



# **Guide de référence NFS pour vSphere 8**

## **NetApp Solutions**

NetApp  
September 10, 2024

# Sommaire

- Guide de référence NFS 3.1 pour vSphere 8 ..... 1
  - Utilisation de NFS 3.1 avec vSphere 8 et les systèmes de stockage ONTAP ..... 1
  - Présentation de la technologie ..... 2
  - Fonctionnalité NFS nConnect avec NetApp et VMware ..... 9
  - Utilisez les outils ONTAP 10 pour configurer les datastores NFS pour vSphere 8 ..... 13
  - Utilisez VMware Site Recovery Manager pour la reprise après incident des datastores NFS ..... 44
  - Protection anti-ransomware autonome pour le stockage NFS ..... 70

# Guide de référence NFS 3.1 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 3.1 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 NFS 3.1 VCF 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 :

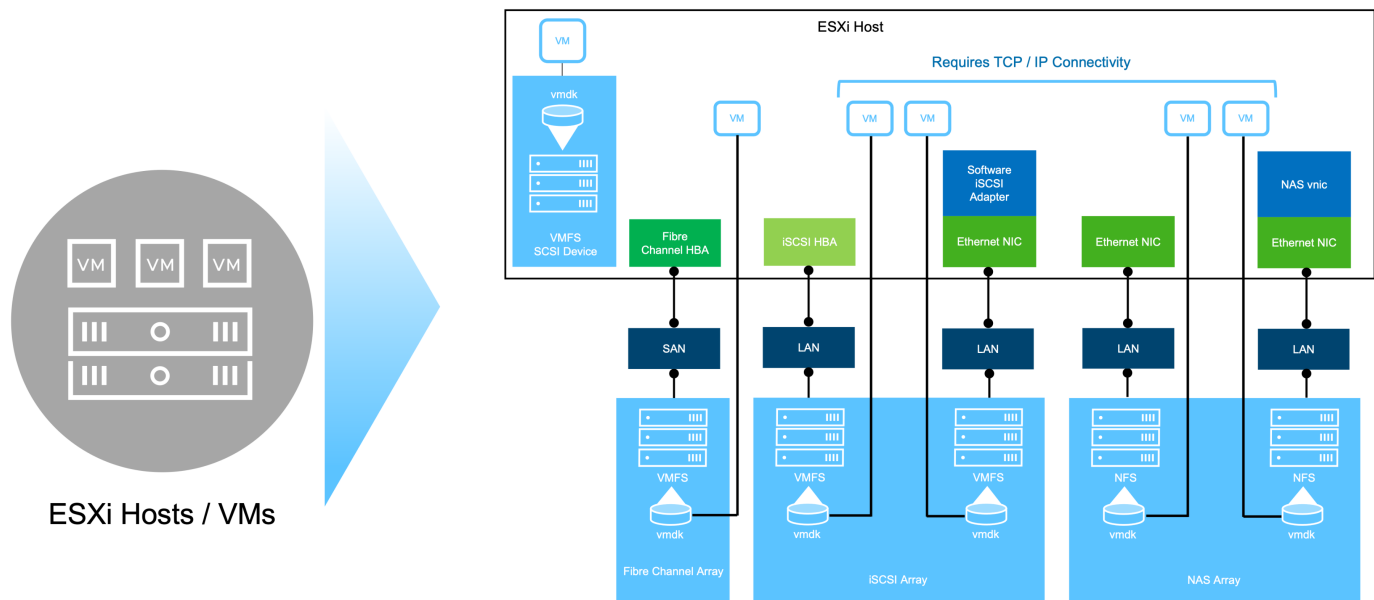
- VMware vSphere
- VMware VSAN
- ARIA Standard
- Service de grid Kubernetes VMware Tanzu pour vSphere
- Switch distribué vSphere

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 vvolfs, 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.

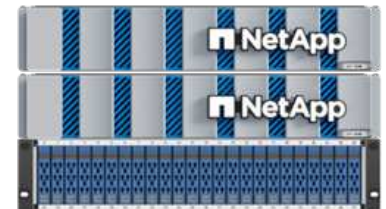
### AFF A70



### 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.

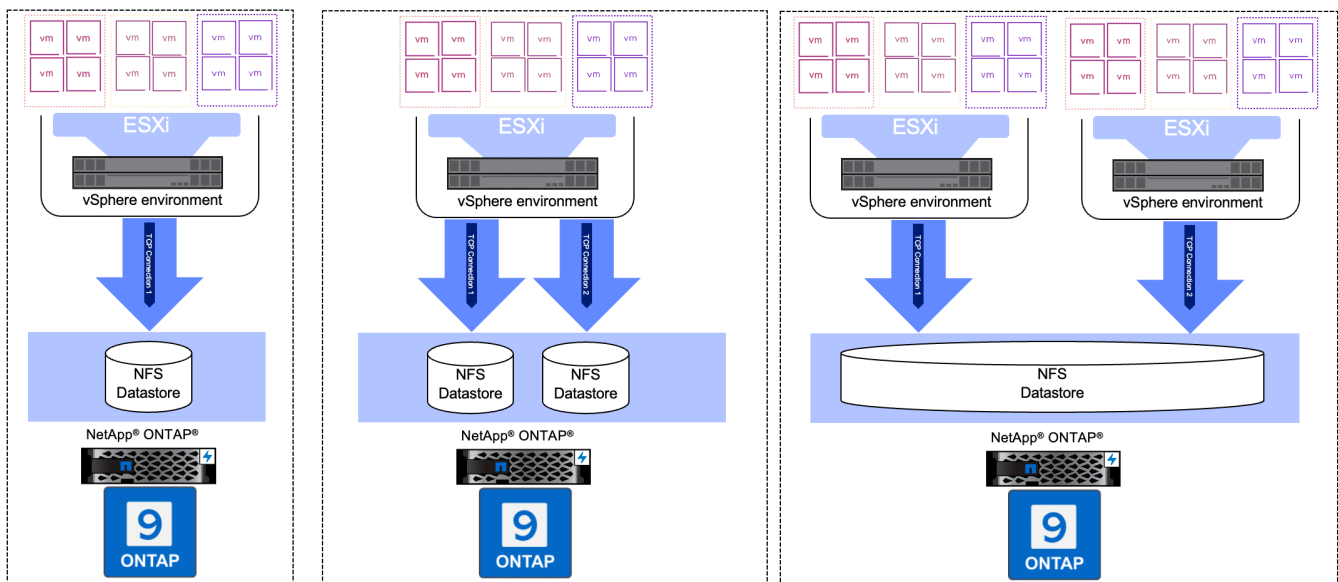
## Détails techniques

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.

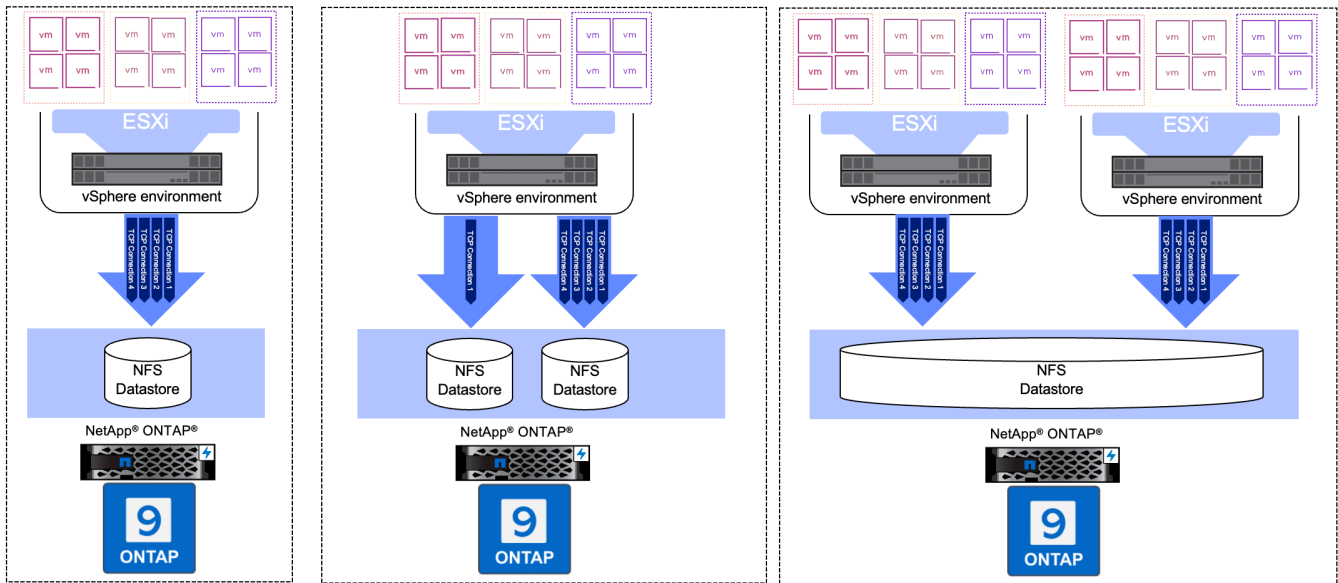
## Without nConnect feature with NetApp and VMware



### 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.

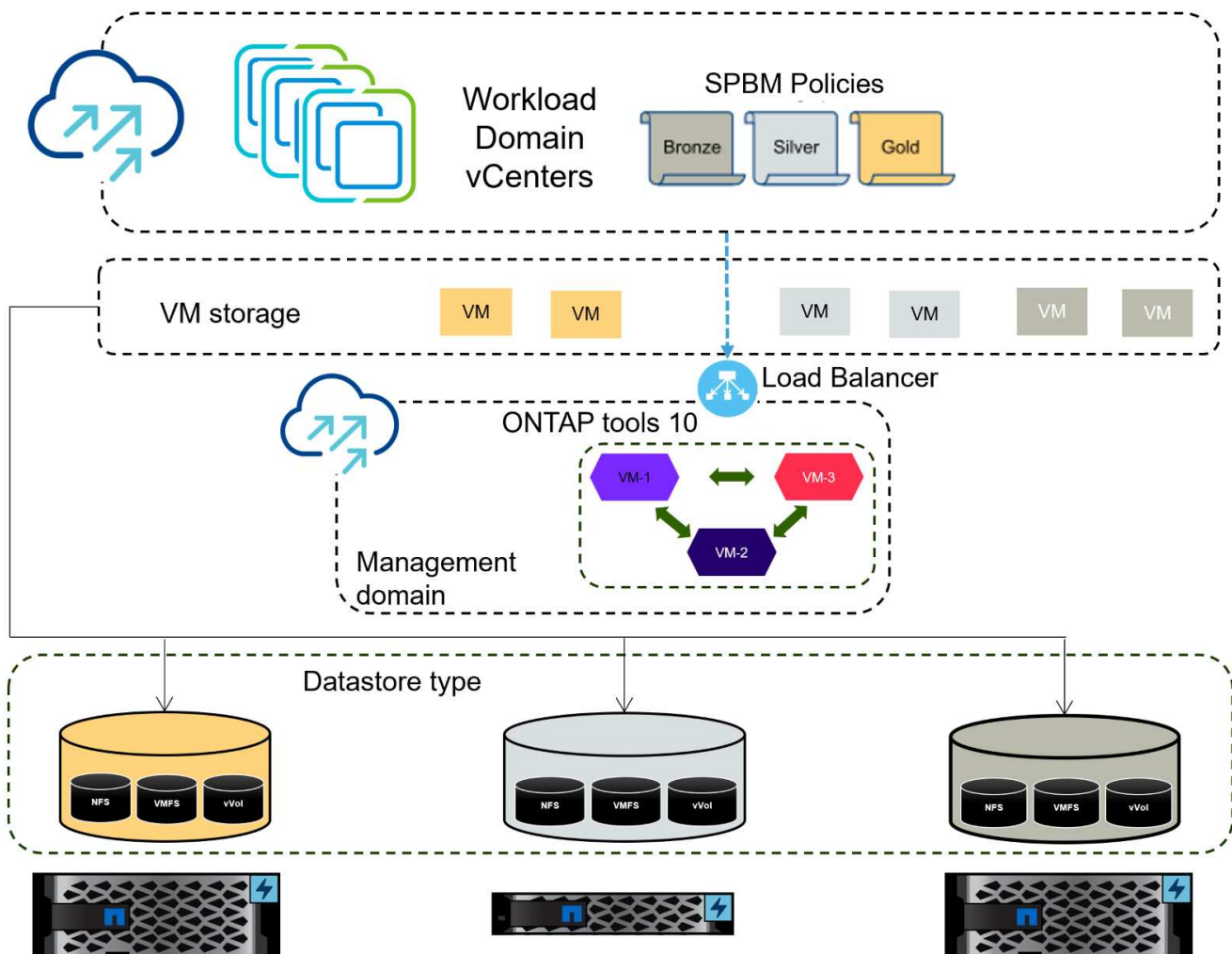
## Présentation de la solution

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 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.

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 :

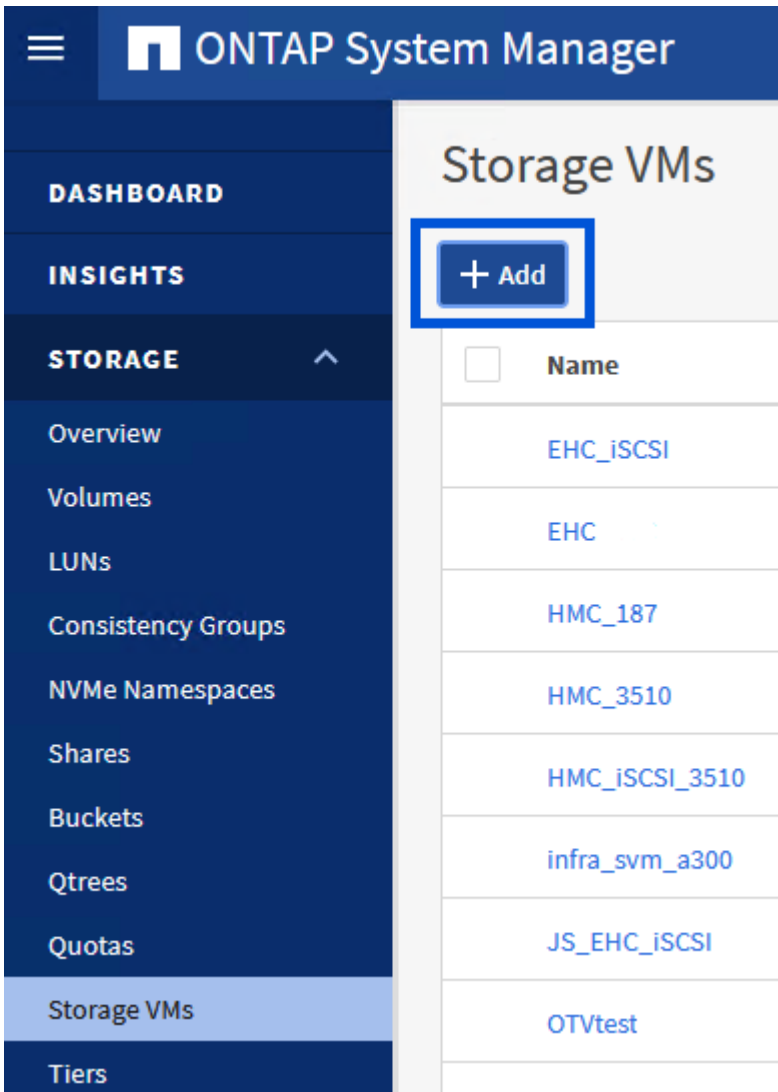
### **Créez un SVM et des LIF sur un système de stockage ONTAP**

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

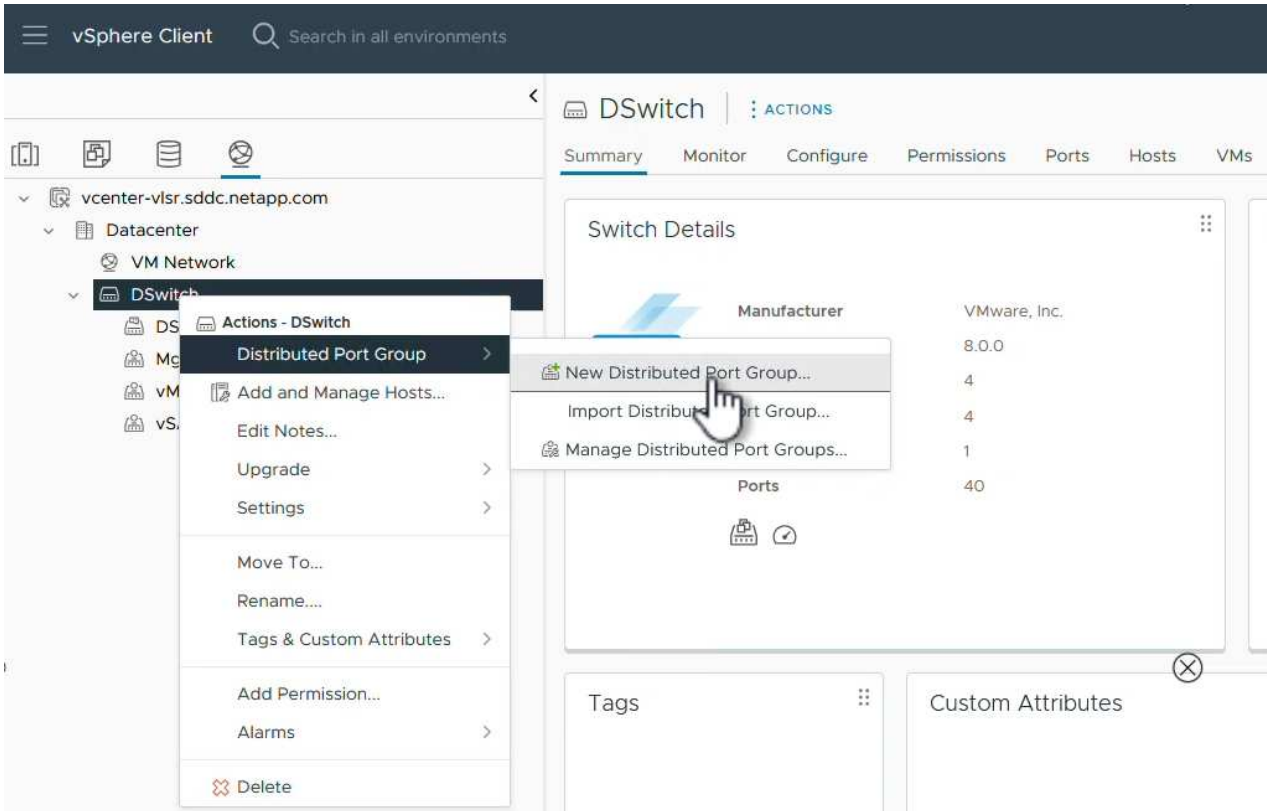
### Configuration de la mise en réseau pour NFS sur les hôtes ESXi

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.

