataCenter Sites Product Keys Static IpAddress Drive Mapping

Save

| | Description | DriveLetter |
|---|-------------|-------------|
| | Shared Data | P |
| | FTP | F |
| ▶ | User Home | H |

Le mappage de lettres de lecteur propre à l'espace de travail pour les données partagées peut être géré par GPO. Les services professionnels ou l'équipe de support peuvent utiliser l'onglet avancé pour personnaliser des paramètres tels que les noms d'UO Active Directory, l'option pour activer ou désactiver le déploiement de FSLogix, diverses valeurs de délai, etc.

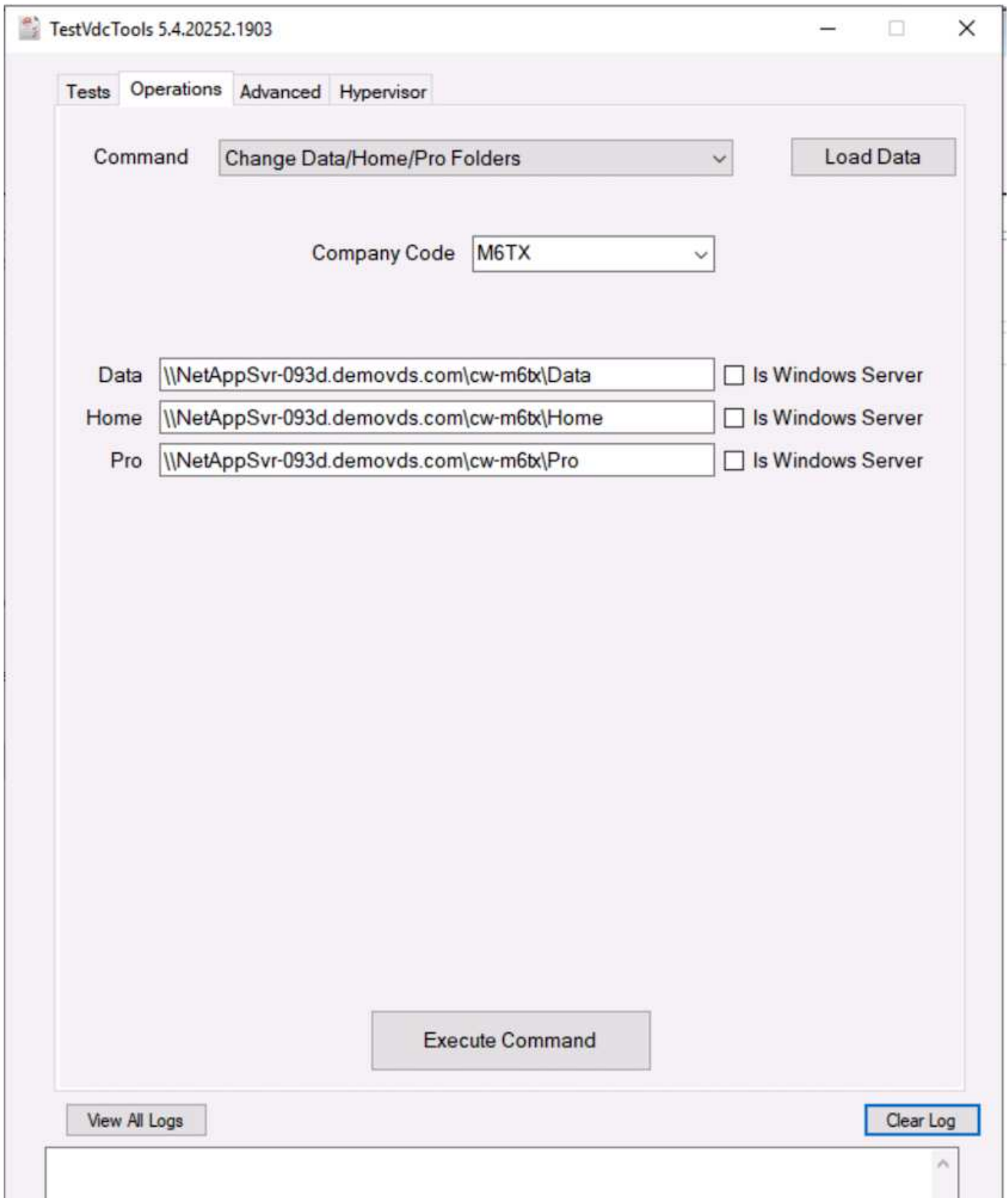


Centre de commande (anciennement appelé Outils TestVcc)

Pour lancer Command Center et le rôle requis, reportez-vous à la section "[Vue d'ensemble du centre de commande](#)".

