VMware

Enterprise applications

NetApp
May 09, 2024

Sommaire

VMware

VMware vSphere avec ONTAP

VMware vSphere avec ONTAP

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

Cette documentation remplace les rapports techniques *TR-4597 : VMware vSphere pour ONTAP*

Les meilleures pratiques complètent d'autres documents, tels que des guides et des listes de compatibilité. Ils sont développés en fonction de tests effectués en laboratoire et d'une vaste expérience sur le terrain par les ingénieurs et les clients NetApp. Non seulement elles sont les seules pratiques prises en charge dans chaque environnement, mais elles constituent généralement les solutions les plus simples qui répondent aux besoins de la plupart des clients.

Ce document est axé sur les fonctionnalités des dernières versions d'ONTAP (9.x) exécutées sur vSphere 7.0 ou version ultérieure. Voir la "Matrice d'interopérabilité NetApp" et "Guide de compatibilité VMware" pour obtenir des détails sur des versions spécifiques.

Pourquoi choisir ONTAP pour vSphere ?

De nombreuses raisons ont poussé des dizaines de milliers de clients à choisir ONTAP comme solution de stockage pour vSphere, par exemple un système de stockage unifié prenant en charge les protocoles SAN et NAS, des fonctionnalités robustes de protection des données à l'aide de copies Snapshot compactes et une multitude d'outils pour vous aider à gérer les données applicatives. 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 vvols, le tout sur un même système de stockage.

Voici les principaux facteurs dont la valeur aujourd'hui est :

- **Stockage unifié.** les systèmes qui exécutent le logiciel ONTAP sont unifiés de plusieurs façons significatives. À l'origine, cette approche était appelée protocoles NAS et SAN, et ONTAP continue d'être une plateforme SAN de premier plan en plus de ses capacités d'origine dans le stockage NAS. Dans le monde de vSphere, cette approche peut également se traduire par un système unifié d'infrastructure de postes de travail virtuels (VDI) avec une infrastructure de serveurs virtuels (VSI). Les systèmes qui exécutent le logiciel ONTAP sont généralement moins coûteux pour VSI que les baies d'entreprise

classiques et offrent cependant des fonctionnalités avancées d'efficacité du stockage permettant de gérer l'infrastructure VDI au sein du même système. ONTAP unifie également une grande variété de supports de stockage, des SSD aux SATA, et peut s'étendre facilement au cloud. Il n'est pas nécessaire d'acheter une baie Flash pour les performances, une baie SATA pour l'archivage ou des systèmes distincts pour le cloud. ONTAP les lie tous ensemble.

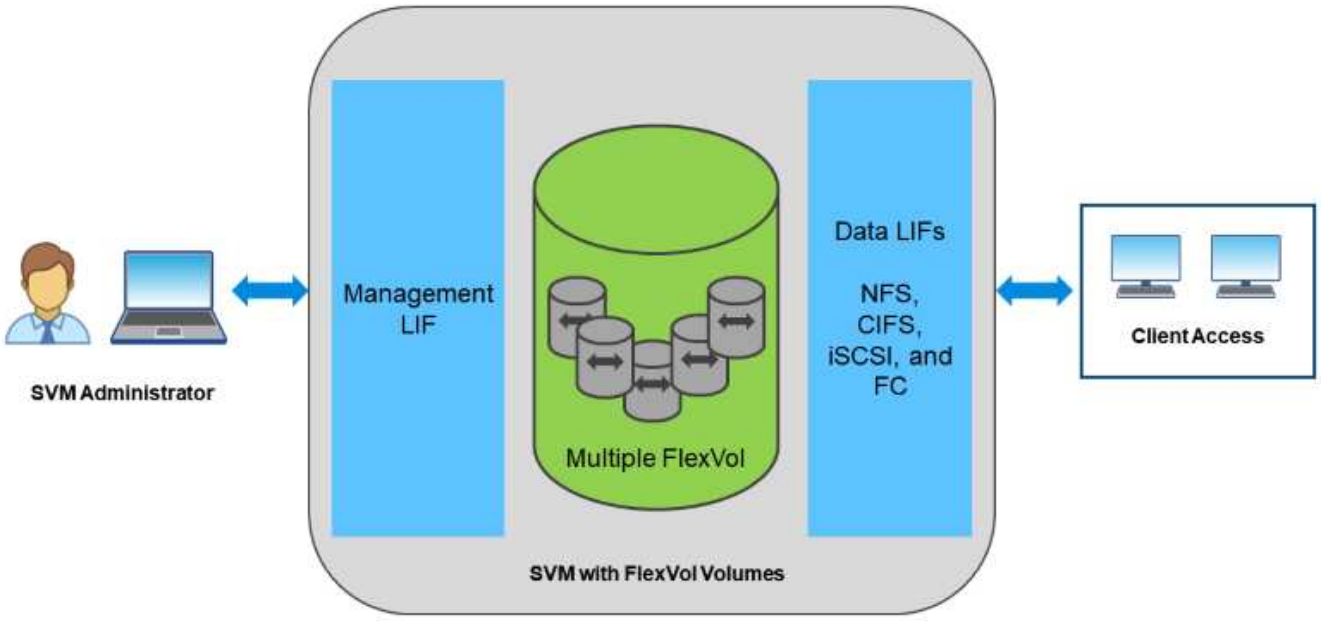
- **Volumes virtuels et gestion basée sur des règles de stockage.** NetApp a été l'un des premiers partenaires de conception avec VMware dans le développement des volumes virtuels vSphere (vVols). Il a fourni des données architecturales et une prise en charge précoce des vVols et des API VMware vSphere pour la sensibilisation au stockage (VASA). Non seulement cette approche intègre la gestion granulaire du stockage des machines virtuelles à VMFS, mais elle a également pris en charge l'automatisation du provisionnement du stockage via la gestion basée sur des règles de stockage. Cette approche permet aux architectes du stockage de concevoir des pools de stockage dont les capacités sont facilement utilisable par les administrateurs de machines virtuelles. ONTAP est leader du secteur du stockage en matière d'évolutivité vvol, en gérant des centaines de milliers de vvols dans un seul cluster, alors que les fournisseurs de baies d'entreprise et de baies Flash de plus petite taille prennent en charge à peine plusieurs milliers de vvols par baie. NetApp pilotant également l'évolution de la gestion granulaire des ordinateurs virtuels avec des fonctionnalités à venir en matière de prise en charge de vvols 3.0.
- **Efficacité du stockage.** bien que NetApp ait été le premier à fournir la déduplication pour les charges de travail de production, cette innovation n'a pas été la première ou la dernière dans ce domaine. Il a commencé par les copies Snapshot, un mécanisme de protection des données peu encombrant et sans impact sur les performances, ainsi que la technologie FlexClone, qui permet de réaliser instantanément des copies en lecture/écriture des machines virtuelles pour la production et la sauvegarde. NetApp a continué à proposer des fonctionnalités en ligne, notamment la déduplication, la compression et la déduplication des blocs « zéro », afin d'exploiter tout le stockage provenant de disques SSD très coûteux. Plus récemment, ONTAP a ajouté la possibilité de stocker des opérations d'E/S et des fichiers de petite taille dans un bloc de disque à l'aide de la compaction. L'association de ces fonctionnalités a permis à des clients d'obtenir des économies allant jusqu'à 5:1 pour VSI et jusqu'à 30:1 pour VDI.
- **Cloud hybride.** qu'il soit utilisé pour le cloud privé sur site, une infrastructure de cloud public ou un cloud hybride qui associe le meilleur des deux types de clouds, les solutions ONTAP vous aident à créer votre Data Fabric pour rationaliser et optimiser la gestion des données. Commencez par des systèmes 100 % Flash haute performance, puis coupler les avec des systèmes de stockage sur disque ou cloud pour la protection des données et le cloud computing. Vous pouvez choisir entre des clouds Azure, AWS, IBM ou Google pour optimiser les coûts et éviter l'enfermement propriétaire. Bénéficiez de la prise en charge avancée des technologies OpenStack et de conteneur, selon vos besoins. NetApp propose également des solutions de sauvegarde cloud (SnapMirror Cloud, Cloud Backup Service et Cloud Sync), ainsi que des outils de Tiering du stockage et d'archivage (FabricPool) pour ONTAP afin de réduire les dépenses d'exploitation et d'exploiter la portée du cloud.
- **Et plus.** tirez parti des performances extrêmes des baies NetApp AFF A-Series pour accélérer votre infrastructure virtualisée tout en gérant les coûts. Assurez la continuité totale de l'activité, qu'il s'agisse de la maintenance ou des mises à niveau, ou du remplacement complet de votre système de stockage à l'aide de clusters ONTAP scale-out. Protégez vos données au repos avec les fonctionnalités de chiffrement NetApp, sans frais supplémentaires. Assurez-vous que les performances respectent les niveaux de service grâce à des fonctionnalités de qualité de service très avancées. Elles font toutes partie du vaste éventail de fonctionnalités fournies par ONTAP, le logiciel de gestion des données d'entreprise leader du secteur.

Stockage unifié

NetApp ONTAP unifie le stockage selon une approche Software-defined simplifiée pour une gestion sécurisée et efficace, des performances améliorées et une évolutivité transparente. Cette approche améliore la protection des données et permet une utilisation efficace des ressources cloud.

À l'origine, cette approche unifiée faisait référence à la prise en charge des protocoles NAS et SAN sur un système de stockage unique. ONTAP continue d'être l'une des principales plateformes pour SAN, tout comme sa puissance initiale en matière de stockage NAS. ONTAP prend désormais également en charge le protocole objet S3. Bien que S3 ne soit pas utilisé pour les datastores, vous pouvez l'utiliser pour les applications hôtes. Pour en savoir plus sur la prise en charge du protocole S3 dans ONTAP, consultez le "Présentation de la configuration S3".

Une machine virtuelle de stockage (SVM) est l'unité de la colocation sécurisée dans ONTAP. Il s'agit d'une structure logique permettant aux clients d'accéder aux systèmes qui exécutent le logiciel ONTAP. Les SVM peuvent transmettre simultanément les données par le biais de plusieurs protocoles d'accès aux données via des interfaces logiques (LIF). Les SVM fournissent un accès aux données de niveau fichier via les protocoles NAS, tels que CIFS et NFS, et un accès aux données de niveau bloc via les protocoles SAN, tels que iSCSI, FC/FCoE et NVMe. Les SVM peuvent fournir des données aux clients SAN et NAS de façon indépendante et en même temps avec S3.



Dans le monde de vSphere, cette approche peut également se traduire par un système unifié d'infrastructure de postes de travail virtuels (VDI) avec une infrastructure de serveurs virtuels (VSI). Les systèmes qui exécutent le logiciel ONTAP sont généralement moins coûteux pour VSI que les baies d'entreprise classiques et offrent cependant des fonctionnalités avancées d'efficacité du stockage permettant de gérer l'infrastructure VDI au sein du même système. ONTAP unifie également une grande variété de supports de stockage, des SSD aux SATA, et peut s'étendre facilement au cloud. Il n'est pas nécessaire d'acheter une baie Flash pour les performances, une baie SATA pour l'archivage ou des systèmes distincts pour le cloud. ONTAP les lie tous ensemble.

REMARQUE : pour plus d'informations sur les SVM, le stockage unifié et l'accès client, voir "Virtualisation du stockage" Dans le centre de documentation ONTAP 9.

Outils de virtualisation pour ONTAP

NetApp propose plusieurs outils logiciels autonomes pouvant être utilisés avec ONTAP et

vSphere pour gérer votre environnement virtualisé.

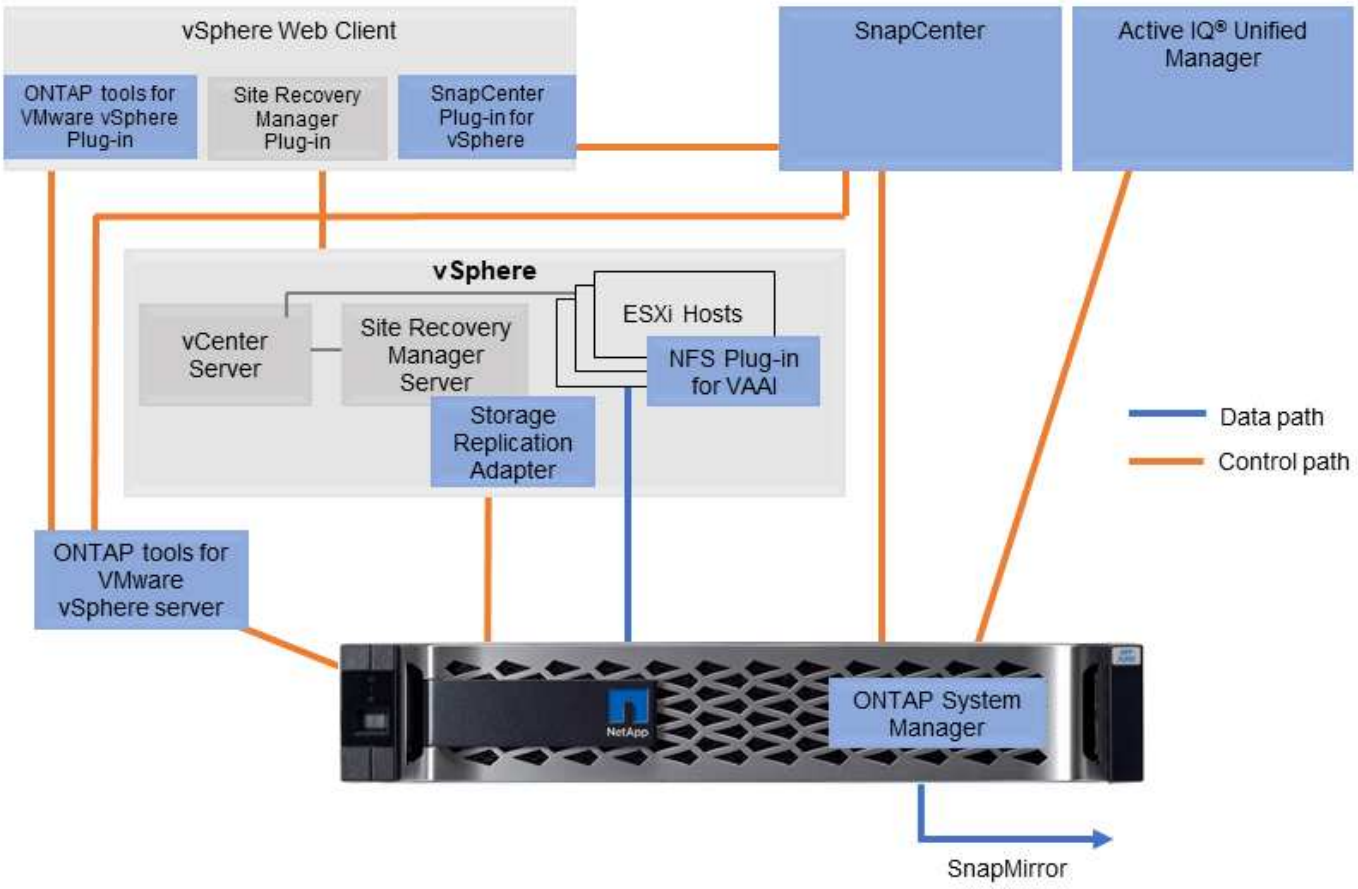
Les outils suivants sont inclus avec la licence ONTAP sans frais supplémentaires. Voir la Figure 1 pour une description du fonctionnement de ces outils dans votre environnement vSphere.

Les outils ONTAP pour VMware vSphere

Les outils ONTAP pour VMware vSphere sont un ensemble d'outils permettant d'utiliser le stockage ONTAP avec vSphere. Le plug-in vCenter, précédemment appelé Virtual Storage Console (VSC), simplifie les fonctionnalités de gestion et d'efficacité du stockage, améliore la disponibilité et réduit les coûts de stockage ainsi que les charges opérationnelles, 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 d'utiliser ces outils ONTAP comme meilleure pratique lorsque vous utilisez vSphere avec les systèmes exécutant le logiciel ONTAP. Elle comprend une appliance serveur, des extensions d'interface utilisateur pour vCenter, VASA Provider et Storage Replication adapter. La quasi-totalité des outils ONTAP peuvent être automatisés à l'aide d'API REST simples et consommables par la plupart des outils d'automatisation modernes.

- **Extensions de l'interface utilisateur vCenter.** les extensions de l'interface utilisateur des outils ONTAP simplifient le travail des équipes opérationnelles et des administrateurs vCenter en intégrant des menus contextuels faciles à utiliser pour gérer les hôtes et le stockage, les portlets d'information et les fonctionnalités d'alerte natives directement dans l'interface utilisateur vCenter pour optimiser les flux de travail.
- **VASA Provider pour ONTAP.** le fournisseur VASA pour ONTAP prend en charge l'infrastructure VMware vStorage APIs for Storage Awareness (VASA). Il est fourni en tant qu'appliance virtuelle unique, avec les outils ONTAP pour VMware vSphere pour une facilité de déploiement. Vasa Provider connecte vCenter Server avec ONTAP pour faciliter le provisionnement et la surveillance du stockage des machines virtuelles. Il assure la prise en charge de VMware Virtual volumes (vvols), la gestion des profils de capacité de stockage et les performances individuelles de VM vvols, ainsi que des alarmes pour le contrôle de la capacité et de la conformité avec les profils.
- **Storage Replication adapter.** l'adaptateur SRA est utilisé avec VMware site Recovery Manager (SRM) pour gérer la réplication des données entre les sites de production et de reprise après incident et tester les répliques de reprise après incident sans interruption. Il permet d'automatiser les tâches de détection, de restauration et de reprotection. Elle inclut une appliance serveur SRA et des adaptateurs SRA pour le serveur Windows SRM et l'appliance SRM.

La figure suivante représente les outils ONTAP pour vSphere.



Plug-in NFS pour VMware VAAI

Le plug-in NetApp NFS pour VMware VAAI est un plug-in pour les hôtes ESXi qui leur permet d'utiliser des fonctionnalités VAAI avec les datastores NFS sur ONTAP. Il prend en charge le déchargement des copies pour les opérations de clonage, la réservation d'espace pour les fichiers de disque virtuel épais et le déchargement des snapshots. Le transfert des opérations de copie vers le stockage n'est pas forcément plus rapide. Toutefois, il réduit les besoins en bande passante réseau et réduit la charge des ressources hôte telles que les cycles de CPU, les tampons et les files d'attente. Vous pouvez utiliser les outils ONTAP pour VMware vSphere pour installer le plug-in sur des hôtes ESXi ou, le cas échéant, vSphere Lifecycle Manager (vLCM).

Volumes virtuels (vvols) et gestion basée sur des règles de stockage (SPBM)

NetApp a été un partenaire de conception précoce avec VMware dans le développement de vSphere Virtual volumes (vvols), en fournissant des informations architecturales et une prise en charge précoce pour vvols et VMware vSphere API for Storage Awareness (VASA). Non seulement cette approche intègre la gestion du stockage granulaire des machines virtuelles à VMFS, mais elle prend également en charge l'automatisation du provisionnement du stockage via la gestion basée sur des règles de stockage (SPBM).

Grâce à la gestion du stockage basée sur des règles, une structure sert de couche d'abstraction entre les services de stockage disponibles pour votre environnement de virtualisation et les éléments de stockage provisionnés via des règles. Cette approche permet aux architectes du stockage de concevoir des pools de stockage dont les capacités sont facilement utilisable par les administrateurs de machines virtuelles. Les administrateurs peuvent ensuite répondre aux exigences des charges de travail des machines virtuelles par rapport aux pools de stockage provisionnés, ce qui permet un contrôle granulaire des divers paramètres au niveau de chaque machine virtuelle ou disque virtuel.

ONTAP est leader du secteur du stockage dans l'évolutivité de vvols, en gérant des centaines de milliers de vvols dans un seul cluster, alors que les fournisseurs de baies d'entreprise et de baies Flash plus petites prennent en charge aussi peu que plusieurs milliers de vvols par baie. NetApp pilotant également l'évolution de la gestion granulaire des machines virtuelles avec des fonctionnalités à venir en matière de prise en charge de vvols 3.0.

Pour plus d'informations sur les volumes virtuels VMware vSphere, SPBM et ONTAP, voir "Tr-4400 : volumes virtuels VMware vSphere avec ONTAP".

Datastores et protocoles

Présentation des fonctionnalités de datastore et de protocole vSphere

Sept protocoles sont utilisés pour connecter VMware vSphere aux datastores sur un système exécutant le logiciel ONTAP :

- FCP
- FCoE
- NVMe/FC
- NVMe/TCP
- ISCSI
- NFS v3
- NFS v4.1

FCP, FCoE, NVMe/FC, NVMe/TCP et iSCSI sont des protocoles de bloc qui utilisent vSphere Virtual machine File System (VMFS) pour stocker des VM au sein de LUN ONTAP ou des espaces de noms NVMe contenus dans un volume ONTAP FlexVol. Notez que depuis vSphere 7.0, VMware ne prend plus en charge la technologie FCoE dans les environnements de production. NFS est un protocole de fichier qui place les machines virtuelles dans des datastores (qui sont simplement des volumes ONTAP) sans avoir besoin de VMFS. SMB (CIFS), iSCSI, NVMe/TCP ou NFS peuvent également être utilisés directement d'un système d'exploitation invité à ONTAP.

Les tableaux suivants présentent les fonctionnalités de datastore traditionnel prises en charge par vSphere avec ONTAP. Ces informations ne s'appliquent pas aux datastores vvols, mais elles s'appliquent généralement aux versions vSphere 6.x et ultérieures utilisant des versions ONTAP prises en charge. Vous pouvez également consulter "Valeurs maximales de la configuration VMware" Pour les versions de vSphere spécifiques afin de confirmer les limites spécifiques.

Capacités/fonctionnalités	FC/FCoE	ISCSI	NVMe-of	NFS
Format	Mappage de périphériques VMFS ou bruts (RDM)	VMFS ou RDM	VMFS	S/O

Capacités/fonctionnalités	FC/FCoE	ISCSI	NVMe-of	NFS
Nombre maximal de datastores ou de LUN	1024 LUN par hôte	1024 LUN par serveur	256 Namespeces par serveur	256 supports NFS par défaut. MaxVolumes est 8. Utilisez les outils ONTAP pour VMware vSphere et augmentez jusqu'à 256.
Taille maximale des datastores	64 TO	64 TO	64 TO	Volume FlexVol de 100 To ou supérieur avec FlexGroup volume
Taille maximale des fichiers du datastore	62TO	62TO	62TO	62 To avec ONTAP 9.12.1P2 et versions ultérieures
Profondeur de file d'attente optimale par LUN ou par système de fichiers	64-256	64-256	Négociation automatique	Se reporter à NFS.MaxQueueDepth dans "Hôte ESXi recommandé et autres paramètres ONTAP recommandés".

Le tableau suivant répertorie les fonctionnalités de stockage VMware prises en charge.

Capacité/fonctionnalité	FC/FCoE	ISCSI	NVMe-of	NFS
VMotion	Oui.	Oui.	Oui.	Oui.
Stockage vMotion	Oui.	Oui.	Oui.	Oui.
Haute disponibilité VMware	Oui.	Oui.	Oui.	Oui.
Storage Distributed Resource Scheduler (SDRS)	Oui.	Oui.	Oui.	Oui.
Logiciel de sauvegarde VMware vStorage APIs for Data protection (VADP)	Oui.	Oui.	Oui.	Oui.
Microsoft Cluster Service (MSCS) ou mise en cluster de basculement au sein d'une machine virtuelle	Oui.	Oui*	Oui*	Non pris en charge

Capacité/fonctionnalité	FC/FCoE	ISCSI	NVMe-of	NFS
Tolérance aux pannes	Oui.	Oui.	Oui.	Oui.
Gestionnaire de reprise de site	Oui.	Oui.	Non**	V3 uniquement**
Machines virtuelles à provisionnement fin (disques virtuels)	Oui.	Oui.	Oui.	Oui. Ce paramètre est le paramètre par défaut pour toutes les machines virtuelles sur NFS lorsqu'elles n'utilisent pas VAAI.
Chemins d'accès multiples natifs VMware	Oui.	Oui.	Oui, en utilisant le nouveau plug-in haute performance (HPP)	L'agrégation de sessions NFS v4.1 requiert ONTAP 9.14.1 et versions ultérieures

Le tableau suivant répertorie les fonctionnalités de gestion du stockage ONTAP prises en charge.

Capacités/fonctionnalités	FC/FCoE	ISCSI	NVMe-of	NFS
Déduplication des données	D'économies sur la baie	D'économies sur la baie	D'économies sur la baie	Économies au niveau du datastore
Provisionnement fin	Datastore ou RDM	Datastore ou RDM	Datastore	Datastore
Redimensionnement datastore	Évoluer uniquement	Évoluer uniquement	Évoluer uniquement	Croissance, croissance automatique et réduction des volumes
Plug-ins SnapCenter pour applications Windows, Linux (invités)	Oui.	Oui.	Non	Oui.
Contrôle et configuration de l'hôte à l'aide des outils ONTAP pour VMware vSphere	Oui.	Oui.	Non	Oui.
Provisionnement avec les outils ONTAP pour VMware vSphere	Oui.	Oui.	Non	Oui.

Le tableau suivant répertorie les fonctionnalités de sauvegarde prises en charge.

Capacités/fonctionnalités	FC/FCoE	ISCSI	NVMe-of	NFS
Snapshots ONTAP	Oui.	Oui.	Oui.	Oui.
SRM pris en charge par les sauvegardes répliquées	Oui.	Oui.	Non**	V3 uniquement**
SnapMirror volume	Oui.	Oui.	Oui.	Oui.
Accès image VMDK	Logiciel de sauvegarde VADP	Logiciel de sauvegarde VADP	Logiciel de sauvegarde VADP	Logiciel de sauvegarde VADP, vSphere client et le navigateur du datastore du client Web vSphere
Accès niveau fichier VMDK	Logiciel de sauvegarde VADP, Windows uniquement	Logiciel de sauvegarde VADP, Windows uniquement	Logiciel de sauvegarde VADP, Windows uniquement	Logiciels de sauvegarde VADP et applications tierces
Granularité NDMP	Datastore	Datastore	Datastore	Datastore ou VM

*NetApp recommande l'utilisation d'iSCSI « in-guest » pour les clusters Microsoft, plutôt que de VMDK « multiwriter » dans un datastore VMFS. Cette approche est entièrement prise en charge par Microsoft et VMware, et offre une grande flexibilité avec ONTAP (SnapMirror vers des systèmes ONTAP sur site ou dans le cloud), est facile à configurer et à automatiser et peut être protégée avec SnapCenter. VSphere 7 intègre une nouvelle option clustered VMDK. Cette approche est différente des VMDK compatibles avec plusieurs enregistreurs, qui requièrent un datastore présenté via le protocole FC pour lequel la prise en charge de VMDK en cluster est activée. D'autres restrictions s'appliquent. Voir VMware "Configuration de Windows Server Failover Clustering" documentation pour les instructions de configuration.

**Les datastores utilisant NVMe-of et NFS v4.1 nécessitent une réplication vSphere. SRM ne prend pas en charge la réplication basée sur les baies.

Sélection d'un protocole de stockage

Les systèmes exécutant le logiciel ONTAP prennent en charge les principaux protocoles de stockage. Les clients peuvent ainsi choisir ce qui convient le mieux à leur environnement, en fonction de l'infrastructure réseau planifiée et du personnel. Les tests effectués par NetApp n'ont généralement pas permis de faire la différence entre les protocoles s'exécutant à des vitesses de ligne similaires. Il est donc préférable de se concentrer sur votre infrastructure réseau et sur les capacités des équipes par rapport aux performances des protocoles bruts.

Les facteurs suivants peuvent être utiles lors de l'examen d'un choix de protocole :

- **Environnement client actuel.** même si les équipes INFORMATIQUES sont généralement compétentes en matière de gestion de l'infrastructure IP Ethernet, elles ne sont pas toutes qualifiées pour la gestion d'une structure SAN FC. Cependant, l'utilisation d'un réseau IP générique non conçu pour le trafic de stockage risque de ne pas fonctionner correctement. Considérez l'infrastructure de réseau que vous avez en place, toutes les améliorations planifiées, ainsi que les compétences et la disponibilité du personnel pour les gérer.
- **Simplicité d'installation.** au-delà de la configuration initiale de la structure FC (commutateurs et câblage supplémentaires, segmentation et vérification de l'interopérabilité des HBA et des micrologiciels), les

protocoles de bloc exigent également la création et le mappage de LUN, ainsi que la découverte et le formatage par le système d'exploitation invité. Une fois les volumes NFS créés et exportés, ils sont montés par l'hôte ESXi et prêts à être utilisés. Avec NFS, il n'a pas de qualification de matériel ni de firmware à gérer.

- * Facilité de gestion.* avec les protocoles SAN, si plus d'espace est nécessaire, plusieurs étapes sont nécessaires, y compris l'expansion d'un LUN, de recanning pour découvrir la nouvelle taille, puis de développer le système de fichiers). Bien que la croissance d'une LUN soit possible, la réduction de la taille d'une LUN n'est pas possible et la restauration de l'espace inutilisé peut nécessiter un effort supplémentaire. NFS facilite le dimensionnement et le redimensionnement peut être automatisé par le système de stockage. LE SYSTÈME SAN permet de réclamer de l'espace via les commandes TRIM/UNMAP du système d'exploitation invité. L'espace des fichiers supprimés est ainsi renvoyé à la baie. Ce type de récupération d'espace est plus difficile avec les datastores NFS.
- **Transparence de l'espace de stockage.** l'utilisation du stockage est généralement plus facile à voir dans les environnements NFS parce que le provisionnement fin renvoie immédiatement des économies. De même, les économies de déduplication et de clonage sont immédiatement disponibles pour les autres VM dans le même datastore ou pour les autres volumes du système de stockage. La densité des machines virtuelles est également meilleure généralement dans un datastore NFS, ce qui permet d'améliorer les économies de déduplication et de réduire les coûts de gestion en utilisant moins de datastores à gérer.

Disposition des datastores

Les systèmes de stockage ONTAP offrent une grande flexibilité de création de datastores pour les machines virtuelles et les disques virtuels. Bien que la plupart des meilleures pratiques relatives à ONTAP soient appliquées lors du provisionnement de datastores pour vSphere (voir la section dans cette section) "Hôte ESXi recommandé et autres paramètres ONTAP recommandés"), voici quelques lignes directrices supplémentaires à prendre en compte :

- Le déploiement de vSphere avec des datastores NFS ONTAP offre une implémentation très performante et facile à gérer qui fournit des ratios VM/datastore qui ne peuvent pas être obtenus avec des protocoles de stockage de niveau bloc. Cette architecture peut entraîner une multiplication par dix de la densité des datastores avec une corrélation réduction du nombre de datastores. Bien qu'un datastore plus volumineux puisse améliorer l'efficacité du stockage et offrir des avantages opérationnels, envisagez d'utiliser au moins quatre datastores (volumes FlexVol) pour stocker vos machines virtuelles sur un seul contrôleur ONTAP afin d'optimiser les performances des ressources matérielles. Cette approche vous permet également de créer des datastores avec différentes règles de restauration. Certaines peuvent être sauvegardées ou répliquées plus fréquemment que d'autres, en fonction des besoins de l'entreprise. Les volumes FlexGroup n'ont pas besoin de plusieurs datastores pour améliorer les performances, car ils évoluent indépendamment de la conception.
- NetApp recommande l'utilisation de volumes FlexVol pour la plupart des datastores NFS. À partir de ONTAP 9.8, les volumes FlexGroup sont également pris en charge en tant que datastores et sont généralement recommandés pour certaines utilisations. Les autres conteneurs de stockage ONTAP, tels que les qtrees, ne sont généralement pas recommandés, car ils ne sont actuellement pas pris en charge par les outils ONTAP pour VMware vSphere ou par le plug-in NetApp SnapCenter pour VMware vSphere. Cela étant, le déploiement de datastores sous forme de plusieurs qtrees dans un seul volume peut s'avérer utile dans les environnements hautement automatisés qui peuvent bénéficier de quotas au niveau du datastore ou de clones de fichiers de machine virtuelle.
- La taille correcte des datastores de volumes FlexVol est d'environ 4 To à 8 To. Cette taille constitue un bon équilibre pour les performances, la facilité de gestion et la protection des données. Démarrer petit (4 To, par exemple) et étendre le datastore en fonction des besoins (jusqu'à 100 To maximum). Les datastores plus petits peuvent être plus rapides à restaurer depuis la sauvegarde ou après un incident, et déplacés rapidement dans l'ensemble du cluster. Envisagez d'utiliser la fonction de dimensionnement automatique de ONTAP pour augmenter et réduire automatiquement le volume en fonction des modifications de l'espace utilisé. Les outils ONTAP de l'assistant de provisionnement des datastores VMware vSphere

utilisent la taille automatique par défaut pour les nouveaux datastores. Vous pouvez également personnaliser davantage les seuils d'extension et de réduction ainsi que la taille maximale et minimale, avec System Manager ou la ligne de commandes.