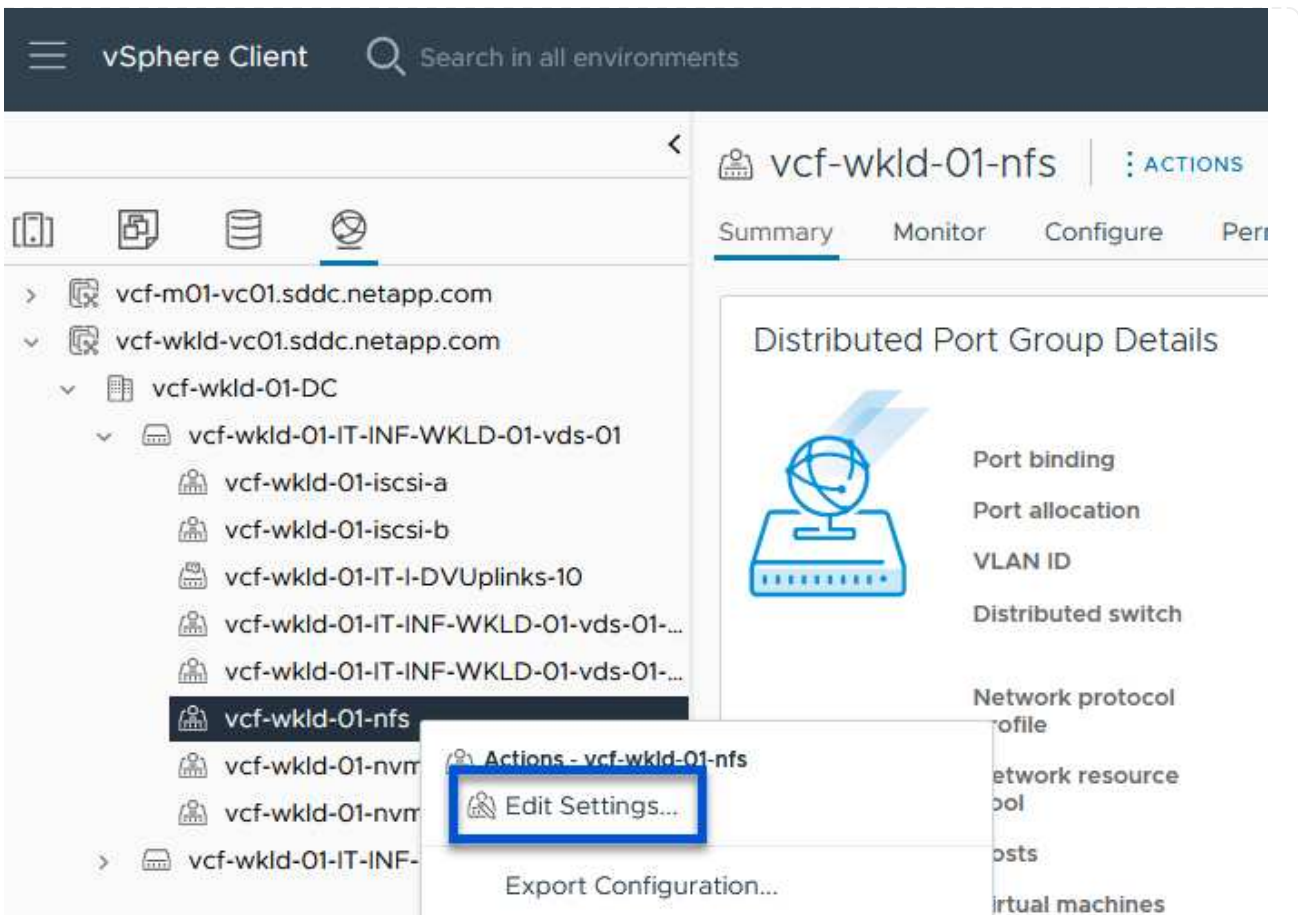
<b>Port binding</b>	Static binding ▾
<b>Port allocation</b>	Elastic ▾ ⓘ
<b>Number of ports</b>	8 ▾
<b>Network resource pool</b>	(default) ▾
<b>VLAN</b>	
<b>VLAN type</b>	VLAN ▾
<b>VLAN ID</b>	3374 ▾
<b>Advanced</b>	
<input type="checkbox"/> Customize default policies configuration	

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

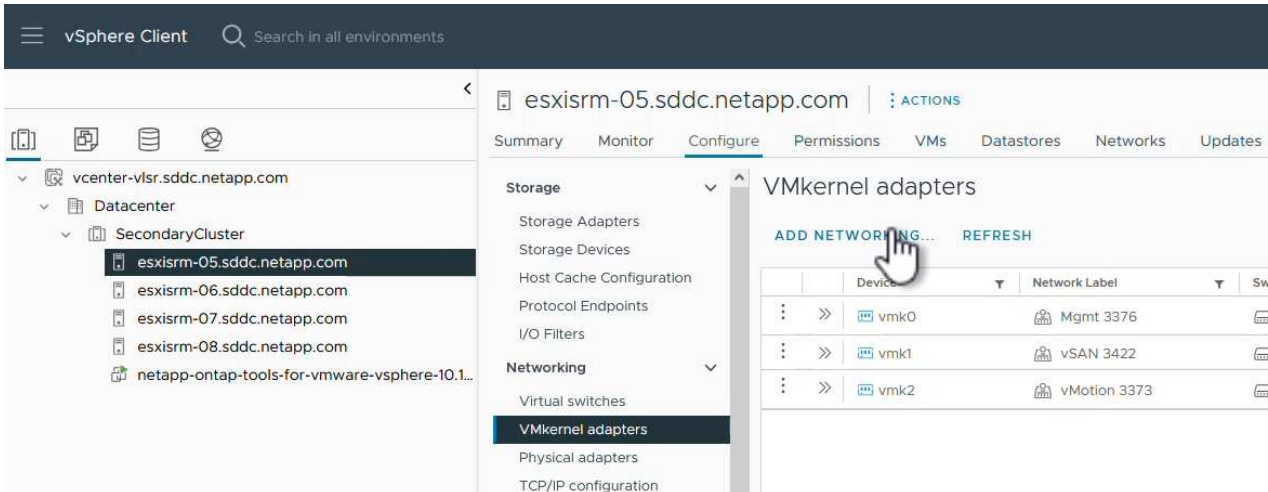
7. Répétez ce processus pour chaque hôte ESXi du cluster.



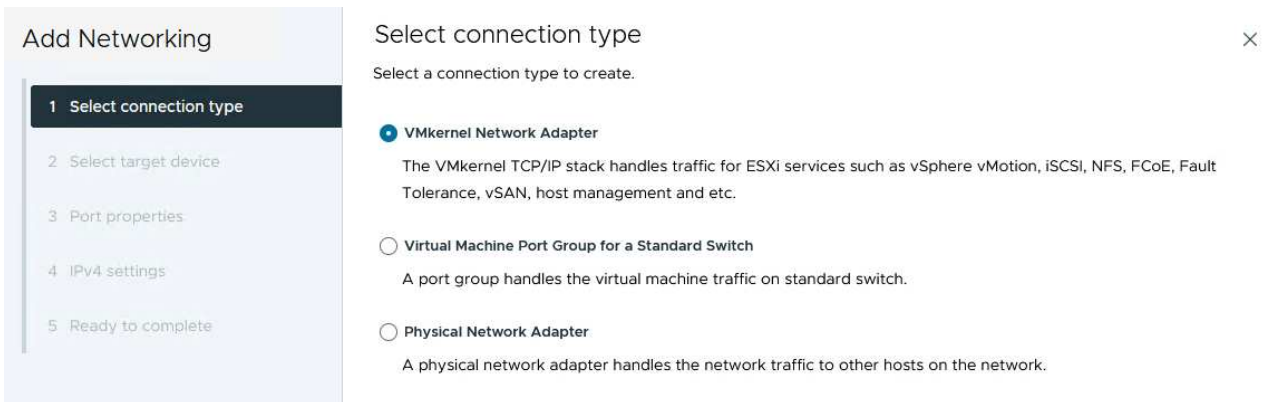
## Créez un adaptateur VMkernel sur chaque hôte ESXi

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

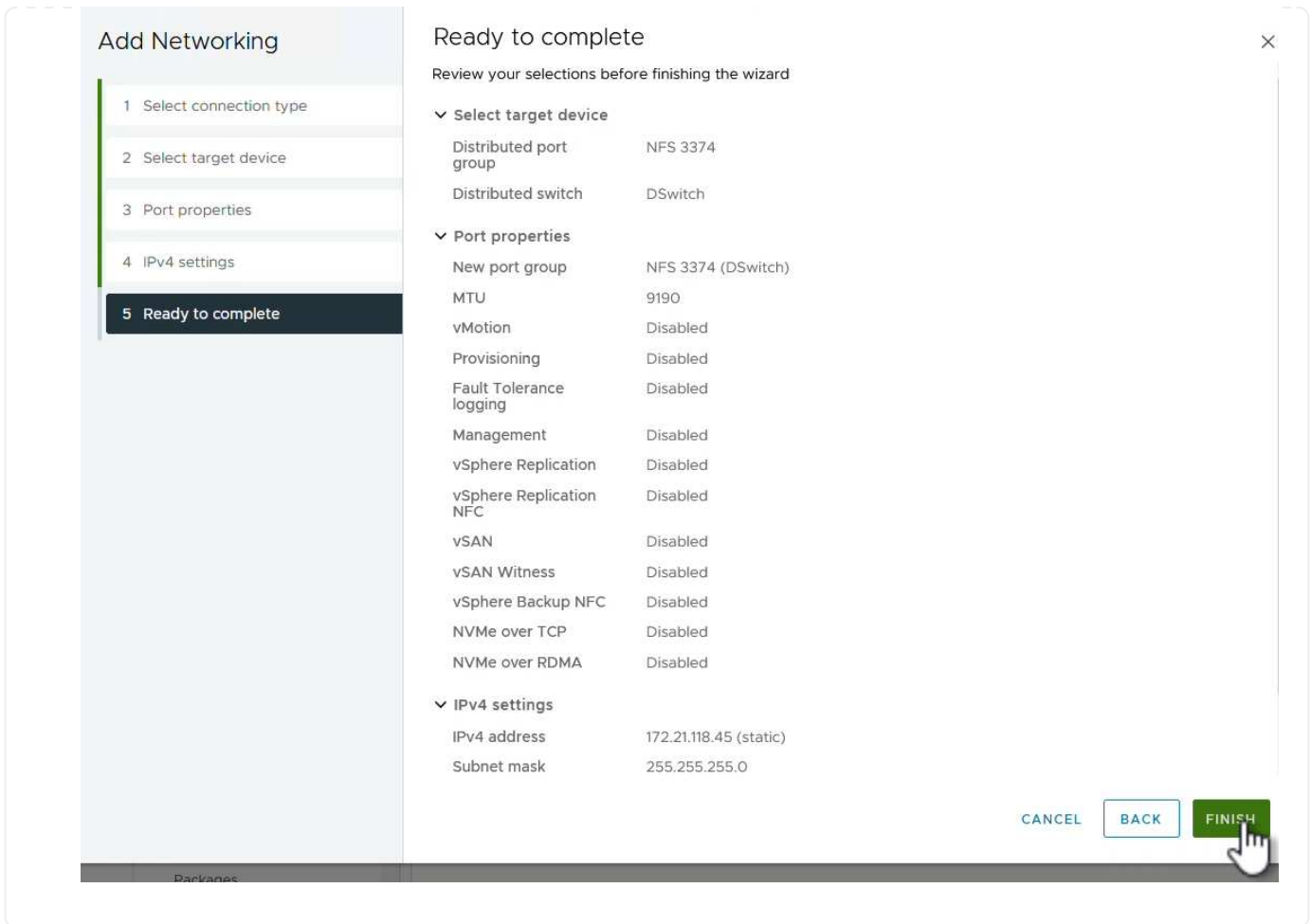
DNS server addresses

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

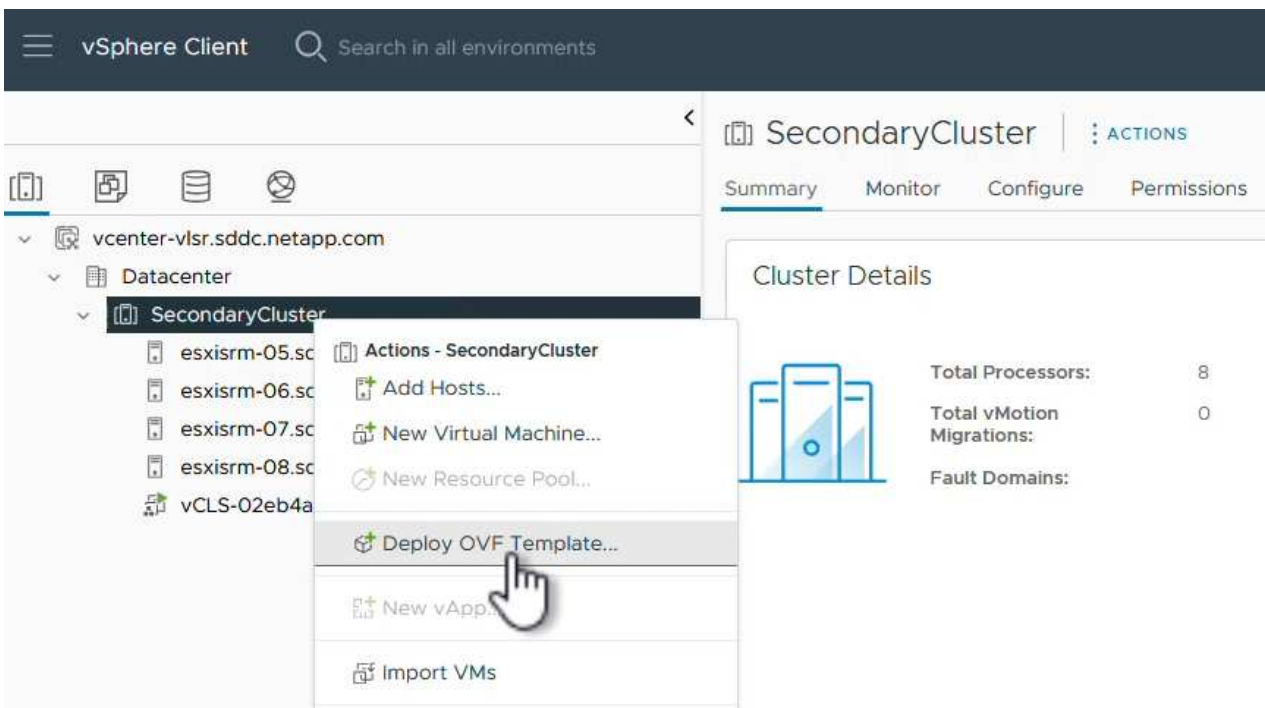
Les outils ONTAP pour VMware vSphere 10 sont déployés en tant qu'appliance de machine virtuelle et fournissent une interface utilisateur vCenter intégrée pour la gestion du stockage ONTAP. ONTAP Tools 10 inclut un nouveau portail de gestion global pour la gestion des connexions à plusieurs serveurs vCenter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