Vous pouvez effectuer les opérations suivantes :

- Modifiez le chemin SMB d'un espace de travail.



- Modifier le site de collecte de provisionnement.

Tests Operations **Advanced** Hypervisor

Command Edit Provisioning Collection

Load Data

Provisioning Collection Windows2019

Description On vSphere Site 2

Share Drive P

Minimum Cache Level 1

Operating System Windows Server 2019

Collection Type Shared







| | Data Center Site | Role | Template | Storage |
|---|------------------|---------|-------------|---------|
| ▶ | Site 2 | TSDData | Windows2019 | DS01 |
| * | | | | |

Execute Command

View All Logs

Clear Log

Fichiers journaux

| Name | Date modified | Type | Size |
|---|--------------------|---------------------|--------|
|  CwAgent | 9/19/2020 12:35 PM | File folder | |
|  CWAutomationService | 9/19/2020 12:34 PM | File folder | |
|  CWManagerX | 9/19/2020 12:53 PM | File folder | |
|  CwVmAutomationService | 9/19/2020 12:34 PM | File folder | |
|  TestVdcTools | 9/22/2020 8:20 PM | File folder | |
|  report | 9/19/2020 12:18 PM | Executable Jar File | 705 KB |

Pour plus d'informations, consultez ["journaux d'automatisation"](#) .

Considérations relatives aux GPU

Grâce aux calculs arithmétiques répétitifs, les GPU sont généralement utilisés pour la visualisation graphique (rendu). Ces fonctionnalités de calcul répétitives sont souvent utilisées pour l'IA et l'apprentissage profond.

Pour les applications graphiques exigeantes, Microsoft Azure propose la gamme NV basée sur la carte NVIDIA Tesla M60 avec un à quatre GPU par machine virtuelle. Chaque carte NVIDIA Tesla M60 comprend deux processeurs graphiques Maxwell, chacun avec 8 Go de mémoire GDDR5, pour un total de 16 Go.



Une licence NVIDIA est incluse dans la gamme NV.


TechPowerUp GPU-Z 2.36.0


Graphics Card | Sensors | Advanced | Validation

Name: NVIDIA Tesla M60 [Lookup](#)

GPU: GM204 Revision: FF

Technology: 28 nm Die Size: 398 mm²

Release Date: Aug 30, 2015 Transistors: 5200M 

BIOS Version: 84.04.85.00.03  UEFI

Subvendor: NVIDIA Device ID: 10DE 13F2 - 10DE 115E

ROPs/TMUs: 64 / 128 Bus Interface: PCI ?

Shaders: 2048 Unified DirectX Support: 12 (12_1)

Pixel Fillrate: 75.4 GPixel/s Texture Fillrate: 150.8 GTexel/s

Memory Type: GDDR5 (Hynix) Bus Width: 256 bit

Memory Size: 8192 MB Bandwidth: 160.4 GB/s

Driver Version: 27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date: Oct 22, 2020 Digital Signature: WHQL