- Les datastores VMFS peuvent également être configurés avec des LUN accessibles via FC, iSCSI ou FCoE. VMFS permet d'accéder simultanément aux LUN classiques par chaque serveur ESX d'un cluster. Les datastores VMFS peuvent être jusqu'à 64 To et comprennent jusqu'à 32 LUN de 2 To (VMFS 3) ou un seul LUN de 64 To (VMFS 5). La taille de LUN maximale de ONTAP est de 16 To sur la plupart des systèmes et de 128 To sur les baies SAN. Il est donc possible de créer un datastore VMFS 5 de taille maximale sur la plupart des systèmes ONTAP en utilisant quatre LUN de 16 To. Bien que les charges de travail E/S élevées puissent bénéficier de la performance de plusieurs LUN (avec les systèmes FAS ou AFF haut de gamme), cet avantage peut être compensé par la complexité de gestion supplémentaire qui permet de créer, de gérer et de protéger les LUN des datastores et un risque de disponibilité accru. NetApp recommande généralement d'utiliser un volume LUN unique et important pour chaque datastore et ne peut être étendu que si le besoin de dépasser 16 To de data store. Comme pour NFS, envisagez l'utilisation de plusieurs datastores (volumes) pour optimiser les performances d'un seul contrôleur ONTAP.
- Les anciens systèmes d'exploitation invités (OS) devaient s'aligner sur le système de stockage pour obtenir des performances et une efficacité du stockage optimales. Cependant, les systèmes d'exploitation actuels pris en charge par les fournisseurs de Microsoft et de distributeurs Linux tels que Red Hat ne nécessitent plus d'ajustements pour aligner la partition du système de fichiers sur les blocs du système de stockage sous-jacent dans un environnement virtuel. Si vous utilisez un ancien système d'exploitation pouvant nécessiter un alignement, recherchez dans la base de connaissances de support NetApp des articles utilisant « alignement de machines virtuelles » ou demandez une copie du rapport TR-3747 à un contact partenaire ou commercial NetApp.
- Évitez d'utiliser des utilitaires de défragmentation au sein du système d'exploitation invité, car cela n'améliore pas les performances et affecte l'efficacité du stockage et l'utilisation de l'espace Snapshot. Envisagez également de désactiver l'indexation des recherches sur le système d'exploitation invité pour les postes de travail virtuels.
- ONTAP s'est leader du marché en proposant des fonctionnalités innovantes d'efficacité du stockage qui vous permettent d'exploiter au maximum votre espace disque utilisable. Les systèmes AFF renforcent cette efficacité avec la compression et la déduplication à la volée par défaut. Les données sont dédupliquées sur tous les volumes d'un agrégat. Ainsi, vous n'avez plus besoin de regrouper des systèmes d'exploitation similaires et des applications similaires au sein d'un même datastore pour optimiser les économies.
- Dans certains cas, vous n'aurez même pas besoin d'un datastore. Pour obtenir des performances et une gestion optimales, évitez d'utiliser un datastore pour des applications d'E/S élevées telles que les bases de données et certaines applications. Prenez plutôt en compte les systèmes de fichiers invités, tels que les systèmes de fichiers NFS ou iSCSI, gérés par l'invité ou par RDM. Pour une assistance spécifique aux applications, consultez les rapports techniques de NetApp pour votre application. Par exemple : "Les bases de données Oracle sur ONTAP" dispose d'une section sur la virtualisation avec des détails utiles.
- Les disques de première classe (ou des disques virtuels améliorés) permettent de gérer des disques gérés par vCenter indépendamment d'une machine virtuelle dotée de vSphere 6.5 et versions ultérieures. Lorsqu'elles sont principalement gérées par API, elles peuvent être utiles avec vvols, en particulier lorsqu'elles sont gérées par les outils OpenStack ou Kubernetes. Ils sont pris en charge par ONTAP ainsi que par les outils ONTAP pour VMware vSphere.

Migration des datastores et des machines virtuelles

Lorsque vous migrez des machines virtuelles depuis un datastore existant sur un autre système de stockage vers ONTAP, voici quelques principes à prendre en compte :

- Utilisez Storage vMotion pour déplacer la masse de vos machines virtuelles vers ONTAP. Cette approche n'assure pas seulement une exécution sans interruption des machines virtuelles. Elle permet également

d'exploiter des fonctionnalités d'efficacité du stockage de ONTAP, comme la déduplication et la compression à la volée, pour traiter les données lors de leur migration. Envisagez d'utiliser les fonctionnalités de vCenter pour sélectionner plusieurs machines virtuelles dans la liste d'inventaire, puis planifiez la migration (utilisez la touche Ctrl tout en cliquant sur actions) à un moment opportun.

- Bien que vous puissiez planifier avec soin une migration vers des datastores de destination appropriés, il est souvent plus simple de les migrer en bloc, puis de les organiser ultérieurement, si nécessaire. Utilisez cette approche pour orienter la migration vers différents datastores si vous avez besoin de protection des données spécifique, par exemple des calendriers Snapshot différents.
- La plupart des machines virtuelles et leur stockage peuvent être migrées lors de l'exécution (à chaud), mais pour migrer le stockage attaché (hors datastore) tel qu'un ISO (ISO), une LUN ou des volumes NFS à partir d'un autre système de stockage, il peut exiger une migration à froid.
- Les machines virtuelles qui nécessitent une migration plus minutieuse incluent les bases de données et les applications qui utilisent le stockage associé. De manière générale, envisagez l'utilisation des outils de l'application pour gérer la migration. Pour Oracle, envisagez d'utiliser des outils Oracle tels que RMAN ou ASM pour migrer les fichiers de base de données. Voir "TR-4534" pour en savoir plus. De même, pour SQL Server, envisagez d'utiliser soit SQL Server Management Studio, soit des outils NetApp tels qu'SnapManager pour SQL Server, soit SnapCenter.

Les outils ONTAP pour VMware vSphere

Lors de l'utilisation de vSphere avec des systèmes exécutant le logiciel ONTAP, la meilleure pratique la plus importante consiste à installer et à utiliser les outils ONTAP pour le plug-in VMware vSphere (anciennement Virtual Storage Console). Ce plug-in vCenter simplifie la gestion du stockage, améliore la disponibilité et réduit les coûts de stockage ainsi que les charges opérationnelles, que ce soit via SAN ou NAS. Il tire parti des bonnes pratiques pour le provisionnement des datastores et optimise les paramètres des hôtes ESXi pour les délais entre les chemins d'accès multiples et les HBA (ces paramètres sont décrits dans l'annexe B). Comme il s'agit d'un plug-in vCenter, il est disponible pour tous les clients Web vSphere qui se connectent au serveur vCenter.

Le plug-in permet également d'utiliser d'autres outils ONTAP dans les environnements vSphere. Il vous permet d'installer le plug-in NFS pour VMware VAAI, ce qui permet d'alléger la copie vers ONTAP pour les opérations de clonage de machines virtuelles, de réserver de l'espace pour les fichiers de disques virtuels lourds et de décharger les snapshots ONTAP.

Le plug-in est également l'interface de gestion de nombreuses fonctions de VASA Provider pour ONTAP, prenant en charge la gestion basée sur des règles de stockage avec vvols. Une fois les outils ONTAP pour VMware vSphere enregistrés, utilisez-le pour créer des profils de capacité de stockage, les mapper au stockage, et assurez-vous que le datastore est conforme aux profils au fil du temps. Vasa Provider fournit également une interface pour créer et gérer les datastores vvol.

En règle générale, NetApp recommande d'utiliser les outils ONTAP pour l'interface VMware vSphere dans vCenter afin de provisionner les datastores classiques et vvols pour garantir le respect de bonnes pratiques.

Réseau général

La configuration des paramètres réseau lors de l'utilisation de vSphere avec des systèmes exécutant le logiciel ONTAP est simple et similaire à celle d'autres configurations réseau. Voici quelques points à prendre en compte :

- Trafic du réseau de stockage séparé des autres réseaux Un réseau distinct peut être obtenu à l'aide d'un VLAN dédié ou de commutateurs distincts pour le stockage. Si le réseau de stockage partage des chemins physiques, tels que des liaisons ascendantes, vous pouvez avoir besoin de la qualité de service ou de ports supplémentaires pour garantir une bande passante suffisante. Ne connectez pas les hôtes directement au stockage ; utilisez les commutateurs pour disposer de chemins redondants et permettez à

VMware HA de fonctionner sans intervention. Voir "Connexion directe au réseau" pour plus d'informations.

- Les trames Jumbo peuvent être utilisées si vous le souhaitez et prises en charge par votre réseau, en particulier lors de l'utilisation d'iSCSI. Si elles sont utilisées, assurez-vous qu'elles sont configurées de manière identique sur tous les périphériques réseau, VLAN, etc. Dans le chemin entre le stockage et l'hôte ESXi. Vous pourriez voir des problèmes de performances ou de connexion. La MTU doit également être définie de manière identique sur le switch virtuel ESXi, le port VMkernel et également sur les ports physiques ou les groupes d'interface de chaque nœud ONTAP.
- NetApp recommande uniquement la désactivation du contrôle de flux réseau sur les ports réseau du cluster dans un cluster ONTAP. NetApp ne recommande pas d'autres recommandations sur les meilleures pratiques pour les ports réseau restants utilisés pour le trafic de données. Vous devez activer ou désactiver si nécessaire. Voir "TR-4182" pour plus d'informations sur le contrôle de flux.
- Lorsque les baies de stockage ESXi et ONTAP sont connectées aux réseaux de stockage Ethernet, NetApp recommande de configurer les ports Ethernet auxquels ces systèmes se connectent en tant que ports de périphérie RSTP (Rapid Spanning Tree Protocol) ou en utilisant la fonctionnalité Cisco PortFast. NetApp recommande d'activer la fonction de jonction Spanning-Tree PortFast dans les environnements qui utilisent la fonction Cisco PortFast et dont le agrégation VLAN 802.1Q est activée soit au serveur ESXi, soit aux baies de stockage ONTAP.
- NetApp recommande les meilleures pratiques suivantes pour l'agrégation de liens :
  - Utilisez des commutateurs qui prennent en charge l'agrégation de liens des ports sur deux châssis de commutateurs distincts grâce à une approche de groupe d'agrégation de liens multichâssis, telle que Virtual PortChannel (VPC) de Cisco.
  - Désactiver LACP pour les ports de switch connectés à ESXi, sauf si vous utilisez dvswitches 5.1 ou version ultérieure avec LACP configuré.
  - Utilisez LACP pour créer des agrégats de liens pour les systèmes de stockage ONTAP avec des groupes d'interfaces multimode dynamiques avec un hachage de port ou d'IP. Reportez-vous à la section "Gestion de réseau" pour obtenir des conseils supplémentaires.
  - Utilisez une stratégie de regroupement de hachage IP sur ESXi lors de l'agrégation de liens statiques (EtherChannel, par exemple) et des vSwitch standard ou de l'agrégation de liens basée sur LACP avec des commutateurs distribués vSphere. Si l'agrégation de liens n'est pas utilisée, utilisez plutôt « route basée sur l'ID de port virtuel d'origine ».

Le tableau suivant fournit un récapitulatif des éléments de configuration réseau et indique l'emplacement d'application des paramètres.

Élément	VMware ESXi	Commutateur	Nœud	SVM
Adresse IP	VMkernel	Non**	Non**	Oui.
Agrégation de liens	Commutateur virtuel	Oui.	Oui.	Non*
VLAN	Groupes de ports VMKernel et VM	Oui.	Oui.	Non*
Contrôle de flux	NIC	Oui.	Oui.	Non*
Spanning Tree	Non	Oui.	Non	Non
MTU (pour les trames jumbo)	Commutateur virtuel et port VMkernel (9000)	Oui (défini sur max)	Oui (9000)	Non*
Groupes de basculement	Non	Non	Oui (créer)	Oui (sélectionner)

*Les LIF SVM se connectent aux ports, aux groupes d'interface ou aux interfaces VLAN dotés de VLAN, MTU et d'autres paramètres. Cependant, les paramètres ne sont pas gérés au niveau de la SVM.

**Ces périphériques ont leur propre adresse IP pour la gestion, mais ces adresses ne sont pas utilisées dans le contexte du réseau de stockage VMware ESXi.

SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

NetApp ONTAP fournit un stockage en mode bloc de grande qualité pour VMware vSphere via iSCSI, Fibre Channel Protocol(FCP ou FC pour Short) et NVMe over Fabrics (NVMe-of). Les meilleures pratiques suivantes sont appliquées pour l'implémentation de protocoles en mode bloc pour le stockage de machines virtuelles avec vSphere et ONTAP.

Dans vSphere, il existe trois façons d'utiliser les LUN de stockage bloc :

- Avec les datastores VMFS
- Avec mappage de périphériques bruts (RDM)
- En tant que LUN accessible et contrôlée par un initiateur logiciel à partir d'un système d'exploitation invité de machine virtuelle

VMFS est un système de fichiers en cluster hautes performances qui fournit des datastores sous forme de pools de stockage partagés. Les datastores VMFS peuvent être configurés avec des LUN accessibles via FC, iSCSI, FCoE ou avec des espaces de noms NVMe accessibles via les protocoles NVMe/FC ou NVMe/TCP. VMFS permet à chaque serveur ESX d'un cluster d'accéder simultanément au stockage. La taille de LUN maximale est généralement de 128 To à partir de ONTAP 9.12.1P2 (et versions antérieures avec les systèmes ASA). Par conséquent, un datastore VMFS 5 ou 6 de 64 To de taille maximale peut être créé à l'aide d'une seule LUN.

VSphere inclut la prise en charge intégrée de plusieurs chemins d'accès aux périphériques de stockage, appelés chemins d'accès multiples natifs (NMP). NMP peut détecter le type de stockage pour les systèmes de stockage pris en charge et configure automatiquement la pile NMP afin de prendre en charge les capacités du système de stockage utilisé.

NMP et ONTAP prennent en charge le protocole ALUA (Asymmetric Logical Unit Access) pour négocier des chemins optimisés et non optimisés. Dans ONTAP, un chemin optimisé pour le protocole ALUA suit un chemin d'accès direct aux données, utilisant un port cible sur le nœud qui héberge la LUN accédée. ALUA est activé par défaut dans vSphere et ONTAP. Le NMP reconnaît le cluster ONTAP en tant que ALUA, et il utilise le plug-in ALUA de type baie de stockage (`VMW_SATP_ALUA`) et sélectionne le plug-in de sélection de chemin de tourniquet (`VMW_PSP_RR`).

ESXi 6 prend en charge jusqu'à 256 LUN et jusqu'à 1,024 chemins d'accès aux LUN au total. ESXi ne voit pas de LUN ni de chemins au-delà de ces limites. En supposant un nombre maximum de LUN, la limite de chemin autorise quatre chemins par LUN. Dans un cluster ONTAP plus grand, il est possible d'atteindre la limite de chemin avant la limite de LUN. Pour résoudre cette limitation, ONTAP prend en charge le mappage de LUN sélectif (SLM) dans la version 8.3 et les versions ultérieures.

SLM limite les nœuds qui annoncent les chemins vers une LUN donnée. Il est recommandé à NetApp d'utiliser au moins une LIF par nœud par SVM et SLM pour limiter les chemins annoncés vers le nœud hébergeant la LUN et son partenaire de haute disponibilité. Bien que d'autres chemins existent, ils ne sont pas annoncés par défaut. Il est possible de modifier les chemins annoncés avec les arguments de noeud de rapport ajouter et supprimer dans SLM. Notez que les LUN créées dans les versions antérieures à 8.3 annoncent tous les chemins et doivent être modifiés uniquement pour annoncer les chemins vers la paire HA d'hébergement.

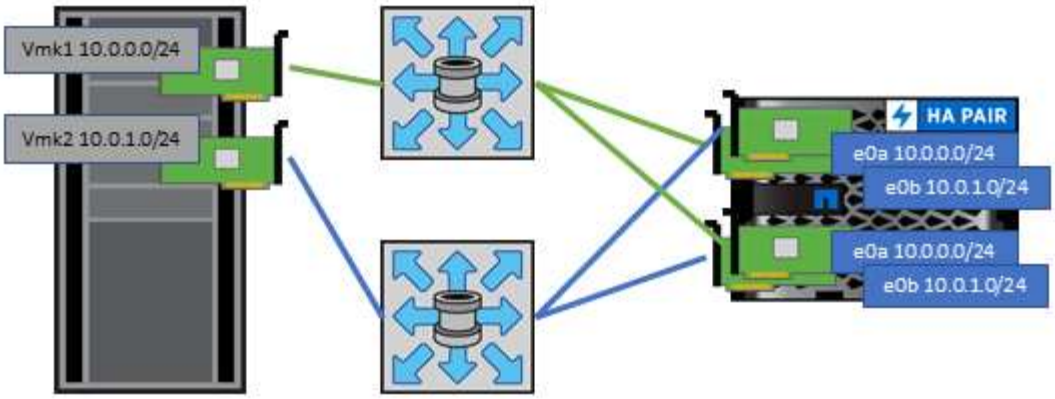
Pour plus d'informations sur SLM, consultez la section 5.9 de "TR-4080". La méthode précédente de ensembles de ports peut également être utilisée pour réduire davantage les chemins disponibles pour une LUN. Les jeux de ports permettent de réduire le nombre de chemins visibles via lesquels les initiateurs d'un groupe initiateur peuvent voir les LUN.

- SLM est activé par défaut. Sauf si vous utilisez des ensembles de ports, aucune configuration supplémentaire n'est requise.
- Pour les LUN créées avant Data ONTAP 8.3, appliquez manuellement SLM en exécutant le `lun mapping remove-reporting-nodes` Commande permettant de supprimer les nœuds présentant les rapports LUN et de limiter l'accès des LUN au nœud propriétaire de la LUN et à son partenaire haute disponibilité.

Des protocoles de bloc (iSCSI, FC et FCoE) accèdent aux LUN à l'aide d'identifiants de LUN, de numéros de série et de noms uniques. Les protocoles FC et FCoE utilisent des noms mondiaux (WWN et WWPN) et iSCSI utilise les noms qualifiés iSCSI (IQN). Le chemin vers les LUN à l'intérieur du stockage n'a aucun sens avec les protocoles de bloc et n'est pas présenté au niveau du protocole. Par conséquent, un volume contenant uniquement des LUN n'a pas besoin d'être monté en interne et un chemin de jonction n'est pas nécessaire pour les volumes contenant les LUN utilisées dans les datastores. Le sous-système NVMe dans ONTAP fonctionne de la même manière.

D'autres meilleures pratiques à prendre en compte :

- Vérifier qu'une interface logique (LIF) est créée pour chaque SVM sur chaque nœud du cluster ONTAP pour optimiser la disponibilité et la mobilité. La meilleure pratique du SAN de ONTAP est d'utiliser deux ports physiques et LIF par nœud, un pour chaque structure. ALUA sert à analyser les chemins et à identifier les chemins (directs) optimisés actifs/actifs au lieu de chemins non optimisés actifs. ALUA est utilisé pour FC, FCoE et iSCSI.
- Pour les réseaux iSCSI, utilisez plusieurs interfaces réseau VMkernel sur différents sous-réseaux du réseau avec le regroupement de cartes réseau lorsque plusieurs commutateurs virtuels sont présents. Vous pouvez également utiliser plusieurs cartes réseau physiques connectées à plusieurs commutateurs physiques pour fournir la haute disponibilité et un débit accru. La figure suivante fournit un exemple de connectivité multivoie. Dans ONTAP, configurez soit un groupe d'interface en mode unique pour basculement avec deux liaisons ou plus connectées à deux ou plusieurs switchs, soit au moyen de LACP ou d'une autre technologie d'agrégation de liens avec des groupes d'interfaces multimode afin d'assurer la haute disponibilité et les avantages de l'agrégation de liens.
- Si le protocole CHAP (Challenge-Handshake Authentication Protocol) est utilisé dans ESXi pour l'authentification de la cible, il doit également être configuré dans ONTAP à l'aide de l'interface de ligne de commande (`vserver iscsi security create`) Ou avec System Manager (modifier la sécurité de l'initiateur sous Storage > SVM > SVM Settings > protocoles > iSCSI).
- Utilisez les outils ONTAP pour VMware vSphere pour créer et gérer des LUN et des igroups. Le plug-in détermine automatiquement les WWPN des serveurs et crée les igroups appropriés. Il configure également les LUN en fonction des meilleures pratiques et les mappe avec les groupes initiateurs appropriés.
- Utilisez les RDM avec soin car ils peuvent être plus difficiles à gérer et ils utilisent également des chemins, qui sont limités comme décrit précédemment. Les LUN ONTAP prennent en charge les deux "mode de compatibilité physique et virtuelle" RDM.
- Pour en savoir plus sur l'utilisation de NVMe/FC avec vSphere 7.0, consultez cette "Guide de configuration d'hôte NVMe/FC de ONTAP" et "TR-4684"La figure suivante décrit la connectivité multivoie d'un hôte vSphere vers un LUN ONTAP.



NFS

NetApp ONTAP est, entre autres, une baie NAS scale-out de grande qualité. ONTAP permet à VMware vSphere d'accéder simultanément aux datastores connectés par NFS à partir de nombreux hôtes VMware ESXi, ce qui dépasse 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, comme indiqué dans le "les datastores" section.

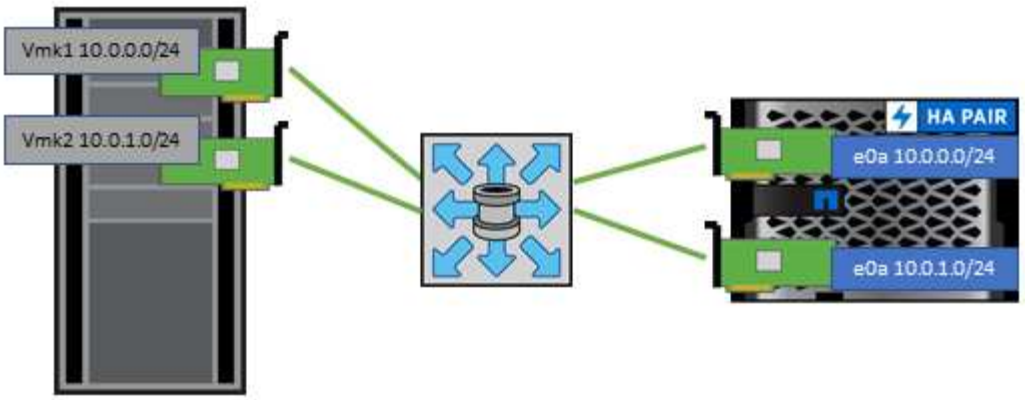
Nous vous recommandons les meilleures pratiques suivantes lorsque vous utilisez ONTAP NFS avec vSphere :

- Utiliser une interface logique (LIF) unique pour chaque SVM sur chaque nœud du cluster ONTAP. Les recommandations précédentes d'une LIF par datastore ne sont plus nécessaires. L'accès direct (LIF et datastore sur le même nœud) est idéal, mais ne vous inquiétez pas pour l'accès indirect, car l'effet de performance est généralement minimal (microsecondes).
- VMware prend en charge NFSv3 depuis VMware Infrastructure 3. VSphere 6.0 a ajouté la prise en charge de NFSv4.1, offrant des fonctionnalités avancées telles que la sécurité Kerberos. Dans le cas où NFSv3 utilise un verrouillage côté client, NFSv4.1 utilise un verrouillage côté serveur. Bien qu'un volume ONTAP puisse être exporté via les deux protocoles, ESXi ne peut être monté que via un seul protocole. Ce montage de protocole unique n'empêche pas les autres hôtes ESXi de monter le même datastore dans une version différente. Veillez à spécifier la version du protocole à utiliser lors du montage de sorte que tous les hôtes utilisent la même version et, par conséquent, le même style de verrouillage. Ne pas mélanger les versions NFS sur les hôtes. Si possible, utilisez des profils hôtes pour vérifier la conformité.
  - Étant donné qu'il n'existe pas de conversion automatique de datastore entre NFS v3 et NFS v4.1, créez un nouveau datastore NFSv4.1 et utilisez Storage vMotion pour migrer les machines virtuelles vers le nouveau datastore.
  - Reportez-vous aux notes du tableau interopérabilité NFS v4.1 dans le "Matrice d'interopérabilité NetApp" Pour les niveaux de correctifs VMware ESXi spécifiques requis pour la prise en charge.
  - VMware prend en charge nconnect avec NFSv3 à partir de vSphere 8.0U2. Pour plus d'informations sur nconnect, consultez le "Fonctionnalité NFSv3 nConnect avec NetApp et VMware"
- Les export policy NFS permettent de contrôler l'accès des hôtes vSphere. Vous pouvez utiliser une seule règle avec plusieurs volumes (datastores). Avec NFSv3, ESXi utilise le style de sécurité sys (UNIX) et requiert l'option de montage root pour exécuter les VM. Dans ONTAP, cette option est appelée superutilisateur et, lorsque l'option superutilisateur est utilisée, il n'est pas nécessaire de spécifier l'ID utilisateur anonyme. Notez que l'export-policy rules avec des valeurs différentes de `-anon` et `-allow -suid` Peut entraîner des problèmes de découverte des SVM à l'aide des outils ONTAP. Voici un exemple

de politique :

- Protocole d'accès : nfs (qui inclut nfs3 et nfs4)
- Spéc. Correspondance client : 192.168.42.21
- Règle d'accès RO : sys
- Règle d'accès RW : sys
- UID anonyme
- Superutilisateur : sys

- Si vous utilisez le plug-in NetApp NFS pour VMware VAAI, le protocole doit être défini en tant que `nfs` au lieu de `nfs3` lorsque la règle export-policy est créée ou modifiée. La fonctionnalité de déchargement des copies VAAI nécessite le fonctionnement du protocole NFSv4, même si le protocole de données est NFSv3. Spécification du protocole en tant que `nfs` Inclut les versions NFSv3 et NFSv4.
- Les volumes des datastores NFS sont rassemblés dans le volume racine du SVM. Par conséquent, ESXi doit également avoir accès au volume racine pour naviguer et monter des volumes de datastores. La export policy pour le volume root, et pour tout autre volume dans lequel la jonction du volume de datastore est imbriquée, doit inclure une règle ou des règles pour les serveurs ESXi leur accordant un accès en lecture seule. Voici un exemple de règle pour le volume racine, également à l'aide du plug-in VAAI :
  - Protocole d'accès : nfs (qui inclut nfs3 et nfs4)
  - Spéc. Correspondance client : 192.168.42.21
  - Règle d'accès RO : sys
  - Règle d'accès RW : jamais (meilleure sécurité pour le volume racine)
  - UID anonyme
  - Superutilisateur : sys (également requis pour le volume racine avec VAAI)
- Utilisez les outils ONTAP pour VMware vSphere (meilleure pratique la plus importante) :
  - Utilisez les outils ONTAP pour VMware vSphere pour provisionner les datastores, car cela simplifie automatiquement la gestion des règles d'exportation.
  - Lors de la création de datastores pour clusters VMware avec le plug-in, sélectionnez le cluster plutôt qu'un seul serveur ESX. Ce choix permet de monter automatiquement le datastore sur tous les hôtes du cluster.
  - Utilisez la fonction de montage du plug-in pour appliquer les datastores existants aux nouveaux serveurs.
  - Lorsque vous n'utilisez pas les outils ONTAP pour VMware vSphere, utilisez une export policy unique pour tous les serveurs ou pour chaque cluster de serveurs où un contrôle d'accès supplémentaire est nécessaire.
- Bien que ONTAP offre une structure d'espace de noms de volume flexible permettant d'organiser les volumes dans une arborescence à l'aide de jonctions, cette approche n'a aucune valeur pour vSphere. Il crée un répertoire pour chaque machine virtuelle à la racine du datastore, quelle que soit la hiérarchie de l'espace de noms du stockage. Il est donc recommandé de simplement monter le Junction path pour les volumes pour vSphere au volume root du SVM, c'est-à-dire comment les outils ONTAP pour VMware vSphere provisionne les datastores. Sans chemins de jonction imbriqués, aucun volume ne dépend d'aucun volume autre que le volume root et que mettre un volume hors ligne ou le détruire, même intentionnellement, n'affecte pas le chemin d'accès aux autres volumes.
- Une taille de bloc de 4 Ko convient parfaitement aux partitions NTFS sur les datastores NFS. La figure suivante décrit la connectivité d'un hôte vSphere vers un datastore NFS ONTAP.



Le tableau suivant répertorie les versions NFS et les fonctionnalités prises en charge.

Fonctionnalités de vSphere	NFSv3	NFSv4.1
VMotion et Storage vMotion	Oui.	Oui.
Haute disponibilité	Oui.	Oui.
Tolérance aux pannes	Oui.	Oui.
DRS	Oui.	Oui.
Profils hôtes	Oui.	Oui.
DRS de stockage	Oui.	Non
Contrôle des E/S du stockage	Oui.	Non
SRM	Oui.	Non
Volumes virtuels	Oui.	Non
Accélération matérielle (VAAI)	Oui.	Oui.
Authentification Kerberos	Non	Oui (optimisé avec vSphere 6.5 et versions ultérieures pour prendre en charge AES et krb5i)
Prise en charge des chemins d'accès	Non	Oui.

Volumes FlexGroup

Utilisez des volumes ONTAP et FlexGroup avec VMware vSphere pour disposer de datastores simples et évolutifs exploitant toute la puissance d'un cluster ONTAP.

ONTAP 9.8, ainsi que les outils ONTAP pour VMware vSphere 9.8 et le plug-in SnapCenter pour VMware 4.4, ont ajouté la prise en charge des datastores FlexGroup avec volumes dans vSphere. Les volumes FlexGroup simplifient la création de grands datastores et créent automatiquement les volumes distribués nécessaires sur le cluster ONTAP afin d'optimiser les performances d'un système ONTAP.

Pour en savoir plus sur les volumes FlexGroup, consultez la section "Rapports techniques de volume sur FlexCache et FlexGroup".

Utilisez les volumes FlexGroup avec vSphere si vous avez besoin d'un datastore vSphere unique et évolutif

doté de la puissance d'un cluster ONTAP complet ou si vous disposez de charges de travail de clonage très importantes pouvant bénéficier du nouveau mécanisme de clonage FlexGroup.

Copie auxiliaire

Outre les tests approfondis du système avec les charges de travail vSphere, ONTAP 9.8 a ajouté un nouveau mécanisme de déchargement des copies pour les datastores FlexGroup. Ce nouveau système utilise un moteur de copie amélioré pour répliquer les fichiers entre les composants en arrière-plan tout en permettant l'accès à la source et à la destination. Ce cache local est ensuite utilisé pour instancier rapidement des clones de machine virtuelle à la demande.

Pour activer le déchargement de copie optimisé pour FlexGroup, reportez-vous à la section "Comment configurer les FlexGroups ONTAP pour permettre le déchargement des copies VAAI"

Si vous utilisez le clonage VAAI, mais que le clonage n'est pas suffisant pour maintenir le cache chaud, vos clones ne seront peut-être pas plus rapides qu'une copie basée sur hôte. Si c'est le cas, vous pouvez régler le délai d'expiration du cache pour mieux répondre à vos besoins.