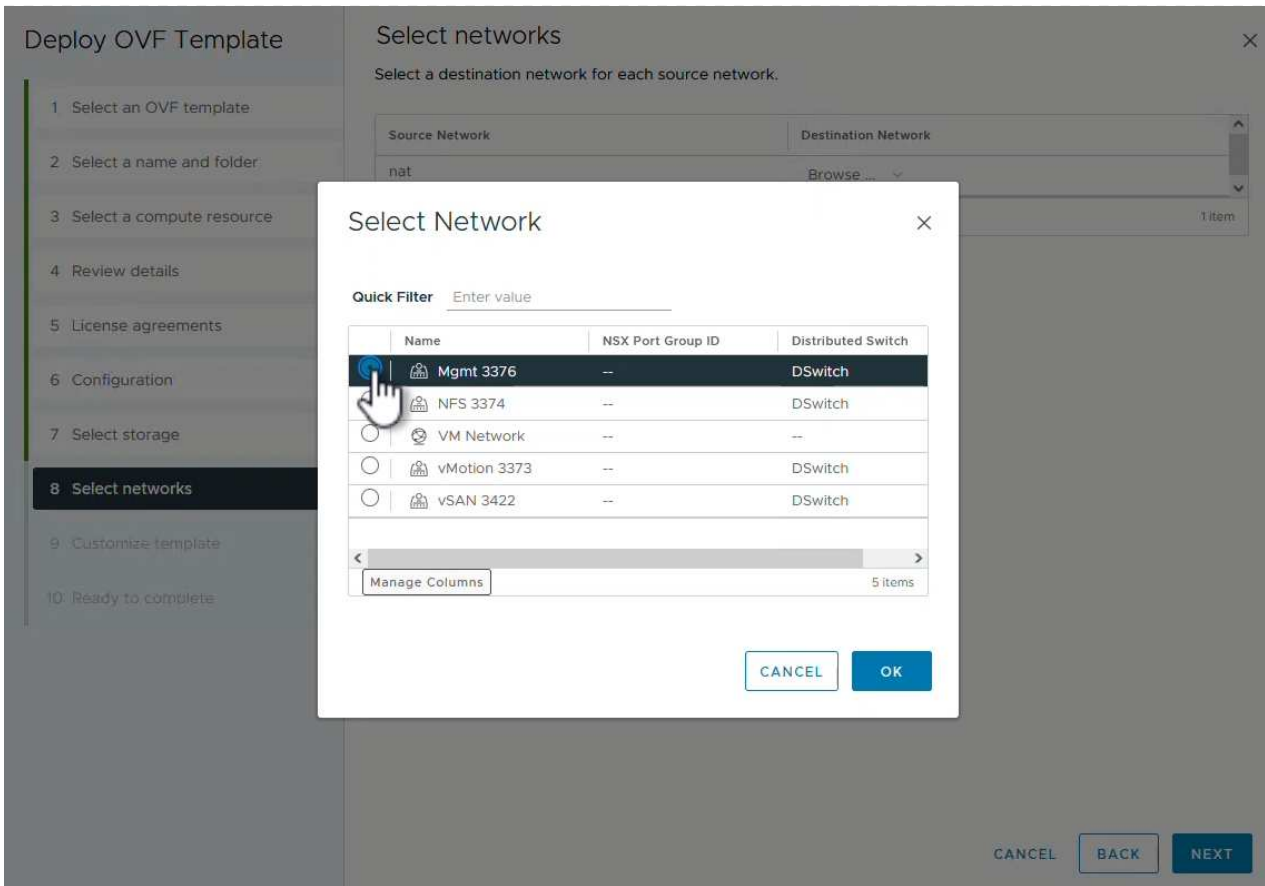
Disable Storage DRS for this virtual machine

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

<b>Maintenance user password(*)</b>	Password to assign to maint user account	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
Deployment Configuration		3 settings
<b>Load balancer IP(*)</b>	Load balancer IP (*)	<input type="text" value="172.21.120.57"/>
<b>Virtual IP for K8s control plane(*)</b>	Provide the virtual IP address for K8s control plane	<input type="text" value="172.21.120.58"/>
<b>Primary VM</b>	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
<b>HostName(*)</b>	Specify the hostname for the VM	<input type="text"/>
<b>IP Address(*)</b>	Specify the IP address for the appliance	<input type="text"/>
<b>IPv6 Address</b>	Specify the IPv6 address on the deployed network only when you need dual stack	<input type="text"/>

CANCEL BACK NEXT

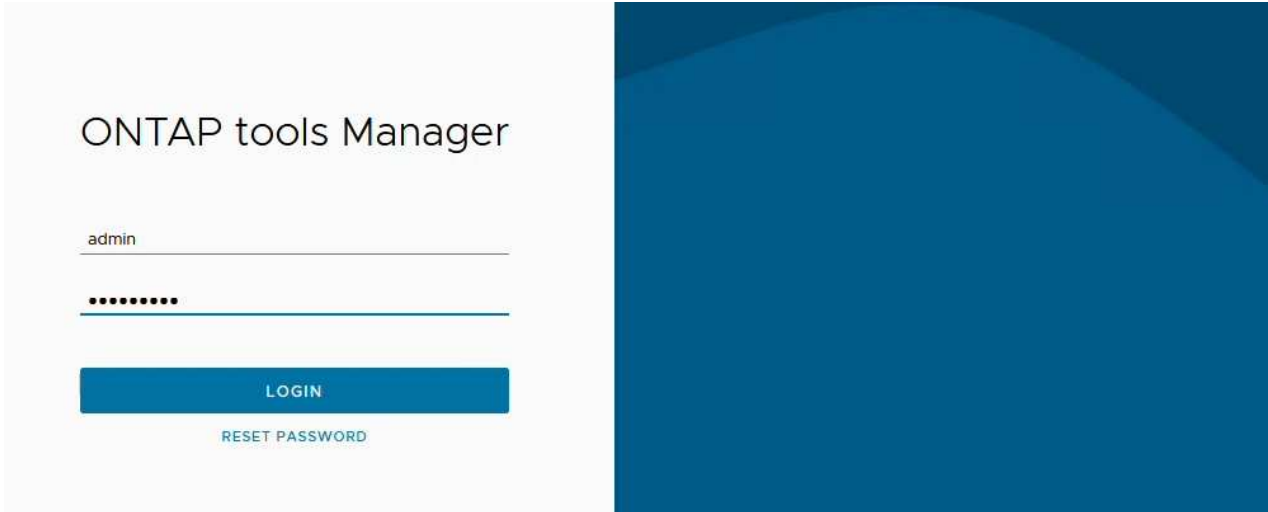
10. Passez en revue toutes les informations de la page prêt à terminer et cliquez sur Terminer pour

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](#)



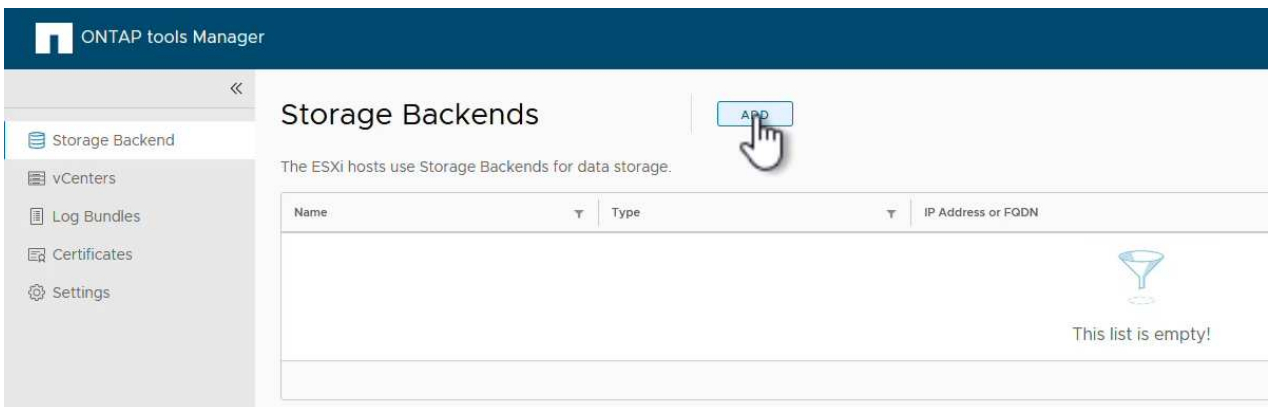
## Log Bundles

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.




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

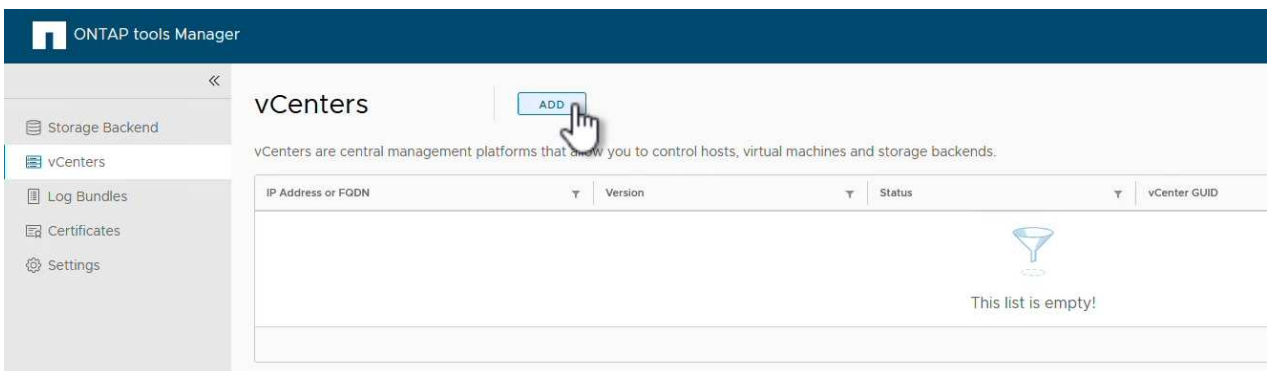
Password: \* ●●●●●●●● 

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: \*

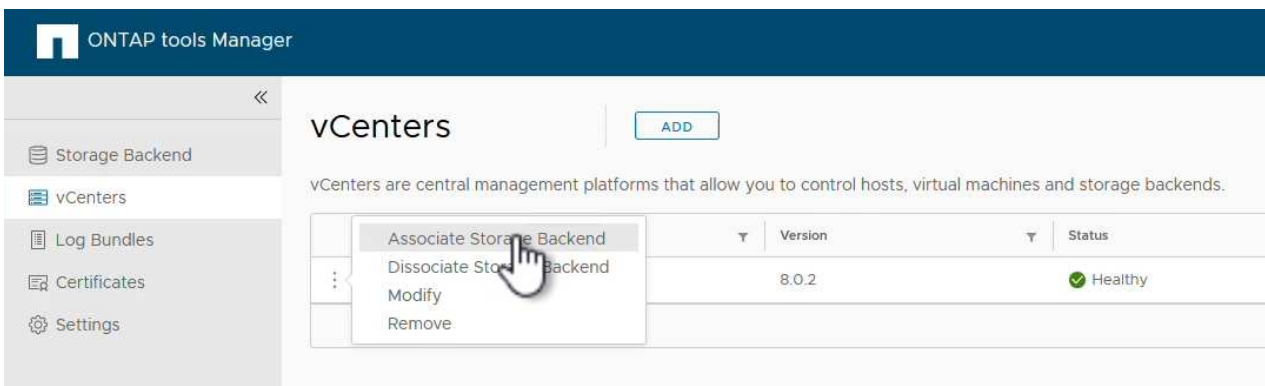
Password: \*  

Port: \*

CANCEL

ADD 


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



ONTAP tools Manager

vCenters

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

	Version	Status
 Associate Storage Backend Dissociate Storage Backend Modify Remove	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

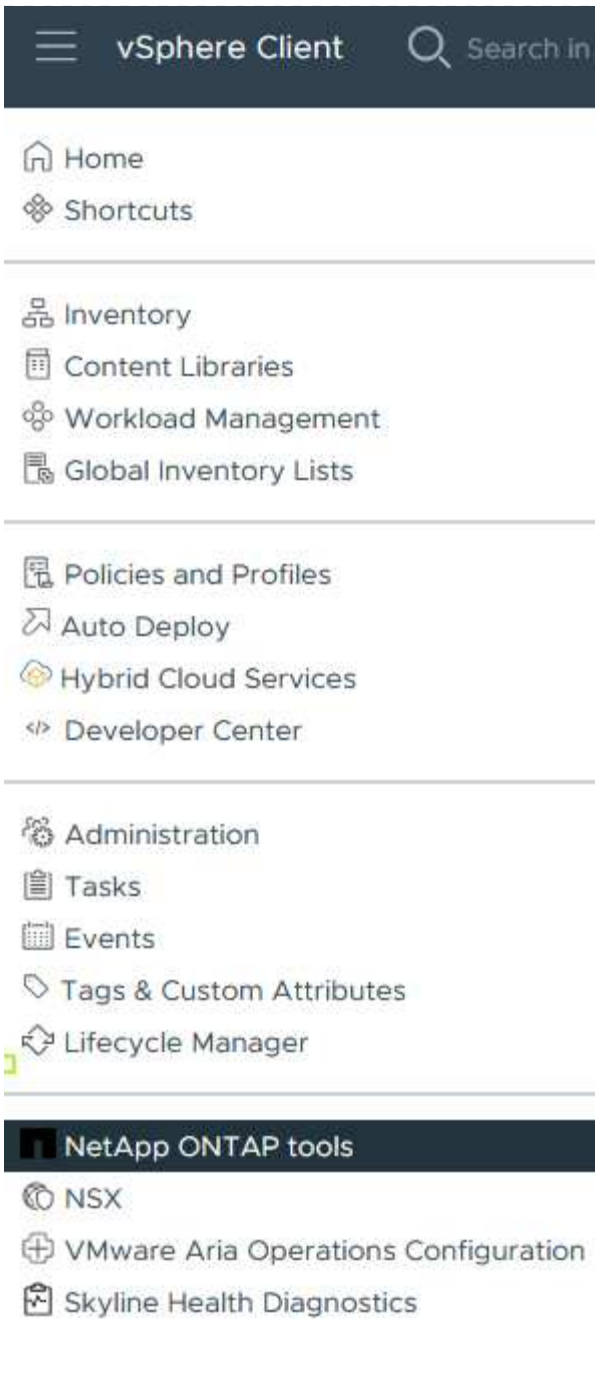


CANCEL

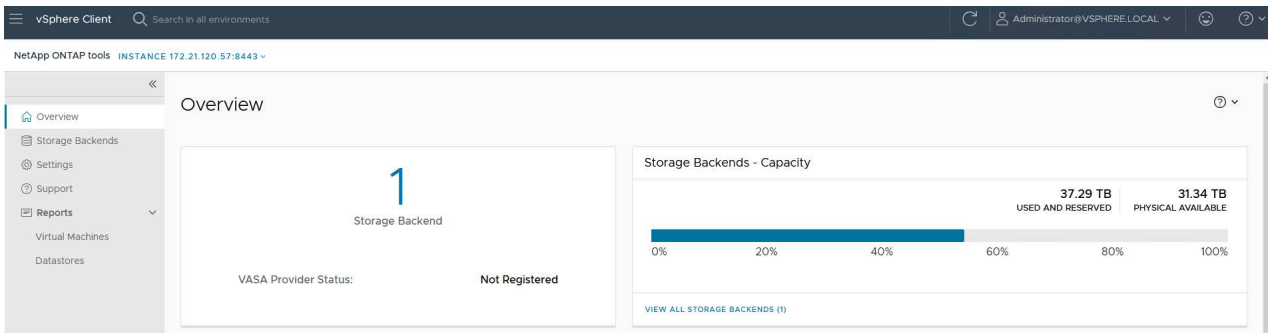
ASSOCIATE



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.