GPU Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz

Default Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz

NVIDIA SLI: Disabled

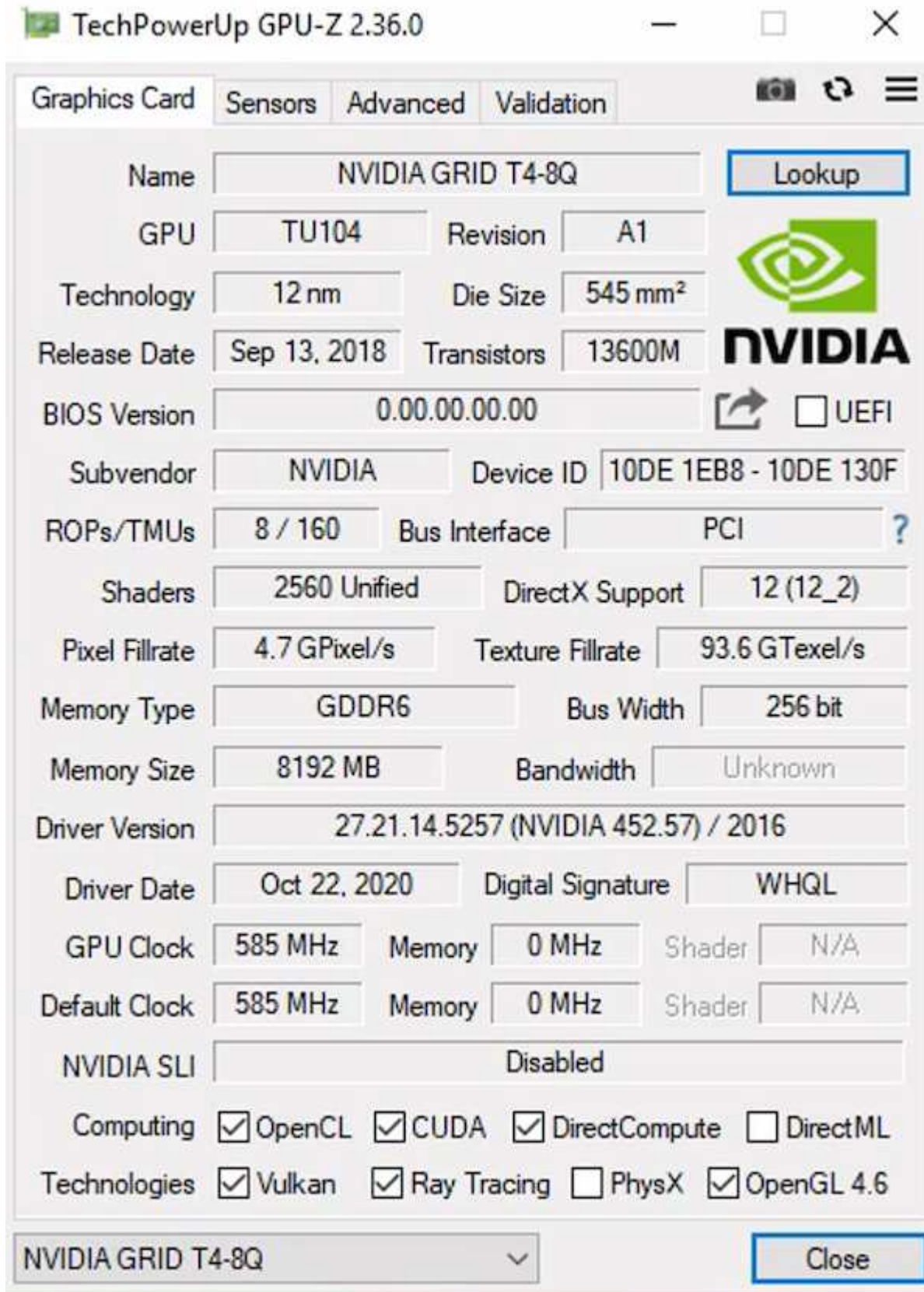
Computing OpenCL CUDA DirectCompute DirectML

Technologies Vulkan Ray Tracing PhysX OpenGL 4.6

NVIDIA Tesla M60 [Close](#)

Avec NetApp HCI, le GPU H615C contient trois cartes NVIDIA Tesla T4. Chaque carte NVIDIA Tesla T4 dispose d'un processeur graphique Turing avec 16 Go de mémoire GDDR6. Lorsqu'elles sont utilisées dans un environnement VMware vSphere, les serveurs virtuels peuvent partager les GPU, chaque machine virtuelle disposant d'une mémoire tampon dédiée. Le suivi des rayons est disponible avec les processeurs graphiques de la NetApp HCI H615C pour produire des images réalistes comprenant les réflexions de lumière. Notez que

vous devez disposer d'un serveur de licences NVIDIA avec une licence pour les fonctionnalités GPU.