Prenons le scénario suivant :

- Vous avez créé un nouveau FlexGroup avec 8 composants
- Le délai d'expiration du cache pour le nouveau FlexGroup est défini sur 160 minutes

Dans ce scénario, les 8 premiers clones à terminer seront des copies complètes, et non des clones de fichiers locaux. Tout clonage supplémentaire de cette machine virtuelle avant l'expiration du délai de 160 secondes utilisera le moteur de clonage de fichiers à l'intérieur de chaque composant de manière circulaire pour créer des copies quasi immédiates réparties uniformément sur les volumes constitutifs.

Chaque nouvelle tâche de clonage reçue par un volume réinitialise le délai d'expiration. Si un volume composant de l'exemple FlexGroup ne reçoit pas de requête de clone avant le délai d'expiration, le cache de cette machine virtuelle sera effacé et le volume devra être à nouveau rempli. De même, si la source du clone d'origine change (par exemple, si vous avez mis à jour le modèle), le cache local de chaque composant sera invalidé pour éviter tout conflit. Comme indiqué précédemment, le cache peut être réglé en fonction des besoins de votre environnement.

Pour plus d'informations sur l'utilisation de FlexGroups avec VAAI, consultez l'article de la base de connaissances suivant : "VAAI : comment la mise en cache fonctionne-t-elle avec les volumes FlexGroup ?"

Dans les environnements où vous ne pouvez pas tirer pleinement parti du cache FlexGroup, mais où vous avez toujours besoin d'un clonage rapide entre plusieurs volumes, envisagez d'utiliser les vVols. Le clonage entre volumes avec vVols est beaucoup plus rapide qu'avec les datastores traditionnels et ne repose pas sur un cache.

Paramètres QoS

La configuration de la qualité de service au niveau FlexGroup à l'aide de ONTAP System Manager ou du shell du cluster est prise en charge, mais elle ne prend pas en charge la reconnaissance des machines virtuelles ni l'intégration de vCenter.

La qualité de service (IOPS max/min) peut être définie sur des VM individuelles ou sur toutes les VM d'un datastore à ce moment dans l'interface utilisateur vCenter ou via les API REST à l'aide des outils ONTAP. La définition de la qualité de service sur toutes les VM remplace tous les paramètres distincts par VM. Les paramètres ne s'étendent pas ultérieurement aux nouvelles machines virtuelles ou aux machines virtuelles migrées ; définissez la qualité de service sur les nouvelles machines virtuelles ou appliquez à nouveau la qualité de service à toutes les machines virtuelles du datastore.

Notez que VMware vSphere traite toutes les E/S d'un datastore NFS comme une seule file d'attente par hôte, et que la limitation de la qualité de service sur une machine virtuelle peut avoir un impact sur les performances des autres machines virtuelles du même datastore. Cela contraste avec les vVols qui peuvent maintenir leurs paramètres de politique de QoS s'ils migrent vers un autre datastore et n'ont pas d'impact sur les E/S d'autres machines virtuelles lorsqu'ils sont restreints.

Métriques

ONTAP 9.8 a également ajouté de nouveaux metrics de performance basés sur des fichiers (IOPS, débit et latence) pour FlexGroup Files. Ces metrics peuvent être consultées dans les outils ONTAP pour les rapports sur les machines virtuelles et le tableau de bord VMware vSphere. Les outils ONTAP pour le plug-in VMware vSphere vous permettent également de définir des règles de qualité de service (QoS) en combinant des IOPS minimales et/ou maximales. Ils peuvent être définis au sein de toutes les machines virtuelles d'un datastore ou individuellement pour des machines virtuelles spécifiques.

Et des meilleures pratiques

- Utilisez les outils ONTAP pour créer des datastores FlexGroup afin de vous assurer que votre FlexGroup est créé de manière optimale et que les règles d'exportation sont configurées pour correspondre à votre environnement vSphere. Cependant, après avoir créé le volume FlexGroup avec les outils ONTAP, vous constaterez que tous les nœuds de votre cluster vSphere utilisent une seule adresse IP pour monter le datastore. Cela pourrait entraîner un goulot d'étranglement sur le port réseau. Pour éviter ce problème, démontez le datastore, puis remontez-le à l'aide de l'assistant standard vSphere datastore en utilisant un nom DNS round-Robin qui équilibre la charge entre les LIF du SVM. Après le remontage, les outils ONTAP pourront à nouveau gérer le datastore. Si les outils ONTAP ne sont pas disponibles, utilisez les paramètres par défaut de FlexGroup et créez votre règle d'export en suivant les instructions de la section "Datastores et protocoles - NFS".
- Lors du dimensionnement d'un datastore FlexGroup, n'oubliez pas que le FlexGroup est constitué de plusieurs petits volumes FlexVol qui créent un espace de noms plus important. Par conséquent, dimensionnez le datastore pour qu'il soit au moins 8 fois (en supposant que les 8 composants par défaut) la taille de votre fichier VMDK le plus volumineux, plus une marge inutilisée de 10 à 20 % pour permettre un rééquilibrage flexible. Par exemple, si votre environnement comporte 6 To de VMDK, dimensionnez le datastore FlexGroup d'une capacité inférieure à 52,8 To (6 x 8 + 10 %).
- VMware et NetApp prennent en charge la mise en circuit de session NFSv4.1 à partir de ONTAP 9.14.1. Pour plus d'informations sur les versions, reportez-vous aux notes de la matrice d'interopérabilité NetApp NFS 4.1. NFSv3 ne prend pas en charge plusieurs chemins physiques vers un volume, mais prend en charge nconnect à partir de vSphere 8.0U2. Pour plus d'informations sur nconnect, consultez le "Fonctionnalité NFSv3 nConnect avec NetApp et VMware".
- Utilisez le plug-in NFS pour VMware VAAI pour la copie auxiliaire. Notez que même si le clonage est amélioré dans un datastore FlexGroup, comme mentionné précédemment, ONTAP n'offre pas d'avantages significatifs en termes de performances par rapport à la copie hôte ESXi lors de la copie de machines virtuelles entre des volumes FlexVol et/ou FlexGroup. Prenez donc en compte vos charges de travail de clonage lorsque vous décidez d'utiliser VAAI ou FlexGroups. L'une des façons d'optimiser le clonage basé sur FlexGroup consiste à modifier le nombre de volumes constitutifs. Tout comme le réglage du délai d'expiration du cache mentionné précédemment.
- Utilisez les outils ONTAP pour VMware vSphere 9.8 ou version ultérieure pour surveiller les performances des machines virtuelles FlexGroup à l'aide de metrics ONTAP (tableaux de bord et rapports sur les machines virtuelles) et gérer la qualité de service sur chaque machine virtuelle. Ces metrics ne sont pas encore disponibles via les commandes ou les API ONTAP.
- Le plug-in SnapCenter pour VMware vSphere version 4.4 et ultérieure prend en charge la sauvegarde et la restauration des machines virtuelles dans un datastore FlexGroup sur le système de stockage principal. Le distributeur sélectif 4.6 ajoute la prise en charge de SnapMirror pour les datastores basés sur FlexGroup.

L'utilisation de snapshots basés sur les baies et de la réplication est le moyen le plus efficace de protéger vos données.

Configuration du réseau

La configuration des paramètres réseau lors de l'utilisation de vSphere avec des systèmes exécutant le logiciel ONTAP est simple et similaire à celle d'autres configurations réseau.

Voici quelques points à prendre en compte :

- Trafic du réseau de stockage séparé des autres réseaux Un réseau distinct peut être obtenu à l'aide d'un VLAN dédié ou de commutateurs distincts pour le stockage. Si le réseau de stockage partage des chemins physiques, tels que des liaisons ascendantes, vous pouvez avoir besoin de la qualité de service ou de ports supplémentaires pour garantir une bande passante suffisante. Ne connectez pas les hôtes directement au stockage ; utilisez les commutateurs pour disposer de chemins redondants et permettez à VMware HA de fonctionner sans intervention. Voir "Connexion directe au réseau" pour plus d'informations.
- Les trames Jumbo peuvent être utilisées si vous le souhaitez et prises en charge par votre réseau, en particulier lors de l'utilisation d'iSCSI. Si elles sont utilisées, assurez-vous qu'elles sont configurées de manière identique sur tous les périphériques réseau, VLAN, etc. Dans le chemin entre le stockage et l'hôte ESXi. Vous pourriez voir des problèmes de performances ou de connexion. La MTU doit également être définie de manière identique sur le switch virtuel ESXi, le port VMkernel et également sur les ports physiques ou les groupes d'interface de chaque nœud ONTAP.
- NetApp recommande uniquement la désactivation du contrôle de flux réseau sur les ports réseau du cluster dans un cluster ONTAP. NetApp ne recommande pas d'autres recommandations sur les meilleures pratiques pour les ports réseau restants utilisés pour le trafic de données. Vous devez l'activer ou la désactiver si nécessaire. Voir "TR-4182" pour plus d'informations sur le contrôle de flux.
- Lorsque les baies de stockage ESXi et ONTAP sont connectées aux réseaux de stockage Ethernet, NetApp recommande de configurer les ports Ethernet auxquels ces systèmes se connectent en tant que ports de périphérie RSTP (Rapid Spanning Tree Protocol) ou en utilisant la fonctionnalité Cisco PortFast. NetApp recommande d'activer la fonction de jonction Spanning-Tree PortFast dans les environnements qui utilisent la fonction Cisco PortFast et dont le agrégation VLAN 802.1Q est activée soit au serveur ESXi, soit aux baies de stockage ONTAP.
- NetApp recommande les meilleures pratiques suivantes pour l'agrégation de liens :
  - Utilisez des commutateurs qui prennent en charge l'agrégation de liens des ports sur deux châssis de commutateurs distincts grâce à une approche de groupe d'agrégation de liens multichâssis, telle que Virtual PortChannel (VPC) de Cisco.
  - Désactiver LACP pour les ports de switch connectés à ESXi, sauf si vous utilisez dvswitches 5.1 ou version ultérieure avec LACP configuré.
  - Utilisez LACP pour créer des agrégats de liens pour les systèmes de stockage ONTAP avec des groupes d'interface multimode dynamiques avec un hachage IP.
  - Utilisez une stratégie de regroupement de hachage IP sur ESXi.

Le tableau suivant fournit un récapitulatif des éléments de configuration réseau et indique l'emplacement d'application des paramètres.

Élément	VMware ESXi	Commutateur	Nœud	SVM
Adresse IP	VMkernel	Non**	Non**	Oui.

Élément	VMware ESXi	Commutateur	Nœud	SVM
Agrégation de liens	Commutateur virtuel	Oui.	Oui.	Non*
VLAN	Groupes de ports VMKernel et VM	Oui.	Oui.	Non*
Contrôle de flux	NIC	Oui.	Oui.	Non*
Spanning Tree	Non	Oui.	Non	Non
MTU (pour les trames jumbo)	Commutateur virtuel et port VMkernel (9000)	Oui (défini sur max)	Oui (9000)	Non*
Groupes de basculement	Non	Non	Oui (créer)	Oui (sélectionner)

*Les LIF SVM se connectent aux ports, aux groupes d'interface ou aux interfaces VLAN dotés de VLAN, MTU et d'autres paramètres. Cependant, les paramètres ne sont pas gérés au niveau de la SVM.

**Ces périphériques ont leur propre adresse IP pour la gestion, mais ces adresses ne sont pas utilisées dans le contexte du réseau de stockage VMware ESXi.

SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

Dans vSphere, il existe trois façons d'utiliser les LUN de stockage bloc :

- Avec les datastores VMFS
- Avec mappage de périphériques bruts (RDM)
- En tant que LUN accessible et contrôlée par un initiateur logiciel à partir d'un système d'exploitation invité de machine virtuelle

VMFS est un système de fichiers en cluster hautes performances qui fournit des datastores sous forme de pools de stockage partagés. Les datastores VMFS peuvent être configurés avec des LUN accessibles via des espaces de noms FC, iSCSI, FCoE ou NVMe accessibles via le protocole NVMe/FC. VMFS permet d'accéder simultanément aux LUN classiques par chaque serveur ESX d'un cluster. La taille de LUN maximale du ONTAP est généralement de 16 To. Par conséquent, un datastore VMFS 5 de 64 To (voir le premier tableau de cette section) est créé avec quatre LUN de 16 To (tous les systèmes SAN prennent en charge la taille de LUN VMFS de 64 To maximum). Dans la mesure où l'architecture LUN ONTAP ne dispose pas de petites profondeurs de files d'attente individuelles, les datastores VMFS en ONTAP peuvent évoluer plus largement qu'avec les architectures de baies traditionnelles de manière relativement simple.

VSphere inclut la prise en charge intégrée de plusieurs chemins d'accès aux périphériques de stockage, appelés chemins d'accès multiples natifs (NMP). NMP peut détecter le type de stockage pour les systèmes de stockage pris en charge et configure automatiquement la pile NMP afin de prendre en charge les capacités du système de stockage utilisé.

NMP et ONTAP prennent en charge le protocole ALUA (Asymmetric Logical Unit Access) pour négocier des chemins optimisés et non optimisés. Dans ONTAP, un chemin optimisé pour le protocole ALUA suit un chemin d'accès direct aux données, utilisant un port cible sur le nœud qui héberge la LUN accédée. ALUA est activé par défaut dans vSphere et ONTAP. Le NMP reconnaît le cluster ONTAP en tant que ALUA, et il utilise le plug-in ALUA de type baie de stockage (`VMW_SATP_ALUA`) et sélectionne le plug-in de sélection de chemin d'accès rond (`VMW_PSP_RR`).

ESXi 6 prend en charge jusqu'à 256 LUN et jusqu'à 1,024 chemins d'accès aux LUN au total. Les LUN et les

chemins au-delà de ces limites ne sont pas visibles par ESXi. En supposant un nombre maximum de LUN, la limite de chemin autorise quatre chemins par LUN. Dans un cluster ONTAP plus grand, il est possible d'atteindre la limite de chemin avant la limite de LUN. Pour résoudre cette limitation, ONTAP prend en charge le mappage de LUN sélectif (SLM) dans la version 8.3 et les versions ultérieures.

SLM limite les nœuds qui annoncent les chemins vers une LUN donnée. Il est recommandé à NetApp d'utiliser au moins une LIF par nœud par SVM et SLM pour limiter les chemins annoncés vers le nœud hébergeant la LUN et son partenaire de haute disponibilité. Bien que d'autres chemins existent, ils ne sont pas annoncés par défaut. Il est possible de modifier les chemins annoncés avec les arguments de noeud de rapport ajouter et supprimer dans SLM. Notez que les LUN créées dans les versions antérieures à la version 8.3 annoncent tous les chemins et doivent être modifiés pour uniquement annoncer les chemins d'accès à la paire HA d'hébergement. Pour plus d'informations sur SLM, consultez la section 5.9 de "TR-4080". La méthode précédente de ensembles de ports peut également être utilisée pour réduire davantage les chemins disponibles pour une LUN. Les jeux de ports permettent de réduire le nombre de chemins visibles via lesquels les initiateurs d'un groupe initiateur peuvent voir les LUN.

- SLM est activé par défaut. Sauf si vous utilisez des ensembles de ports, aucune configuration supplémentaire n'est requise.
- Pour les LUN créées avant Data ONTAP 8.3, appliquez manuellement SLM en exécutant `lun mapping remove-reporting-nodes` Commande permettant de supprimer les nœuds présentant les rapports LUN et de limiter l'accès des LUN au nœud propriétaire de la LUN et à son partenaire haute disponibilité.

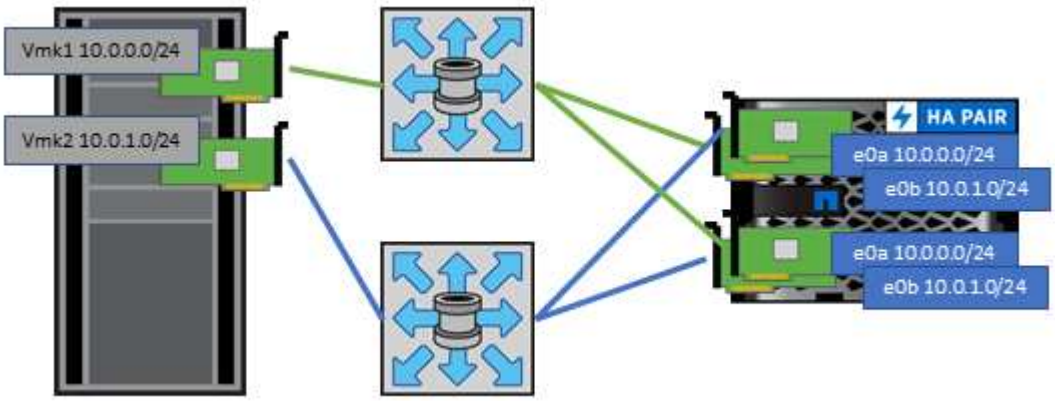
Des protocoles de bloc (iSCSI, FC et FCoE) accèdent aux LUN à l'aide d'identifiants de LUN, de numéros de série et de noms uniques. Les protocoles FC et FCoE utilisent des noms mondiaux (WWN et WWPN) et iSCSI utilise les noms qualifiés iSCSI (IQN). Le chemin vers les LUN à l'intérieur du stockage n'a aucun sens avec les protocoles de bloc et n'est pas présenté au niveau du protocole. Par conséquent, un volume contenant uniquement des LUN n'a pas besoin d'être monté en interne et un chemin de jonction n'est pas nécessaire pour les volumes contenant les LUN utilisées dans les datastores. Le sous-système NVMe dans ONTAP fonctionne de la même manière.

D'autres meilleures pratiques à prendre en compte :

- Vérifier qu'une interface logique (LIF) est créée pour chaque SVM sur chaque nœud du cluster ONTAP pour optimiser la disponibilité et la mobilité. La meilleure pratique du SAN de ONTAP est d'utiliser deux ports physiques et LIF par nœud, un pour chaque structure. ALUA sert à analyser les chemins et à identifier les chemins (directs) optimisés actifs/actifs au lieu de chemins non optimisés actifs. ALUA est utilisé pour FC, FCoE et iSCSI.
- Pour les réseaux iSCSI, utilisez plusieurs interfaces réseau VMkernel sur différents sous-réseaux du réseau avec le regroupement de cartes réseau lorsque plusieurs commutateurs virtuels sont présents. Vous pouvez également utiliser plusieurs cartes réseau physiques connectées à plusieurs commutateurs physiques pour fournir la haute disponibilité et un débit accru. La figure suivante fournit un exemple de connectivité multivoie. Dans ONTAP, utilisez un groupe d'interface monomode avec plusieurs liaisons vers différents commutateurs ou LACP avec des groupes d'interface multimode pour la haute disponibilité et les avantages d'agrégation de liens.
- Si le protocole CHAP (Challenge-Handshake Authentication Protocol) est utilisé dans ESXi pour l'authentification de la cible, il doit également être configuré dans ONTAP à l'aide de l'interface de ligne de commande (`vserver iscsi security create`) Ou avec System Manager (modifier la sécurité de l'initiateur sous Storage > SVM > SVM Settings > protocoles > iSCSI).
- Utilisez les outils ONTAP pour VMware vSphere pour créer et gérer des LUN et des igroups. Le plug-in détermine automatiquement les WWPN des serveurs et crée les igroups appropriés. Il configure également les LUN en fonction des meilleures pratiques et les mappe avec les groupes initiateurs appropriés.
- Utilisez les RDM avec soin car ils peuvent être plus difficiles à gérer et ils utilisent également des chemins,

qui sont limités comme décrit précédemment. Les LUN ONTAP prennent en charge les deux "mode de compatibilité physique et virtuelle" RDM.

- Pour en savoir plus sur l'utilisation de NVMe/FC avec vSphere 7.0, consultez cette "Guide de configuration d'hôte NVMe/FC de ONTAP" et "TR-4684". La figure suivante illustre la connectivité multivoie entre un hôte vSphere et un LUN ONTAP.



NFS

VSphere permet aux clients d'utiliser des baies NFS de classe entreprise pour fournir un accès simultané aux datastores à tous les nœuds d'un cluster ESXi. Comme mentionné dans la section datastore, la facilité d'utilisation et la visibilité sur l'efficacité du stockage présentent des avantages avec NFS avec vSphere.

Nous vous recommandons les meilleures pratiques suivantes lorsque vous utilisez ONTAP NFS avec vSphere :

- Utiliser une interface logique (LIF) unique pour chaque SVM sur chaque nœud du cluster ONTAP. Les recommandations précédentes d'une LIF par datastore ne sont plus nécessaires. L'accès direct (LIF et datastore sur le même nœud) est préférable, mais ne vous inquiétez pas pour l'accès indirect, car l'effet de performance est généralement minimal (microsecondes).
- Toutes les versions de VMware vSphere actuellement prises en charge peuvent utiliser NFS v3 et v4.1. La prise en charge officielle de nconnect a été ajoutée à vSphere 8.0 mise à jour 2 pour NFS v3. Pour NFS v4.1, vSphere continue à prendre en charge l'agrégation de sessions, l'authentification Kerberos et l'authentification Kerberos avec intégrité. Il est important de noter que l'agrégation de session nécessite ONTAP 9.14.1 ou une version ultérieure. Vous pouvez en savoir plus sur la fonctionnalité nconnect et sur la manière dont elle améliore les performances à "Fonctionnalité NFSv3 nConnect avec NetApp et VMware".

Notez que NFS v3 et NFS v4.1 utilisent différents mécanismes de verrouillage. NFS v3 utilise un verrouillage côté client, tandis que NFS v4.1 utilise un verrouillage côté serveur. Bien qu'un volume ONTAP puisse être exporté via les deux protocoles, ESXi ne peut monter qu'un datastore via un protocole. Cependant, cela ne signifie pas que d'autres hôtes ESXi ne peuvent pas monter le même datastore via une version différente. Pour éviter tout problème, il est essentiel de spécifier la version du protocole à utiliser lors du montage, en veillant à ce que tous les hôtes utilisent la même version et, par conséquent, le même style de verrouillage. Il est essentiel d'éviter de mélanger les versions NFS entre les hôtes. Si possible, utilisez les profils hôtes pour vérifier la conformité.
Comme il n'y a pas de conversion automatique des datastores entre NFSv3 et NFSv4.1, créez un nouveau datastore NFSv4.1 et utilisez Storage vMotion pour migrer les machines virtuelles vers le nouveau datastore.
Reportez-vous aux notes du tableau interopérabilité NFS v4.1 dans le "Matrice d'interopérabilité NetApp" Pour les niveaux de correctifs VMware ESXi spécifiques requis pour la prise en charge.

* Les règles d'exportation NFS sont utilisées pour contrôler l'accès par les hôtes vSphere. Vous pouvez utiliser une seule règle avec plusieurs volumes (datastores). Avec NFSv3, ESXi utilise le style de sécurité sys (UNIX) et requiert l'option de montage root pour exécuter les VM. Dans ONTAP, cette option est appelée superutilisateur et, lorsque l'option superutilisateur est utilisée, il n'est pas nécessaire de spécifier l'ID utilisateur anonyme. Notez que l'export-policy rules avec des valeurs différentes de `-anon` et `-allow-suid` Peut entraîner des problèmes de découverte des SVM à l'aide des outils ONTAP. Voici un exemple de politique :

Protocole d'accès : nfs3
Client Match Spec : 192.168.42.21
Règle d'accès RO : sys
RW règle d'accès : sys
UID anonyme
Superutilisateur : sys

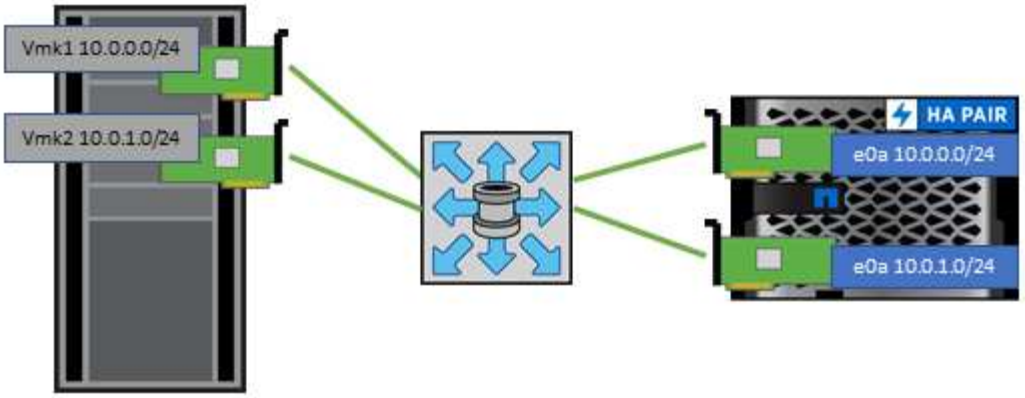
* Si le plug-in NetApp NFS pour VMware VAAI est utilisé, le protocole doit être défini comme `nfs` lorsque la règle export-policy est créée ou modifiée. Le protocole NFSv4 est requis pour que le déchargement des copies VAAI fonctionne et que vous spécifiez le protocole comme `nfs` Inclut automatiquement les versions NFSv3 et NFSv4.
* Les volumes de datastore NFS sont reliés par jonction au volume root du SVM ; par conséquent, ESXi doit également avoir accès au volume root pour naviguer et monter les volumes de datastore. La export policy pour le volume root, et pour tout autre volume dans lequel la jonction du volume de datastore est imbriquée, doit inclure une règle ou des règles pour les serveurs ESXi leur accordant un accès en lecture seule. Voici un exemple de règle pour le volume racine, également à l'aide du plug-in VAAI :

Protocole d'accès : nfs (qui inclut nfs3 et nfs4)
Client Match Spec : 192.168.42.21
Règle d'accès RO : sys
RW Access Rule: Never (meilleure sécurité pour le volume root)
UID anonyme
Superuser : sys (également requis pour le volume root avec VAAI)

* Utilisez les outils ONTAP pour VMware vSphere (meilleure pratique la plus importante) :

Utiliser les outils ONTAP pour VMware vSphere pour provisionner les datastores car cela simplifie automatiquement la gestion des règles d'exportation.
Lors de la création de datastores pour clusters VMware avec le plug-in, sélectionnez le cluster plutôt qu'un seul serveur ESX. Ce choix permet de monter automatiquement le datastore sur tous les hôtes du cluster.
Utilisez la fonction de montage du plug-in pour appliquer les datastores existants aux nouveaux serveurs.
Lorsque vous n'utilisez pas les outils ONTAP pour VMware vSphere, utilisez une règle d'exportation unique pour tous les serveurs ou pour chaque cluster de serveurs pour lesquels un contrôle d'accès supplémentaire est nécessaire.

* Bien que ONTAP offre une structure d'espace de noms de volume flexible pour organiser les volumes dans une arborescence à l'aide de jonctions, cette approche n'a pas de valeur pour vSphere. Il crée un répertoire pour chaque machine virtuelle à la racine du datastore, quelle que soit la hiérarchie de l'espace de noms du stockage. Il est donc recommandé de simplement monter le Junction path pour les volumes pour vSphere au volume root du SVM, c'est-à-dire comment les outils ONTAP pour VMware vSphere provisionne les datastores. Sans chemins de jonction imbriqués, aucun volume ne dépend d'aucun volume autre que le volume root et que mettre un volume hors ligne ou le détruire, même intentionnellement, n'affecte pas le chemin d'accès aux autres volumes.
* Une taille de bloc de 4 Ko convient pour les partitions NTFS sur les datastores NFS. La figure suivante décrit la connectivité d'un hôte vSphere vers un datastore NFS ONTAP.



Le tableau suivant répertorie les versions NFS et les fonctionnalités prises en charge.

Fonctionnalités de vSphere	NFSv3	NFSv4.1
VMotion et Storage vMotion	Oui.	Oui.
Haute disponibilité	Oui.	Oui.
Tolérance aux pannes	Oui.	Oui.
DRS	Oui.	Oui.
Profils hôtes	Oui.	Oui.
DRS de stockage	Oui.	Non
Contrôle des E/S du stockage	Oui.	Non
SRM	Oui.	Non
Volumes virtuels	Oui.	Non
Accélération matérielle (VAAI)	Oui.	Oui.
Authentification Kerberos	Non	Oui (optimisé avec vSphere 6.5 et versions ultérieures pour prendre en charge AES et krb5i)
Prise en charge des chemins d'accès	Non	Oui (ONTAP 9.14.1)

Connexion directe au réseau

Les administrateurs du stockage préfèrent parfois simplifier leurs infrastructures en supprimant les commutateurs réseau de la configuration. Cela peut être pris en charge dans certains scénarios.

ISCSI et NVMe/TCP

Un hôte utilisant iSCSI ou NVMe/TCP peut être directement connecté à un système de stockage et fonctionner normalement. La raison en est le chemin d'accès. Les connexions directes à deux contrôleurs de stockage distincts donnent lieu à deux chemins de flux de données indépendants. La perte du chemin, du port ou du contrôleur n'empêche pas l'autre chemin d'être utilisé.

NFS

Vous pouvez utiliser un stockage NFS à connexion directe, mais avec une limitation importante : le basculement ne fonctionnera pas sans script important, ce qui incombera au client.

Ce qui complique la reprise après incident avec un stockage NFS à connexion directe, c'est le routage qui se produit sur le système d'exploitation local. Par exemple, supposons qu'un hôte a une adresse IP 192.168.1.1/24 et qu'il est directement connecté à un contrôleur ONTAP avec une adresse IP 192.168.1.50/24. Lors du basculement, cette adresse 192.168.1.50 peut basculer vers l'autre contrôleur et sera disponible pour l'hôte, mais comment l'hôte peut-il détecter sa présence ? L'adresse 192.168.1.1 d'origine existe toujours sur la carte réseau hôte qui ne se connecte plus à un système opérationnel. Le trafic destiné à 192.168.1.50 continuerait d'être envoyé à un port réseau inutilisable.

Le second NIC du système d'exploitation peut être configuré sur 19 2.168.1.2 et serait capable de communiquer avec l'adresse en panne sur 192.168.1.50, mais les tables de routage locales auraient par défaut l'utilisation d'une adresse **et d'une seule adresse** pour communiquer avec le sous-réseau 192.168.1.0/24. Un administrateur système pourrait créer un framework de scripts qui détecterait une connexion réseau défaillante et modifierait les tables de routage locales ou rendrait les interfaces « up and down ». La procédure exacte dépend du système d'exploitation utilisé.

Dans la pratique, les clients NetApp disposent d'un protocole NFS à connexion directe, mais généralement uniquement pour les charges de travail où une pause des E/S est acceptable pendant les basculements. Lorsque des montages durs sont utilisés, aucune erreur d'E/S ne doit se produire lors de ces pauses. L'E/S doit se bloquer jusqu'à ce que les services soient restaurés, soit par un retour arrière, soit par une intervention manuelle pour déplacer les adresses IP entre les cartes réseau de l'hôte.

Connexion directe FC

Il n'est pas possible de connecter directement un hôte à un système de stockage ONTAP à l'aide du protocole FC. La raison en est l'utilisation de NPIV. Le WWN qui identifie un port FC ONTAP sur le réseau FC utilise un type de virtualisation appelé NPIV. Tout périphérique connecté à un système ONTAP doit pouvoir reconnaître un WWN NPIV. Aucun fournisseur actuel de HBA ne propose de HBA pouvant être installé sur un hôte et capable de prendre en charge une cible NPIV.