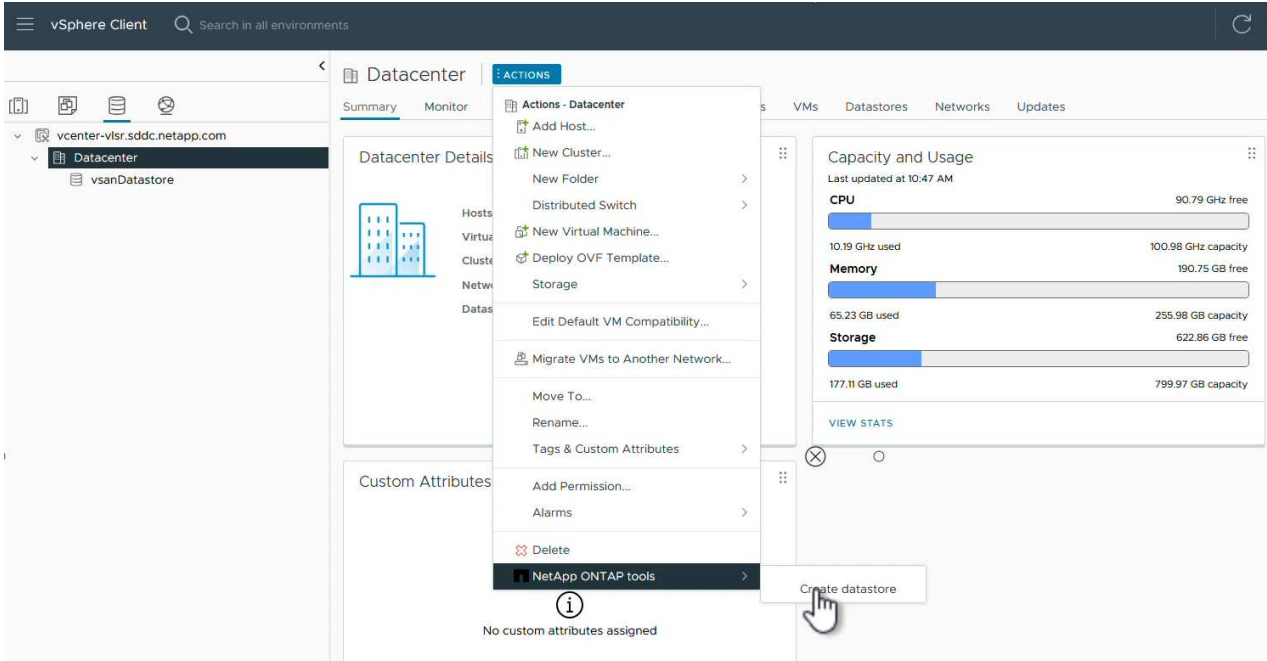




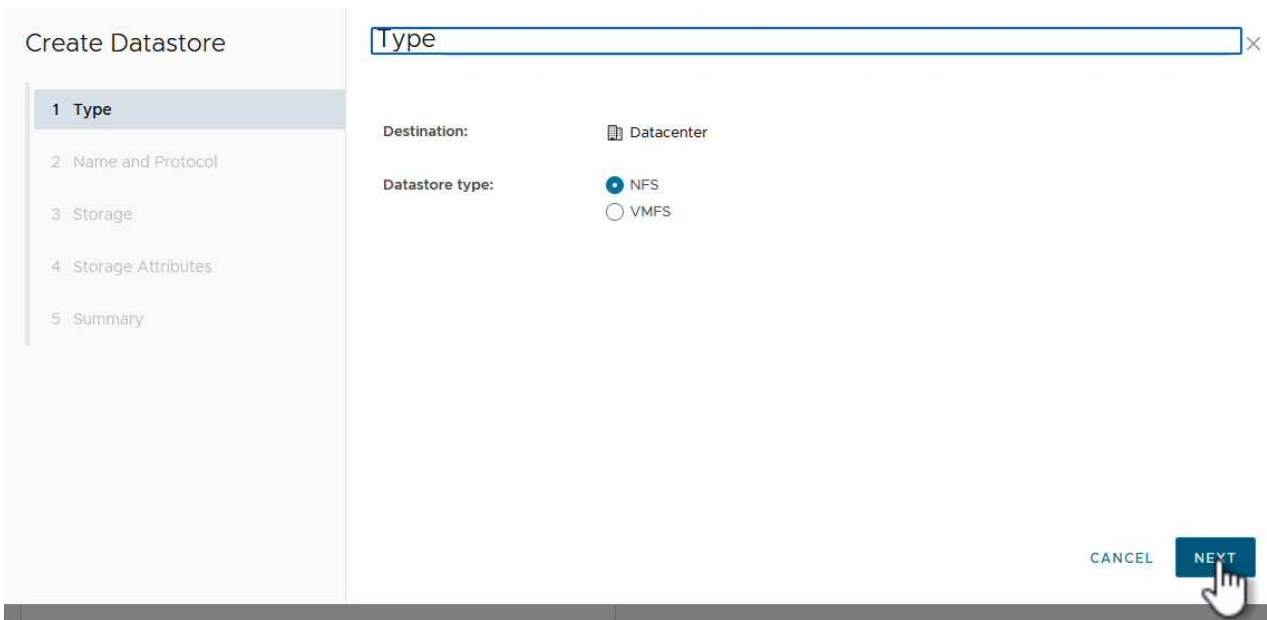
## Créer un datastore NFS à l'aide des outils ONTAP 10

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 with the 'Name and Protocol' step selected. The left sidebar lists the steps: 1 Type, 2 Name and Protocol, 3 Storage, 4 Storage Attributes, and 5 Summary. The main content 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)
- 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 with the 'Storage' step selected. The left sidebar lists the steps: 1 Type, 2 Name and Protocol, 3 Storage, 4 Storage Attributes, and 5 Summary. The main content area is titled 'Storage' and contains the following fields:

- Platform: \*** Performance (A)
- Storage VM: \*** VCF\_NFS (with IP address: ntaphci-a300e9u25 (172.16.9.25))
- Advanced Options:** (expanded)
- 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

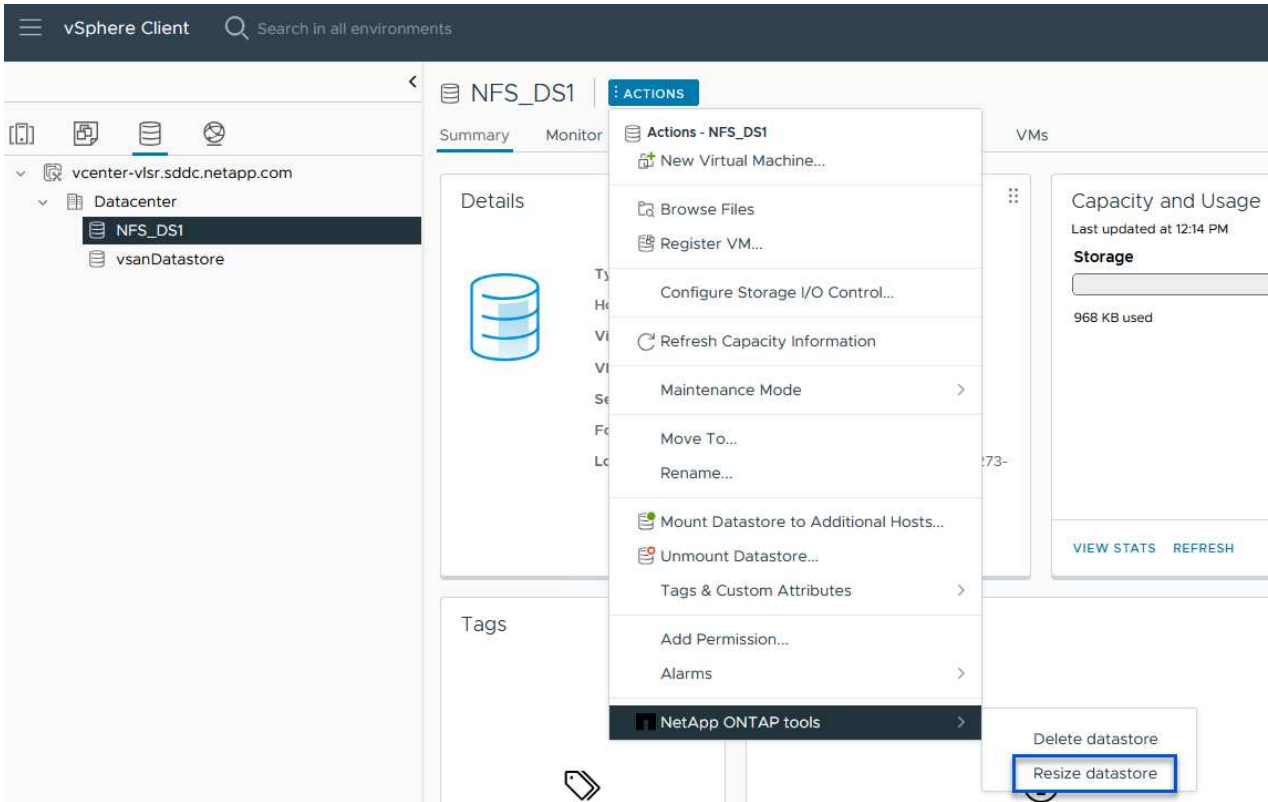
BACK

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 <input type="text"/>

CANCEL

RESIZE

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

Task Name	Target	Status	Details
Expand Datastore	<a href="https://vcenter-vlsr.sddc.net/app.com">vcenter-vlsr.sddc.net app.com</a>	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 disruptifs 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.

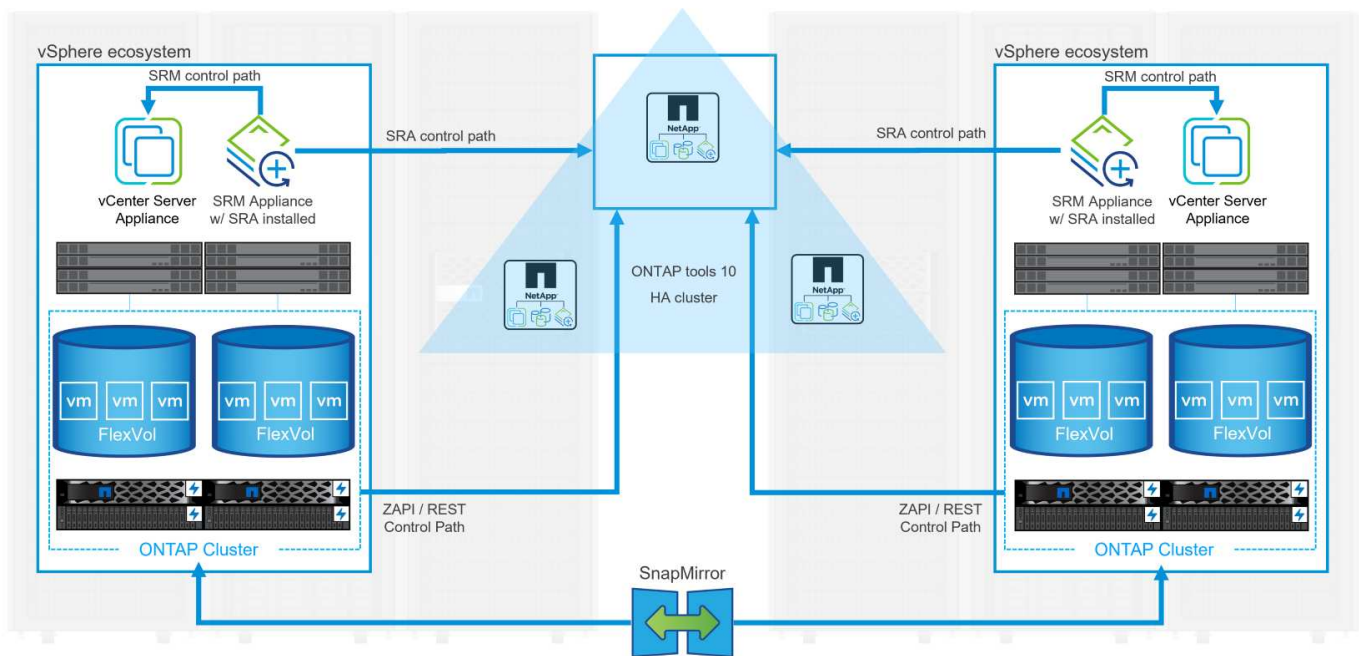
## Présentation du scénario

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.

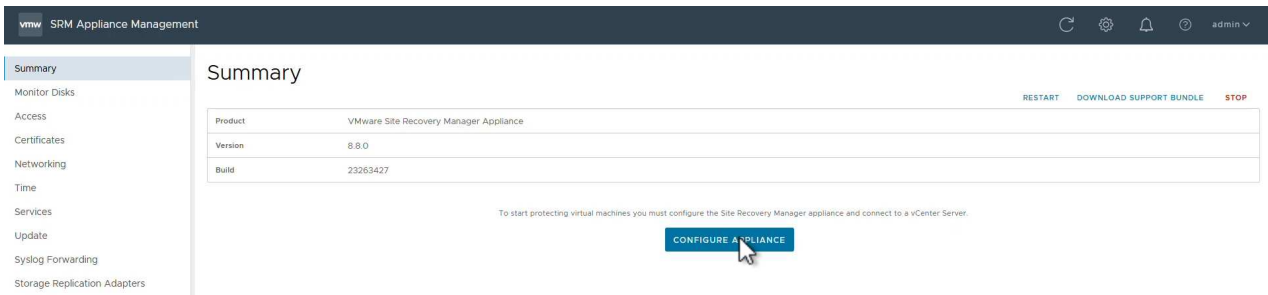
## **Configurez l'appliance SRM**

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

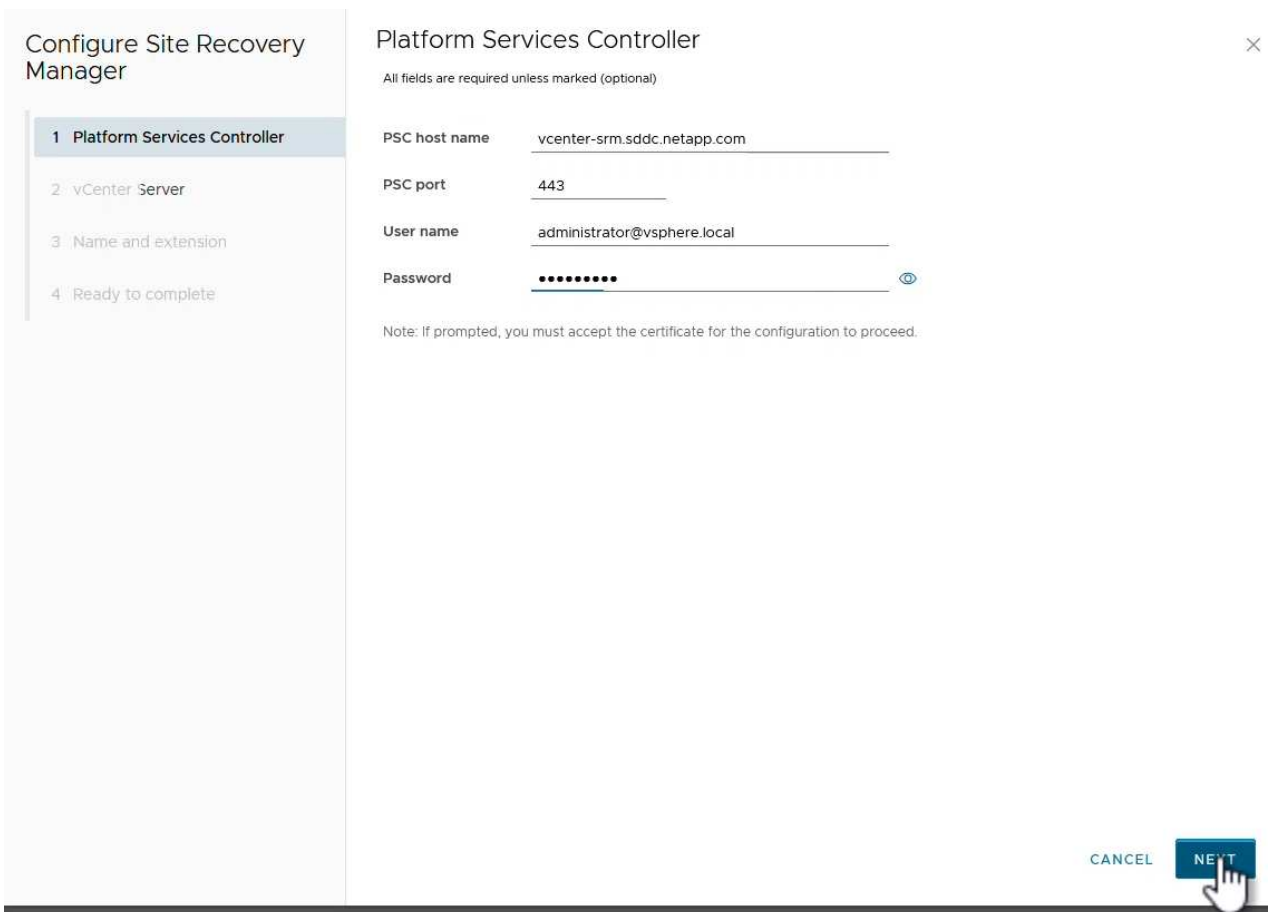
## Connectez l'appliance SRM aux sites principaux et secondaires

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

1. Dans un navigateur Web, accédez à [https://<SRM\\_appliance\\_IP>:5480](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

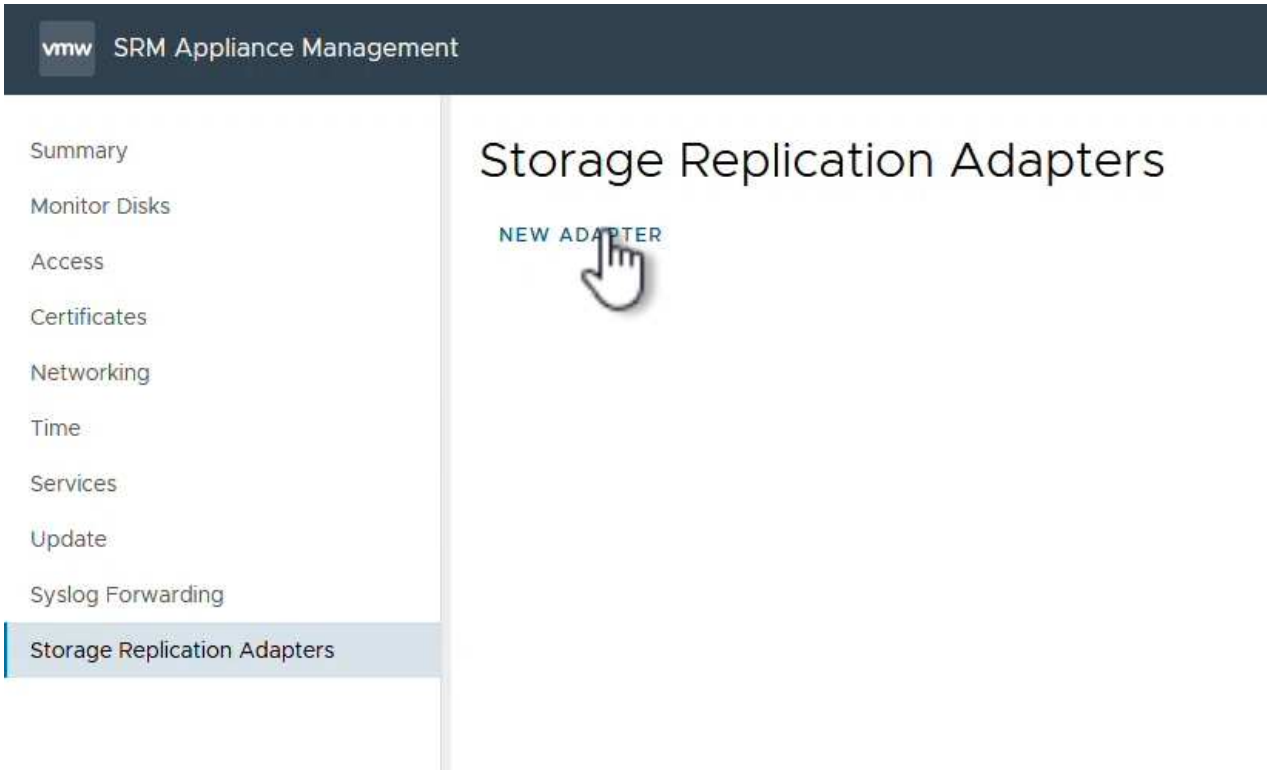
CANCEL BACK **NEXT**

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.