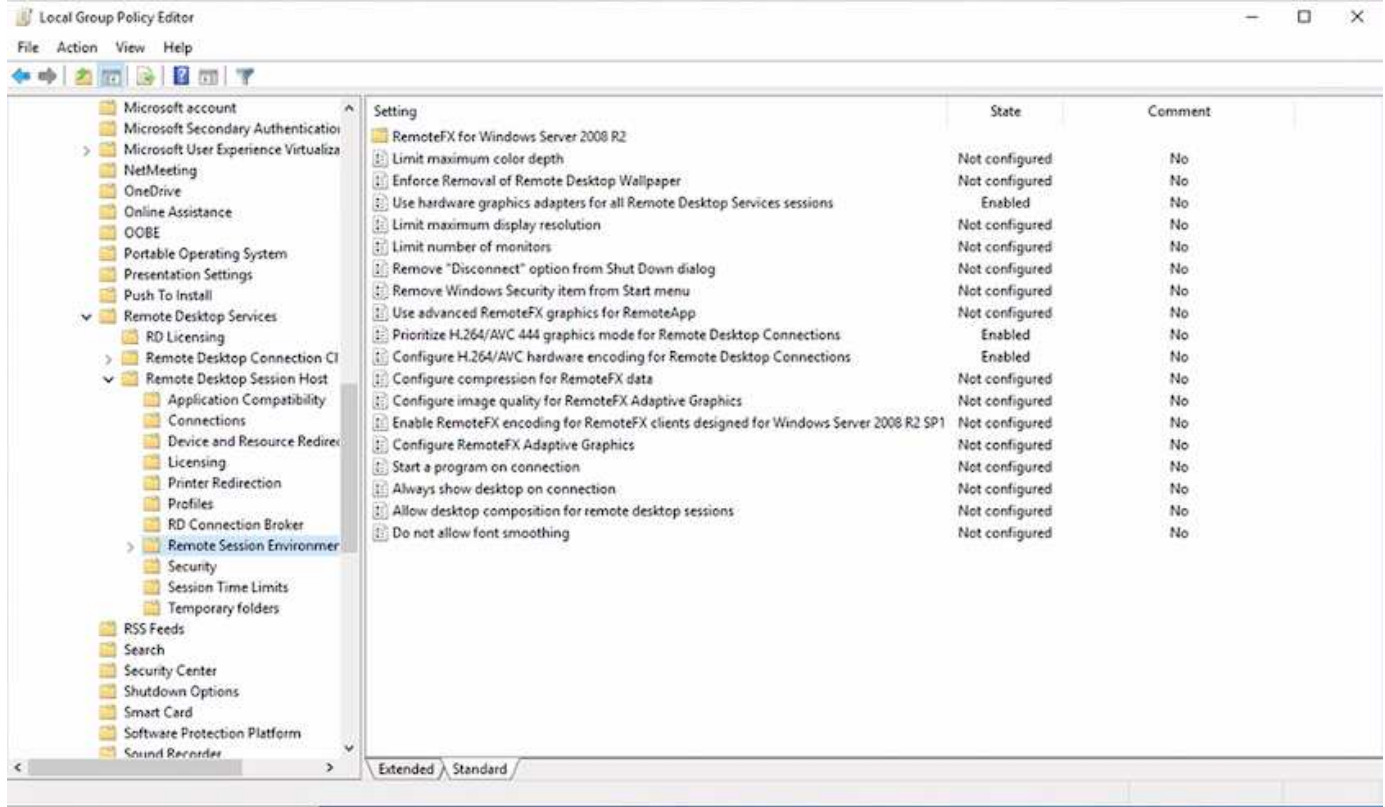
The image shows the TechPowerUp GPU-Z 2.36.0 application window. The window title is "TechPowerUp GPU-Z 2.36.0". The main content area displays the following information:

- Graphics Card:** Sensors, Advanced, Validation
- Name:** NVIDIA GRID T4-8Q (with a "Lookup" button)
- GPU:** TU104, **Revision:** A1
- Technology:** 12 nm, **Die Size:** 545 mm²
- Release Date:** Sep 13, 2018, **Transistors:** 13600M
- BIOS Version:** 0.00.00.00.00 (with a "UEFI" checkbox)
- Subvendor:** NVIDIA, **Device ID:** 10DE 1EB8 - 10DE 130F
- ROPs/TMUs:** 8 / 160, **Bus Interface:** PCI
- Shaders:** 2560 Unified, **DirectX Support:** 12 (12_2)
- Pixel Fillrate:** 4.7 GPixel/s, **Texture Fillrate:** 93.6 GTexel/s
- Memory Type:** GDDR6, **Bus Width:** 256 bit
- Memory Size:** 8192 MB, **Bandwidth:** Unknown
- Driver Version:** 27.21.14.5257 (NVIDIA 452.57) / 2016
- Driver Date:** Oct 22, 2020, **Digital Signature:** WHQL
- GPU Clock:** 585 MHz, **Memory:** 0 MHz, **Shader:** N/A
- Default Clock:** 585 MHz, **Memory:** 0 MHz, **Shader:** N/A
- NVIDIA SLI:** Disabled
- Computing:** OpenCL, CUDA, DirectCompute, DirectML
- Technologies:** Vulkan, Ray Tracing, PhysX, OpenGL 4.6