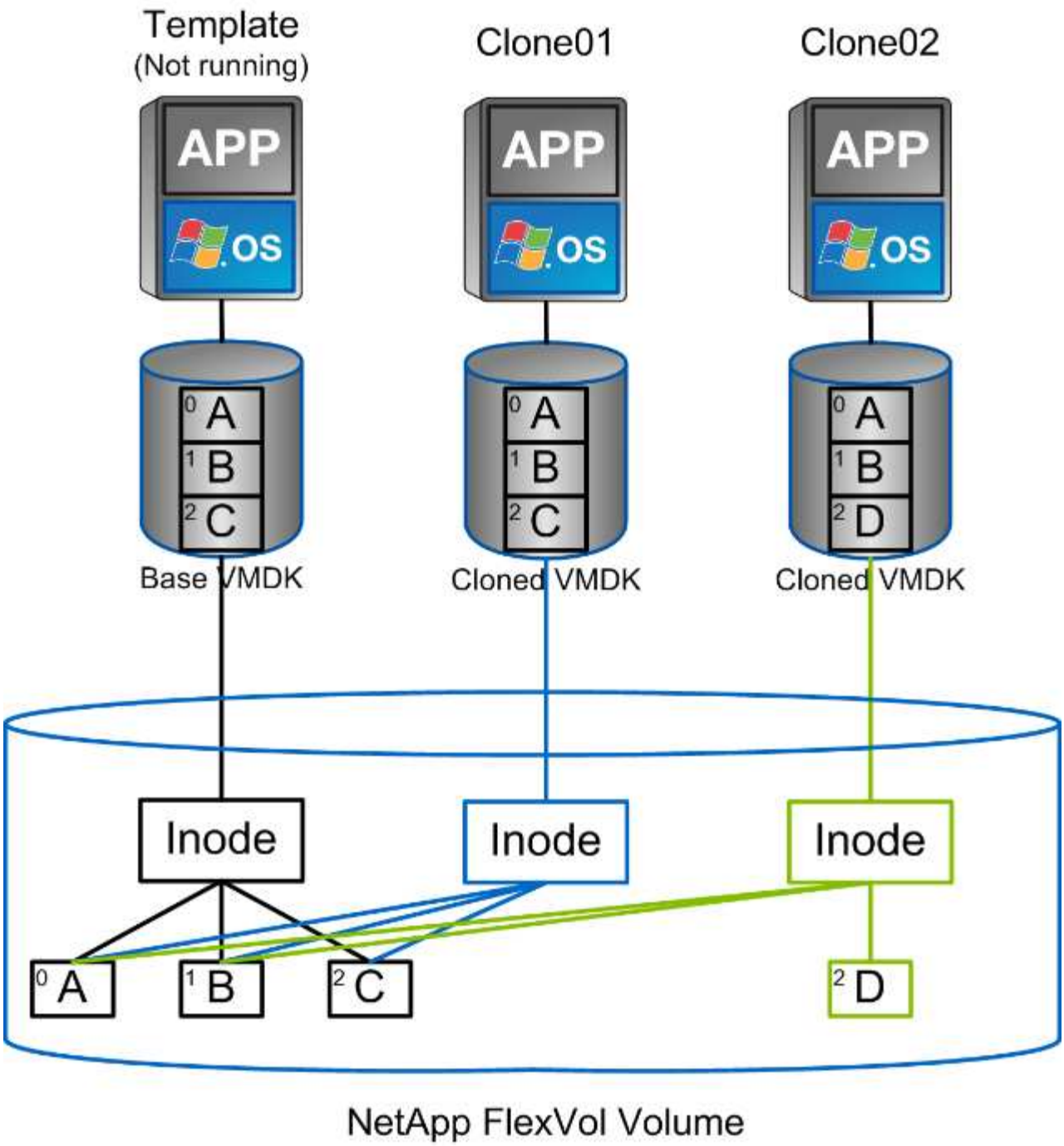
Clonage des VM et des datastores

Le clonage d'un objet de stockage vous permet de créer rapidement des copies pour ensuite les utiliser, par exemple le provisionnement de machines virtuelles supplémentaires, les opérations de sauvegarde/restauration, etc.

Dans vSphere, vous pouvez cloner une machine virtuelle, un disque virtuel, un volume virtuel ou un datastore. Une fois cloné, l'objet peut être davantage personnalisé, souvent par le biais d'un processus automatisé. VSphere prend en charge les clones de copie complète ainsi que les clones liés, pour assurer le suivi séparé des modifications apportées à l'objet d'origine.

Les clones liés permettent un gain d'espace considérable, mais ils augmentent la quantité d'E/S que vSphere gère pour la machine virtuelle, ce qui affecte les performances de cette machine virtuelle, et peut-être de l'hôte dans son ensemble. C'est pourquoi les clients NetApp utilisent souvent des clones basés sur des systèmes de stockage pour profiter d'un double avantage : une utilisation efficace du stockage et des performances supérieures.

La figure suivante représente le clonage ONTAP.



Le clonage peut être déchargé sur les systèmes qui exécutent le logiciel ONTAP via plusieurs mécanismes, en général au niveau de la machine virtuelle, du volume ou du datastore. Ces champs d'application incluent :

- Vvols avec le fournisseur NetApp vSphere APIs for Storage Awareness (VASA). Les clones ONTAP sont utilisés pour prendre en charge les snapshots vVol gérés par vCenter. Ces snapshots sont peu encombrants avec un impact E/S minimal en termes de création et de suppression. Les machines virtuelles peuvent également être clonées via vCenter, qui sont également déchargées vers ONTAP, que ce soit dans un datastore/volume unique ou entre les datastores/volumes.
- Clonage et migration de vSphere à l'aide des API vSphere – intégration de baies (VAAI). Les opérations de clonage de VM peuvent être déchargées sur ONTAP dans les environnements SAN et NAS (NetApp fournit un plug-in ESXi pour que VAAI for NFS). VSphere ne décharge les opérations sur les machines virtuelles inactives (désactivées) dans un datastore NAS, tandis que les opérations sur les machines virtuelles fortement sollicitées (clonage et stockage vMotion) sont également déchargées pour le système

SAN. ONTAP utilise l'approche la plus efficace selon la source, la destination et les licences des produits installés. Cette fonctionnalité est également utilisée par VMware Horizon View.

- SRA (utilisé avec VMware site Recovery Manager). Ici, des clones sont utilisés pour tester la restauration de la réplique de reprise après incident sans interruption.
- Sauvegarde et restauration à l'aide d'outils NetApp tels que SnapCenter. Les clones de machine virtuelle sont utilisés pour vérifier les opérations de sauvegarde ainsi que pour monter une sauvegarde de machine virtuelle, de sorte que les fichiers individuels puissent être copiés.

Le clonage ONTAP Offloaded peut être appelé par les outils VMware, NetApp et tiers. Les clones déchargés sur ONTAP présentent plusieurs avantages. Elles sont peu gourmandes en espace dans la plupart des cas, et n'ont besoin que de systèmes de stockage pour modifier les objets. Cela n'a aucun impact supplémentaire sur les performances en lecture et en écriture. Dans certains cas, le partage des blocs dans des caches haute vitesse améliore les performances. Ils délester également le serveur ESXi de la charge des cycles CPU et des E/S réseau. Il est possible de décharger des copies dans un data store traditionnel grâce à un volume FlexVol, de manière rapide et efficace avec une licence FlexClone, mais les copies entre volumes FlexVol peuvent être plus lentes. Si vous maintenez les modèles de machine virtuelle comme source de clones, envisagez de les placer dans le volume du datastore (utilisez les dossiers ou les bibliothèques de contenu pour les organiser) afin de créer des clones rapides et compacts.

Vous pouvez également cloner un volume ou une LUN directement au sein de ONTAP afin de cloner un datastore. Grâce aux datastores NFS, la technologie FlexClone peut cloner un volume entier. Le clone peut être exporté depuis ONTAP et monté par ESXi en tant qu'autre datastore. Pour les datastores VMFS, ONTAP peut cloner une LUN au sein d'un volume ou d'un volume complet, y compris une ou plusieurs LUN au sein de celle-ci. Une LUN contenant un VMFS doit être mappée sur un groupe d'initiateurs ESXi, puis une nouvelle signature définie par ESXi doit être montée et utilisée comme datastore standard. Pour certains cas d'utilisation temporaire, un VMFS cloné peut être monté sans nouvelle signature. Une fois le datastore cloné, les ordinateurs virtuels internes peuvent être enregistrés, reconfigurés et personnalisés comme s'ils étaient individuellement clonés.

Dans certains cas, des fonctionnalités supplémentaires sous licence peuvent être utilisées pour améliorer le clonage, telles que SnapRestore pour la sauvegarde ou FlexClone. Ces licences sont souvent incluses dans les packs de licence sans frais supplémentaires. Une licence FlexClone est requise pour les opérations de clonage vVol, ainsi que pour la prise en charge des snapshots gérés d'un VVol (qui sont déchargés de l'hyperviseur vers ONTAP). Une licence FlexClone peut également améliorer certains clones VAAI lorsqu'ils sont utilisés dans un datastore/volume (création de copies instantanées et compactes à la place de copies de bloc). Elle est également utilisée par SRA pour tester la restauration d'une réplique de reprise après incident et SnapCenter pour les opérations de clonage, et pour parcourir les copies de sauvegarde afin de restaurer des fichiers individuels.

Protection des données

La sauvegarde et la restauration rapide de vos machines virtuelles font partie des grands atouts de ONTAP pour vSphere. C'est facile à gérer au sein de vCenter grâce au plug-in SnapCenter pour VMware vSphere.

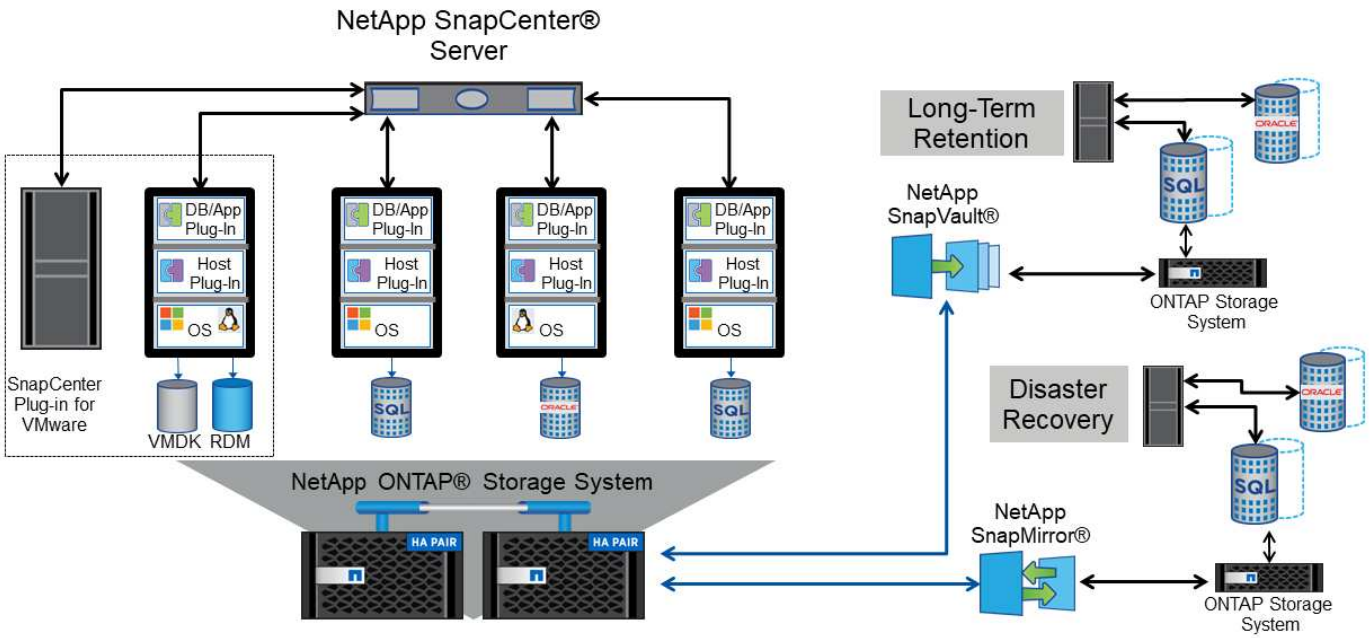
Utilisez les snapshots pour créer des copies rapides de votre machine virtuelle ou de votre datastore sans affecter les performances, puis envoyez-les à un système secondaire à l'aide de SnapMirror pour une protection des données hors site à plus long terme. Cette approche réduit l'espace de stockage et la bande passante réseau en stockant uniquement les informations modifiées.

SnapCenter vous permet de créer des règles de sauvegarde qui peuvent être appliquées à plusieurs tâches. Ces règles peuvent définir des fonctionnalités de planification, de conservation, de réplication et autres. Ils continuent d'autoriser la sélection facultative de snapshots cohérents avec les machines virtuelles, ce qui

exploite la capacité de l'hyperviseur à suspendre les E/S avant de prendre un snapshot VMware. Cependant, en raison de l'impact des snapshots VMware sur les performances, ils ne sont généralement pas recommandés sauf si vous devez suspendre le système de fichiers invité. Utilisez plutôt les snapshots pour une protection générale et des outils applicatifs tels que les plug-ins SnapCenter pour protéger les données transactionnelles comme SQL Server ou Oracle. Ces snapshots sont différents des snapshots VMware (cohérence) et sont adaptés à une protection à plus long terme. Les snapshots VMware ne sont que de "recommandé" pour une utilisation à court terme en raison de performances et d'autres effets.

Ces plug-ins offrent des fonctionnalités étendues pour protéger les bases de données dans les environnements physiques et virtuels. VSphere permet de protéger les bases de données SQL Server ou Oracle dans lesquelles les données sont stockées sur des LUN RDM, des LUN iSCSI directement connectées au système d'exploitation invité ou des fichiers VMDK dans des datastores VMFS ou NFS. Les plug-ins permettent de spécifier différents types de sauvegardes de bases de données, de prendre en charge les sauvegardes en ligne ou hors ligne, et de protéger les fichiers de bases de données avec les fichiers journaux. Outre la sauvegarde et la restauration, ces plug-ins prennent également en charge le clonage des bases de données à des fins de développement ou de test.

La figure suivante représente un exemple de déploiement SnapCenter.



Pour des fonctionnalités améliorées de reprise sur incident, utilisez l'outil NetApp SRA pour ONTAP avec VMware site Recovery Manager. Outre la prise en charge de la réplication de datastores sur un site de reprise après incident, il permet également d'effectuer des tests sans interruption dans l'environnement de reprise après incident en clonant les datastores répliqués. L'automatisation intégrée à SRA simplifie également la reprise après incident et la reprotection de la production après panne.

Enfin, pour obtenir le plus haut niveau de protection des données, pensez à une configuration VMware vSphere Metro Storage Cluster (vMSC) utilisant NetApp MetroCluster. VMSC est une solution certifiée VMware qui combine la réplication synchrone à la mise en cluster basée sur baie, offrant les mêmes avantages qu'un cluster haute disponibilité, mais distribuée sur des sites distincts pour une protection contre les incidents sur site. NetApp MetroCluster permet de réaliser des configurations économiques pour la réplication synchrone avec restauration transparente depuis n'importe quel composant de stockage défaillant, et récupération par commande unique en cas d'incident sur le site. VMSC est décrit plus en détail dans "TR-4128".

La qualité de service (QoS)

Les systèmes qui exécutent le logiciel ONTAP peuvent utiliser la fonctionnalité de QoS du stockage de ONTAP pour limiter le débit en Mbit/s et/ou E/S par seconde (IOPS) pour différents objets de stockage tels que des fichiers, des LUN, des volumes, ou des SVM entiers.

Les limites de débit sont utiles pour contrôler les charges de travail inconnues ou de test avant le déploiement afin de s'assurer qu'elles n'affectent pas les autres charges de travail. Elles peuvent également être utilisées pour contraindre une charge de travail dominante après son identification. Des niveaux minimaux de service basés sur des IOPS sont également pris en charge pour assurer des performances prévisibles pour les objets SAN d'ONTAP 9.2 et pour les objets NAS d'ONTAP 9.3.

Avec un datastore NFS, une politique de qualité de services peut s'appliquer à tout le volume FlexVol ou à tous les fichiers VMDK de l'environnement IT. Avec les datastores VMFS utilisant des LUN ONTAP, les règles de QoS peuvent être appliquées au volume FlexVol contenant les LUN ou les LUN individuels, mais pas aux fichiers VMDK individuels, car ONTAP ne connaît pas le système de fichiers VMFS. Lors de l'utilisation de vvols, il est possible de définir une qualité de service minimale et/ou maximale sur des machines virtuelles individuelles en utilisant le profil de capacité de stockage et la règle de stockage des machines virtuelles.

Le débit maximal de QoS sur un objet peut être défini en Mbit/s et/ou IOPS. Si les deux sont utilisés, la première limite atteinte est appliquée par ONTAP. Une charge de travail peut contenir plusieurs objets et une règle de QoS peut être appliquée à un ou plusieurs workloads. Lorsqu'une règle est appliquée à plusieurs workloads, celle-ci partage la limite totale de la règle. Les objets imbriqués ne sont pas pris en charge (par exemple, les fichiers d'un volume ne peuvent pas chacun avoir leur propre stratégie). La valeur minimale de qualité de service ne peut être définie que dans les IOPS.

Les outils suivants sont actuellement disponibles pour la gestion des règles de QoS de ONTAP et leur application aux objets :

- INTERFACE DE LIGNE DE COMMANDES DE ONTAP
- ONTAP System Manager
- OnCommand Workflow Automation
- Active IQ Unified Manager
- Kit d'outils NetApp PowerShell pour ONTAP
- Outils ONTAP pour VMware vSphere VASA Provider

Pour affecter une politique de QoS à un VMDK sur NFS, suivez les consignes suivantes :

- La politique doit être appliquée au `vmname- flat.vmdk` qui contient l'image réelle du disque virtuel, pas le `vmname.vmdk` (fichier de descripteur de disque virtuel) ou `vmname.vmx` (Fichier de descripteur de machine virtuelle).
- N'appliquez pas de règles aux autres fichiers VM tels que les fichiers d'échange virtuels (`vmname.vswp`).
- Lors de l'utilisation du client Web vSphere pour trouver des chemins de fichiers (datastore > fichiers), notez qu'il combine les informations de l' `- flat.vmdk` et `. vmdk` et montre simplement un fichier avec le nom du `. vmdk` mais la taille du `- flat.vmdk`. Autres `-flat` dans le nom du fichier pour obtenir le chemin correct.

Pour affecter une QoS à une LUN, y compris VMFS et RDM, le SVM ONTAP (affiché comme vServer), le chemin LUN et le numéro de série peuvent être obtenus du menu systèmes de stockage de la page d'accueil

des outils ONTAP pour VMware vSphere. Sélectionner le système de stockage (SVM), puis objets associés > SAN. Utilisez cette approche lors de la spécification de QoS à l'aide de l'un des outils ONTAP.

Il est possible de définir une qualité de service minimale et maximale facilement sur une machine virtuelle basée sur des volumes grâce aux outils ONTAP pour VMware vSphere ou Virtual Storage Console 7.1 et versions ultérieures. Lors de la création du profil de capacité de stockage pour le conteneur vVol, spécifiez une valeur IOPS max et/ou min sous la fonctionnalité de performance, puis indiquez ce SCP avec la stratégie de stockage de la VM. Utilisez cette règle lors de la création de la machine virtuelle ou appliquez-la à une machine virtuelle existante.

Les datastores FlexGroup offrent des fonctionnalités QoS améliorées lors de l'utilisation des outils ONTAP pour VMware vSphere 9.8 et versions ultérieures. Vous pouvez facilement définir la qualité de service sur toutes les machines virtuelles d'un datastore ou sur des machines virtuelles spécifiques. Consultez la section FlexGroup de ce rapport pour plus d'informations.

QoS ONTAP et SIOC VMware

La QoS ONTAP et la fonctionnalité VMware vSphere Storage I/O Control (SIOC) sont des technologies complémentaires que les administrateurs vSphere et du stockage peuvent utiliser ensemble pour gérer les performances des VM vSphere hébergées sur des systèmes exécutant le logiciel ONTAP. Chaque outil a ses propres forces, comme le montre le tableau suivant. En raison des différents champs d'application de VMware vCenter et de ONTAP, certains objets peuvent être vus et gérés par un système et non par l'autre.

Propriété	QoS de ONTAP	SIOC VMware
Lorsqu'il est actif	La règle est toujours active	Actif en cas de conflit (latence du datastore supérieure au seuil)
Type d'unités	IOPS, Mo/sec	IOPS, partages
Étendue vCenter ou des applications	Plusieurs environnements vCenter, d'autres hyperviseurs et applications	Un seul serveur vCenter
Définir la qualité de service sur la machine virtuelle ?	VMDK sur NFS uniquement	VMDK sur NFS ou VMFS
Définir la qualité de service sur la LUN (RDM) ?	Oui.	Non
Définir la QoS sur LUN (VMFS) ?	Oui.	Non
Définir la qualité de service sur le volume (datastore NFS) ?	Oui.	Non
Qualité de service définie sur un SVM (locataire) ?	Oui.	Non
Approche basée sur des règles ?	Oui. Elles peuvent être partagées par toutes les charges de travail dans la règle ou appliquées en totalité à chaque charge de travail dans la règle.	Oui, avec vSphere 6.5 et versions ultérieures.
Licence requise	Inclus avec ONTAP	Enterprise plus

Planificateur de ressources distribué de stockage VMware

VMware Storage Distributed Resource Scheduler (SDRS) est une fonctionnalité vSphere qui place les machines virtuelles sur un stockage en fonction de la latence d'E/S actuelle et de l'utilisation de l'espace. Il déplace ensuite la machine virtuelle ou les VMDK sans interruption entre les datastores d'un cluster de datastores (également appelé pod), en sélectionnant le meilleur datastore pour placer la machine virtuelle ou les VMDK dans le cluster de datastore. Un cluster de data stores est un ensemble de datastores similaires agrégés dans une unité de consommation unique du point de vue de l'administrateur vSphere.

Lorsque vous utilisez DES DTS avec les outils ONTAP pour VMware vSphere, vous devez d'abord créer un datastore avec le plug-in, utiliser vCenter pour créer le cluster de datastores, puis y ajouter le datastore. Une fois le cluster datastore créé, des datastores supplémentaires peuvent être ajoutés au cluster datastore directement à partir de l'assistant de provisionnement sur la page Détails.

Les autres meilleures pratiques ONTAP en matière DE SDRS sont les suivantes :

- Tous les datastores du cluster doivent utiliser le même type de stockage (SAS, SATA ou SSD, par exemple), être tous des datastores VMFS ou NFS et disposer des mêmes paramètres de réplication et de protection.
- Envisagez d'utiliser DES DTS en mode par défaut (manuel). Cette approche vous permet d'examiner les recommandations et de décider s'il faut les appliquer ou non. Notez les effets suivants des migrations VMDK :
  - Lorsque DES DTS déplacent des VMDK entre les datastores, les économies d'espace éventuelles obtenues grâce au clonage ou à la déduplication ONTAP sont perdues. Vous pouvez réexécuter la déduplication pour récupérer ces économies.
  - Une fois que les DTS ont déplacé les VMDK, NetApp recommande de recréer les snapshots au niveau du datastore source car l'espace est autrement verrouillé par la machine virtuelle déplacée.
  - Le déplacement des VMDK entre les datastores du même agrégat n'a que peu d'avantages et LES DTS n'ont pas de visibilité sur d'autres charges de travail qui pourraient partager l'agrégat.

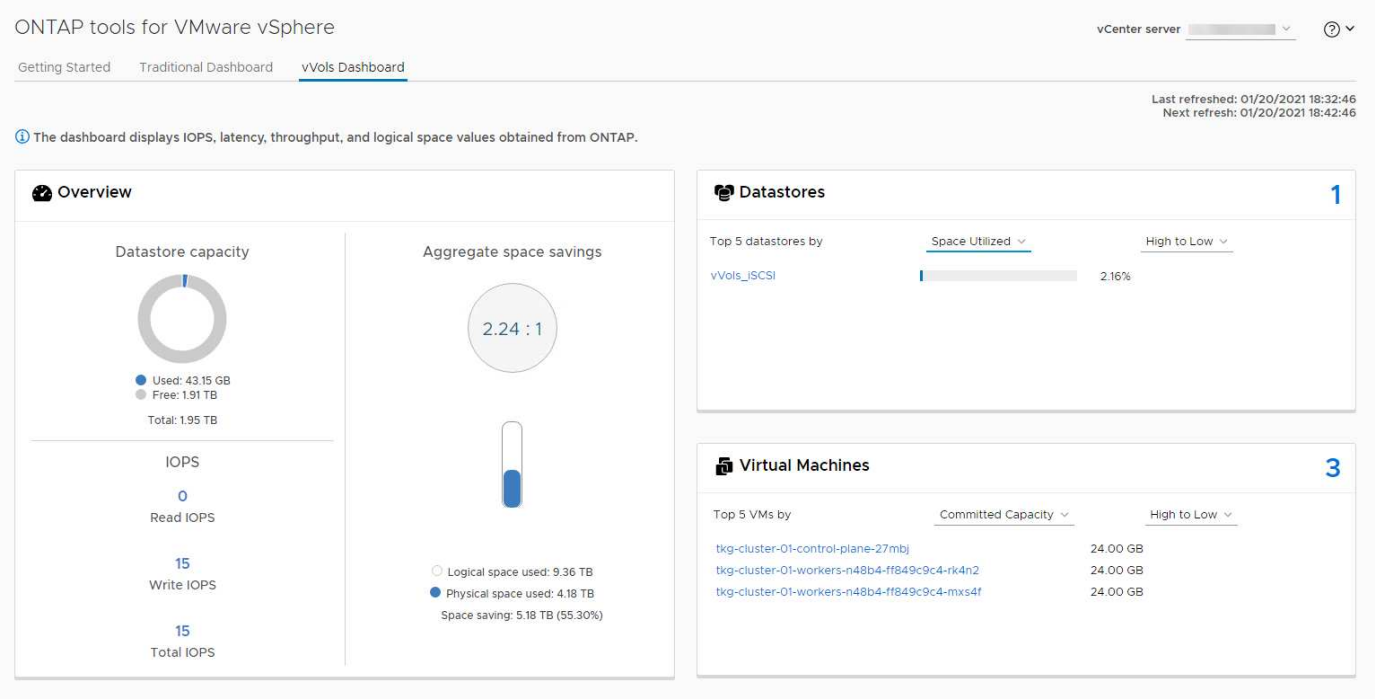
Gestion basée sur des règles de stockage et vVols

Les API VMware vSphere pour Storage Awareness (VASA) permettent à un administrateur du stockage de configurer des datastores avec des fonctionnalités bien définies et de permettre à l'administrateur des VM de les utiliser chaque fois que nécessaire pour provisionner des machines virtuelles sans avoir à interagir les unes avec les autres. Il est intéressant d'étudier cette approche pour savoir comment rationaliser vos opérations de stockage de virtualisation et éviter un travail insignifiant.

Avant de procéder à VASA, les administrateurs des VM pouvaient définir des règles de stockage des VM, mais ils devaient travailler avec l'administrateur du stockage pour identifier les datastores appropriés, souvent à l'aide de la documentation ou des conventions de nom. Grâce à VASA, l'administrateur du stockage peut définir un éventail de fonctionnalités de stockage, notamment la performance, le Tiering, le chiffrement et la réplication. Un ensemble de capacités pour un volume ou un ensemble de volumes est appelé « profil de capacité de stockage » (SCP).

Le SCP prend en charge la QoS minimale et/ou maximale pour les vVols de données d'une machine virtuelle. La QoS minimale est prise en charge uniquement sur les systèmes AFF. Les outils ONTAP pour VMware vSphere comprennent un tableau de bord affichant des performances granulaires de machine virtuelle et une capacité logique pour vVvols sur les systèmes ONTAP.

La figure suivante représente le tableau de bord des outils ONTAP pour VMware vSphere 9.8 vvols.



Une fois le profil de capacité de stockage défini, il peut être utilisé pour provisionner les machines virtuelles à l'aide de la règle de stockage qui identifie ses exigences. Le mappage entre la stratégie de stockage de la machine virtuelle et le profil de capacité de stockage du datastore permet à vCenter d'afficher la liste des datastores compatibles à sélectionner. Cette approche est appelée gestion basée sur des règles de stockage.

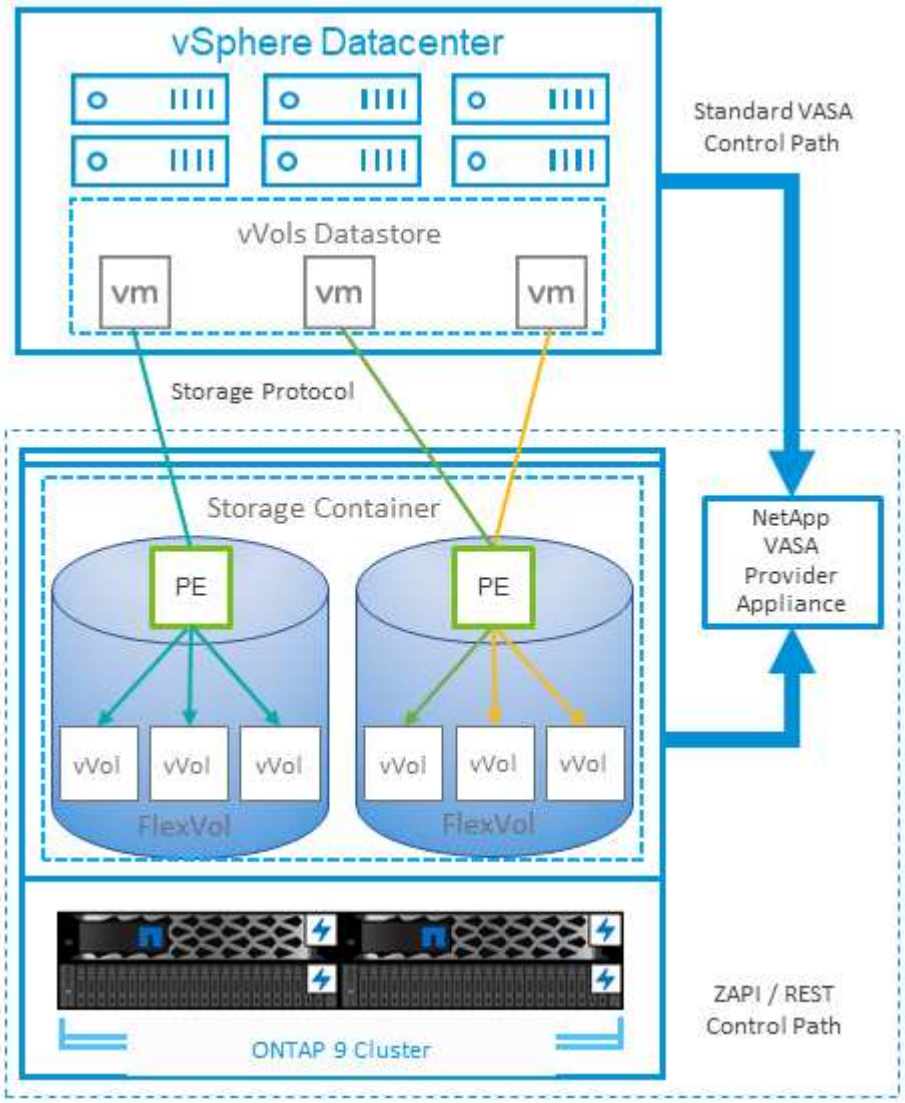
Vasa fournit la technologie permettant d'interroger le stockage et de renvoyer un ensemble de fonctionnalités de stockage vers vCenter. Les fournisseurs de VASA fournissent la traduction entre les API et les constructions du système de stockage et les API VMware que vCenter comprend. Le fournisseur VASA de NetApp pour ONTAP est proposé dans le cadre des outils ONTAP pour la machine virtuelle de l'appliance VMware vSphere. Le plug-in vCenter fournit l'interface de provisionnement et de gestion des datastores vVol, ainsi que la possibilité de définir des profils SCP (Storage Capability Profiles).