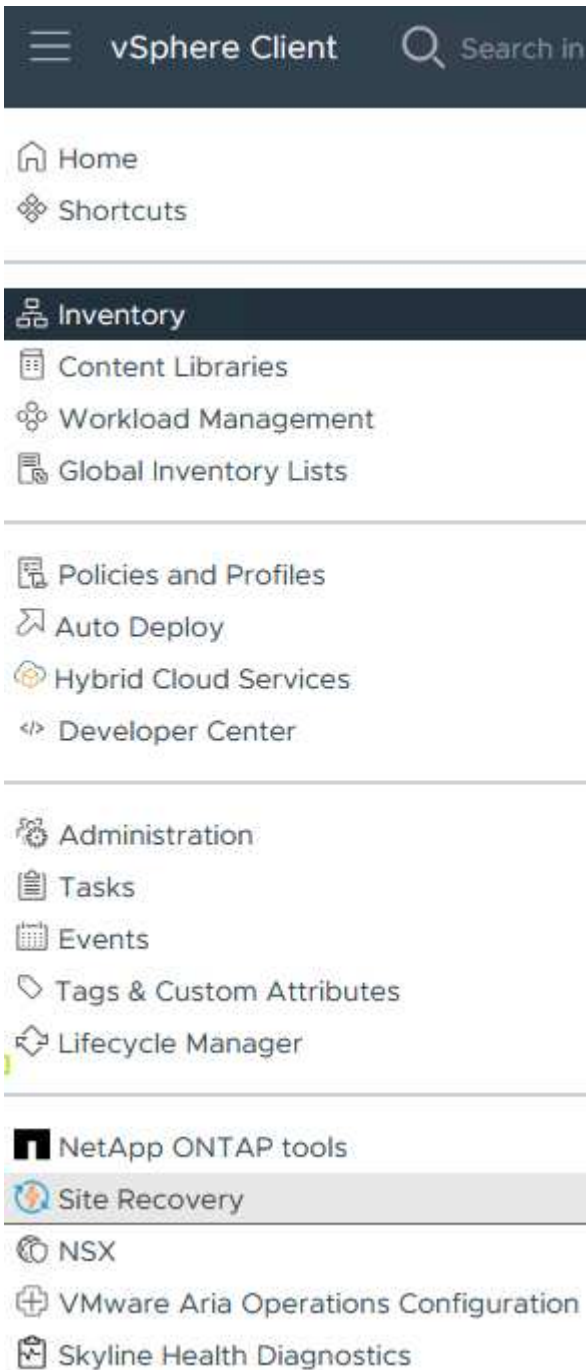
## Configurer site Recovery pour SRM

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 progress indicator with four steps: 1. Pair type (selected), 2. Peer vCenter Server, 3. Services, and 4. Ready to complete. The main area is titled 'Pair type' and contains the following elements:

- A dropdown menu labeled 'vCenter Server' with a search icon and a downward arrow. The selected item is 'vcenter-vlsr.sddc.netapp.com'.
- A section titled 'Pair type' with two radio button options:
  - Pair with a peer vCenter Server located in a different SSO domain
  - Pair with a peer vCenter Server located in the same SSO domain
- At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'. A mouse cursor is pointing at 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

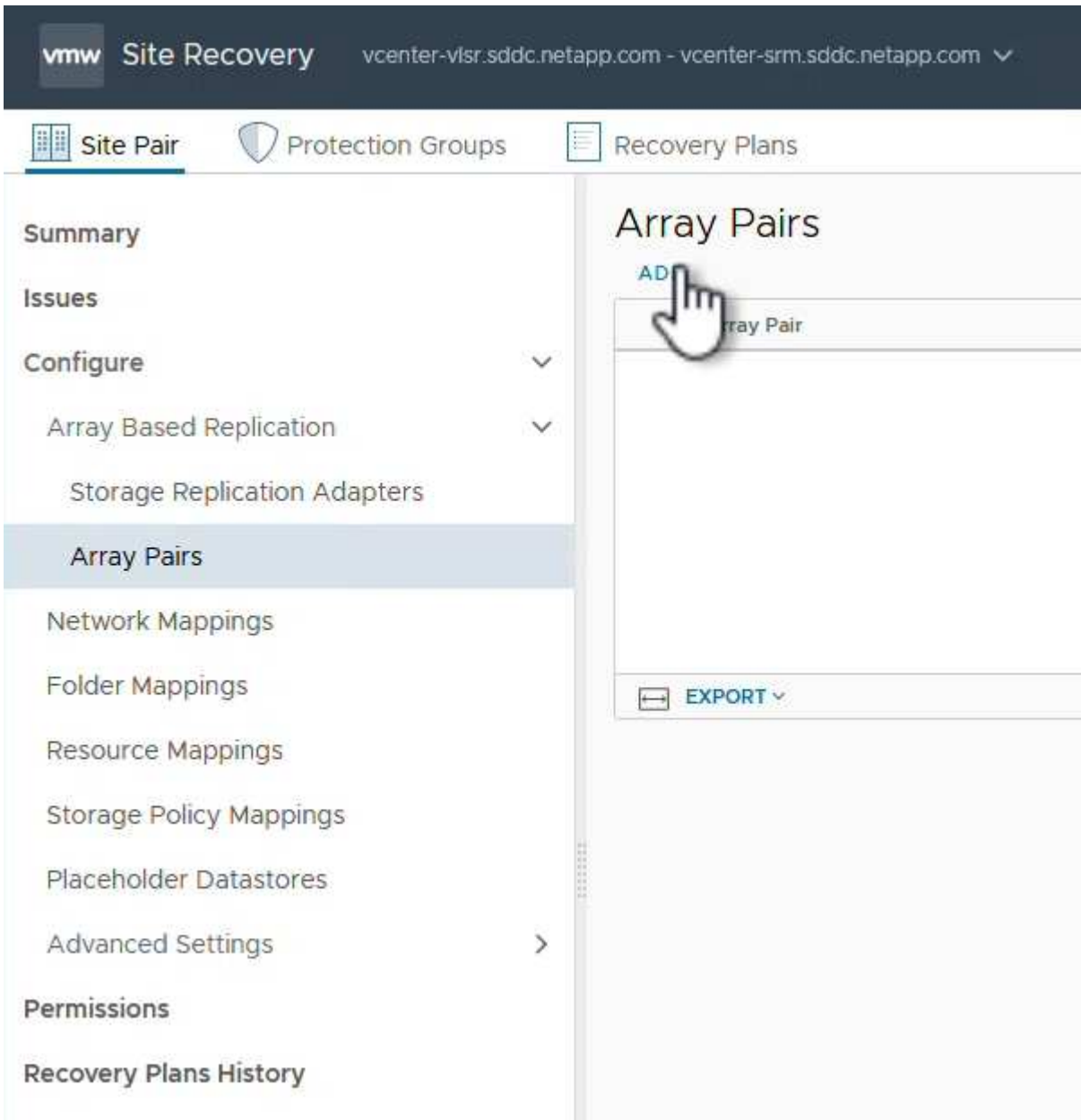
Name	Site 1 <a href="#">RENAME</a>	Site 2 <a href="#">RENAME</a>
Server	srm-site1.sddc.netapp.com:443 <a href="#">ACTIONS</a>	srm-site2.sddc.netapp.com:443 <a href="#">ACTIONS</a>
Version	8.8.0, 23263429	8.8.0, 23263429
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
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

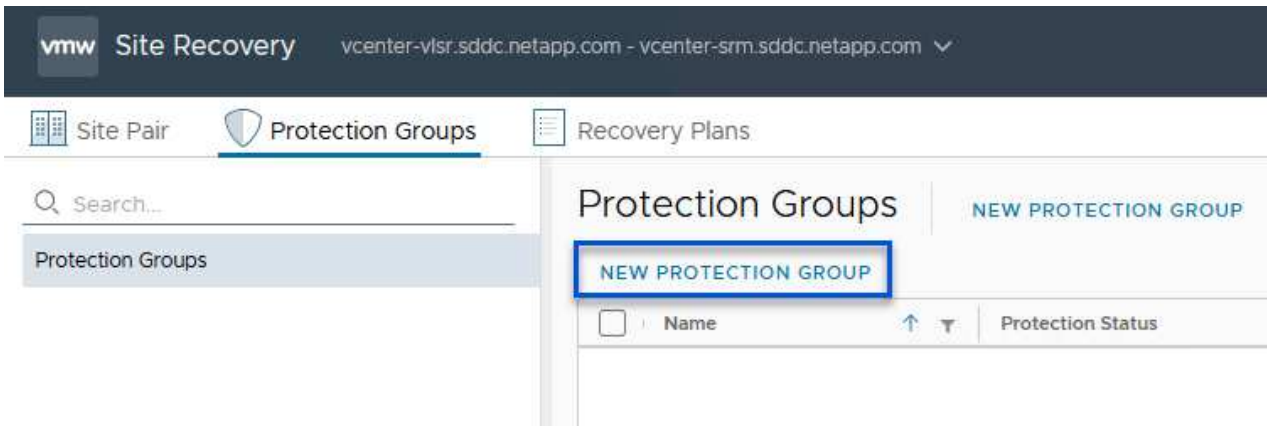
NEXT

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

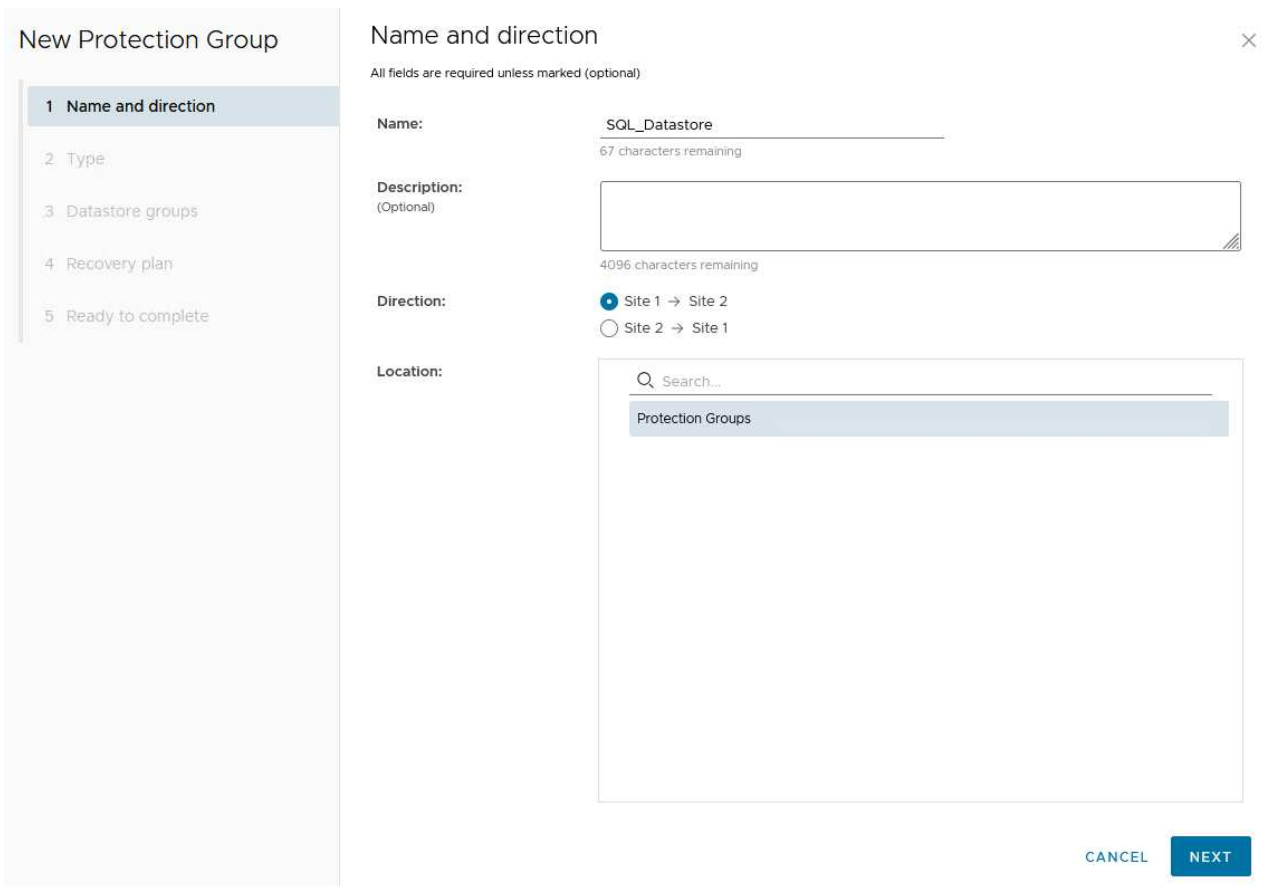
## Configurer les groupes de protection pour SRM

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' (selected), '2 Type', '3 Datastore groups', '4 Recovery plan', and '5 Ready to complete'. The main area is titled 'Name and direction' and contains the following fields:

- Name:** A text input field containing 'SQL\_Datastore' with a character count of '67 characters remaining'.
- Description:** An optional text area with a character count of '4096 characters remaining'.
- Direction:** Two radio button options: 'Site 1 -> Site 2' (selected) and 'Site 2 -> Site 1'.
- Location:** A search dropdown menu with 'Protection Groups' selected.

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"/> ✓ ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
<input type="radio"/> ✓ 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.

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

CANCEL

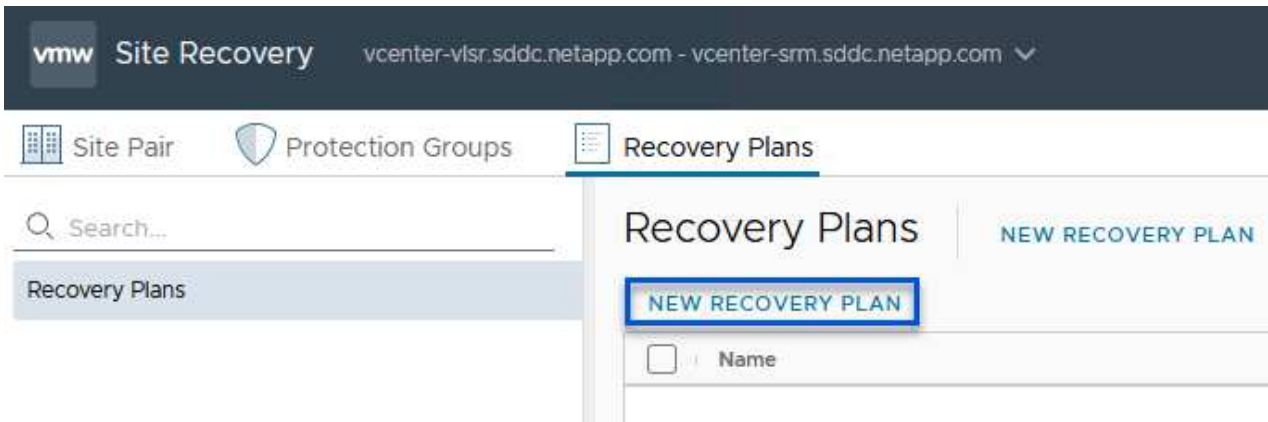
BACK

FINISH

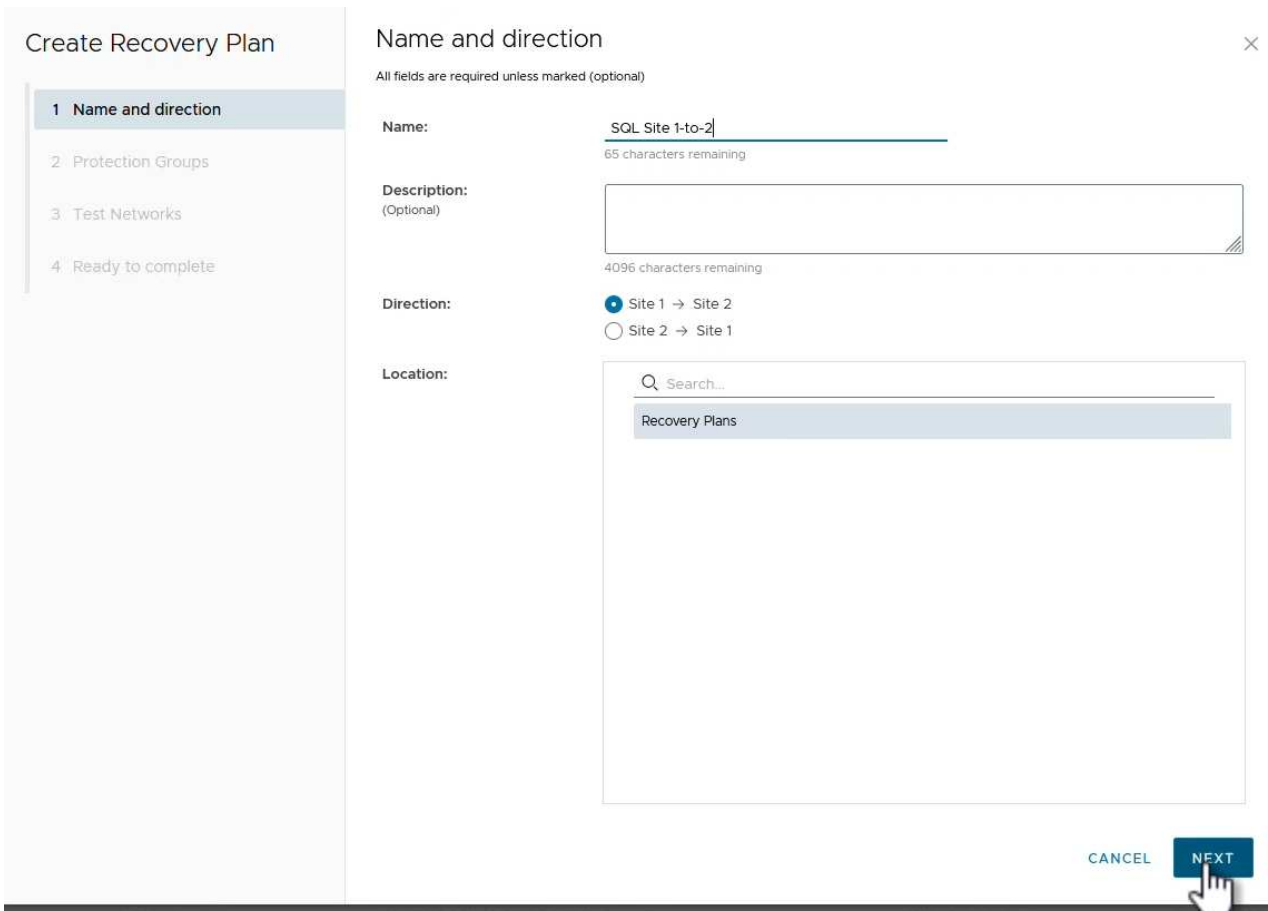
## Configurer le plan de reprise pour SRM

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'. A mouse cursor is clicking the 'NEXT' button.