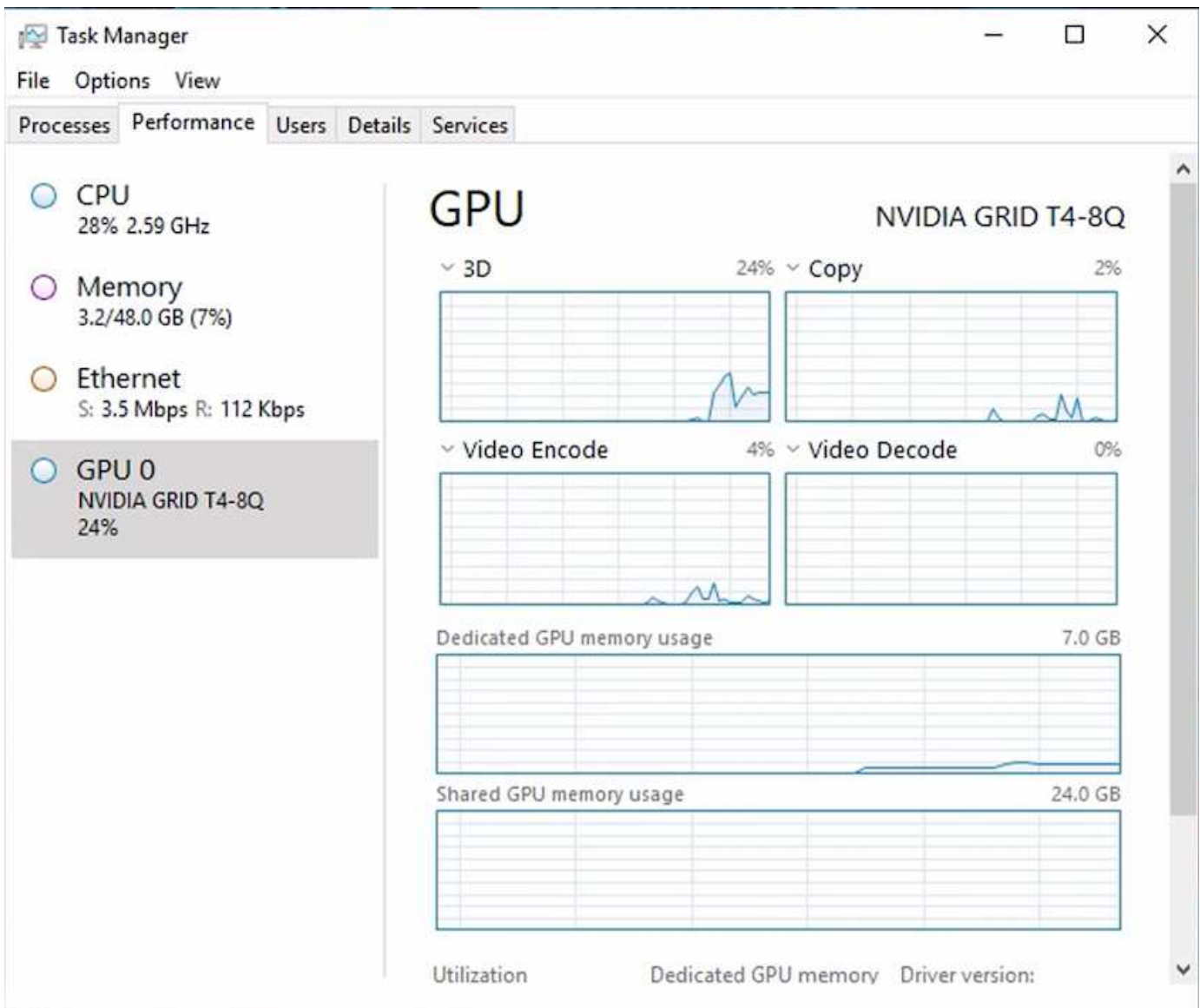
At the bottom, there is a dropdown menu showing "NVIDIA GRID T4-8Q" and a "Close" button.

Pour utiliser le GPU, vous devez installer le pilote approprié, qui peut être téléchargé à partir du portail de licences NVIDIA. Dans un environnement Azure, le pilote NVIDIA est disponible en tant qu'extension de pilote GPU. Ensuite, les stratégies de groupe de la capture d'écran suivante doivent être mises à jour pour utiliser le

matériel GPU pour les sessions de service de bureau à distance. Vous devez hiérarchiser le mode graphique H.264 et activer la fonctionnalité d'encodeur.



Validez la surveillance des performances du GPU avec Task Manager ou à l'aide de l'interface de ligne de commande nvidia-smi lors de l'exécution d'échantillons WebGL. Assurez-vous que les ressources GPU, mémoire et encodeur sont utilisées.



Pour s'assurer que la machine virtuelle est déployée dans NetApp HCI H615C avec le service de bureau virtuel, définissez un site avec la ressource de cluster vCenter dotée d'hôtes H615C. Le profil vGPU requis doit être associé au modèle VM.

Pour les environnements partagés multi-sessions, envisagez d'allouer plusieurs profils vGPU homogènes. Cependant, pour une application graphique professionnelle haut de gamme, il est préférable que chaque machine virtuelle soit dédiée à un utilisateur afin d'isoler les machines virtuelles.