ONTAP prend en charge les datastores VMFS et NFS vvol. L'utilisation de vvols avec des datastores SAN apporte certains des avantages de NFS tels que la granularité au niveau des VM. Voici quelques meilleures pratiques à prendre en compte, et vous trouverez des informations supplémentaires dans le "TR-4400":

- Un datastore vvol peut être constitué de plusieurs volumes FlexVol sur plusieurs nœuds de cluster. L'approche la plus simple est un datastore unique, même si les volumes ont des capacités différentes. Grâce à la gestion du stockage basée sur des règles, un volume compatible est utilisé pour la machine virtuelle. Cependant, ces volumes doivent tous faire partie d'un seul SVM ONTAP et être accessibles via un seul protocole. Une LIF par nœud suffit pour chaque protocole. Évitez d'utiliser plusieurs versions de ONTAP dans un datastore vvol unique car les capacités de stockage peuvent varier d'une version à l'autre.
- Utilisez les outils ONTAP pour le plug-in VMware vSphere pour créer et gérer des datastores vvol. En plus de gérer le datastore et son profil, il crée automatiquement un terminal de protocole permettant d'accéder aux vvols si nécessaire. Si les LUN sont utilisées, notez que les terminaux PE sont mappés à l'aide des ID de LUN 300 et supérieurs. Vérifiez que le paramètre système avancé de l'hôte ESXi est défini `Disk.MaxLUN` Autorise un ID de LUN supérieur à 300 (la valeur par défaut est 1,024). Pour ce faire, sélectionnez l'hôte ESXi dans vCenter, puis l'onglet configurer et Rechercher `Disk.MaxLUN` Dans la liste des paramètres système avancés.
- N'installez pas ni ne migrez de VASA Provider, vCenter Server (appliance ou base Windows), ou les outils ONTAP pour VMware vSphere lui-même vers un datastore vvols, car ils sont ensuite interdépendants et limitent votre capacité à les gérer en cas de panne de courant ou d'autre perturbation du data Center.

- Sauvegarder régulièrement la machine virtuelle de VASA Provider. Créez au moins des copies Snapshot toutes les heures du datastore classique contenant VASA Provider. Pour en savoir plus sur la protection et la restauration de VASA Provider, consultez cette section "Article de la base de connaissances".

La figure suivante montre les composants de vvols.



Migration et sauvegarde dans le cloud

ONTAP permet également la prise en charge étendue du cloud hybride en fusionnant les systèmes de votre cloud privé sur site avec des capacités de cloud public. Voici quelques solutions clouds NetApp qui peuvent être utilisées en association avec vSphere :

- **Cloud volumes.** NetApp Cloud Volumes Service pour Amazon Web Services ou Google Cloud Platform et Azure NetApp Files pour ANF offrent des services de stockage gérés multiprotocole haute performance dans les principaux environnements de cloud public. Ils peuvent être utilisés directement par les invités de machine virtuelle VMware Cloud.
- **Cloud Volumes ONTAP.** le logiciel de gestion des données NetApp Cloud Volumes ONTAP permet de contrôler et de protéger les données et d'optimiser l'efficacité du stockage, tout en bénéficiant de la flexibilité du cloud de votre choix. Cloud Volumes ONTAP est un logiciel de gestion des données cloud basé sur le stockage ONTAP. Utilisez-les conjointement avec Cloud Manager pour déployer et gérer des instances Cloud Volumes ONTAP avec vos systèmes ONTAP sur site. Profitez des fonctionnalités NAS

avancées et SAN iSCSI combinées à la gestion unifiée des données, notamment les copies Snapshot et la réplication SnapMirror.

- **Services cloud.** utilisez Cloud Backup Service ou SnapMirror Cloud pour protéger les données des systèmes sur site qui utilisent un stockage de cloud public. Cloud Sync vous aide à migrer et à synchroniser vos données sur les systèmes NAS, les magasins d'objets et le stockage Cloud Volumes Service.
- **FabricPool.** FabricPool offre un Tiering simple et rapide pour les données ONTAP. Les blocs inactifs peuvent être migrés vers un magasin d'objets dans des clouds publics ou un magasin d'objets StorageGRID privé. Ils sont automatiquement rappelés lorsque vous accédez de nouveau aux données ONTAP. Vous pouvez également utiliser le Tier objet comme troisième niveau de protection pour les données déjà gérées par SnapVault. Cette approche peut vous permettre de "Stockez davantage de snapshots de vos machines virtuelles" Sur les systèmes de stockage ONTAP primaires et/ou secondaires.
- **ONTAP Select.** utilisez le stockage Software-defined NetApp pour étendre votre cloud privé sur Internet aux sites et bureaux distants, où vous pouvez utiliser ONTAP Select pour prendre en charge les services de blocs et de fichiers ainsi que les mêmes fonctionnalités de gestion de données vSphere que votre data Center d'entreprise.

Lors de la conception de vos applications basées sur une VM, pensez à la mobilité future du cloud. Par exemple, plutôt que de placer les fichiers d'application et de données en même temps que les fichiers de données, utilisez une exportation LUN ou NFS distincte. Cela vous permet de migrer la machine virtuelle et les données séparément vers des services cloud.

Chiffrement pour les données vSphere

Aujourd'hui, les exigences croissantes en matière de protection des données au repos sont liées au chiffrement. Bien que la priorité initiale ait été donnée aux informations financières et de santé, il est de plus en plus intéressant de protéger toutes les informations, qu'elles soient stockées dans des fichiers, des bases de données ou tout autre type de données.

Les systèmes qui exécutent le logiciel ONTAP simplifient la protection de toutes les données au repos. NetApp Storage Encryption (NSE) utilise des lecteurs de disque à chiffrement automatique avec ONTAP pour protéger les données SAN et NAS. NetApp propose également NetApp Volume Encryption et NetApp Aggregate Encryption comme une approche logicielle simple pour le chiffrement des volumes sur tous les disques. Ce chiffrement logiciel ne nécessite pas de disques spéciaux ni de gestionnaires de clés externes. Il est disponible gratuitement pour les clients ONTAP. Vous pouvez procéder à une mise à niveau et commencer à l'utiliser sans perturber vos clients ou applications. Elles sont validées par la norme FIPS 140-2 de niveau 1, y compris le gestionnaire de clés intégré.

Il existe plusieurs approches de protection des données des applications virtualisées qui s'exécutent sur VMware vSphere. L'une d'elles consiste à protéger les données avec les logiciels internes à la machine virtuelle au niveau du système d'exploitation invité. Les nouveaux hyperviseurs, tels que vSphere 6.5, prennent désormais en charge le cryptage au niveau des machines virtuelles. Cependant, le chiffrement logiciel NetApp est simple et facile :

- **Aucun effet sur la CPU du serveur virtuel.** certains environnements de serveurs virtuels nécessitent chaque cycle CPU disponible pour leurs applications, mais les tests ont montré que jusqu'à 5x ressources CPU sont nécessaires avec le cryptage au niveau de l'hyperviseur. Même si le logiciel de chiffrement prend en charge l'ensemble d'instructions AES-ni d'Intel pour décharger la charge de travail de chiffrement (comme le fait le chiffrement du logiciel NetApp), cette approche peut ne pas être possible en raison de l'exigence de nouveaux processeurs non compatibles avec les anciens serveurs.
- **Gestionnaire de clés intégré inclus.** le chiffrement logiciel NetApp inclut un gestionnaire de clés intégré sans frais supplémentaires, ce qui simplifie les prises en main sans serveurs de gestion des clés haute disponibilité complexes à acheter et à utiliser.

- **Aucun effet sur l'efficacité du stockage.** les techniques d'efficacité du stockage comme la déduplication et la compression sont largement utilisées aujourd'hui et sont essentielles pour exploiter les supports disque Flash de façon rentable. Toutefois, les données cryptées ne sont en général pas dédupliquées ou compressées. Le cryptage du stockage et du matériel NetApp fonctionne à un niveau inférieur et permet l'utilisation totale des fonctionnalités d'efficacité du stockage NetApp, contrairement aux autres approches.
- **Chiffrement granulaire simple des datastores.** avec NetApp Volume Encryption, chaque volume bénéficie de sa propre clé AES 256 bits. Si vous devez le modifier, utilisez une seule commande. Cette approche est idéale si vous disposez de plusieurs locataires ou si vous devez prouver votre chiffrement indépendant pour différents services ou applications. Ce chiffrement est géré au niveau du datastore, ce qui est bien plus simple que de gérer des machines virtuelles individuelles.

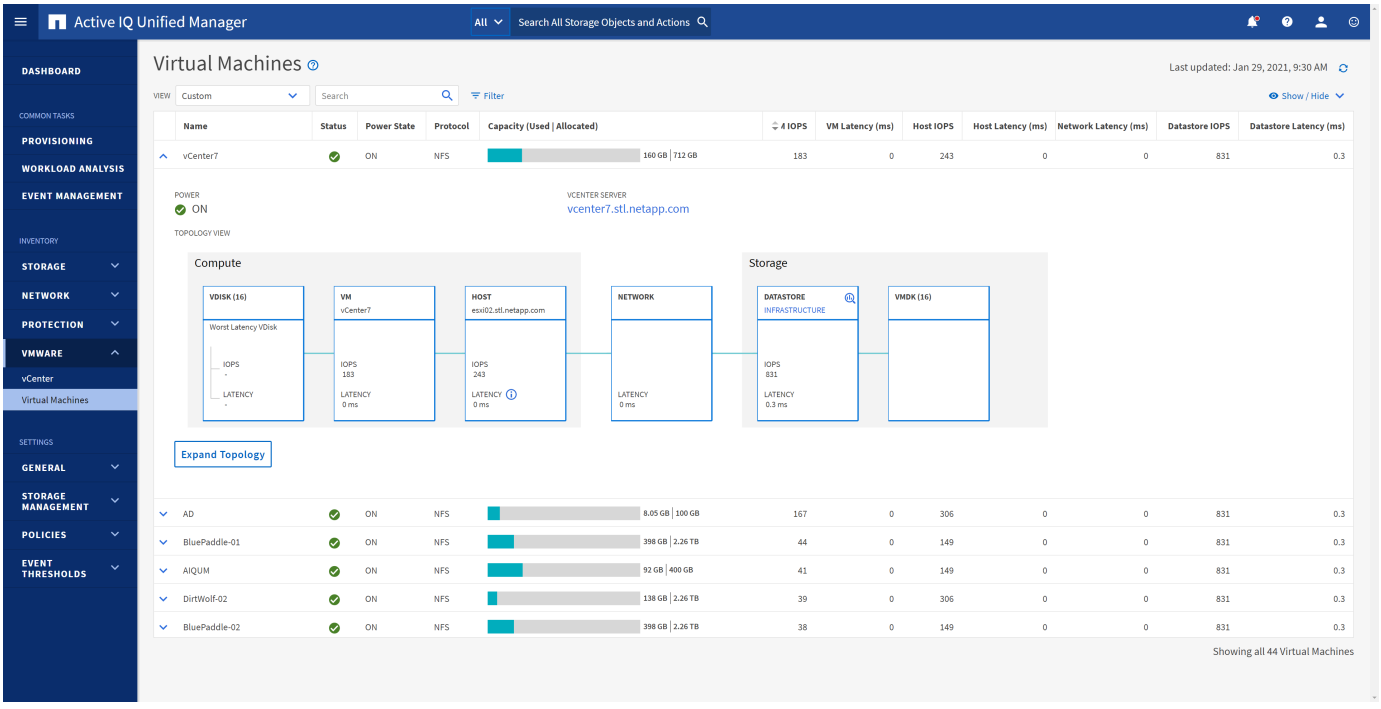
La prise en main du chiffrement logiciel est très simple. Une fois la licence installée, il vous suffit de configurer le gestionnaire de clés intégré en spécifiant une phrase secrète, puis de créer un volume ou de déplacer un volume côté stockage pour activer le chiffrement. NetApp travaille à ajouter une prise en charge plus intégrée des fonctionnalités de cryptage dans les prochaines versions de ses outils VMware.

Active IQ Unified Manager

Active IQ Unified Manager permet d'avoir une grande visibilité sur les machines virtuelles de votre infrastructure virtuelle et assure la surveillance et le dépannage des problèmes de stockage et de performances dans votre environnement virtuel.

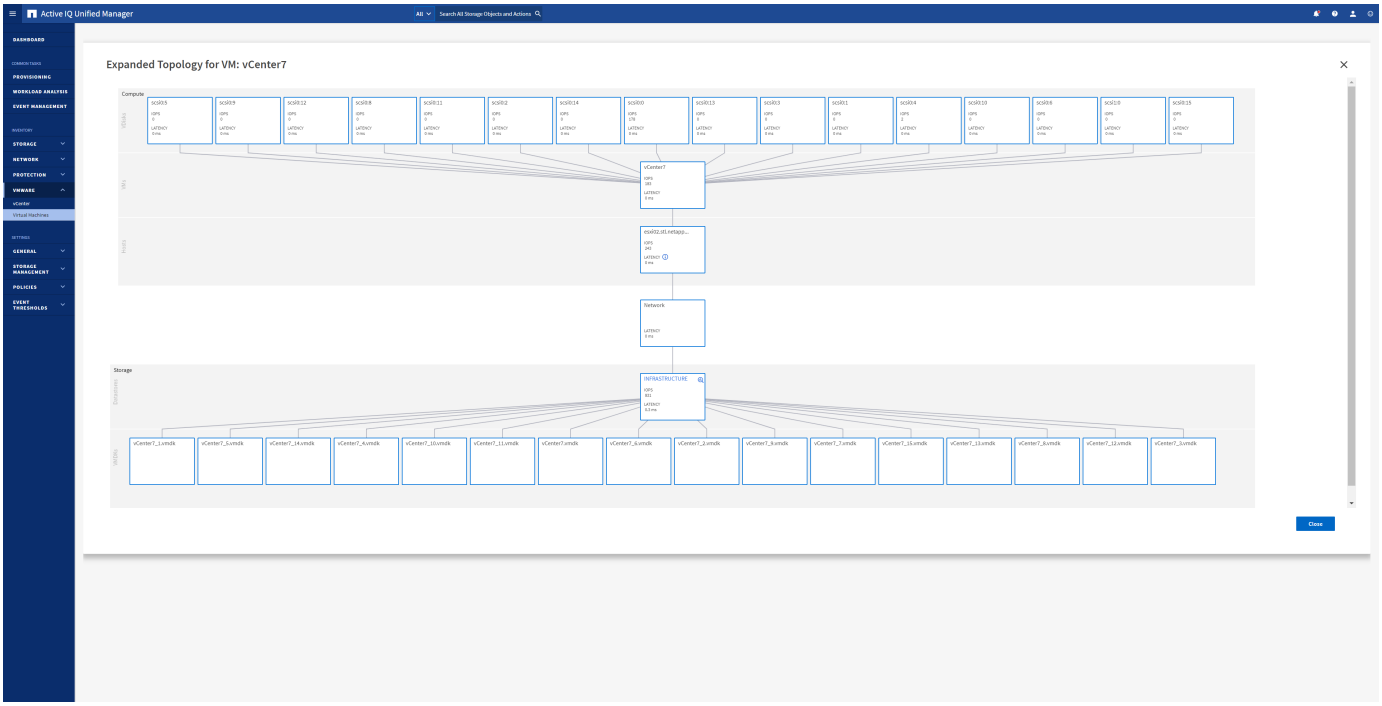
Un déploiement d'infrastructure virtuelle standard sur ONTAP comporte divers composants répartis sur les couches de calcul, de réseau et de stockage. Tout ralentissement des performances dans une application VM peut survenir en raison de la combinaison de latences rencontrées par les différents composants au niveau des couches respectives.

La capture d'écran suivante présente la vue des machines virtuelles Active IQ Unified Manager.



Unified Manager présente le sous-système sous-jacent d'un environnement virtuel dans une vue topologique afin de déterminer si un problème de latence a eu lieu dans le nœud de calcul, le réseau ou le stockage. La vue indique également l'objet spécifique qui provoque le décalage des performances lors de la réalisation des étapes correctives et de la résolution du problème sous-jacent.

La capture d’écran suivante montre la topologie étendue AIQUM.



Gestion basée sur des règles de stockage et vVols

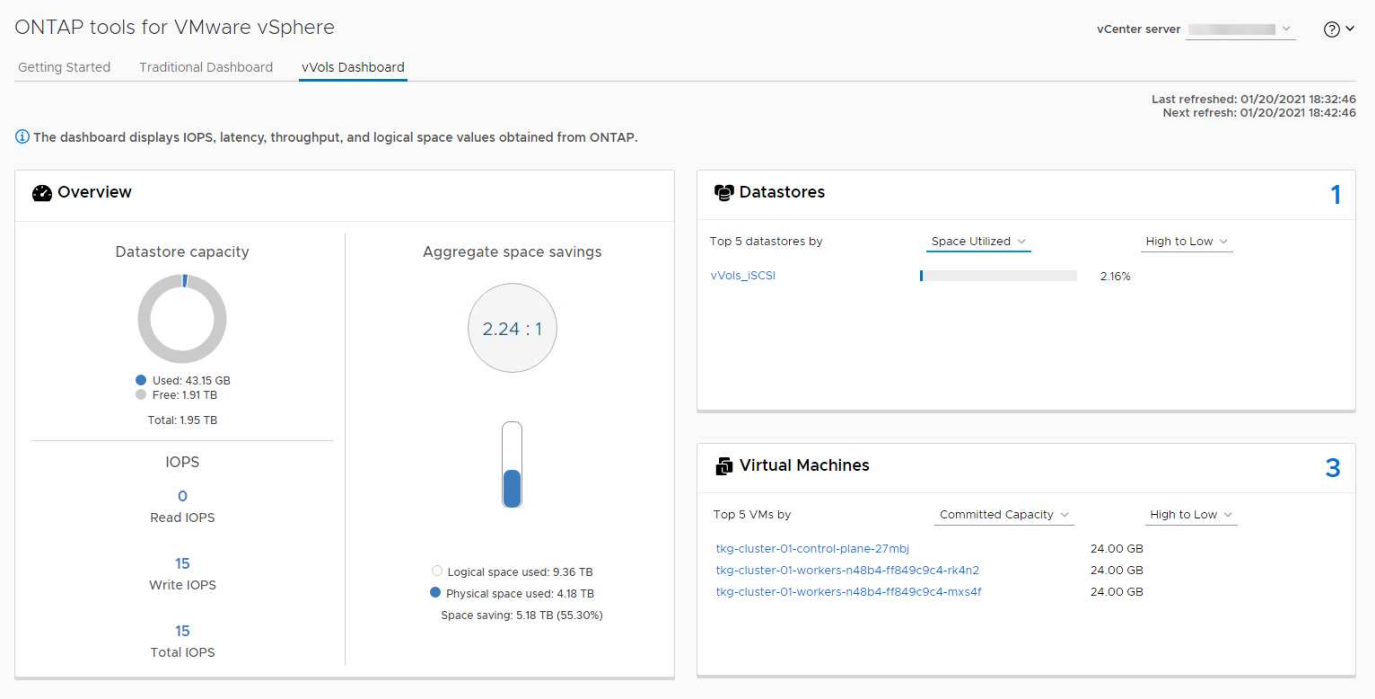
Les API VMware vSphere pour Storage Awareness (VASA) permettent à un administrateur du stockage de configurer des datastores avec des fonctionnalités bien définies et de permettre à l’administrateur des VM de les utiliser chaque fois que nécessaire pour provisionner des machines virtuelles sans avoir à interagir les unes avec les autres.

Il est intéressant d’étudier cette approche pour savoir comment rationaliser vos opérations de stockage de virtualisation et éviter un travail insignifiant.

Avant de procéder à VASA, les administrateurs des VM pouvaient définir des règles de stockage des VM, mais ils devaient travailler avec l’administrateur du stockage pour identifier les datastores appropriés, souvent à l’aide de la documentation ou des conventions de nom. Grâce à VASA, l’administrateur du stockage peut définir un éventail de fonctionnalités de stockage, notamment la performance, le Tiering, le chiffrement et la réplication. Un ensemble de capacités pour un volume ou un ensemble de volumes est appelé « profil de capacité de stockage » (SCP).

Le SCP prend en charge la QoS minimale et/ou maximale pour les vVols de données d’une machine virtuelle. La QoS minimale est prise en charge uniquement sur les systèmes AFF. Les outils ONTAP pour VMware vSphere comprennent un tableau de bord affichant des performances granulaires de machine virtuelle et une capacité logique pour vVvols sur les systèmes ONTAP.

La figure suivante représente le tableau de bord des outils ONTAP pour VMware vSphere 9.8 vvols.



Une fois le profil de capacité de stockage défini, il peut être utilisé pour provisionner les machines virtuelles à l'aide de la règle de stockage qui identifie ses exigences. Le mappage entre la stratégie de stockage de la machine virtuelle et le profil de capacité de stockage du datastore permet à vCenter d'afficher la liste des datastores compatibles à sélectionner. Cette approche est appelée gestion basée sur des règles de stockage.

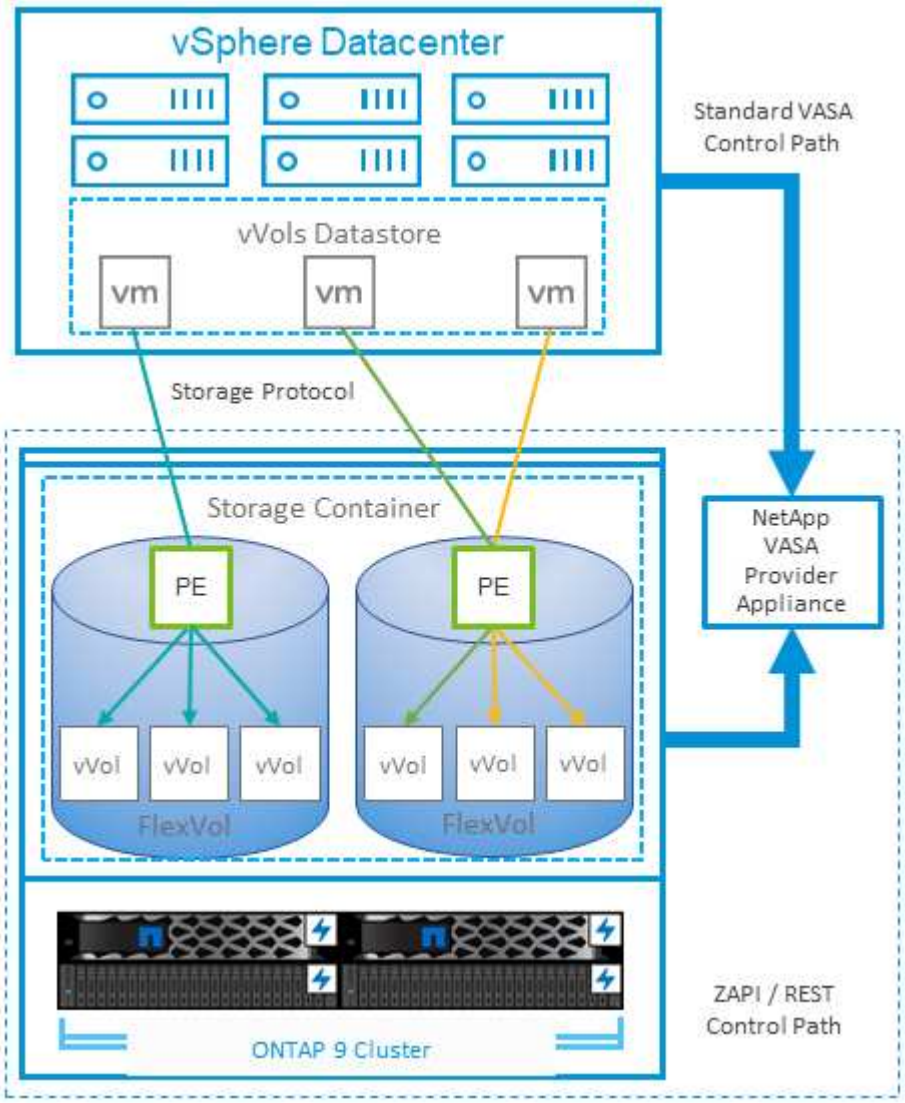
Vasa fournit la technologie permettant d'interroger le stockage et de renvoyer un ensemble de fonctionnalités de stockage vers vCenter. Les fournisseurs de VASA fournissent la traduction entre les API et les constructions du système de stockage et les API VMware que vCenter comprend. Le fournisseur VASA de NetApp pour ONTAP est proposé dans le cadre des outils ONTAP pour la machine virtuelle de l'appliance VMware vSphere. Le plug-in vCenter fournit l'interface de provisionnement et de gestion des datastores vVol, ainsi que la possibilité de définir des profils SCP (Storage Capability Profiles).

ONTAP prend en charge les datastores VMFS et NFS vvol. L'utilisation de vvols avec des datastores SAN apporte certains des avantages de NFS tels que la granularité au niveau des VM. Voici quelques meilleures pratiques à prendre en compte, et vous trouverez des informations supplémentaires dans le "TR-4400":

- Un datastore vvol peut être constitué de plusieurs volumes FlexVol sur plusieurs nœuds de cluster. L'approche la plus simple est un datastore unique, même si les volumes ont des capacités différentes. Grâce à la gestion du stockage basée sur des règles, un volume compatible est utilisé pour la machine virtuelle. Cependant, ces volumes doivent tous faire partie d'un seul SVM ONTAP et être accessibles via un seul protocole. Une LIF par nœud suffit pour chaque protocole. Évitez d'utiliser plusieurs versions de ONTAP dans un datastore vvol unique car les capacités de stockage peuvent varier d'une version à l'autre.
- Utilisez les outils ONTAP pour le plug-in VMware vSphere pour créer et gérer des datastores vvol. En plus de gérer le datastore et son profil, il crée automatiquement un terminal de protocole permettant d'accéder aux vvols si nécessaire. Si les LUN sont utilisées, notez que les terminaux PE sont mappés à l'aide des ID de LUN 300 et supérieurs. Vérifiez que le paramètre système avancé de l'hôte ESXi est défini `Disk.MaxLUN` Autorise un ID de LUN supérieur à 300 (la valeur par défaut est 1,024). Pour ce faire, sélectionnez l'hôte ESXi dans vCenter, puis l'onglet configurer et Rechercher `Disk.MaxLUN` Dans la liste des paramètres système avancés.
- N'installez pas ni ne migrez de VASA Provider, vCenter Server (appliance ou base Windows), ou les outils ONTAP pour VMware vSphere lui-même vers un datastore vvols, car ils sont ensuite interdépendants et limitent votre capacité à les gérer en cas de panne de courant ou d'autre perturbation du data Center.

- Sauvegarder régulièrement la machine virtuelle de VASA Provider. Créez au moins des copies Snapshot toutes les heures du datastore classique contenant VASA Provider. Pour en savoir plus sur la protection et la restauration de VASA Provider, consultez cette section "Article de la base de connaissances".

La figure suivante montre les composants de vvols.



Planificateur de ressources distribué de stockage VMware

VMware Storage Distributed Resource Scheduler (SDRS) est une fonctionnalité vSphere qui place les machines virtuelles sur un stockage en fonction de la latence d'E/S actuelle et de l'utilisation de l'espace.

Il déplace ensuite la machine virtuelle ou les VMDK sans interruption entre les datastores d'un cluster de datastores (également appelé pod), en sélectionnant le meilleur datastore pour placer la machine virtuelle ou les VMDK dans le cluster de datastore. Un cluster de data stores est un ensemble de datastores similaires agrégés dans une unité de consommation unique du point de vue de l'administrateur vSphere.

Lorsque vous utilisez DES DTS avec les outils ONTAP pour VMware vSphere, vous devez d'abord créer un datastore avec le plug-in, utiliser vCenter pour créer le cluster de datastores, puis y ajouter le datastore. Une fois le cluster datastore créé, des datastores supplémentaires peuvent être ajoutés au cluster datastore

directement à partir de l'assistant de provisionnement sur la page Détails.

Les autres meilleures pratiques ONTAP en matière DE SDRS sont les suivantes :

- Tous les datastores du cluster doivent utiliser le même type de stockage (SAS, SATA ou SSD, par exemple), être tous des datastores VMFS ou NFS et disposer des mêmes paramètres de réplication et de protection.
- Envisagez d'utiliser DES DTS en mode par défaut (manuel). Cette approche vous permet d'examiner les recommandations et de décider s'il faut les appliquer ou non. Notez les effets suivants des migrations VMDK :
  - Lorsque DES DTS déplacent des VMDK entre les datastores, les économies d'espace éventuelles obtenues grâce au clonage ou à la déduplication ONTAP sont perdues. Vous pouvez réexécuter la déduplication pour récupérer ces économies.
  - Une fois que les DTS ont déplacé les VMDK, NetApp recommande de recréer les snapshots au niveau du datastore source car l'espace est autrement verrouillé par la machine virtuelle déplacée.
  - Le déplacement des VMDK entre les datastores du même agrégat n'a que peu d'avantages et LES DTS n'ont pas de visibilité sur d'autres charges de travail qui pourraient partager l'agrégat.

Hôte ESXi recommandé et autres paramètres ONTAP recommandés

NetApp a développé un ensemble de paramètres hôtes ESXi optimaux pour les protocoles NFS et les protocoles en mode bloc. Des conseils spécifiques sont également fournis concernant les paramètres de chemins d'accès multiples et de délai d'expiration des HBA pour un comportement correct avec ONTAP basé sur les tests internes NetApp et VMware.

Ces valeurs sont facilement définies à l'aide des outils ONTAP pour VMware vSphere : dans le tableau de bord Résumé, cliquez sur Modifier les paramètres dans le portlet systèmes hôtes ou cliquez avec le bouton droit de la souris sur l'hôte dans vCenter, puis accédez à Outils ONTAP > définir les valeurs recommandées.

Voici les paramètres d'hôte actuellement recommandés pour les versions 9.8-9.13.

Paramètres hôte	Valeur recommandée par NetApp	Redémarrer requis
Configuration avancée ESXi		
VMFS3.HardwareAccélérationde la localisation	Conserver la valeur par défaut (1)	Non
VMFS3.EnableBlockDelete	Conserver la valeur par défaut (0), mais peut être modifiée si nécessaire. Pour plus d'informations, voir "VMware KB 2007427"	Non
VMFS3.EnableVMFS6Unmap	Conserver la valeur par défaut (1) Pour plus d'informations, voir "API VMware vSphere : intégration des baies (VAAI)"	Non
Paramètres NFS		

Net.TcpipeHeapSize	VSphere 6.0 ou version ultérieure, défini sur 32. Toutes les autres configurations NFS, définies sur 30	Oui.
Net.TcpipeHeapMax	Défini sur 512 Mo pour la plupart des versions vSphere 6.X. Défini sur 1024 Mo pour 6.5U3, 6.7U3 et 7.0 ou version ultérieure.	Oui.
NFS.MaxVolumes	VSphere 6.0 ou version ultérieure, défini sur 256 Toutes les autres configurations NFS définies sur 64.	Non
NFS41.Maxvolumes	VSphere 6.0 ou version ultérieure, défini sur 256.	Non
NFS.MaxQueueDepth[1]	VSphere 6.0 ou version ultérieure, défini sur 128	Oui.
NFS.HeartbeatMaxFailures	Définissez sur 10 pour l'ensemble des configurations NFS	Non
NFS.HeartbeatFrequency	Définissez la valeur 12 pour toutes les configurations NFS	Non
NFS.HeartbeatTimeout	Définissez sur 5 pour l'ensemble des configurations NFS.	Non
Sunrpc.MaxConnPerIP	VSphere 7.0 ou version ultérieure, défini sur 128.	Non
Paramètres FC/FCoE		
Stratégie de sélection de chemin	Définissez-le sur RR (Round Robin) lorsque des chemins FC avec ALUA sont utilisés. Défini sur FIXE pour toutes les autres configurations. La définition de cette valeur sur RR permet d'équilibrer la charge sur l'ensemble des chemins actifs/optimisés. La valeur FIXÉE est pour les anciennes configurations non ALUA et contribue à empêcher les E/S proxy En d'autres termes, il contribue à empêcher les E/S de se diriger vers l'autre nœud d'une paire haute disponibilité dans un environnement doté de Data ONTAP 7-mode	Non
Disk.QFullSampleSize	Définissez sur 32 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.	Non

Disk.QFullThreshold	Réglez à 8 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.	Non
Délais d'expiration de la carte HBA FC Emulex	Utilisez la valeur par défaut.	Non
Délais de connexion HBA FC QLogic	Utilisez la valeur par défaut.	Non
Paramètres iSCSI		
Stratégie de sélection de chemin	Définissez à RR (Round Robin) pour tous les chemins iSCSI. La définition de cette valeur sur RR permet d'équilibrer la charge sur l'ensemble des chemins actifs/optimisés.	Non
Disk.QFullSampleSize	Définissez sur 32 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.	Non
Disk.QFullThreshold	Réglez à 8 pour toutes les configurations. La définition de cette valeur permet d'éviter les erreurs d'E/S.	Non

1 : l'option de configuration avancée NFS MaxQueueDepth peut ne pas fonctionner comme prévu avec VMware vSphere ESXi 7.0.1 et VMware vSphere ESXi 7.0.2. Veuillez vous reporter à "VMware KB 86331" pour en savoir plus.