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

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

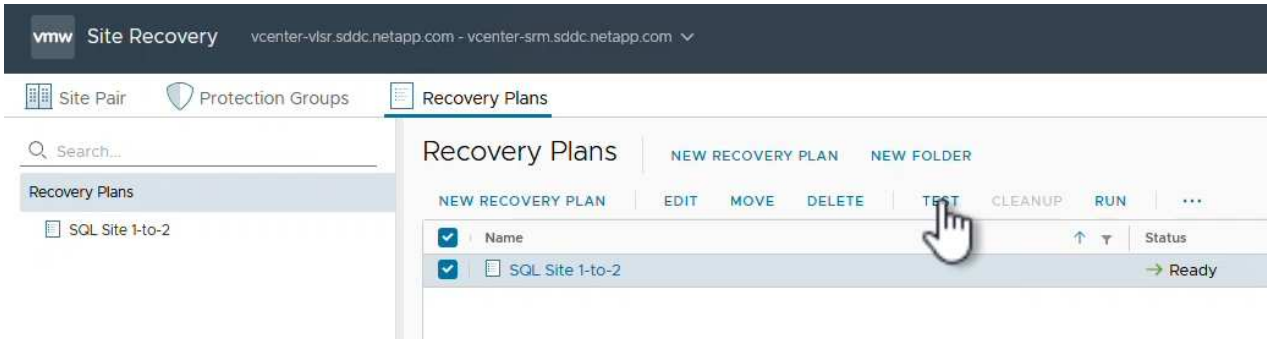
Cette section traite des différentes fonctions d'utilisation de la reprise sur incident avec SRM, notamment le test du basculement, l'exécution du basculement, la reprotection et la restauration.

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.

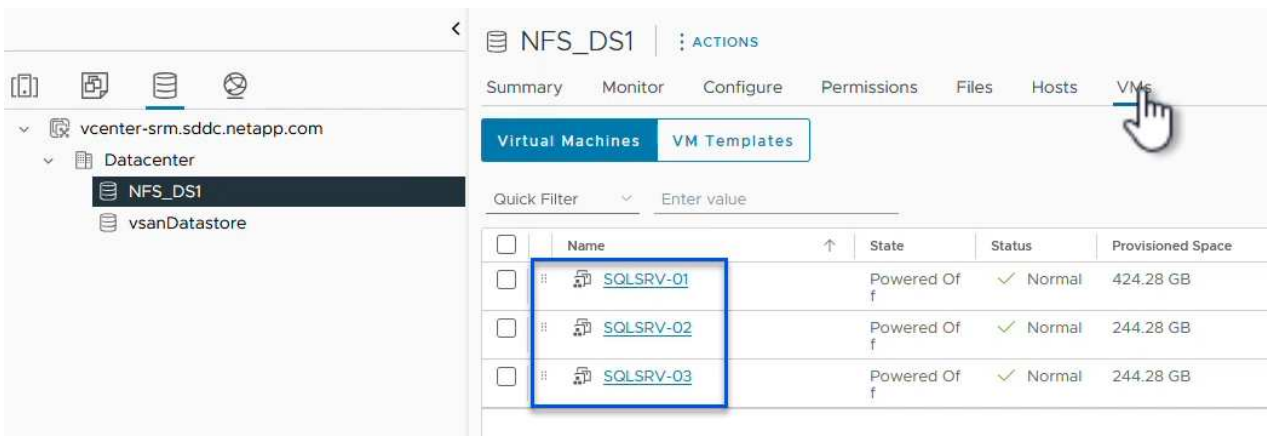
1. Dans l'interface de récupération de site, cliquez sur l'onglet **Plan de récupération**, puis sélectionnez un plan de récupération. Cliquez sur le bouton **Test** pour commencer le test du basculement vers le site secondaire.



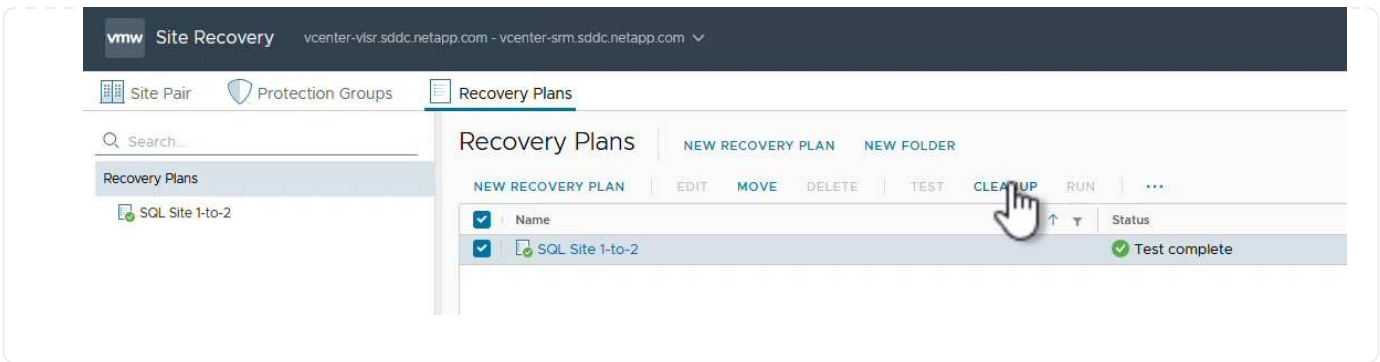
2. Vous pouvez afficher la progression du test à partir du volet des tâches site Recovery ainsi que du volet des tâches vCenter.

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



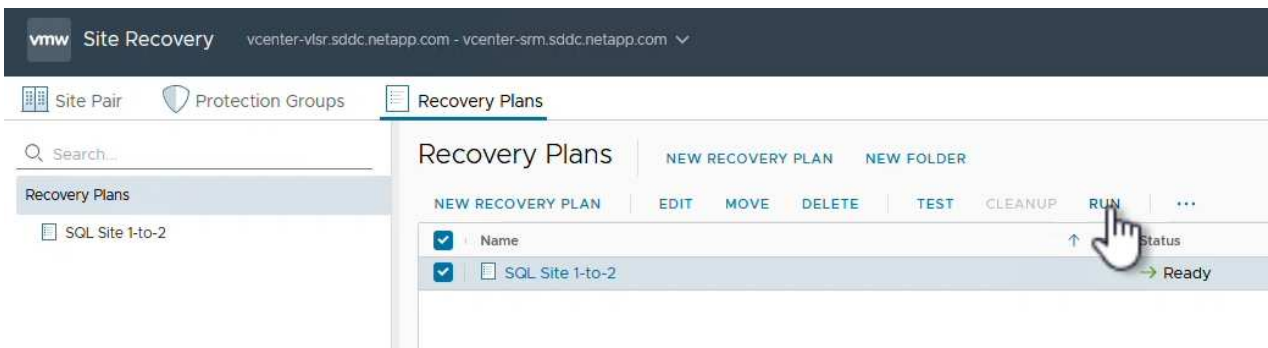
4. Une fois le test terminé, cliquez sur **Cleanup** pour démonter le datastore et revenir à l'environnement d'origine.



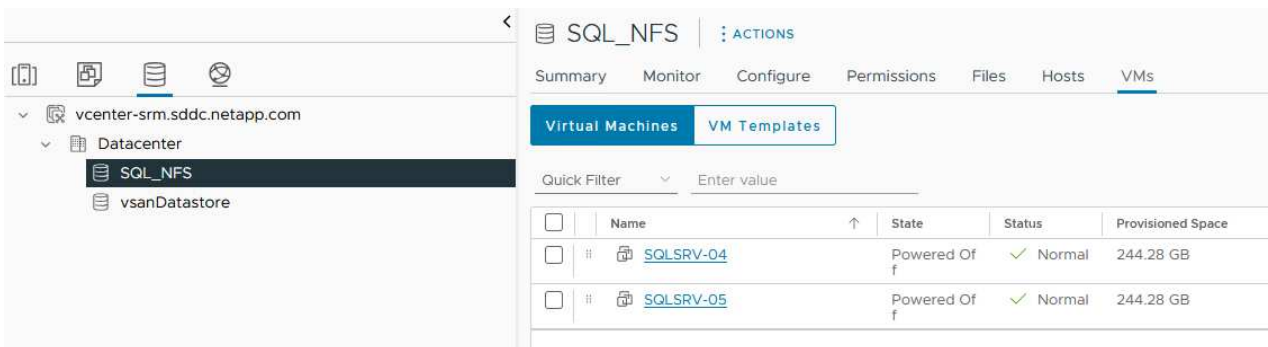
## Exécuter un plan de reprise avec SRM

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 reprotction 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 reprotction 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.

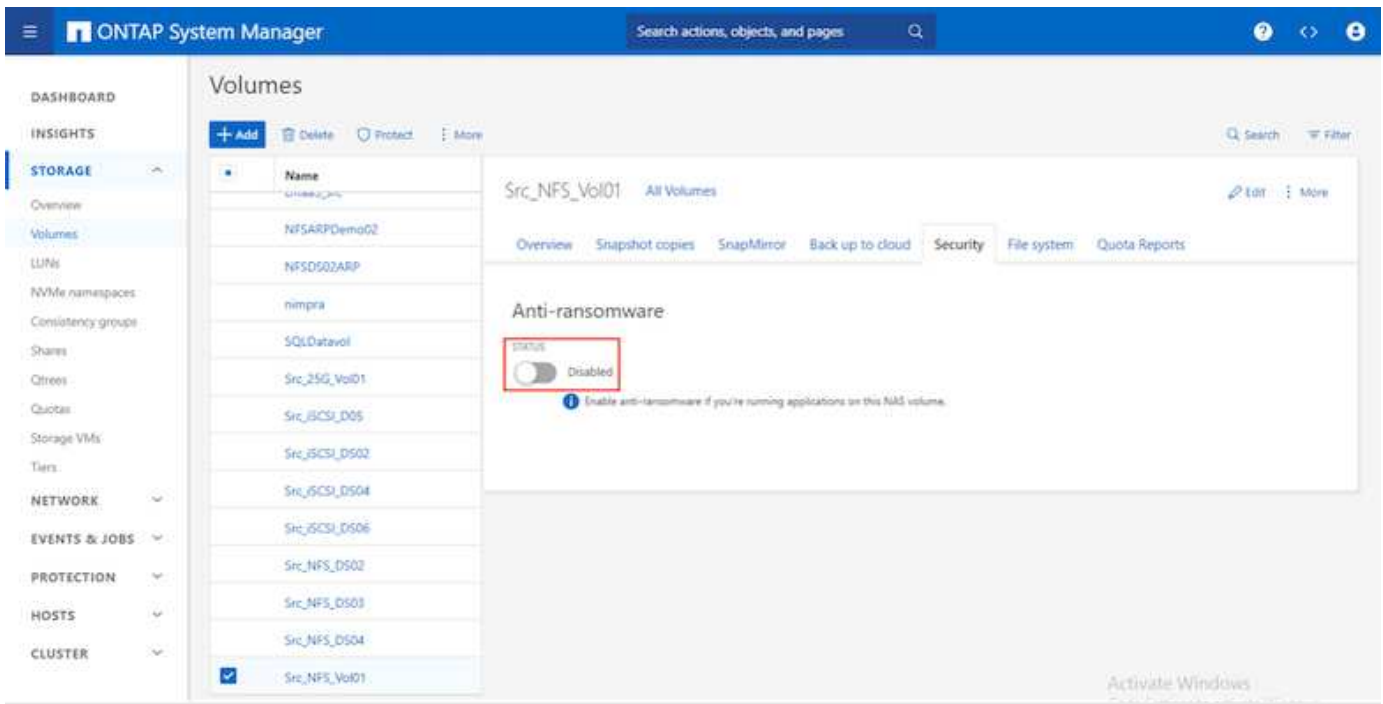
Pour plus d'informations sur la configuration de VCF, reportez-vous à la section "[Documentation de VMware Cloud Foundation](#)".

## 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.



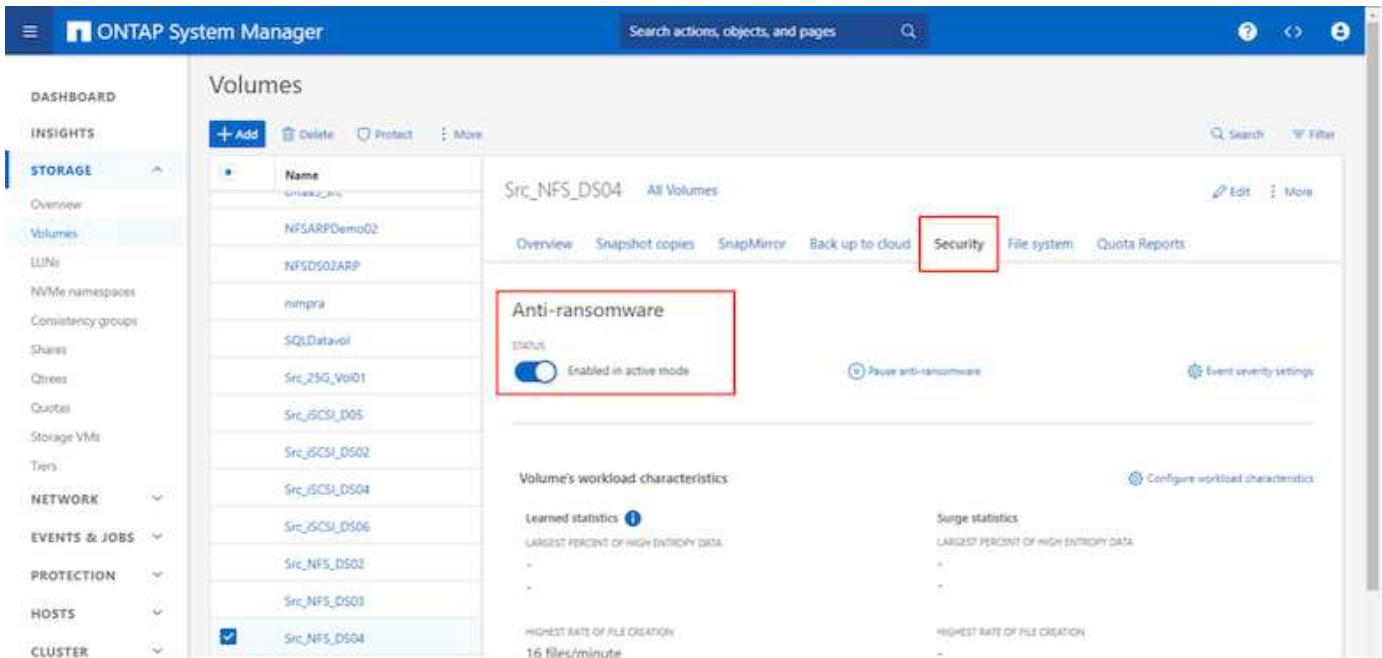


Avec le nouveau NetApp ARP/ai, actuellement en préversion technique, il n'est pas nécessaire de disposer d'un mode d'apprentissage. Il peut plutôt passer directement en mode actif grâce à sa fonctionnalité de détection des ransomwares optimisée par l'IA.



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.