Le processeur GPU peut être contrôlé par une stratégie QoS et chaque profil vGPU peut disposer de tampons de trame dédiés. Cependant, l'encodeur et le décodeur sont partagés pour chaque carte. Le placement d'un profil vGPU sur une carte GPU est contrôlé par la règle d'affectation des GPU de l'hôte vSphere, qui peut mettre en avant les performances (répartir les VM) ou la consolidation (regrouper les VM de groupe).

Solutions industrielles

Les postes de travail graphiques sont généralement utilisés dans des secteurs tels que l'industrie, la santé, l'énergie, les médias et le divertissement, l'éducation, accidentelle, etc. La mobilité est souvent limitée pour les applications graphiques.

Pour résoudre les problèmes de mobilité, les services de postes de travail virtuels proposent un environnement de postes de travail pour tous les types de collaborateurs, des travailleurs chargés des tâches aux utilisateurs experts, en utilisant des ressources matérielles dans le cloud ou avec NetApp HCI, et en proposant notamment des options de configurations de processeurs graphiques flexibles. VDS permet aux utilisateurs d'accéder à leur environnement de travail depuis n'importe où avec des ordinateurs portables, des tablettes et d'autres appareils mobiles.

Pour exécuter des charges de travail de fabrication avec des logiciels tels que ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault systèmes SOLIDWORKS, Dassault systèmes CATIA, PTC Creo, Siemens PLM NX, etc. En janvier 2021, les GPU disponibles sur différents clouds sont répertoriés dans le tableau suivant.

| Modèle de GPU | Microsoft Azure | Google Compute (GCP) | Services Web Amazon (AWS) | Sur site (NetApp HCI) |
|----------------------|------------------------|-----------------------------|----------------------------------|------------------------------|
| NVIDIA M60 | Oui. | Oui. | Oui. | Non |
| NVIDIA T4 | Non | Oui. | Oui. | Oui. |
| NVIDIA P100 | Non | Oui. | Non | Non |
| NVIDIA P4 | Non | Oui. | Non | Non |

Des sessions de postes de travail partagés avec d'autres utilisateurs et des postes de travail personnels dédiés sont également disponibles. Les postes de travail virtuels peuvent disposer de un à quatre processeurs graphiques ou utiliser des GPU partiels avec NetApp HCI. NVIDIA T4 est une carte graphique polyvalente qui répond aux demandes d'un large éventail de charges de travail des utilisateurs. Chaque carte graphique du NetApp HCI H615C dispose de 16 Go de mémoire tampon trame et de trois cartes par serveur. Le nombre d'utilisateurs pouvant être hébergés sur un seul serveur H615C dépend de la charge de travail de l'utilisateur.

| Utilisateurs/serveur | Lumière (4 Go) | Moyen (8 Go) | Lourd (16 Go) |
|-----------------------------|-----------------------|---------------------|----------------------|
| H615C | 12 | 6 | 3 |

Pour déterminer le type d'utilisateur, exécutez l'outil de profileur GPU lorsque les utilisateurs travaillent avec des applications exécutant des tâches types. Le profileur GPU capture les demandes en mémoire, le nombre d'affichages et la résolution dont les utilisateurs ont besoin. Vous pouvez ensuite choisir le profil vGPU qui répond à vos besoins.

Les postes de travail virtuels avec processeurs graphiques peuvent prendre en charge une résolution d'affichage pouvant atteindre 8 Ko. Par ailleurs, l'utilitaire nView permet de diviser un seul moniteur en régions pour travailler avec différents jeux de données.

Grâce au stockage de fichiers ONTAP, vous bénéficiez de nombreux avantages :

- Un seul espace de nom pouvant atteindre 20 po de stockage avec 400 milliards de fichiers, sans qu'il soit nécessaire d'effectuer des tâches d'administration
- Espace de noms pouvant s'étendre sur le globe avec un cache de fichiers global
- Colocation sécurisée avec le stockage NetApp géré
- La migration de données inactives vers des magasins d'objets à l'aide de NetApp FabricPool
- Statistiques rapides sur les fichiers et analytique du système de fichiers
- Évolutivité d'un cluster de stockage jusqu'à 24 nœuds pour de meilleures capacités et performances
- La possibilité de contrôler l'espace de stockage à l'aide de quotas, de performances garanties et des

limites de QoS

- Sécurisation des données avec le chiffrement
- Répondre aux exigences générales de conformité et de protection des données
- Des options flexibles de continuité de l'activité

Conclusion

NetApp Virtual Desktop Service fournit un environnement d'applications et de postes de travail virtuels très facile à utiliser, qui répond parfaitement aux enjeux métier. L'extension de VDS à l'environnement ONTAP local vous permet d'utiliser des fonctionnalités NetApp puissantes dans un environnement VDS, notamment le clonage rapide, la déduplication à la volée, la compaction et le provisionnement fin et à la compression. Réduisez les coûts de stockage et améliorez la performance avec le stockage 100 % Flash. Avec l'hyperviseur VMware vSphere, réduisez les délais de provisionnement des serveurs grâce aux volumes virtuels et à l'API vSphere pour l'intégration des baies. Avec le cloud hybride, les clients peuvent choisir l'environnement qui convient à leurs workloads exigeants et réaliser des économies. La session de postes de travail exécutée sur site peut accéder à des ressources clouds basées sur des règles.