Lors de la création de volumes et de LUN ONTAP FlexVol, les outils ONTAP permettent également de spécifier certains paramètres par défaut :

Outil ONTAP	Paramètre par défaut
Réserve Snapshot (-percent-snapshot-space)	0
Réserve fractionnaire (-réserve fractionnaire)	0
Mise à jour de l'heure d'accès (-atime-update)	Faux
Lecture minimum (-min-lecture anticipée)	Faux
Snapshots planifiés	Aucune
Efficacité du stockage	Activé
Garantie de volume	Aucune (provisionnement fin)
Taille automatique du volume	augmenter_réduire
Réservation d'espace par LUN	Désactivé
Allocation d'espace de la LUN	Activé

Paramètres de chemins d'accès multiples pour les performances

Bien qu'il ne soit pas actuellement configuré par les outils ONTAP disponibles, NetApp suggère les options de configuration suivantes :

- Dans les environnements hautes performances ou lors des tests de performances avec un seul datastore LUN, envisagez de modifier le paramètre d'équilibrage de charge de la règle de sélection de chemin Round-Robin (VMW_PSP_RR) entre la valeur de 1000 IOPS par défaut et la valeur de 1. Voir VMware KB "2069356" pour en savoir plus.
- Dans vSphere 6.7 mise à jour 1, VMware a introduit un nouveau mécanisme d'équilibrage de la charge de latence pour la PSP Round Robin. La nouvelle option prend en compte la bande passante d'E/S et la latence de chemin lors de la sélection du chemin optimal pour les E/S. Vous pouvez tirer parti de son utilisation dans des environnements dotés d'une connectivité de chemin non équivalente, tels que des cas avec plus de sauts réseau sur un chemin qu'un autre, ou lors de l'utilisation d'un système NetApp All SAN Array. Voir "Plug-ins et règles de sélection de chemin" pour en savoir plus.

Documentation complémentaire

Pour plus d'informations sur FCP et iSCSI avec vSphere 7, consultez la page "Utilisez VMware vSphere 7.x avec ONTAP"
Pour plus d'informations sur FCP et iSCSI avec vSphere 8, consultez la page "Utilisez VMware vSphere 8.x avec ONTAP"
Pour plus d'informations sur la spécification NVMe-of avec vSphere 7, rendez-vous sur la page "Pour plus de détails sur NVMe-of, consultez la page Configuration d'hôte NVMe-of pour ESXi 7.x avec ONTAP"
Pour plus d'informations sur la spécification NVMe-of avec vSphere 8, rendez-vous sur la page "Pour plus de détails sur NVMe-of, consultez la page Configuration d'hôte NVMe-of pour ESXi 8.x avec ONTAP"

Volumes virtuels (vVols) avec ONTAP

Présentation

ONTAP est une solution de stockage leader pour les environnements VMware vSphere depuis plus de vingt ans et continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts.

Ce document présente les fonctionnalités de ONTAP pour les volumes virtuels VMware vSphere (vVols), notamment les dernières informations sur les produits et les cas d'utilisation, ainsi que les bonnes pratiques et d'autres informations permettant de rationaliser le déploiement et de réduire les erreurs.

Cette documentation remplace les rapports techniques *TR-4400 : VMware vSphere Virtual volumes (vVols) par ONTAP*

Les meilleures pratiques complètent d'autres documents, tels que des guides et des listes de compatibilité. Ils sont développés en fonction de tests effectués en laboratoire et d'une vaste expérience sur le terrain par les ingénieurs et les clients NetApp. Ce ne sont peut-être pas les seules pratiques qui fonctionnent ou sont prises en charge, mais sont généralement les solutions les plus simples qui répondent aux besoins de la plupart des clients.

Ce document a été mis à jour pour inclure les nouvelles fonctionnalités vVols de vSphere 8.0 mise à jour 1 prises en charge par la version 9.12 des outils ONTAP.

Présentation des volumes virtuels (vVols)

En 2012, NetApp a commencé à travailler avec VMware pour prendre en charge les API vSphere pour Storage Awareness (VASA) pour vSphere 5. Ce premier VASA Provider a autorisé la définition des fonctionnalités de stockage dans un profil qui pouvait être utilisé pour filtrer les datastores lors du provisionnement et pour vérifier par la suite la conformité avec la règle. Cette évolution a vu le jour, de nouvelles fonctionnalités permettant d'automatiser davantage le provisionnement, ainsi que l'ajout de volumes virtuels ou de vVols où des objets de stockage individuels sont utilisés pour les fichiers de machines virtuelles et les disques virtuels. Il peut s'agir de LUN, de fichiers et désormais de vSphere 8. NVMe namespaces.NetApp a étroitement collaboré avec VMware en tant que partenaire de référence pour les vVols publiés avec vSphere 6 en 2015, puis en tant que partenaire de conception pour les vVols utilisant NVMe over Fabrics dans vSphere 8. NetApp continue d'améliorer les vVols pour tirer parti des dernières fonctionnalités d'ONTAP.

Plusieurs composants doivent être pris en compte :

VASA Provider
Il s'agit du composant logiciel qui gère la communication entre VMware vSphere et le système de stockage. Pour ONTAP, le fournisseur VASA s'exécute dans une appliance connue sous le nom d'outils ONTAP pour VMware vSphere (outils ONTAP pour, par exemple). Les outils ONTAP incluent également un plug-in vCenter, un adaptateur de réplication du stockage (SRA) pour VMware site Recovery Manager et un serveur d'API REST pour vous permettre de créer votre propre automatisation. Une fois les outils ONTAP configurés et enregistrés dans vCenter, il est désormais peu nécessaire d'interagir directement avec le système ONTAP, puisque la quasi-totalité de vos besoins en stockage peut être gérée directement depuis l'interface utilisateur vCenter ou via l'automatisation de l'API REST.
Point de terminaison de protocole (PE)
Le terminal de protocole est un proxy pour les E/S entre les hôtes ESXi et le datastore vVols. Le fournisseur ONTAP VASA les crée automatiquement, soit une LUN de terminal de protocole (4 Mo) par volume FlexVol du datastore vVols, soit un point de montage NFS par interface NFS (LIF) sur le nœud de stockage hébergeant un volume FlexVol dans le datastore. L'hôte ESXi monte ces terminaux de protocole directement plutôt que des LUN vVol individuelles et des fichiers de disque virtuel. Il n'est pas nécessaire de gérer les terminaux PE lorsqu'ils sont créés, montés, démontés et supprimés automatiquement par le fournisseur VASA, avec les groupes d'interfaces ou les règles d'exportation nécessaires.
Point de terminaison de protocole virtuel (VPE)
Nouveauté de vSphere 8, lorsque NVMe over Fabrics (NVMe-of) avec vVols, le concept de terminal de protocole n'est plus pertinent dans ONTAP. Au lieu de cela, un PE virtuel est instancié automatiquement par l'hôte ESXi pour chaque groupe ANA dès que la première machine virtuelle est sous tension. ONTAP crée automatiquement des groupes ANA pour chaque volume FlexVol utilisé par le datastore. Autre avantage de NVMe-of pour les vVols : aucune demande de liaison n'est requise du fournisseur VASA. À la place, l'hôte ESXi gère en interne la fonctionnalité de liaison vVol basée sur le VPE. Cela réduit les risques d'impact d'une tempête de liaison vVol sur le service. Pour plus d'informations, voir "NVMe et les volumes virtuels" marche "vmware.com"
Datastore de volume virtuel

Le datastore de volume virtuel est une représentation de datastore logique d'un conteneur vVols créée et gérée par un fournisseur VASA. Le conteneur représente un pool de capacité de stockage provisionné à partir des systèmes de stockage gérés par le fournisseur VASA. Les outils ONTAP prennent en charge l'allocation de plusieurs volumes FlexVol (appelés « volumes de sauvegarde ») à un datastore vVols unique. Ces datastores vVols peuvent couvrir plusieurs nœuds dans un cluster ONTAP, combinant des systèmes Flash et hybrides ayant des fonctionnalités différentes. L'administrateur peut créer de nouveaux volumes FlexVol à l'aide de l'assistant de provisionnement ou de l'API REST, ou sélectionner des volumes FlexVol précréés pour la sauvegarde du stockage, le cas échéant.
Volumes virtuels (vVols)
VVols sont les fichiers et disques de machines virtuelles réellement stockés dans le datastore vVols. L'utilisation du terme vVol (singulier) fait référence à un fichier, une LUN ou un espace de nom spécifique unique. ONTAP crée des namespaces NVMe, des LUN ou des fichiers en fonction du protocole utilisé par le datastore. Il existe plusieurs types distincts de vVols : les plus courants sont Config (fichiers de métadonnées), Data (disque virtuel ou VMDK) et Swap (créé lorsque la machine virtuelle est sous tension). Les vVols protégées par le chiffrement de machines virtuelles VMware seront de type autre. Le chiffrement des machines virtuelles VMware ne doit pas être confondu avec le chiffrement du volume ou de l'agrégat ONTAP.

Gestion stratégique

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

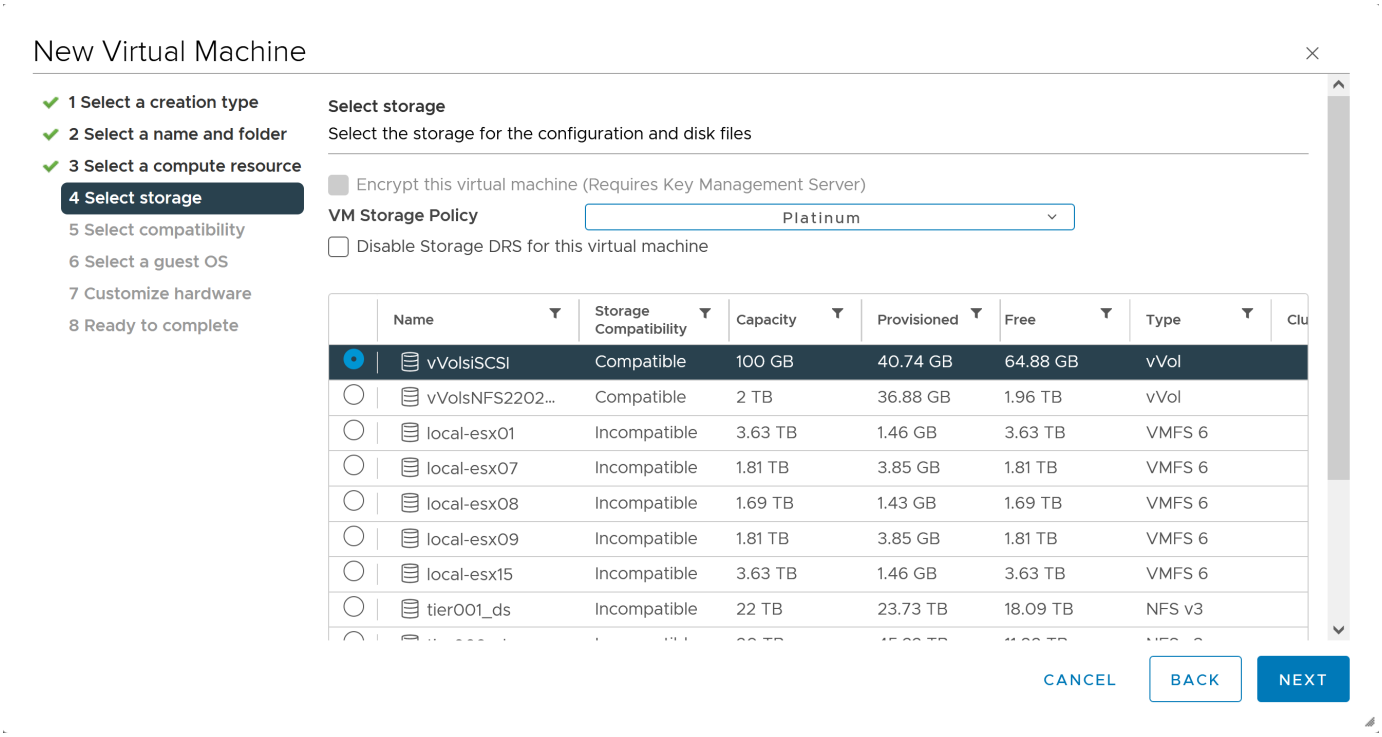
Il existe deux éléments :

Profil de capacité de stockage (SCP)
Un profil de capacité de stockage (SCP) est un modèle de stockage qui permet à l'administrateur vCenter de définir les fonctionnalités de stockage dont ils ont besoin sans avoir à comprendre comment gérer ces fonctionnalités dans ONTAP. En adoptant une approche de type modèle, il permet à l'administrateur de fournir facilement des services de stockage de manière cohérente et prévisible. Les fonctionnalités décrites dans un SCP incluent les performances, le protocole, l'efficacité du stockage et d'autres fonctionnalités. Les fonctionnalités spécifiques varient selon la version. Leur création s'est effectuée à l'aide du menu ONTAP Tools for VMware vSphere de l'interface utilisateur vCenter. Vous pouvez également utiliser des API REST pour créer des SCP. Elles peuvent être créées manuellement en sélectionnant des fonctionnalités individuelles ou générées automatiquement à partir de datastores existants (traditionnels).
Stratégie de stockage VM

Les règles de stockage de serveur virtuel sont créées dans vCenter sous stratégies et profils. Pour les vVols, créez un jeu de règles à l'aide de règles provenant du fournisseur de type de stockage NetApp vVols. Les outils ONTAP offrent une approche simplifiée en vous permettant de sélectionner simplement un SCP plutôt que de vous obliger à spécifier des règles individuelles.

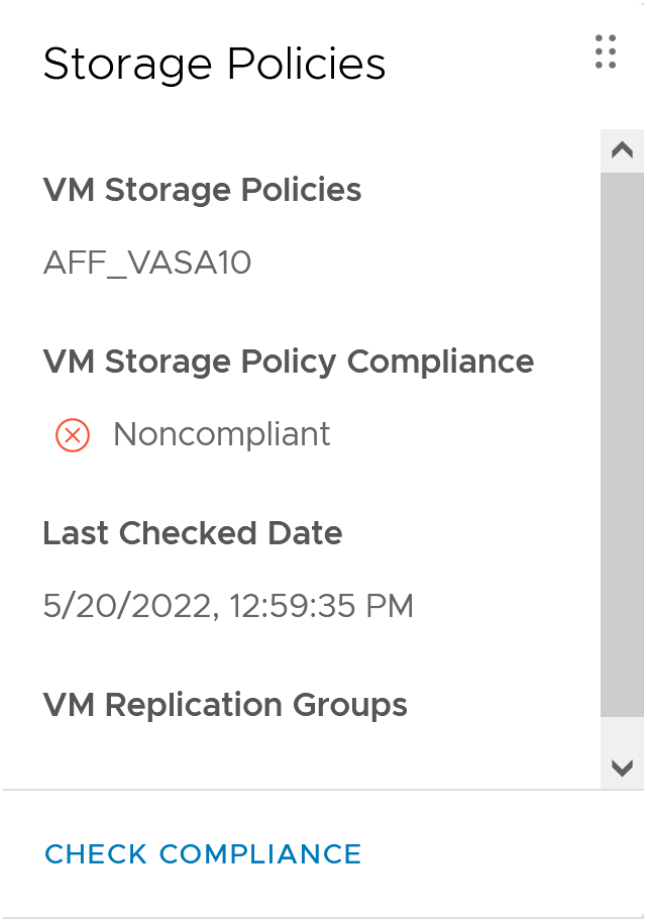
Comme mentionné ci-dessus, l'utilisation des règles peut aider à rationaliser le provisionnement d'un volume. Il suffit de sélectionner une règle appropriée, et le fournisseur VASA affiche les datastores vVols qui prennent en charge cette règle et place le vVol dans un volume FlexVol individuel conforme (Figure 1).

Déployer une machine virtuelle à l'aide de la stratégie de stockage



Une fois qu'une machine virtuelle est provisionnée, le fournisseur VASA continue à vérifier la conformité et alerte l'administrateur de la machine virtuelle en cas d'alarme dans vCenter lorsque le volume de sauvegarde n'est plus conforme à la règle (Figure 2).

Conformité à la règle de stockage VM



Prise en charge des vVols de NetApp

ONTAP prend en charge la spécification VASA depuis sa sortie initiale en 2012. Si d'autres systèmes de stockage NetApp peuvent prendre en charge VASA, ce document est axé sur les versions actuellement prises en charge de ONTAP 9.

ONTAP

Outre ONTAP 9 sur les systèmes AFF, ASA et FAS, NetApp prend en charge les workloads VMware sur ONTAP Select, Amazon FSX pour NetApp avec VMware Cloud sur AWS, Azure NetApp Files avec la solution Azure VMware, Cloud Volumes Service avec Google Cloud VMware Engine et le stockage privé NetApp dans Equinix, mais certaines fonctionnalités peuvent varier en fonction du fournisseur de services et de la connectivité réseau disponible. L'accès, depuis les invités vSphere, aux données stockées dans ces configurations ainsi qu'à Cloud Volumes ONTAP est également disponible.

Au moment de la publication, les environnements hyperscale sont limités aux datastores NFS v3 classiques. Par conséquent, les vVols ne sont disponibles que pour les systèmes ONTAP sur site ou les systèmes connectés au cloud qui offrent l'ensemble des fonctionnalités d'un système sur site, tels que ceux hébergés par les partenaires et fournisseurs de services NetApp à travers le monde.

Pour plus d'informations sur ONTAP, voir "Documentation des produits ONTAP"

Pour plus d'informations sur les meilleures pratiques ONTAP et VMware vSphere, voir "TR-4597"

Avantages de l'utilisation de vVols avec ONTAP

Lorsque VMware a introduit la prise en charge de vVols avec VASA 2.0 en 2015, ils l'ont décrite comme « une

structure d'intégration et de gestion fournissant un nouveau modèle opérationnel pour le stockage externe (SAN/NAS) ». Ce modèle opérationnel présente plusieurs avantages avec le stockage ONTAP.

Gestion stratégique

Comme décrit à la section 1.2, la gestion basée sur des règles permet de provisionner les machines virtuelles et de les gérer par la suite à l'aide de règles prédéfinies. Les opérations INFORMATIQUES peuvent ainsi être réalisées de plusieurs manières :

- **Augmentez la vitesse.** les outils ONTAP éliminent la nécessité pour l'administrateur vCenter d'ouvrir des tickets avec l'équipe chargée du stockage pour les activités de provisionnement du stockage. Cependant, les rôles RBAC des outils ONTAP dans vCenter et sur le système ONTAP permettent toujours l'accès à des équipes indépendantes (telles que les équipes chargées du stockage) ou à des activités indépendantes par la même équipe en limitant l'accès à des fonctions spécifiques si nécessaire.
- **Provisionnement plus intelligent.** les fonctionnalités du système de stockage peuvent être exposées via les API VASA, ce qui permet aux flux de travail de provisionnement de tirer parti de fonctionnalités avancées sans que l'administrateur des machines virtuelles ait besoin de comprendre comment gérer le système de stockage.
- **Provisionnement plus rapide.** différentes capacités de stockage peuvent être prises en charge dans un seul datastore et sélectionnées automatiquement comme approprié pour une machine virtuelle en fonction de la stratégie de la machine virtuelle.
- **Évitez les erreurs.** les stratégies de stockage et de machines virtuelles sont développées à l'avance et appliquées selon les besoins sans avoir à personnaliser le stockage à chaque fois qu'une machine virtuelle est provisionnée. Les alarmes de conformité sont déclenchées lorsque les fonctionnalités de stockage sont différentes des règles définies. Comme mentionné précédemment, les plateformes SCP rendent le provisionnement initial prévisible et reproductible, tandis que la base des règles de stockage des serveurs virtuels sur les plateformes SCP garantit un placement précis.
- **Meilleure gestion de la capacité.** les outils VASA et ONTAP permettent de visualiser la capacité de stockage jusqu'au niveau de l'agrégat industriel si nécessaire et de fournir plusieurs couches d'alertes en cas de début d'exécution de la capacité.

Gestion granulaire des machines virtuelles dans le SAN moderne

Les systèmes DE stockage SAN utilisant Fibre Channel et iSCSI ont été les premiers à être pris en charge par VMware pour ESX, mais ils n'ont pas été en mesure de gérer les disques et les fichiers individuels des machines virtuelles à partir du système de stockage. Au lieu de cela, les LUN sont provisionnées et VMFS gère les fichiers individuels. Il est donc difficile pour le système de stockage de gérer directement les performances, le clonage et la protection du stockage des machines virtuelles individuelles. Les vVols apportent la granularité du stockage dont les clients utilisent déjà le stockage NFS, et les fonctionnalités SAN robustes et hautes performances de ONTAP.

Désormais, avec vSphere 8 et les outils ONTAP pour VMware vSphere 9.12 et versions ultérieures, les mêmes contrôles granulaires utilisés par les vVols pour les anciens protocoles SCSI sont désormais disponibles dans le SAN Fibre Channel moderne utilisant NVMe over Fabrics pour des performances encore plus élevées à grande échelle. Avec vSphere 8.0 mise à jour 1, il est désormais possible de déployer une solution NVMe de bout en bout complète à l'aide de vVols sans déplacement d'E/S dans la pile de stockage de l'hyperviseur.

Meilleures fonctionnalités de déchargement du stockage

Tandis que VAAI offre de nombreuses opérations qui sont déchargées vers le stockage, certaines lacunes sont traitées par le fournisseur VASA. SAN VAAI ne peut pas décharger les snapshots gérés par VMware vers le système de stockage. NFS VAAI peut décharger les snapshots gérés par les machines virtuelles, mais il existe des limites placées pour les machines virtuelles avec des snapshots natifs de stockage. Étant donné que les

vVols utilisent des LUN, des espaces de noms ou des fichiers individuels pour des disques de machines virtuelles, ONTAP peut rapidement et efficacement cloner les fichiers ou les LUN pour créer des snapshots granulaires de machines virtuelles qui ne nécessitent plus de fichiers delta. NFS VAAI ne prend pas non plus en charge les opérations de déchargement des clones pour les migrations Storage vMotion à chaud (basées sur). La machine virtuelle doit être mise hors tension pour permettre la décharge de la migration lors de l'utilisation de VAAI avec des datastores NFS classiques. Le fournisseur VASA des outils ONTAP permet des clones quasi instantanés et efficaces du stockage pour les migrations à chaud et à froid, et prend également en charge les copies quasi instantanées pour les migrations de volumes croisés de vVols. En raison de ces avantages considérables en matière d'efficacité du stockage, vous pouvez tirer pleinement parti des workloads vVols sous le "Garantie d'efficacité" programme. De même, si les clones multi-volumes à l'aide de VAAI ne répondent pas à vos besoins, vous serez probablement en mesure de relever vos défis business grâce aux améliorations apportées à l'expérience de copie des vVols.

Cas d'utilisation courants des vVols

Outre ces avantages, plusieurs cas d'utilisation courants sont également mentionnés ci-dessous pour le stockage vVol :

- **Provisionnement à la demande des machines virtuelles**
  - Cloud privé ou IaaS d'un Service Provider.
  - Exploitez l'automatisation et l'orchestration via la suite Aria (anciennement vRealize), OpenStack, etc
- **Disques de première classe (FCDS)**
  - Volumes persistants VMware Tanzu Kubernetes Grid [TKG].
  - Proposez des services Amazon EBS avec une gestion indépendante du cycle de vie VMDK.
- **Approvisionnement à la demande des machines virtuelles temporaires**
  - Laboratoires de test et de développement
  - Environnements de formation

Bénéfices communs avec les vVols

Lorsqu'ils sont utilisés à leur plein avantage, comme dans les cas d'utilisation ci-dessus, les vVols apportent les améliorations spécifiques suivantes :

- La création de clones est rapide au sein d'un seul volume ou sur plusieurs volumes d'un cluster ONTAP. C'est un avantage par rapport aux clones classiques compatibles VAAI. Ils sont également efficaces en termes de stockage. Les clones d'un volume utilisent un clone de fichier ONTAP, qui ressemble aux volumes FlexClone et ne stockent que les modifications du fichier vVol source, de la LUN ou de l'espace de noms. Ainsi, les machines virtuelles à long terme pour la production ou d'autres applications sont créées rapidement, prennent un minimum d'espace et peuvent bénéficier de la protection au niveau des machines virtuelles (à l'aide du plug-in NetApp SnapCenter pour VMware vSphere, des snapshots gérés par VMware ou de la sauvegarde VADP) et de la gestion des performances (avec ONTAP QoS).
- Les vVols sont la technologie de stockage idéale lors de l'utilisation de TKG avec vSphere CSI, fournissant des classes et des capacités de stockage distinctes gérées par l'administrateur vCenter.
- Les services de type Amazon EBS peuvent être fournis via les disques FCD, car un VMDK FCD, comme son nom l'indique, est citoyen de premier ordre dans vSphere et possède un cycle de vie qui peut être géré de manière indépendante, indépendamment des machines virtuelles auxquelles il peut être rattaché.

Utilisation de vVols avec ONTAP

La clé de l'utilisation des vVols avec ONTAP est le logiciel VASA Provider inclus dans les

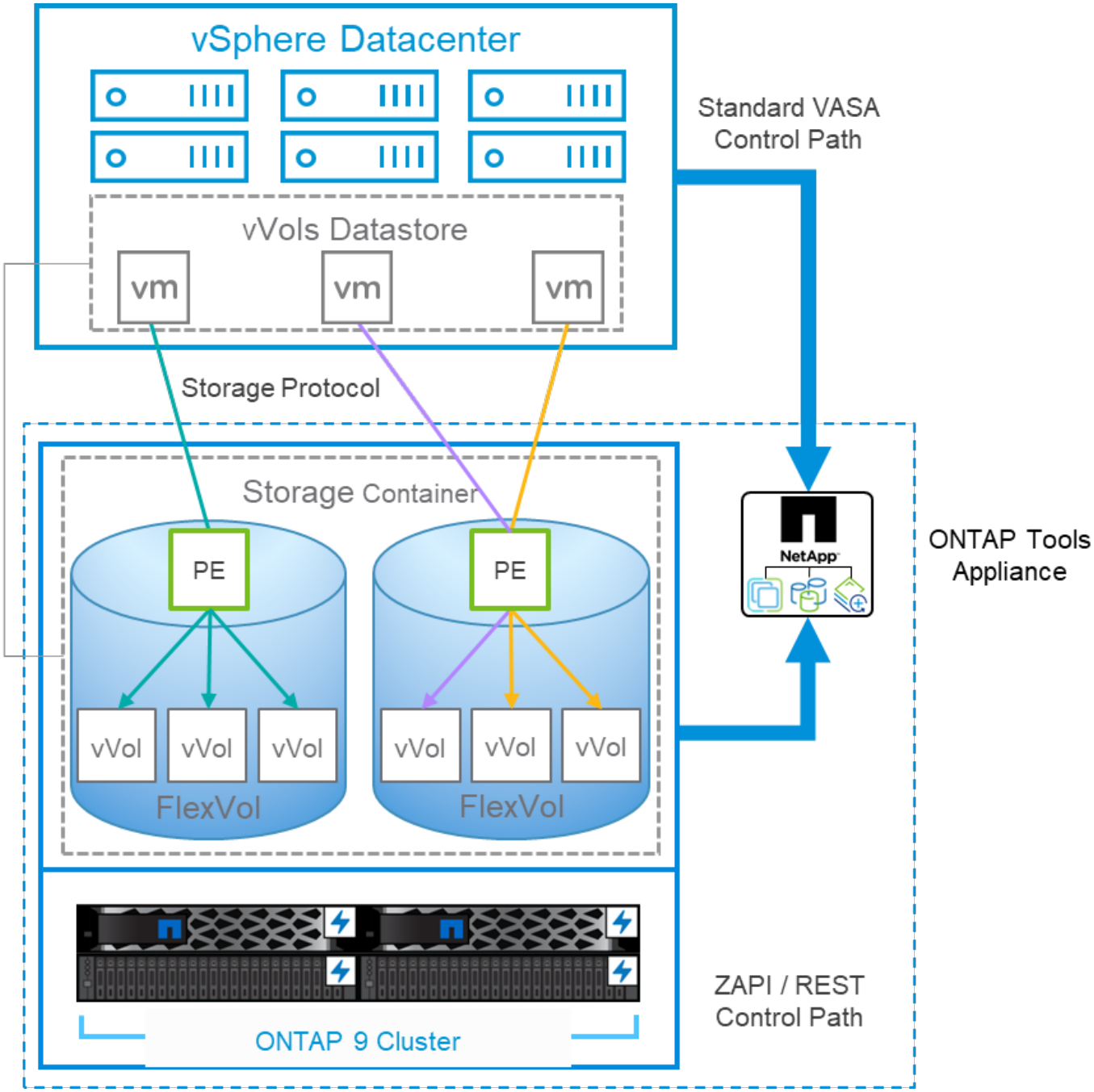
outils ONTAP pour l’appliance virtuelle VMware vSphere.

Les outils ONTAP incluent également les extensions de l’interface utilisateur vCenter, le serveur d’API REST, Storage Replication adapter pour VMware site Recovery Manager, les outils de surveillance et de configuration de l’hôte, ainsi qu’un ensemble de rapports qui vous aident à mieux gérer votre environnement VMware.

Produits et documentation

La licence ONTAP FlexClone (incluse avec ONTAP ONE) et l’appliance ONTAP Tools sont les seuls produits supplémentaires requis pour utiliser les vVols avec ONTAP. Les dernières versions des outils ONTAP sont fournies sous la forme d’une appliance unifiée unique qui s’exécute sur ESXi, et qui offre les fonctionnalités de trois dispositifs et serveurs auparavant différents. Pour les vVols, il est important d’utiliser les extensions de l’interface utilisateur vCenter de l’outil ONTAP ou les API REST en tant qu’outils de gestion généraux et interfaces utilisateur pour les fonctions ONTAP avec vSphere, ainsi que le fournisseur VASA qui offre des fonctionnalités vVols spécifiques. Le composant SRA est inclus pour les datastores classiques, mais VMware site Recovery Manager n’utilise pas SRA pour les vVols pour la mise en œuvre de nouveaux services dans SRM 8.3 et versions ultérieures, qui utilisent VASA Provider pour la réplication des vVols.

Architecture VASA Provider des outils ONTAP lors de l’utilisation d’iSCSI ou FCP



Installation du produit

Pour les nouvelles installations, déployez l'appliance virtuelle dans votre environnement vSphere. Les versions actuelles des outils ONTAP s'inscrivent automatiquement dans votre vCenter et activent le fournisseur VASA par défaut. Outre les informations sur l'hôte ESXi et vCenter Server, vous devez également disposer des détails de configuration de l'adresse IP de l'appliance. Comme indiqué précédemment, le fournisseur VASA nécessite que la licence ONTAP FlexClone soit déjà installée sur les clusters ONTAP que vous prévoyez d'utiliser pour les vVols. Le dispositif est doté d'un dispositif de surveillance intégré pour garantir la disponibilité et, dans le cadre des meilleures pratiques, doit être configuré avec les fonctions VMware High Availability et éventuellement Fault Tolerance. Voir la section 4.1 pour plus de détails. N'installez pas et ne déplacez pas l'appliance ONTAP Tools ou l'appliance vCenter Server (VCSA) vers le stockage vVols, car cela peut empêcher le redémarrage des appliances.

Les mises à niveau des outils ONTAP sur place sont prises en charge grâce au fichier ISO de mise à niveau

disponible en téléchargement sur le site du support NetApp (NSS). Suivez les instructions du Guide de déploiement et de configuration pour mettre à niveau l'appliance.

Pour le dimensionnement de votre appliance virtuelle et la compréhension des limites de configuration, reportez-vous à l'article suivant de la base de connaissances : "Guide de dimensionnement des outils ONTAP pour VMware vSphere"

Documentation produit

La documentation suivante est disponible pour vous aider à déployer les outils ONTAP.