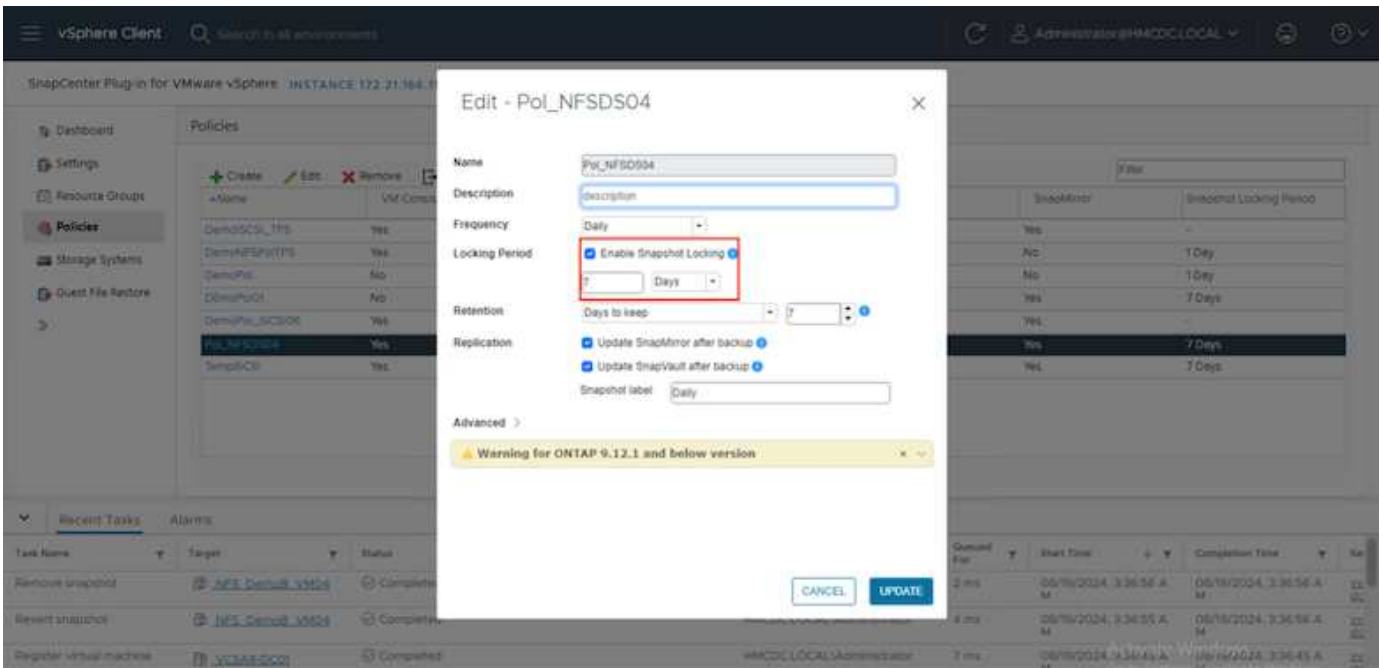
Une fois en mode actif, il commence à rechercher l'activité de volume anormale qui pourrait être une attaque par ransomware. En cas d'activité anormale, une copie Snapshot automatique est immédiatement effectuée, ce qui fournit un point de restauration aussi proche que possible de l'infection par le 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.



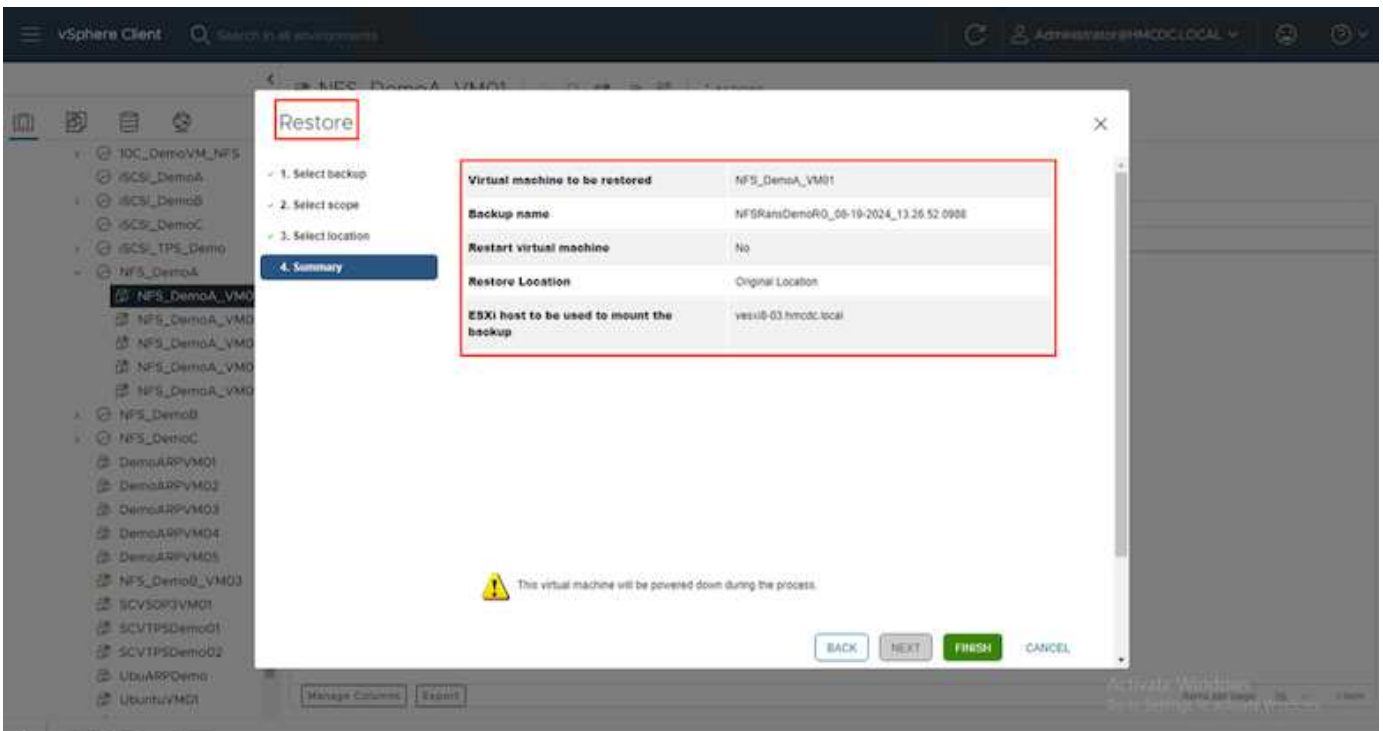
Si une attaque par ransomware cible la machine virtuelle et altère les fichiers au sein de la machine virtuelle sans effectuer de modifications hors de la machine virtuelle, la protection avancée contre les ransomware (ARP) continue de détecter la menace si l'entropie par défaut de la machine virtuelle 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 pérennité 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
Nfsds02arj_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
<b>Src_nfs_ds04</b>	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_B04	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**

Standard Importance

Protected Protection health  
Alerts: 0

Not marked for recovery Recovery

Protection

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

- Pol\_NFS04 Snapshot policy
- 1 Year Daily LTR Backup policy

VM datastore

Location: urn:acvs:svmUI:Resou...

vCenter server: vvcas01-hmcdc.local

Connector: GISABXPConn

Storage

Cluster id: add38d26-348c-11ef-8...

Working Env name: NTAP918\_Src

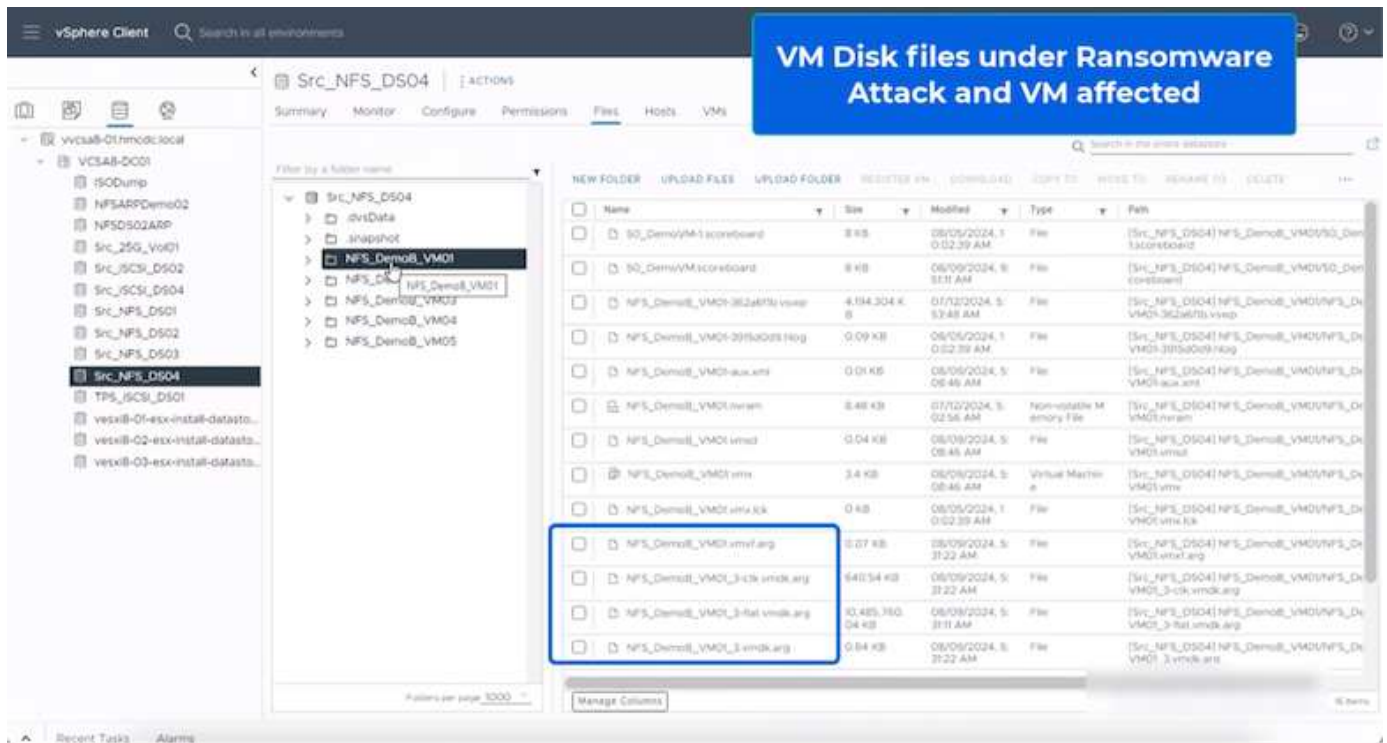
Storage VM name: svm\_NFS

Volume name: Src\_NFS\_DS04

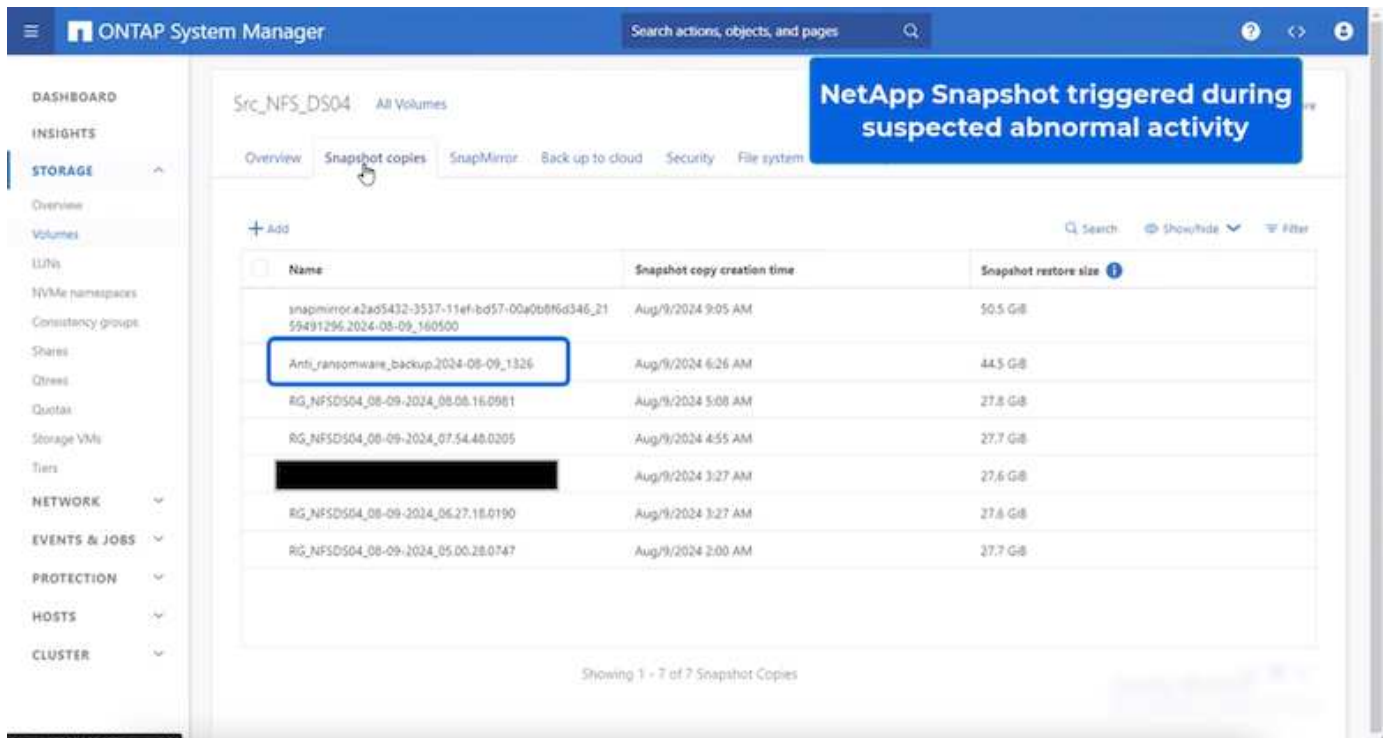
Used size: 29 GiB

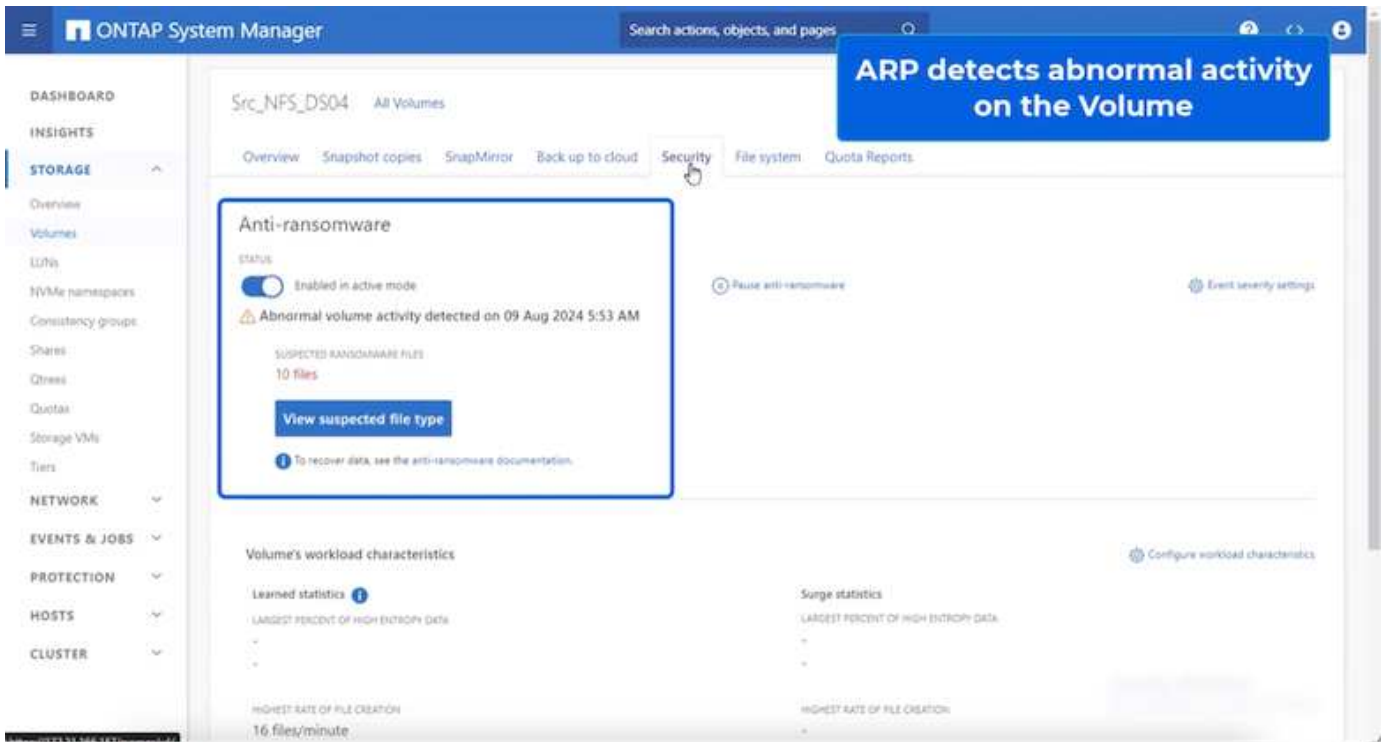
Pour plus d'informations sur la configuration de la protection contre les ransomwares BlueXP , reportez-vous aux sections "Configurez la protection BlueXP contre les ransomware" et "Configurez les paramètres de protection contre les ransomwares BlueXP".

Il est temps de citer un exemple. Dans cette procédure, le datastore "SRC\_NFS\_DS04" est affecté.