Sources d'informations complémentaires

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

- ["Cloud NetApp"](#)
- ["Documentation produit NetApp VDS"](#)
- ["Connectez votre réseau sur site à Azure avec VPN Gateway"](#)
- ["Portail Azure"](#)
- ["Postes de travail virtuels Microsoft Windows"](#)
- ["Inscription Azure NetApp Files"](#)

VMware Horizon

NVA-1132-DESIGN : end-user computing VMware avec NetApp HCI

Technologiques Suresh, NetApp

L'end-user computing VMware avec NetApp HCI est une architecture de data Center prévalidée et conforme aux bonnes pratiques, conçue pour déployer des workloads de postes de travail virtuels à l'échelle de l'entreprise. Ce document décrit la conception de l'architecture et les bonnes pratiques de déploiement de la solution à l'échelle de la production de manière fiable et sans risque.

["NVA-1132-DESIGN : end-user computing VMware avec NetApp HCI"](#)

NVA-1129-DESIGN : calcul des utilisateurs finaux VMware avec NetApp HCI et processeurs graphiques NVIDIA

Technologiques Suresh, NetApp

L'end-user computing VMware avec NetApp HCI est une architecture de data Center prévalidée et conforme aux bonnes pratiques, conçue pour déployer des workloads de postes de travail virtuels à l'échelle de l'entreprise. Ce document décrit la conception de l'architecture et les bonnes pratiques de déploiement de la solution à l'échelle de la production de manière fiable et sans risque.

["NVA-1129-DESIGN : calcul des utilisateurs finaux VMware avec NetApp HCI et processeurs graphiques NVIDIA"](#)

NVA-1129-DEPLOY : end-user computing VMware avec NetApp HCI et processeurs graphiques NVIDIA

Technologiques Suresh, NetApp

L'end-user computing VMware avec NetApp HCI est une architecture de data Center prévalidée, conforme aux meilleures pratiques, qui permet de déployer des charges de travail de postes de travail virtuels à l'échelle de l'entreprise. Ce document explique comment déployer la solution à l'échelle de la production de manière fiable et sans risque.

["NVA-1129-DEPLOY : end-user computing VMware avec NetApp HCI et processeurs graphiques NVIDIA"](#)

NetApp HCI pour l'infrastructure de postes de travail virtuels avec VMware Horizon 7 : offrez aux utilisateurs intensifs des graphiques 3D

Technologiques Suresh, NetApp

Le rapport technique TR-4792 fournit des conseils sur l'utilisation du nœud de calcul NetApp H615C pour les workloads de graphiques 3D dans un environnement VMware Horizon optimisé par les processeurs graphiques (GPU) et le logiciel de virtualisation NVIDIA. Il fournit également les résultats des tests préliminaires de SPECviewperf 13 pour le H615C.

["NetApp HCI pour l'infrastructure de postes de travail virtuels avec VMware Horizon 7 : offrez aux utilisateurs intensifs des graphiques 3D"](#)

Solutions FlexPod de virtualisation des postes de travail

Pour en savoir plus sur les solutions de virtualisation FlexPod, consultez la ["Guides de conception FlexPod"](#)

Démos et tutoriels

Vidéos et démonstrations de virtualisation

Visionnez les vidéos et démonstrations suivantes portant sur des fonctionnalités spécifiques des solutions de cloud hybride, de virtualisation et de conteneurs.

Outils NetApp ONTAP pour VMware vSphere

[Outils ONTAP pour VMware - Présentation](#)

[Provisionnement des datastores iSCSI VMware avec ONTAP](#)

[Provisionnement des datastores VMware NFS avec ONTAP](#)

Plug-in SnapCenter pour VMware vSphere

Le logiciel SnapCenter est 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.

Le plug-in SnapCenter pour VMware vSphere vous permet d'effectuer des sauvegardes, des restaurations et des liaisons pour les machines virtuelles, ainsi que des opérations de sauvegarde et de montage pour les datastores enregistrés auprès de SnapCenter directement dans VMware vCenter.