"Pour consulter le référentiel de documentation complet et accéder à la page 44, cliquez sur ce lien : docs.netapp.com"

Commencez

- "Notes de mise à jour"
- "En savoir plus sur les outils ONTAP pour VMware vSphere"
- "Outils ONTAP démarrage rapide"
- "Déployez les outils ONTAP"
- "Mettez à niveau les outils ONTAP"

Utilisez les outils ONTAP

- "Provisionner les datastores classiques"
- "Provisionner des datastores vVols"
- "Configurez le contrôle d'accès basé sur des rôles"
- "Configurer les diagnostics à distance"
- "Configurez la haute disponibilité"

Protéger et gérer les datastores

- "Protection des datastores classiques" Avec SRM
- "Protection des machines virtuelles basées sur vVols" Avec SRM
- "Surveiller les datastores classiques et les machines virtuelles"
- "Surveillez les datastores vvols et les machines virtuelles"

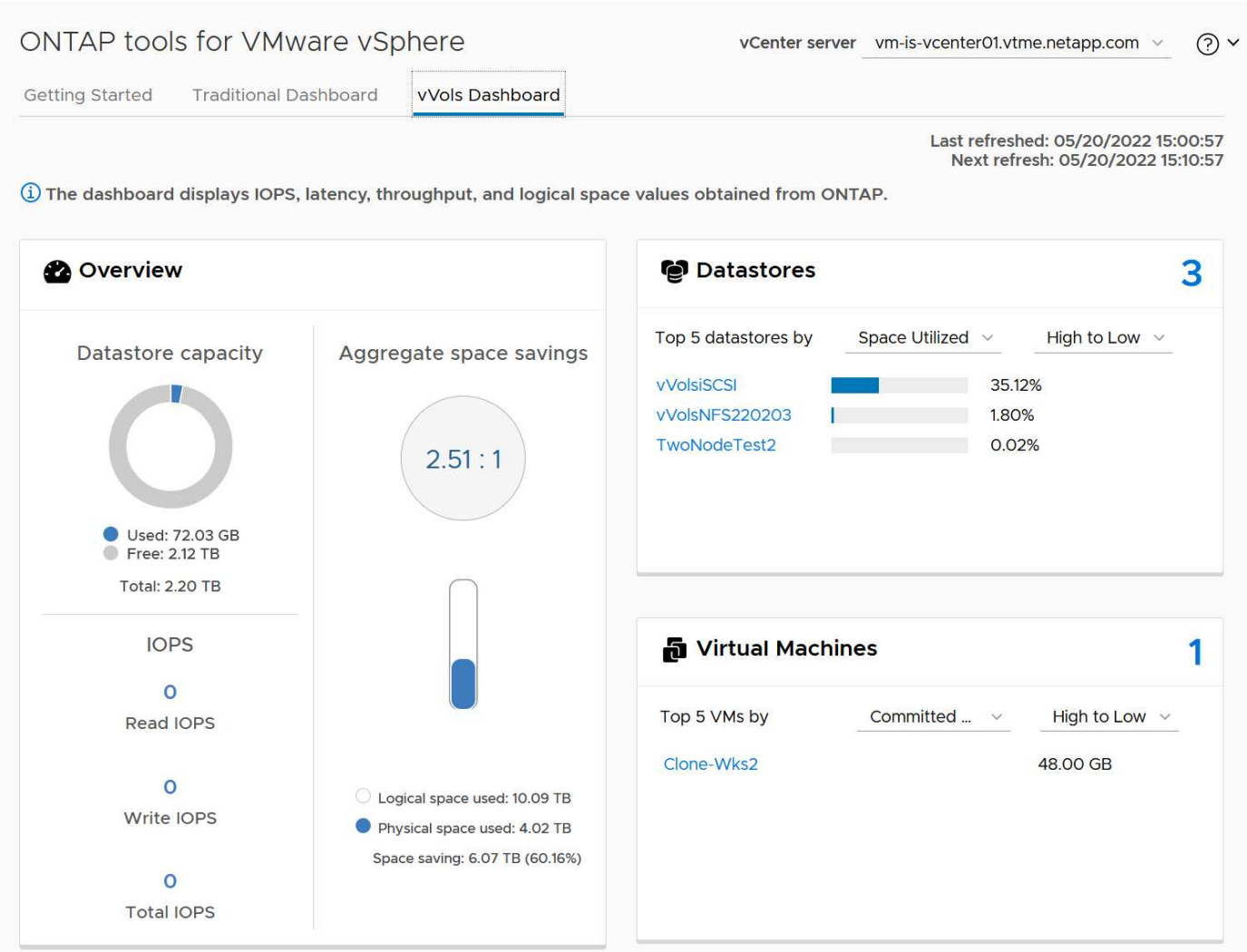
Outre la documentation produit, des articles de la base de connaissances de support peuvent être utiles.

- "Guide de résolution des incidents VASA Provider"

Tableau de bord VASA Provider

Le fournisseur VASA inclut un tableau de bord contenant des informations sur les performances et la capacité des VM vVols individuelles. Ces informations proviennent directement de ONTAP pour les fichiers et les LUN VVol, notamment la latence, les IOPS, le débit et la disponibilité pour les 5 principales VM, ainsi que la latence et les IOPS pour les 5 principaux datastores. Il est activé par défaut lors de l'utilisation de ONTAP 9.7 ou version ultérieure. L'extraction et l'affichage des données initiales dans le tableau de bord peuvent prendre jusqu'à 30 minutes.

Tableau de bord vVols des outils ONTAP



Et des meilleures pratiques

L'utilisation des vVols de ONTAP avec vSphere est simple et suit les méthodes vSphere publiées (consultez la documentation utilisation des volumes virtuels sous vSphere Storage in VMware pour votre version d'ESXi). Voici quelques autres pratiques à prendre en compte avec ONTAP.

Limites

En général, ONTAP supporte les limites vVols définies par VMware (voir publié "Configuration maximale"). Le tableau suivant récapitule les limites de ONTAP spécifiques en taille et en nombre de vVols. Toujours vérifier le "NetApp Hardware Universe" Pour connaître les limites mises à jour concernant les nombres et la taille des LUN et des fichiers.

ONTAP vVols limites

Capacité/fonctionnalité	SAN (SCSI ou NVMe-of)	NFS
Taille maximale des vVols	62 Tio*	62 Tio*
Nombre maximal de vVols par volume FlexVol	1024	2 milliards

Capacité/fonctionnalité	SAN (SCSI ou NVMe-of)	NFS
Nombre maximal de vVols par nœud ONTAP	Jusqu'à 12,288**	50 milliards
Nombre maximal de vVols par paire ONTAP	Jusqu'à 24,576**	50 milliards
Nombre maximal de vVols par cluster ONTAP	Jusqu'à 98,304**	Aucune limite spécifique de cluster
Nombre maximal d'objets QoS (groupe de règles partagé et niveau de service vVols individuel)	12,000 à ONTAP 9.3 ; 40,000 avec ONTAP 9.4 et versions ultérieures	

- Taille limite basée sur les systèmes ASA ou AFF et FAS exécutant ONTAP 9.12.1P2 et versions ultérieures.
  - Le nombre de vVols SAN (espaces de noms NVMe ou LUN) varie en fonction de la plateforme. Toujours vérifier le "NetApp Hardware Universe" Pour connaître les limites mises à jour concernant les nombres et la taille des LUN et des fichiers.

Utilisez les outils ONTAP pour les extensions d'interface utilisateur ou les API REST de VMware vSphere pour provisionner les datastores vVols et les terminaux de protocole.

Bien qu'il soit possible de créer des datastores vVols avec l'interface vSphere générale, l'utilisation des outils ONTAP crée automatiquement des terminaux de protocole selon les besoins et des volumes FlexVol en utilisant les bonnes pratiques ONTAP et conformément aux profils de capacité de stockage que vous avez définis. Il vous suffit de cliquer avec le bouton droit sur l'hôte/le cluster/le data Center, puis de sélectionner *ONTAP Tools* et *provisioning datastore*. Ensuite, il vous suffit de choisir les options vVols souhaitées dans l'assistant.

Ne stockez jamais l'appliance ONTAP Tools ou l'appliance vCenter Server (VCSA) sur un datastore vVols qu'ils gèrent.

Cela peut entraîner une « situation de poulet et d'œuf » si vous devez redémarrer les appareils parce qu'ils ne pourront pas réassocier leurs propres vVols pendant qu'ils redémarrent. Vous pouvez les stocker sur un datastore vVols géré par un autre outil ONTAP et un déploiement vCenter.

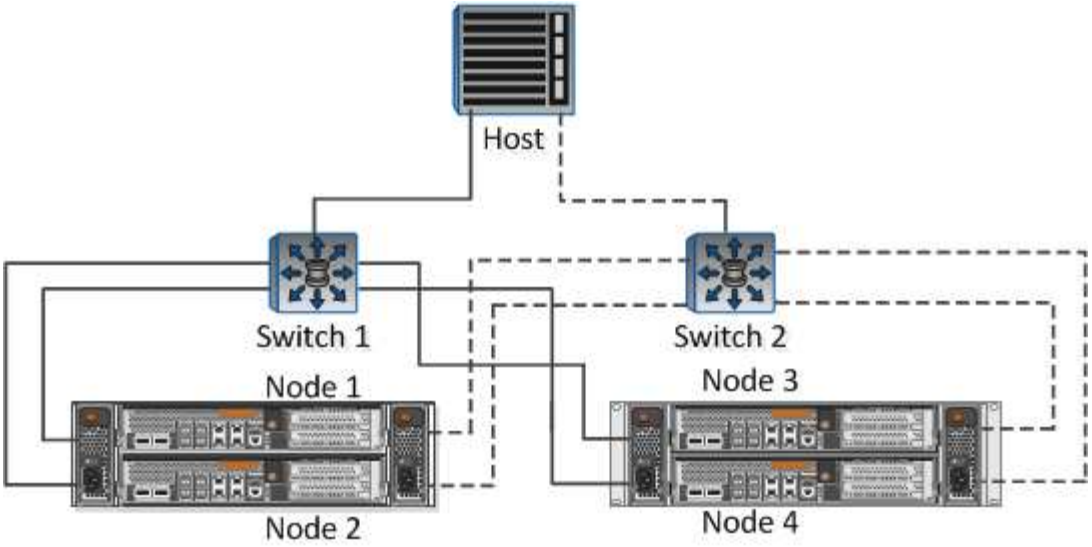
Évitez les opérations vVols sur différentes versions de ONTAP.

Les fonctionnalités de stockage prises en charge telles que la QoS, le personnalité et bien d'autres encore ont changé dans plusieurs versions du fournisseur VASA, et certaines dépendent de la version de ONTAP. L'utilisation de différentes versions dans un cluster ONTAP ou le déplacement de vVols entre clusters avec différentes versions peut entraîner un comportement inattendu ou des alarmes de conformité.

Zone votre fabric Fibre Channel avant d'utiliser NVMe/FC ou FCP pour vVols.

Le fournisseur VASA des outils ONTAP se charge de la gestion des igroups FCP et iSCSI ainsi que des sous-systèmes NVMe dans ONTAP en fonction des initiateurs détectés d'hôtes ESXi gérés. Toutefois, il ne s'intègre pas aux commutateurs Fibre Channel pour gérer la segmentation. La segmentation doit être effectuée conformément aux meilleures pratiques avant tout provisionnement. Voici un exemple de segmentation à un seul initiateur sur quatre systèmes ONTAP :

Segmentation à un seul initiateur :



Pour plus d'informations sur les meilleures pratiques, reportez-vous aux documents suivants :

"*TR-4080 meilleures pratiques pour le SAN moderne ONTAP 9*"

"*TR-4684 implémentation et configuration de SAN modernes avec NVMe-of*"

Planifier vos volumes FlexVol de soutien en fonction de vos besoins.

Il peut être souhaitable d'ajouter plusieurs volumes de sauvegarde à votre datastore vVols pour distribuer la charge de travail au sein du cluster ONTAP, pour prendre en charge différentes options de règles ou pour augmenter le nombre de LUN ou de fichiers autorisés. Toutefois, si vous avez besoin d'une efficacité de stockage maximale, placez l'ensemble de vos volumes en arrière-forme sur un seul agrégat. Si des performances de clonage maximales sont requises, envisagez d'utiliser un seul volume FlexVol et de conserver vos modèles ou votre bibliothèque de contenu dans le même volume. Le fournisseur VASA délègue de nombreuses opérations de stockage vVols à ONTAP, notamment la migration, le clonage et les copies Snapshot. Cette opération est réalisée au sein d'un seul volume FlexVol, ce qui permet d'utiliser des clones de fichiers peu encombrants et de les mettre presque instantanément à disposition. Sur des volumes FlexVol, les copies sont rapidement disponibles et utilisent la déduplication et la compression à la volée. Toutefois, l'efficacité du stockage maximale ne peut pas être restaurée tant que des tâches en arrière-plan ne sont pas exécutées sur des volumes utilisant la déduplication et la compression en arrière-plan. Selon la source et la destination, une certaine efficacité peut être dégradée.

Conserver les profils de capacité de stockage (SCP) simples.

Évitez de spécifier des fonctionnalités qui ne sont pas requises en les configurant sur n'importe quelle option. Cela permet de réduire les problèmes lors de la sélection ou de la création de volumes FlexVol. Par exemple, avec VASA Provider 7.1 et les versions antérieures, si la compression est laissée au paramètre SCP par défaut de non, elle tente de désactiver la compression, même sur un système AFF.

Utilisez les SCP par défaut comme modèles d'exemple pour créer vos propres.

Les SCP inclus sont adaptés à la plupart des utilisations générales, mais vos besoins peuvent être différents.

Pensez à utiliser Max IOPS pour contrôler des machines virtuelles inconnues ou tester des machines virtuelles.

Disponible pour la première fois dans VASA Provider 7.1, Max IOPS peut être utilisé pour limiter les IOPS à un vVol spécifique pour une charge de travail inconnue afin d'éviter tout impact sur d'autres charges de travail

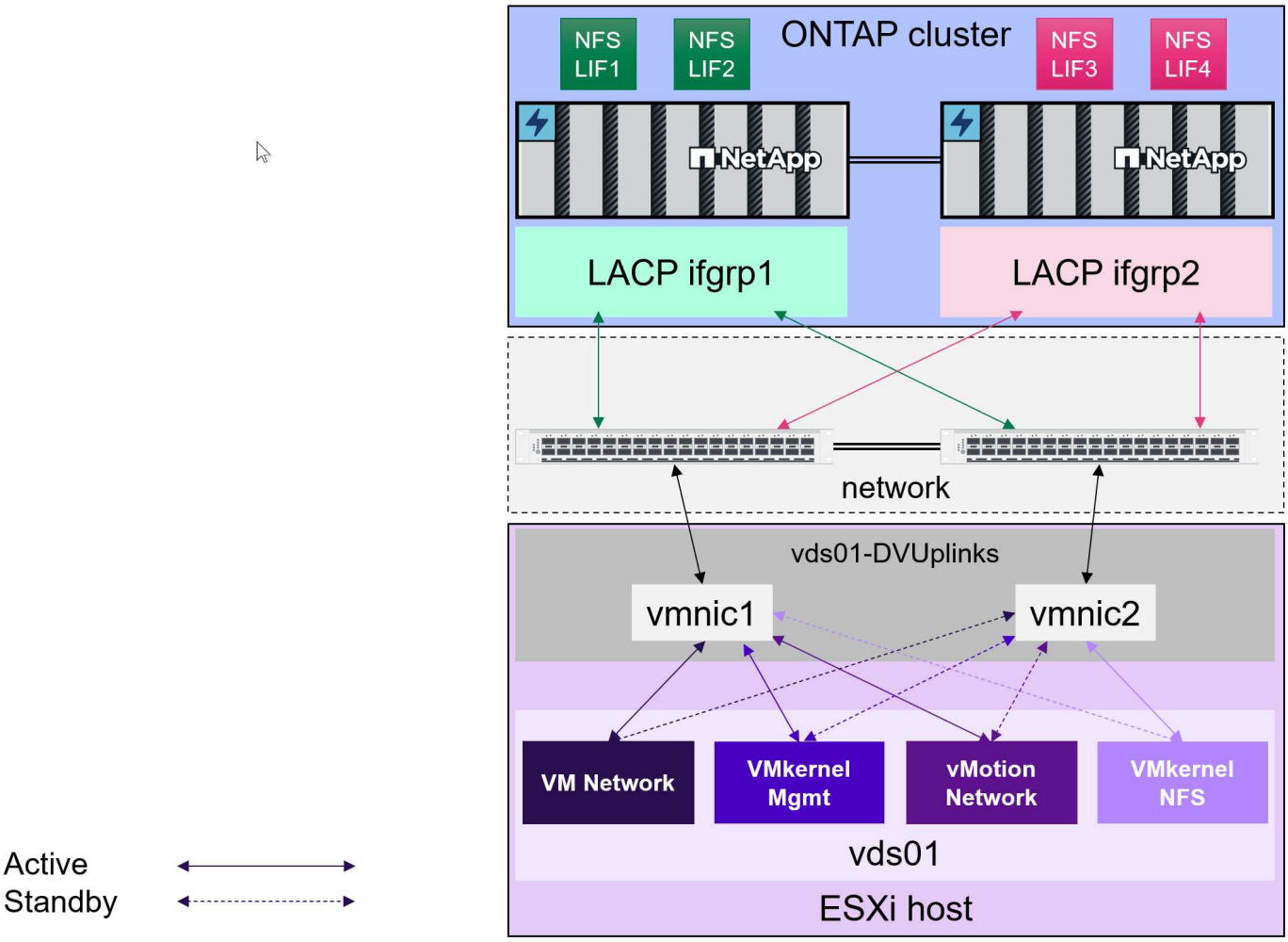
plus stratégiques. Pour plus d'informations sur la gestion des performances, consultez le Tableau 4.

Assurez-vous d'avoir suffisamment de LIFs de données.
Créez au moins deux LIF par nœud et par paire haute disponibilité. Vous devrez peut-être en faire davantage en fonction de votre charge de travail.

Suivre toutes les meilleures pratiques du protocole.

Reportez-vous aux autres guides des meilleures pratiques de NetApp et VMware spécifiques au protocole sélectionné. En général, il n'y a pas d'autres changements que ceux déjà mentionnés.

Exemple de configuration réseau utilisant vVols sur NFS v3



Déploiement du stockage vVols

La création du stockage vVols pour vos machines virtuelles s'est procédure en plusieurs étapes.

Les deux premières étapes peuvent ne pas être nécessaires dans un environnement vSphere existant qui utilise ONTAP pour les datastores traditionnels. Vous utilisez peut-être déjà des outils ONTAP pour la gestion, l'automatisation et la création de rapports avec votre stockage VMFS ou NFS classique. Ces étapes sont décrites plus en détail dans la section suivante.

1. Créer la machine virtuelle de stockage (SVM) et sa configuration de protocole. Vous sélectionnerez

NVMe/FC, NFSv3, NFSv4.1, iSCSI, FCP, ou un mélange de ces options. Vous pouvez utiliser les assistants ONTAP System Manager ou la ligne de commande du cluster shell.

- Au moins une LIF par nœud pour chaque connexion switch/fabric. Il est recommandé de créer au moins deux par nœud pour les protocoles FCP, iSCSI ou NVMe.
- Les volumes peuvent être créés à ce stade, mais il est plus simple de laisser l'assistant *provisioning datastore* les créer. La seule exception à cette règle est que vous prévoyez d'utiliser la réplication vVols avec VMware site Recovery Manager. Cette configuration est plus simple avec des volumes FlexVol préexistants avec des relations SnapMirror existantes. N'oubliez pas d'activer la QoS sur les volumes à utiliser pour les vVols, car ceux-ci doivent être gérés par les outils SPBM et ONTAP.

2. Déployez les outils ONTAP pour VMware vSphere à l'aide de la version OVA téléchargée sur le site de support NetApp.
3. Configurez les outils ONTAP pour votre environnement.
   - Ajoutez le cluster ONTAP aux outils ONTAP sous *systèmes de stockage*
     - Tandis que les outils ONTAP et SRA prennent en charge les informations d'identification au niveau du cluster et du SVM, le fournisseur VASA prend uniquement en charge les informations d'identification au niveau du cluster pour les systèmes de stockage. En effet, de nombreuses API utilisées pour les vVols ne sont disponibles qu'au niveau du cluster. Par conséquent, si vous prévoyez d'utiliser vVols, vous devez ajouter vos clusters ONTAP à l'aide d'identifiants cluster-scoped.
   - Si vos LIFs de données ONTAP se trouvent sur des sous-réseaux différents de vos adaptateurs VMkernel, vous devez ajouter les sous-réseaux de l'adaptateur VMkernel à la liste Selected Subnets (sous-réseaux sélectionnés) dans le menu settings (paramètres) des outils ONTAP. Par défaut, les outils ONTAP sécurisent votre trafic de stockage en autorisant uniquement l'accès au sous-réseau local.
   - Les outils ONTAP sont fournis avec plusieurs règles prédéfinies qui peuvent être utilisées ou non Gestion des machines virtuelles avec des règles Pour obtenir des conseils sur la création de SCP.
4. Utilisez le menu *ONTAP Tools* de vCenter pour démarrer l'assistant *provisioning datastore*.
5. Indiquez un nom significatif et sélectionnez le protocole souhaité. Vous pouvez également fournir une description du datastore.
6. Sélectionnez un ou plusieurs SCP à prendre en charge par le datastore vVols. Ceci permet de filtrer tous les systèmes ONTAP qui ne peuvent pas correspondre au profil. Dans la liste résultat, sélectionner le cluster et le SVM souhaités.
7. Utilisez l'assistant pour créer de nouveaux volumes FlexVol pour chacun des SCP spécifiés ou pour utiliser des volumes existants en sélectionnant le bouton radio approprié.
8. Créez des stratégies VM pour chaque SCP qui sera utilisé dans le datastore à partir du menu *Policies and Profiles* de l'interface utilisateur vCenter.
9. Choisissez le jeu de règles de stockage NetApp.clustered.Data.ONTAP.VP.vvol. Le jeu de règles de stockage NetApp.clustered.Data.ONTAP.VP.VASA10 prend en charge SPBM pour les datastores non-vVols
10. Vous devez spécifier le profil de capacité de stockage par nom lors de la création d'une stratégie de stockage de machine virtuelle. À cette étape, vous pouvez également configurer la mise en correspondance des règles SnapMirror à l'aide de l'onglet réplication et la mise en correspondance basée sur les balises à l'aide de l'onglet balises. Notez que les étiquettes doivent déjà être créées pour pouvoir être sélectionnées.
11. Créez vos machines virtuelles, en sélectionnant la stratégie de stockage VM et le datastore compatible sous Sélectionner le stockage.

Migration des machines virtuelles des datastores classiques vers des vVols

La migration des machines virtuelles des datastores traditionnels vers un datastore vVols est aussi simple que le déplacement de machines virtuelles entre des datastores traditionnels. Il vous suffit de sélectionner la ou les machines virtuelles, puis de sélectionner migrer dans la liste actions et de sélectionner un type de migration de *modifier le stockage uniquement*. Les opérations de copie de migration seront déchargées avec vSphere 6.0 et versions ultérieures pour les migrations de SAN VMFS vers des vVols, mais pas des VMDK NAS vers des vVols.

Gestion des machines virtuelles avec des règles

Pour automatiser le provisionnement du stockage avec la gestion basée sur des règles, nous devons :

- Définissez les fonctionnalités du stockage (nœud ONTAP et volume FlexVol) avec les profils de capacité de stockage (SSP).
- Créez des règles de stockage de machine virtuelle qui correspondent aux SCP définis.

NetApp a simplifié les fonctionnalités et le mappage à partir de VASA Provider 7.2 avec des améliorations continues dans les versions ultérieures. Cette section porte sur cette nouvelle approche. Les versions précédentes prenaient en charge un plus grand nombre de fonctionnalités et permettaient de les mapper individuellement aux stratégies de stockage. Cette approche n'est cependant plus prise en charge.

Fonctionnalités de stockage par version des outils ONTAP

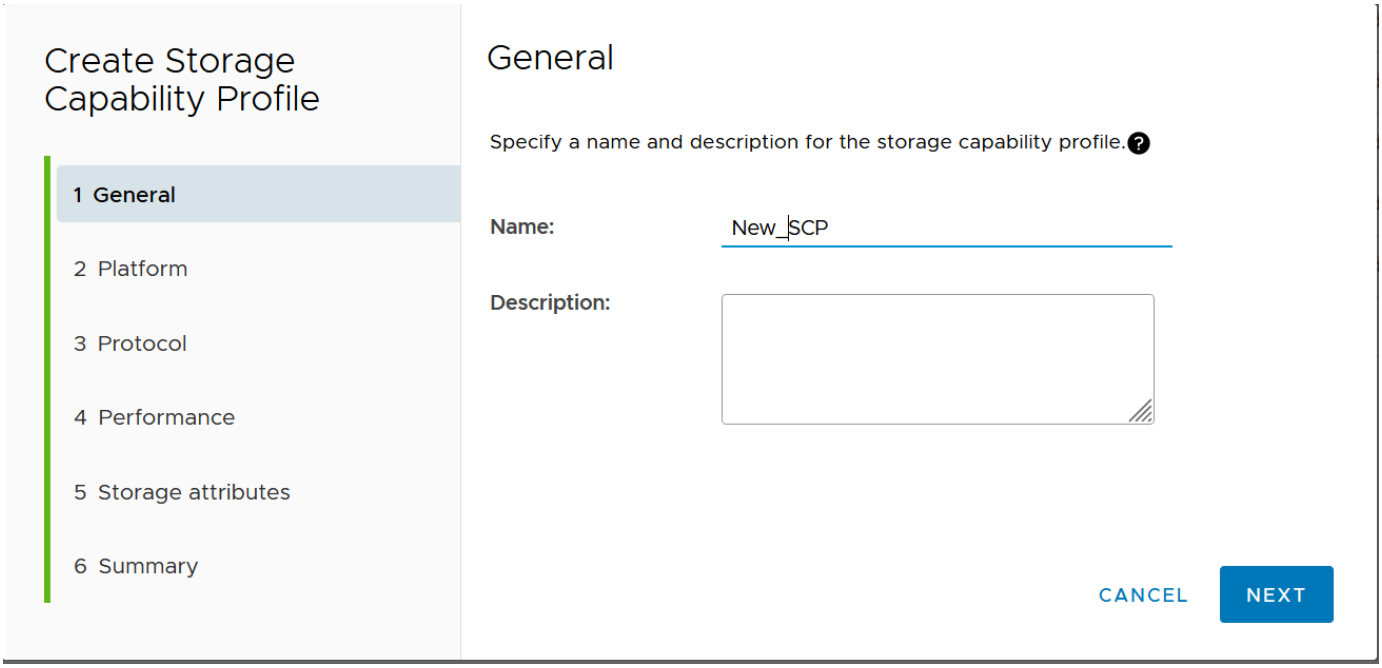
Capacité SCP	Valeurs de capacité	Version prise en charge	Notes
Compression	Oui, non, non	Tout	Obligatoire pour AFF en 7.2 et versions ultérieures.
Déduplication	Oui, non, non	Tout	M andatrice pour AFF en 7.2 et plus tard.
Cryptage	Oui, non, non	7.2 et versions ultérieures	Sélectionne/crée un volume FlexVol chiffré. Licence ONTAP requise.
IOPS max	<number>	7.1 et plus tard, mais différences	Répertorié sous QoS Policy Group pour 7.2 et les versions ultérieures. Voir Gestion de la performance avec les outils ONTAP 9.10 et versions ultérieures pour en savoir plus.
Personnalité	A FF, FAS	7.2 et versions ultérieures	FAS inclut également d'autres systèmes non AFF, tels que ONTAP Select. AFF inclut ASA.
Protocole	NFS, NFS 4.1, iSCSI, FCP, NVMe/FC, Tous	7.1 et versions antérieures, 9.10 et ultérieures	7.2-9.8 est effectivement « tout ». Depuis 9.10, où NFS 4.1 et NVMe/FC ont été ajoutés à la liste d'origine.

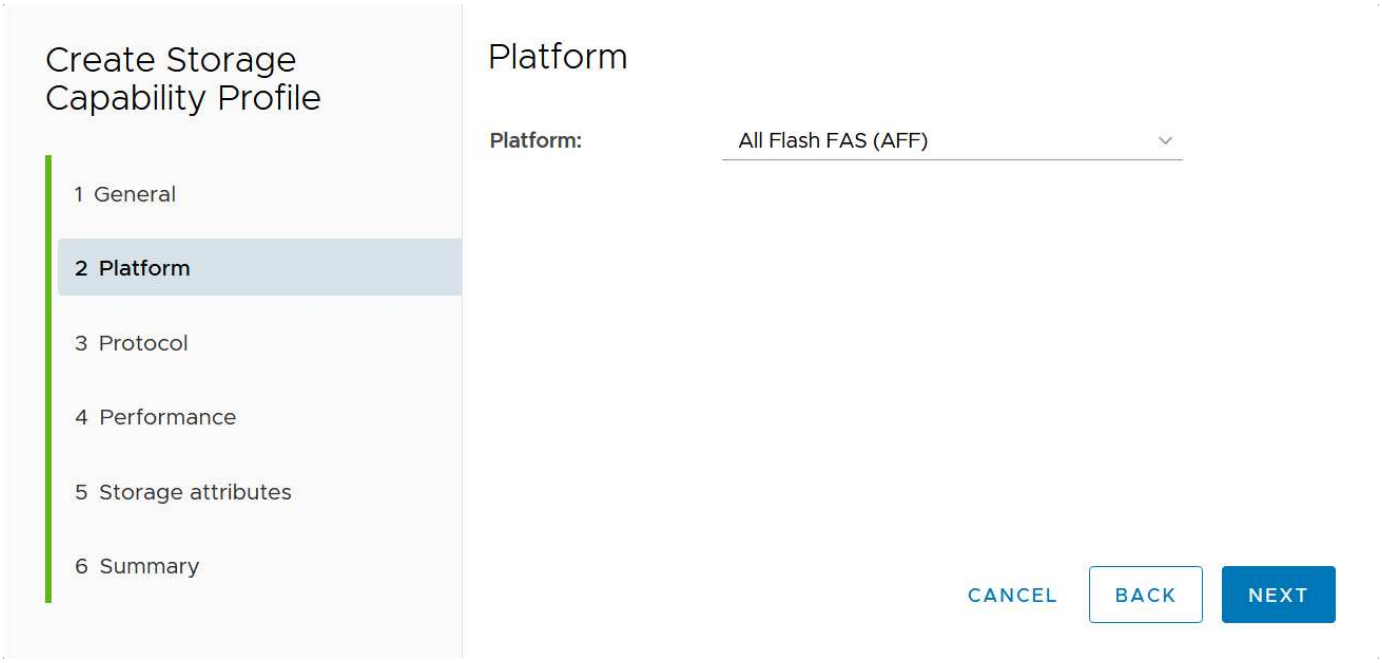
Capacité SCP	Valeurs de capacité	Version prise en charge	Notes
Réserve d'espace (provisionnement fin)	Fin, épais, (tous)	Toutes, sauf les différences	Appelé provisionnement fin en 7.1 et versions antérieures, qui permettait également de valoriser n'importe quel système. Appelé Réserve d'espace en 7.2. Toutes les versions prennent par défaut la valeur Thin.
Politique de hiérarchisation	Tous, aucun, instantané, Auto	7.2 et versions ultérieures	Utilisé pour FabricPool - requiert AFF ou ASA avec ONTAP 9.4 ou version ultérieure. Seul Snapshot est recommandé, à moins d'utiliser une solution S3 sur site telle que NetApp StorageGRID.