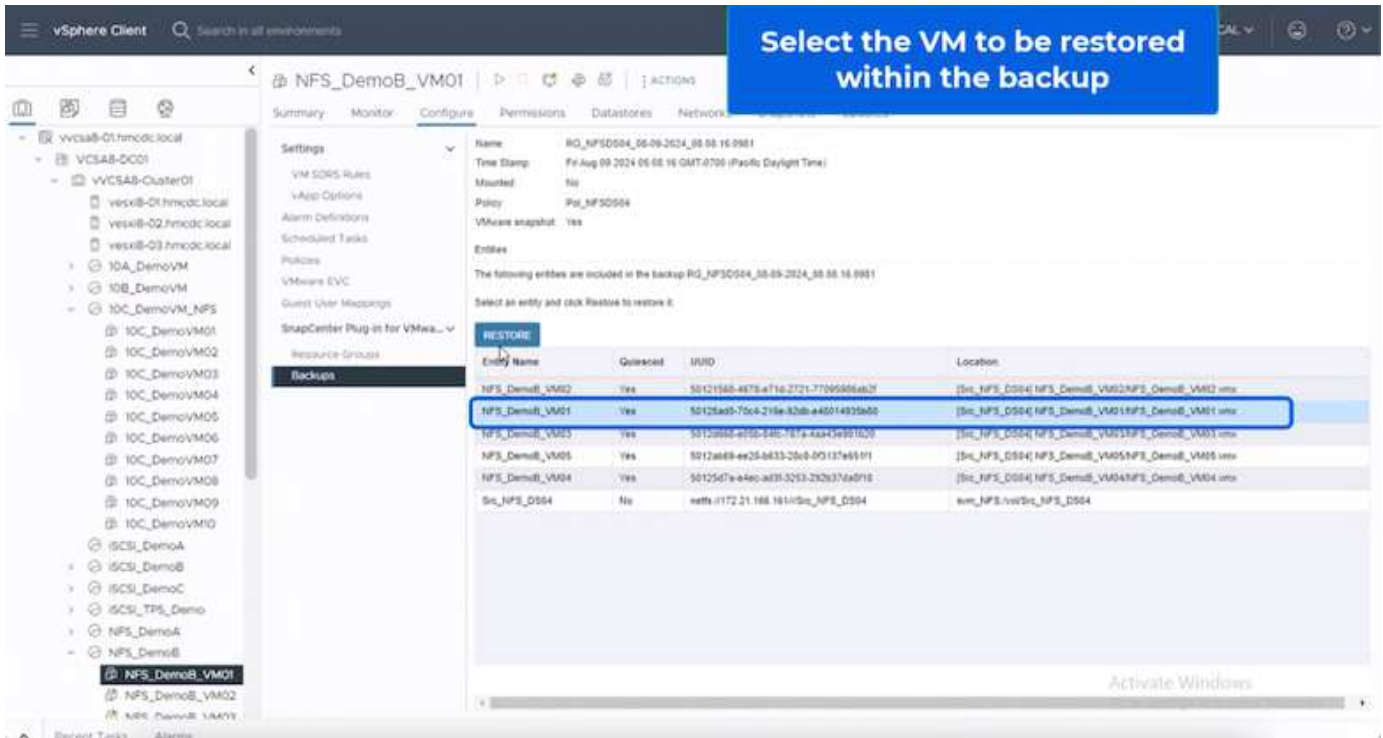


ARP a immédiatement déclenché un snapshot sur le volume lors de la détection.





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

The screenshot shows the NetApp BlueXP interface for the 'Protection View specific to the NFS Volume'. The main view is for 'Src\_NFS\_DS04'. It displays a 'Protected' status with a 'Standard Importance' level. A notification indicates '1 Alerts' and a 'View alerts' button. The 'Not marked for recovery' status is also visible. Below this, there are three panels: 'Protection' (listing policies like 'Pol\_NFSDS04 Snapshot policy' and '1 Year Daily LTR Backup policy'), 'VM datastore' (showing location, vCenter server, and connector), and 'Storage' (showing cluster ID, working environment, storage VM name, volume name, and used size).

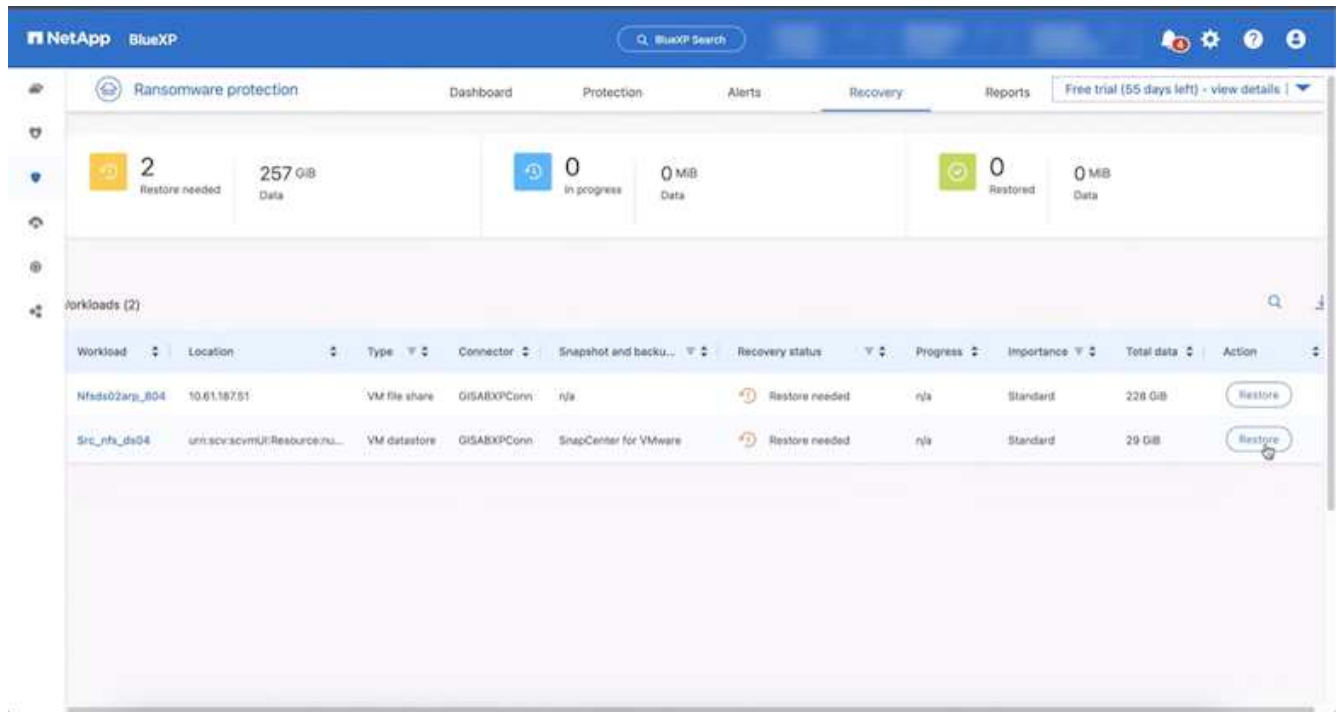
3. Marquer l'incident de ransomware comme étant prêt pour la restauration (après neutralisation des incidents) en sélectionnant « Mark restore READY » (Marquer la restauration nécessaire)

The screenshot shows the NetApp BlueXP interface for the 'Alerts' view, specifically for 'alert2198'. A blue callout box says 'Mark the alert for "restore needed"'. The alert details show 'Workload: Src\_NFS\_DS04', 'Location: urn:scv:scvmUI:Resou...', 'Type: VM datastore', and 'Connector: GISABXPConn'. A 'Mark restore needed' button is visible. Below the alert details, there is a table of incidents. The table has columns for Incident ID, Volume, SVM, Working environment, Type, Status, First detected, Evidence, and Automated responses. One incident is listed with ID 'Inc1820', Volume 'Src\_NFS\_DS04', SVM 'svm\_NFS', Working environment 'NTAP915\_Src', Type 'Potential attack', Status 'New', First detected '4 hours ago', Evidence '1 new extensions detected', and Automated responses '2 Snapshot copies'.

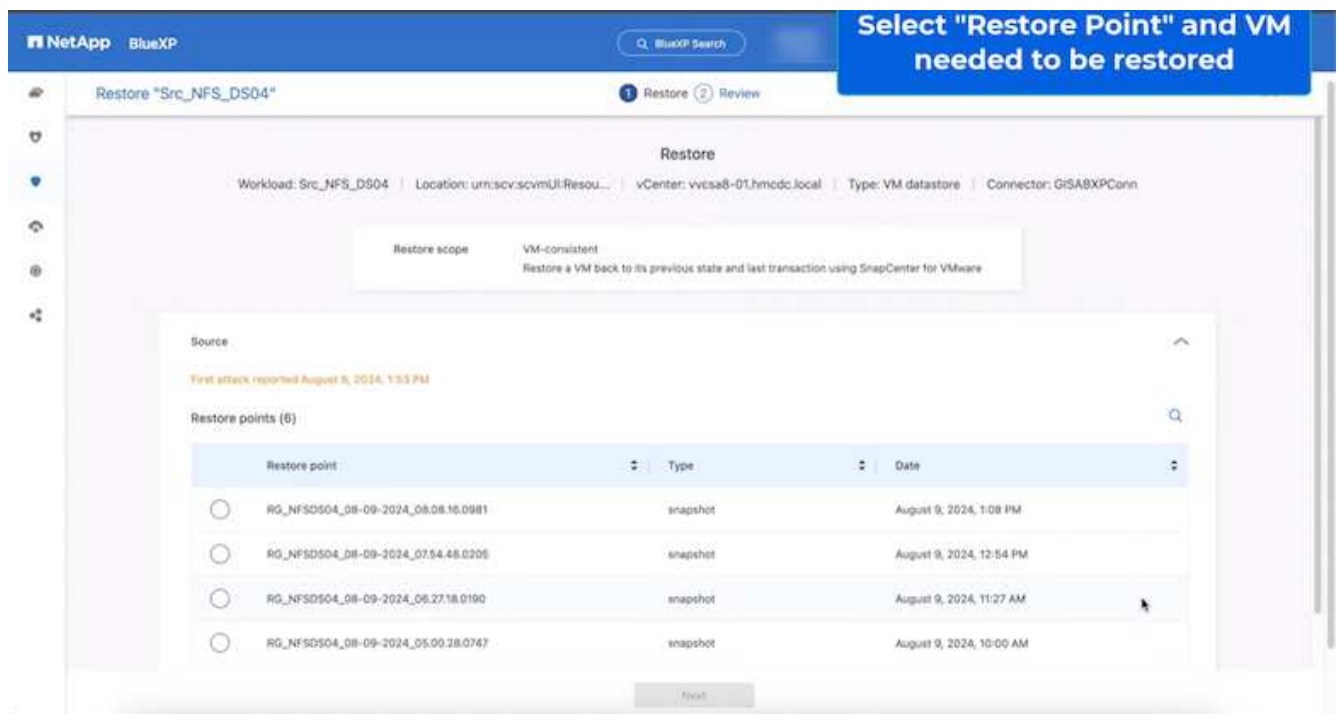


L'alerte peut être rejetée si l'incident s'avère être faux positif.

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.

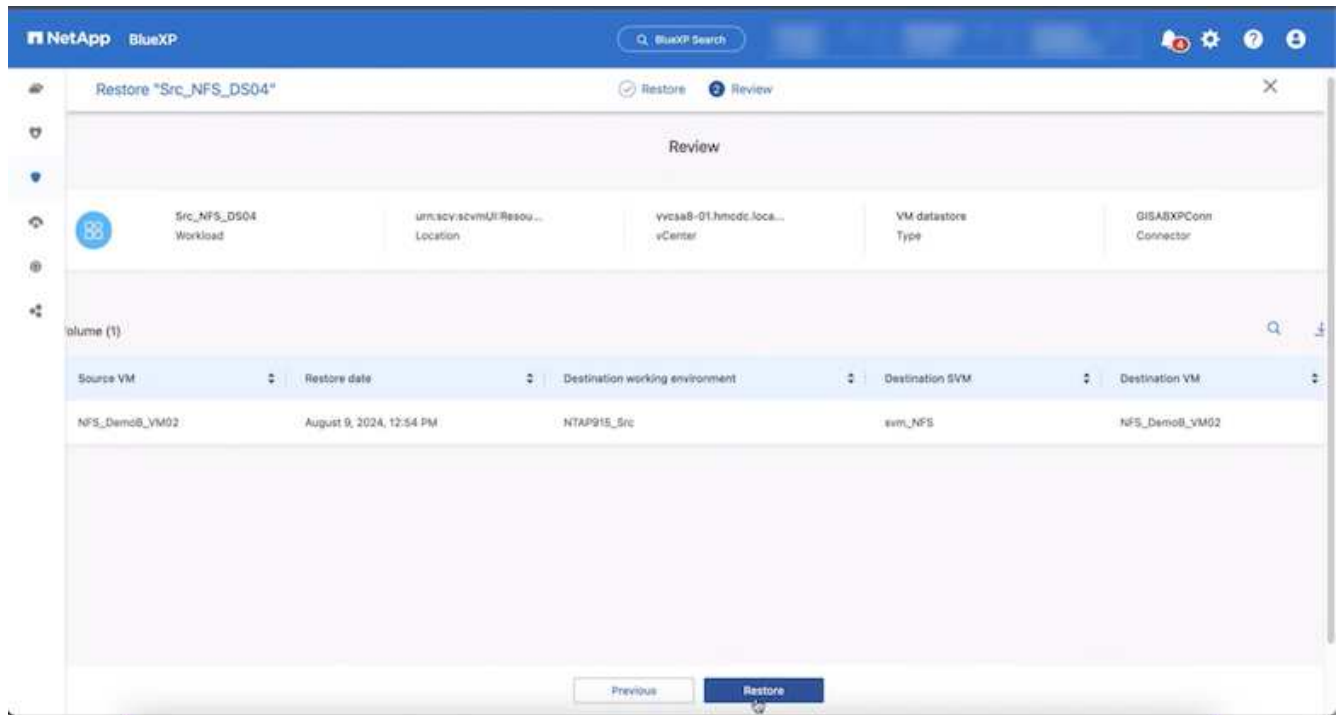


5. Dans ce cas, la portée de la restauration est « par machine virtuelle » (pour SnapCenter pour les machines virtuelles, la portée de la restauration est « par machine virtuelle »)

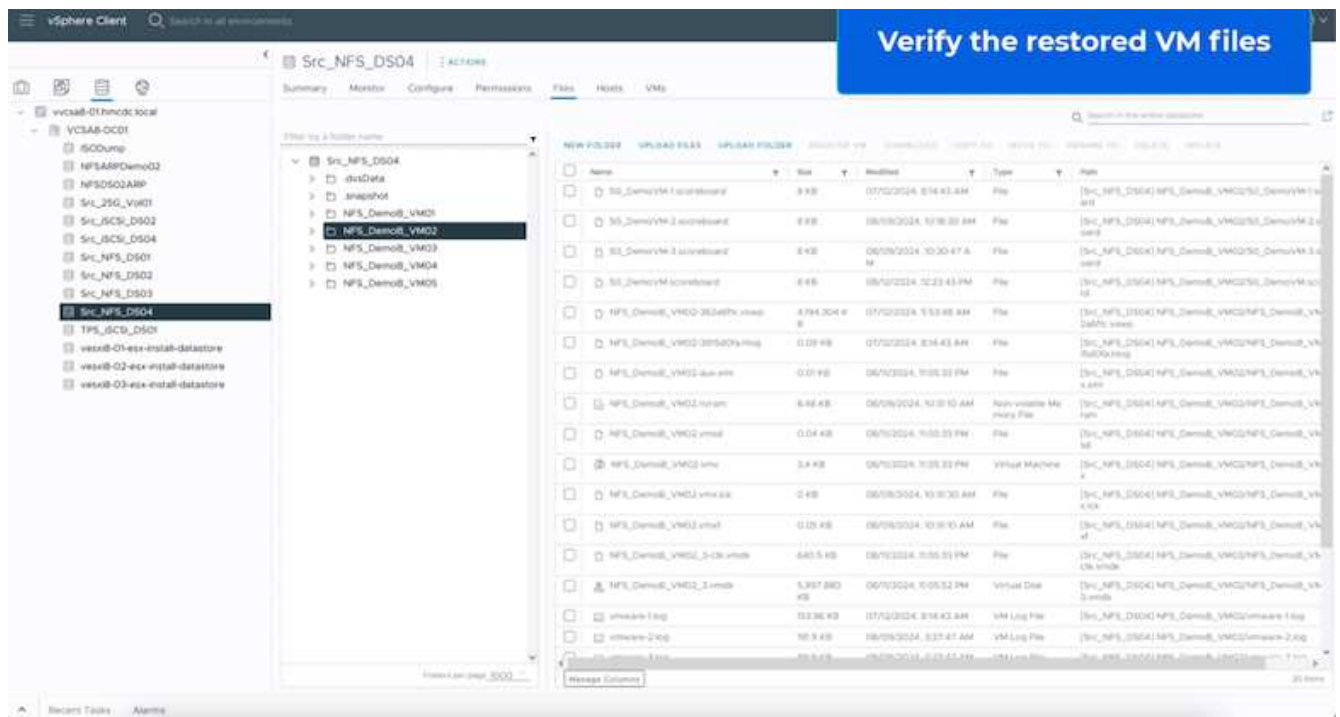


6. Choisissez le point de restauration à utiliser pour restaurer les données, sélectionnez destination et cliquez sur Restaurer.





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.

## 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 DÉLICTEUELLE (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.