Pour plus d'informations sur le plug-in NetApp SnapCenter pour VMware vSphere, consultez le "[Présentation du plug-in NetApp SnapCenter pour VMware vSphere](#)".

[Plug-in SnapCenter pour VMware vSphere : conditions requises pour la solution](#)

[Plug-in SnapCenter pour VMware vSphere : déploiement](#)

[Plug-in SnapCenter pour VMware vSphere - Workflow de sauvegarde](#)

[Plug-in SnapCenter pour VMware vSphere : restaurez les flux de travail](#)

[SnapCenter - flux de travail de restauration SQL](#)

3-2-1 Solutions de protection des données

Les solutions de protection des données 3-2-1 combinent les sauvegardes primaires et secondaires sur site, à l'aide de la technologie SnapMirror, avec les copies répliquées vers le stockage objet à l'aide de la sauvegarde et de la restauration BlueXP.

[3-2-1 protection des données pour les datastores VMFS avec le plug-in SnapCenter pour VMware vSphere et la sauvegarde et restauration BlueXP pour les machines virtuelles](#)

VMware Cloud sur AWS avec AWS FSX pour NetApp ONTAP

Stockage connecté à un invité Windows avec ONTAP FSX utilisant iSCSI

Stockage connecté par un invité Linux avec FSX ONTAP à l'aide de NFS

Économies en termes de coût total de possession de VMware Cloud sur AWS avec Amazon FSX pour NetApp ONTAP

VMware Cloud sur AWS datastore supplémentaire avec Amazon FSX pour NetApp ONTAP

Déploiement et configuration de VMware HCX pour VMC

Démonstration de la migration VMotion avec VMware HCX pour VMC et FSxN

Démonstration de la migration à froid avec VMware HCX pour VMC et FSxN

Azure VMware Services sur Azure avec Azure NetApp Files (ANF)

Solution Azure VMware datastore supplémentaire avec Azure NetApp Files

Solution de reprise après incident Azure VMware avec Cloud Volumes ONTAP, SnapCenter et JetStream

Démonstration de la migration à froid avec VMware HCX pour AVS et ANF

Démonstration de VMotion avec VMware HCX pour AVS et ANF

Démonstration de la migration en bloc avec VMware HCX pour AVS et ANF

Socle VMware Cloud avec NetApp ONTAP

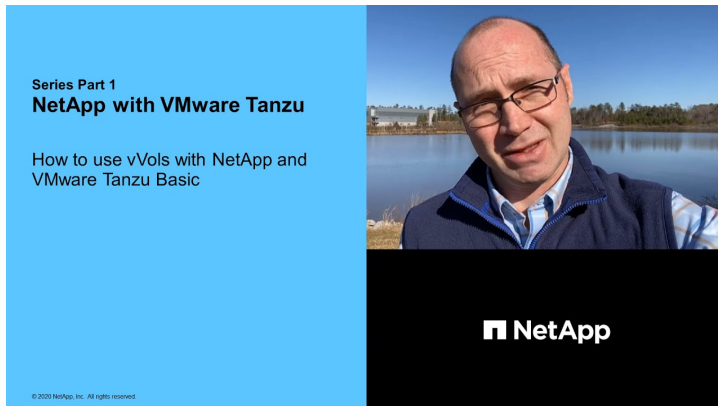
Datastores NFS en tant que stockage principal pour les domaines de charge de travail VCF

Datastores iSCSI en tant que stockage supplémentaire pour les domaines de gestion VCF

NetApp avec VMware Tanzu

VMware Tanzu permet aux clients de déployer, d'administrer et de gérer leur environnement Kubernetes via vSphere ou VMware Cloud Foundation. Cette gamme de produits VMware permet aux clients de gérer tous leurs clusters Kubernetes pertinents à partir d'un seul plan de contrôle en choisissant l'édition VMware Tanzu qui répond le mieux à leurs besoins.

Pour plus d'informations sur VMware Tanzu, reportez-vous au ["Présentation de VMware Tanzu"](#). Cette revue couvre les cas d'utilisation, les ajouts disponibles et plus d'informations sur VMware Tanzu.



Comment utiliser vVols avec NetApp et VMware Tanzu Basic, partie 1



Comment utiliser vVols avec NetApp et VMware Tanzu Basic, partie 2



Comment utiliser vVols avec NetApp et VMware Tanzu Basic, partie 3

NetApp Cloud Insights

NetApp Cloud Insights est une plateforme complète de surveillance et d'analytique conçue pour fournir la visibilité et le contrôle sur votre infrastructure sur site et dans le cloud.

[NetApp Cloud Insights : l'observabilité pour le data Center moderne](#)

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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