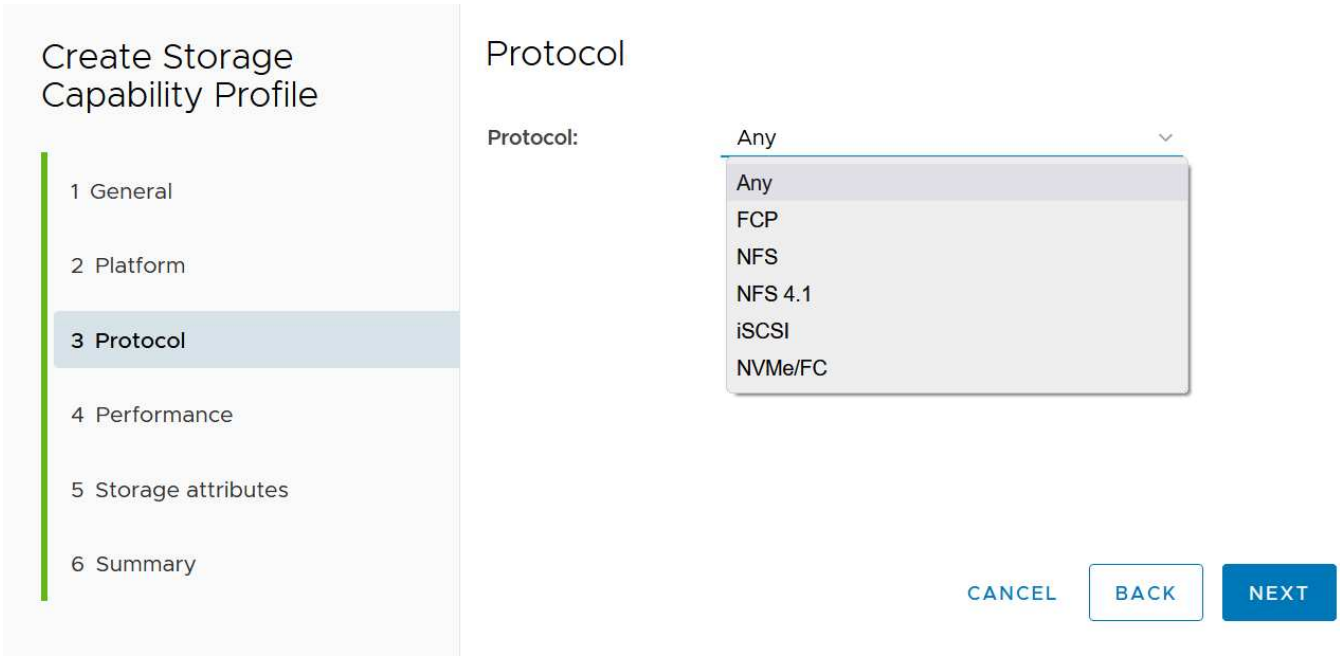
Création des profils de capacité de stockage

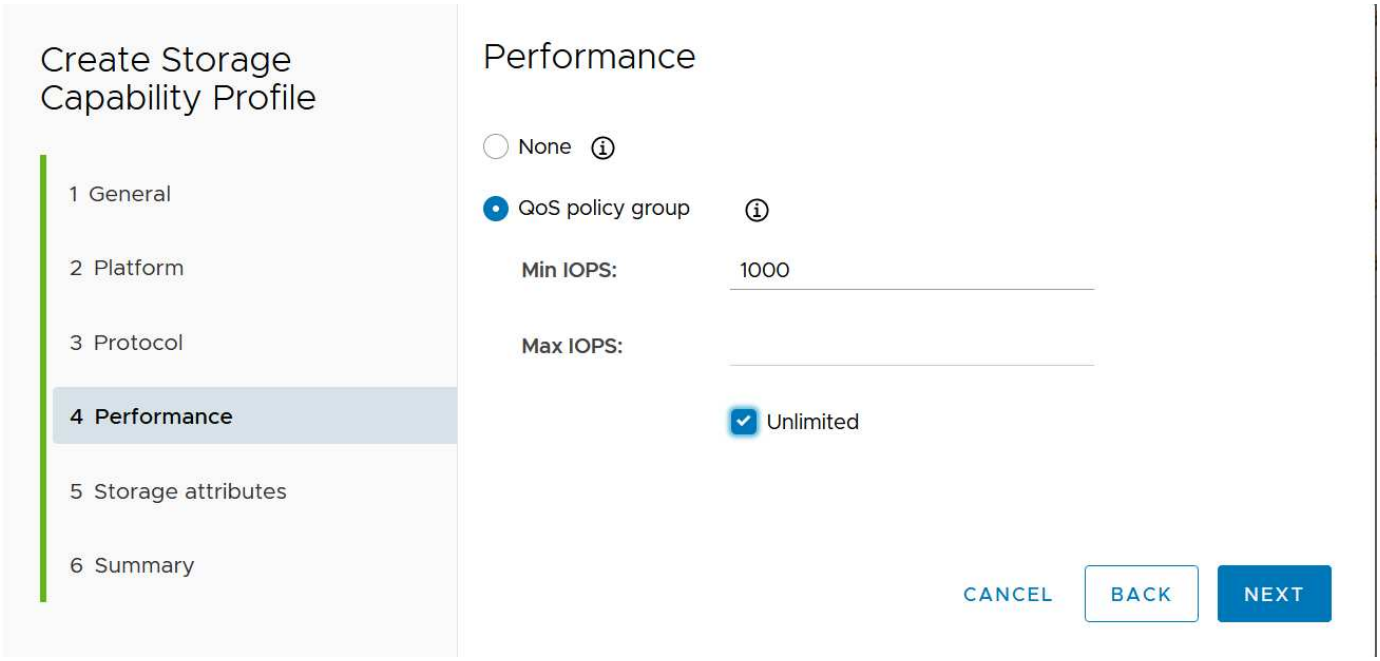
NetApp VASA Provider est fourni avec plusieurs SCP prédéfinis. Les nouveaux SCP peuvent être créés manuellement, à l'aide de l'interface utilisateur vCenter ou via l'automatisation via les API REST. En spécifiant des fonctionnalités dans un nouveau profil, en clonant un profil existant ou en générant automatiquement un ou plusieurs profils à partir de datastores traditionnels existants. Pour ce faire, utilisez les menus sous Outils ONTAP. Utilisez *profils de capacité de stockage* pour créer ou cloner un profil et *mappage de stockage* pour générer automatiquement un profil.

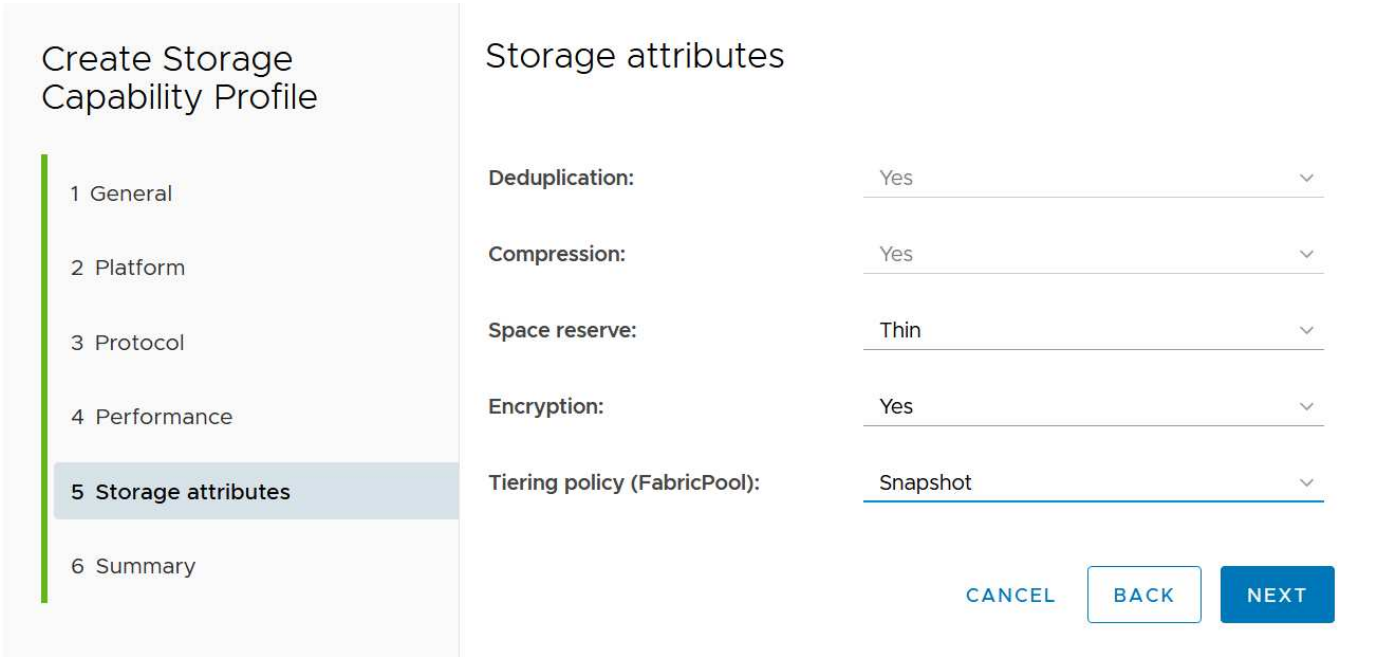
Fonctionnalités de stockage pour les outils ONTAP 9.10 et versions ultérieures

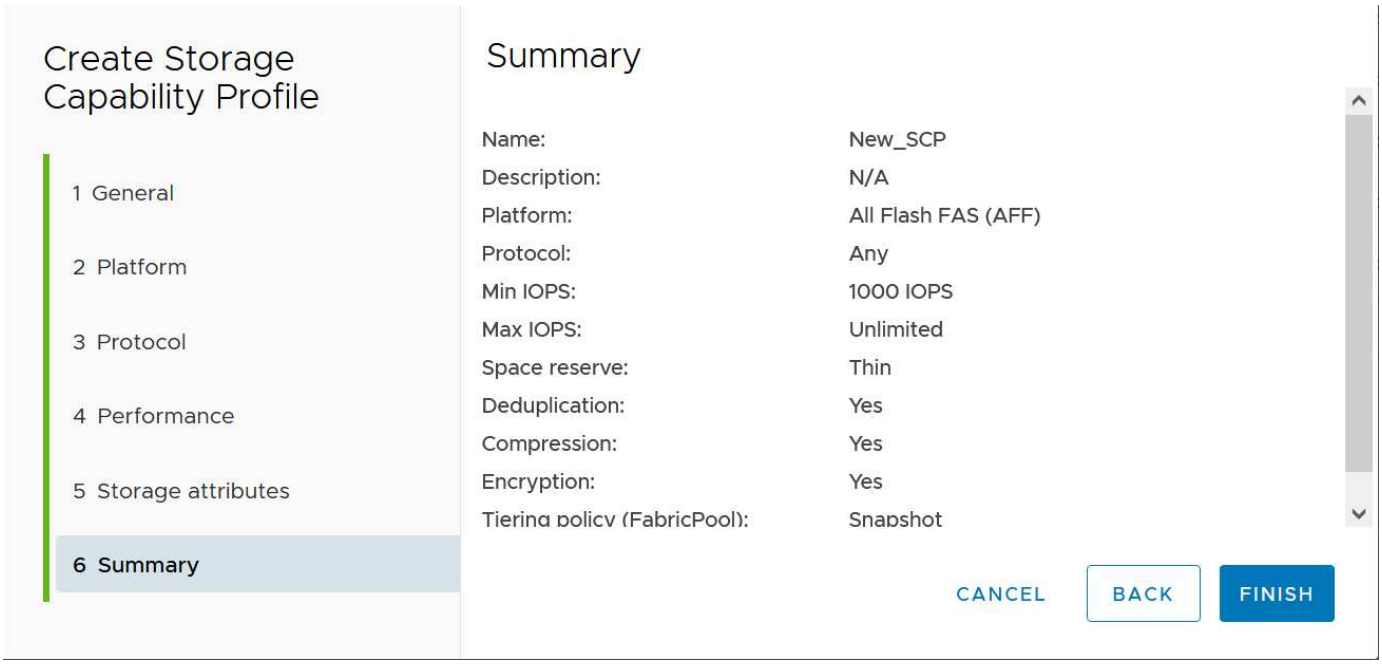



Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Platform
Platform:
All Flash FAS (AFF)
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Protocol
Protocol:
Any
Any
FCP
NFS
NFS 4.1
iSCSI
NVMe/FC
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Performance
None
QoS policy group
Min IOPS:
1000
Max IOPS:
Unlimited
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Storage attributes
Deduplication:
Yes
Compression:
Yes
Space reserve:
Thin
Encryption:
Yes
Tiering policy (FabricPool):
Snapshot
CANCEL
BACK
NEXT



Création des datastores vVols

Une fois les SCP nécessaires créés, ils peuvent être utilisés pour créer le datastore vVols (et éventuellement, les volumes FlexVol pour le datastore). Cliquez avec le bouton droit de la souris sur l'hôte, le cluster ou le data Center sur lequel vous souhaitez créer le datastore vVols, puis sélectionnez *ONTAP Tools > Provision datastore*. Sélectionnez un ou plusieurs SCP à prendre en charge par le datastore, puis faites votre choix parmi les volumes FlexVol existants et/ou provisionnez de nouveaux volumes FlexVol pour le datastore. Enfin, spécifiez le SCP par défaut pour le datastore, qui sera utilisé pour les machines virtuelles sur lesquelles aucun SCP n'a été spécifié par la règle, ainsi que pour les vVols de swap (ceux-ci ne nécessitent pas de stockage haute performance).

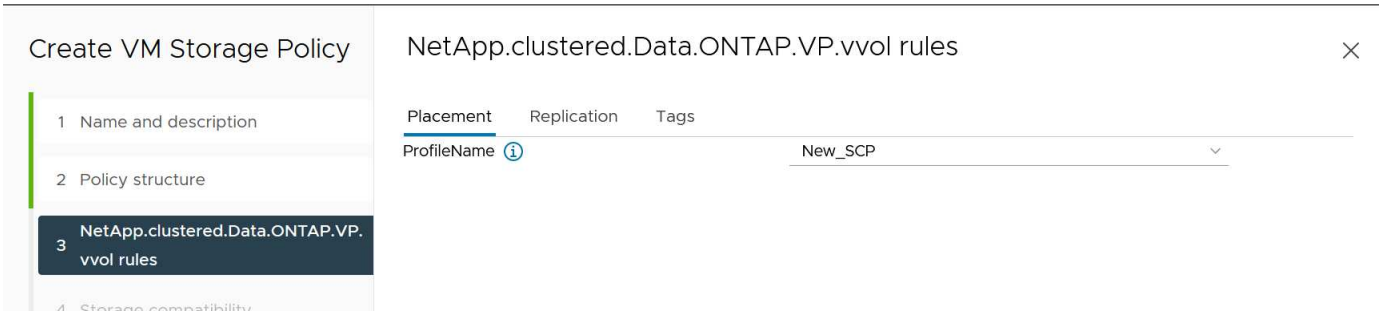
Création de stratégies de stockage de machine virtuelle

Les règles de stockage des machines virtuelles sont utilisées dans vSphere pour gérer les fonctionnalités facultatives telles que le contrôle des E/S du stockage ou le chiffrement vSphere. Ils sont également utilisés avec les vVols pour appliquer des fonctionnalités de stockage spécifiques à la machine virtuelle. Utilisez le type de stockage NetApp.clustered.Data.ONTAP.VP.vvol et la règle ProfileName pour appliquer un SCP spécifique aux machines virtuelles à l'aide de la politique. Voir le lien:vmware-vvols-ontap.html#Best Practices[exemple de configuration réseau avec vVols sur NFS v3] pour un exemple de ceci avec les outils ONTAP VASA Provider. Les règles pour le stockage « NetApp.clustered.Data.ONTAP.VP.VASA10 » doivent être utilisées avec les datastores non basés sur vVols.

Les versions précédentes sont similaires, mais comme indiqué dans Fonctionnalités de stockage par version des outils ONTAP, vos options varient.

Une fois la règle de stockage créée, elle peut être utilisée lors du provisionnement de nouvelles machines virtuelles, comme illustré à la "Déployer une machine virtuelle à l'aide de la stratégie de stockage". Les instructions relatives à l'utilisation des fonctionnalités de gestion des performances avec VASA Provider 7.2 sont traitées dans le Gestion de la performance avec les outils ONTAP 9.10 et versions ultérieures.

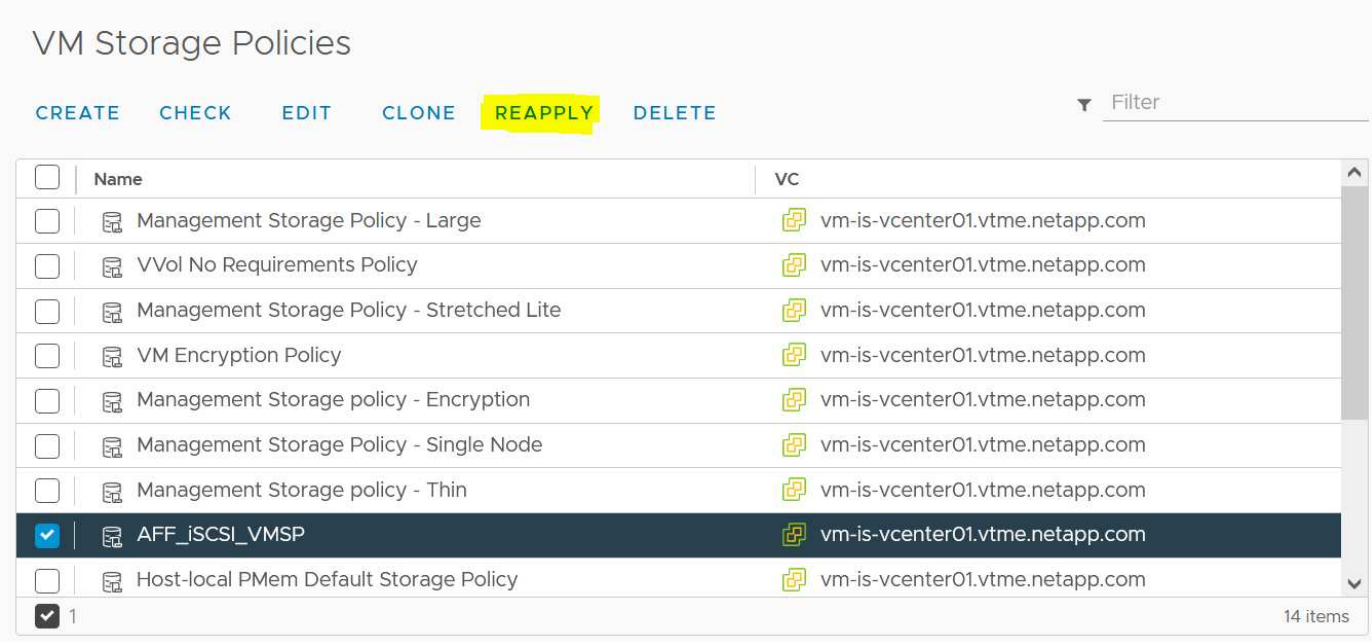
Création de règles de stockage de VM avec les outils ONTAP VASA Provider 9.10



Gestion de la performance avec les outils ONTAP 9.10 et versions ultérieures

- ONTAP Tools 9.10 utilise son propre algorithme de placement équilibré pour placer un nouveau VVol dans le meilleur volume FlexVol d'un datastore vVols. Le placement est basé sur le SCP spécifié et les volumes FlexVol correspondants. Cela permet de s'assurer que le datastore et le stockage de sauvegarde peuvent répondre aux exigences de performances spécifiées.
- La modification des capacités de performance telles que les IOPS min et max requiert une certaine attention particulière à la configuration spécifique.
  - **Les valeurs min et Max IOPS** peuvent être spécifiées dans un SCP et utilisées dans une stratégie VM.
    - La modification des IOPS dans le SCP ne modifie pas la QoS sur les vVols tant que la règle de VM n'est pas modifiée, puis réappliquée aux VM qui l'utilisent (voir Fonctionnalités de stockage pour les outils ONTAP 9.10 et versions ultérieures). Vous pouvez également créer un nouveau SCP avec le nombre d'IOPS souhaité et modifier la règle pour l'utiliser (et appliquer de nouveau aux serveurs virtuels). Il est généralement recommandé de définir simplement des SCP et des règles de stockage VM distincts pour les différents niveaux de service, puis de simplement modifier la stratégie de stockage VM sur la VM.
    - Les personnalités AFF et FAS ont des paramètres d'IOPS différents. Les valeurs min et Max sont disponibles sur AFF. Cependant, les systèmes non-AFF peuvent uniquement utiliser les paramètres Max IOPS.
- Dans certains cas, il peut être nécessaire de migrer un VVol après une modification de règle (manuellement ou automatiquement par VASA Provider et ONTAP) :
  - Certains changements ne nécessitent pas de migration (par exemple, la modification des IOPS maximales qui peuvent être appliquées immédiatement à la machine virtuelle comme indiqué ci-dessus).
  - Si la modification de règle ne peut pas être prise en charge par le volume FlexVol actuel qui stocke le volume vVol (par exemple, la plateforme ne prend pas en charge la règle de chiffrement ou de hiérarchisation demandée), vous devez migrer manuellement la machine virtuelle dans vCenter.
- Les outils ONTAP créent des règles de QoS individuelles non partagées avec les versions de ONTAP actuellement prises en charge. Par conséquent, chaque VMDK individuel recevra sa propre allocation d'IOPS.

Réapplication de la stratégie de stockage VM



Protection des vVols

Les sections suivantes présentent les procédures et les bonnes pratiques d'utilisation de VMware vVols avec le stockage ONTAP.

Haute disponibilité VASA Provider

Le fournisseur NetApp VASA s'exécute en tant que composant de l'appliance virtuelle, avec le plug-in vCenter et le serveur d'API REST (anciennement Virtual Storage Console [VSC]) et Storage Replication adapter. Si le fournisseur VASA n'est pas disponible, les machines virtuelles utilisant des vVols continueront à s'exécuter. Toutefois, il n'est pas possible de créer de nouveaux datastores vVols et ne peut pas être créé ni lié par vSphere. Cela signifie que les machines virtuelles utilisant des vVols ne peuvent pas être activées car vCenter ne pourra pas demander la création du vVol de swap. De plus, les machines virtuelles en cours d'exécution ne peuvent pas utiliser vMotion pour la migration vers un autre hôte, car les vVols ne peuvent pas être liés au nouvel hôte.

Vasa Provider 7.1 et les versions ultérieures prennent en charge de nouvelles fonctionnalités pour s'assurer que les services sont disponibles dès que nécessaire. Elle comprend de nouveaux processus de surveillance qui surveillent VASA Provider et des services de base de données intégrés. S'il détecte une défaillance, il met à jour les fichiers journaux, puis redémarre automatiquement les services.

L'administrateur vSphere doit configurer une protection supplémentaire en utilisant les mêmes fonctionnalités de disponibilité que celles utilisées pour protéger les autres ordinateurs virtuels stratégiques contre les défaillances logicielles, matérielles hôtes et réseau. Aucune configuration supplémentaire n'est requise sur l'appliance virtuelle pour utiliser ces fonctionnalités ; il vous suffit de les configurer à l'aide des approches vSphere standard. Ils ont été testés et sont pris en charge par NetApp.

VSphere High Availability est facilement configuré pour redémarrer une machine virtuelle sur un autre hôte du cluster hôte en cas de panne. VSphere Fault Tolerance offre une plus grande disponibilité en créant une machine virtuelle secondaire répliquée en continu et capable de prendre le relais à tout moment. Des informations supplémentaires sur ces fonctions sont disponibles dans le "Documentation relative aux outils ONTAP pour VMware vSphere (configuration de la haute disponibilité des outils ONTAP)", Ainsi que la documentation VMware vSphere (recherchez vSphere Availability sous ESXi et vCenter Server).

Le fournisseur VASA des outils ONTAP sauvegarde automatiquement la configuration vVols en temps réel vers des systèmes ONTAP gérés où les informations vVols sont stockées dans les métadonnées de volume FlexVol. Si l'appliance ONTAP Tools devient indisponible, quelle qu'en soit la raison, vous pouvez facilement et rapidement en déployer une nouvelle et importer la configuration. Pour plus d'informations sur les étapes de restauration d'un fournisseur VASA, consultez cet article de la base de connaissances :

"Guide de résolution des incidents VASA Provider"

Réplication vVols

De nombreux clients ONTAP répliquent leurs datastores classiques sur des systèmes de stockage secondaires à l'aide de NetApp SnapMirror, puis utilisent le système secondaire pour restaurer des machines virtuelles individuelles ou la totalité d'un site en cas d'incident. Dans la plupart des cas, les clients utilisent un outil logiciel pour gérer ceci, tel qu'un logiciel de sauvegarde tel que le plug-in NetApp SnapCenter pour VMware vSphere ou une solution de reprise après incident telle que site Recovery Manager de VMware (avec l'adaptateur de réplication du stockage dans les outils ONTAP).

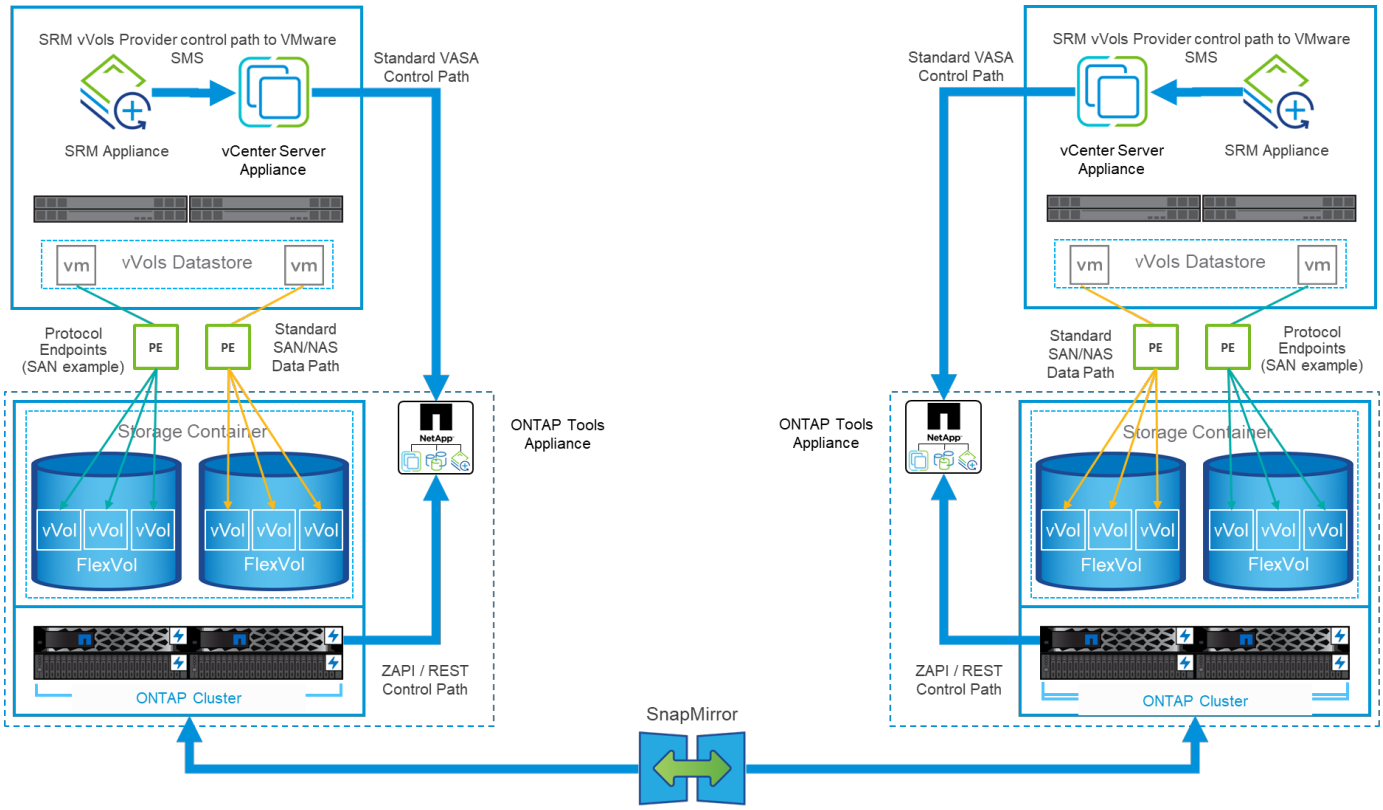
Cette exigence relative à un outil logiciel est encore plus importante pour la gestion de la réplication des vVols. Les fonctionnalités natives permettent de gérer certains aspects (par exemple, les copies Snapshot des vVols gérées par VMware sont déchargées vers ONTAP, qui utilise des clones de fichiers ou de LUN rapides et efficaces). Toutefois, l'orchestration générale est nécessaire pour gérer la réplication et la restauration. Les métadonnées concernant les vVols sont protégées par ONTAP et par le fournisseur VASA, mais des traitements supplémentaires sont nécessaires pour les utiliser sur un site secondaire.

Les outils ONTAP 9.7.1 associés à VMware site Recovery Manager (SRM) 8.3 ont également pris en charge la reprise après incident et l'orchestration des flux de travail de migration en tirant parti de la technologie NetApp SnapMirror.

Dans la version initiale de la prise en charge de SRM avec les outils ONTAP 9.7.1, il était nécessaire de pré-créer les volumes FlexVol et d'activer la protection SnapMirror avant de les utiliser comme volumes de sauvegarde pour un datastore vVols. À partir des outils ONTAP 9.10, ce processus n'est plus nécessaire. Vous pouvez désormais ajouter la protection SnapMirror aux volumes de sauvegarde existants et mettre à jour les règles de stockage de vos machines virtuelles afin de bénéficier d'une gestion basée sur des règles avec reprise après incident, orchestration de la migration et automatisation intégrées à SRM.

Actuellement, VMware SRM est la seule solution d'automatisation de la migration et de la reprise après incident pour les vVols pris en charge par NetApp. Les outils ONTAP vérifient l'existence d'un serveur SRM 8.3 ou version ultérieure enregistré dans votre vCenter avant de vous permettre d'activer la réplication vVols, Vous pouvez exploiter les API REST d'outils ONTAP pour créer vos propres services.

Réplication de vVols avec SRM



Support MetroCluster

Bien que les outils ONTAP ne soient pas capables de déclencher un basculement MetroCluster, ils prennent en charge les systèmes NetApp MetroCluster pour les vVols soutenant les volumes dans une configuration vMSC (vSphere Metro Storage Cluster) uniforme. Le basculement d'un système MetroCluster est géré de la manière habituelle.

Même si NetApp SnapMirror Business Continuity (SM-BC) peut également servir de base pour une configuration vMSC, il n'est pas pris en charge avec les vVols.

Pour plus d'informations sur NetApp MetroCluster, consultez ces guides :

"*TR-4689 Architecture et conception de la solution MetroCluster IP*"

"*TR-4705 Architecture et conception de la solution NetApp MetroCluster*"

"*VMware KB 2031038 prise en charge de VMware vSphere avec NetApp MetroCluster*"

Présentation de la sauvegarde vVols

Il existe plusieurs approches pour protéger les machines virtuelles, telles que l'utilisation d'agents de sauvegarde invités, la connexion de fichiers de données VM à un proxy de sauvegarde ou l'utilisation d'API définies telles que VMware VADP. Les vVols peuvent être protégées à l'aide des mêmes mécanismes et de nombreux partenaires NetApp prennent en charge les sauvegardes de machines virtuelles, y compris les vVols.

Comme mentionné précédemment, les snapshots gérés par VMware vCenter sont déchargés dans des clones de fichiers/LUN ONTAP rapides et compacts. Elles peuvent être utilisées pour des sauvegardes rapides et manuelles, mais vCenter limite le nombre de snapshots à 32. Vous pouvez utiliser vCenter pour créer des snapshots et restaurer les données selon vos besoins.

À partir du plug-in SnapCenter pour VMware vSphere (SCV) 4.6 utilisé conjointement avec les outils ONTAP 9.10 et versions ultérieures, ajoute la prise en charge de la sauvegarde et de la restauration cohérentes après panne des machines virtuelles basées sur vVols exploitant les snapshots de volume ONTAP FlexVol avec prise en charge de la réplication SnapMirror et SnapVault. Jusqu'à 1023 copies Snapshot sont prises en charge par volume. SCV peut également stocker davantage de copies Snapshot avec une conservation plus longue sur des volumes secondaires à l'aide de SnapMirror avec une règle de copie miroir.

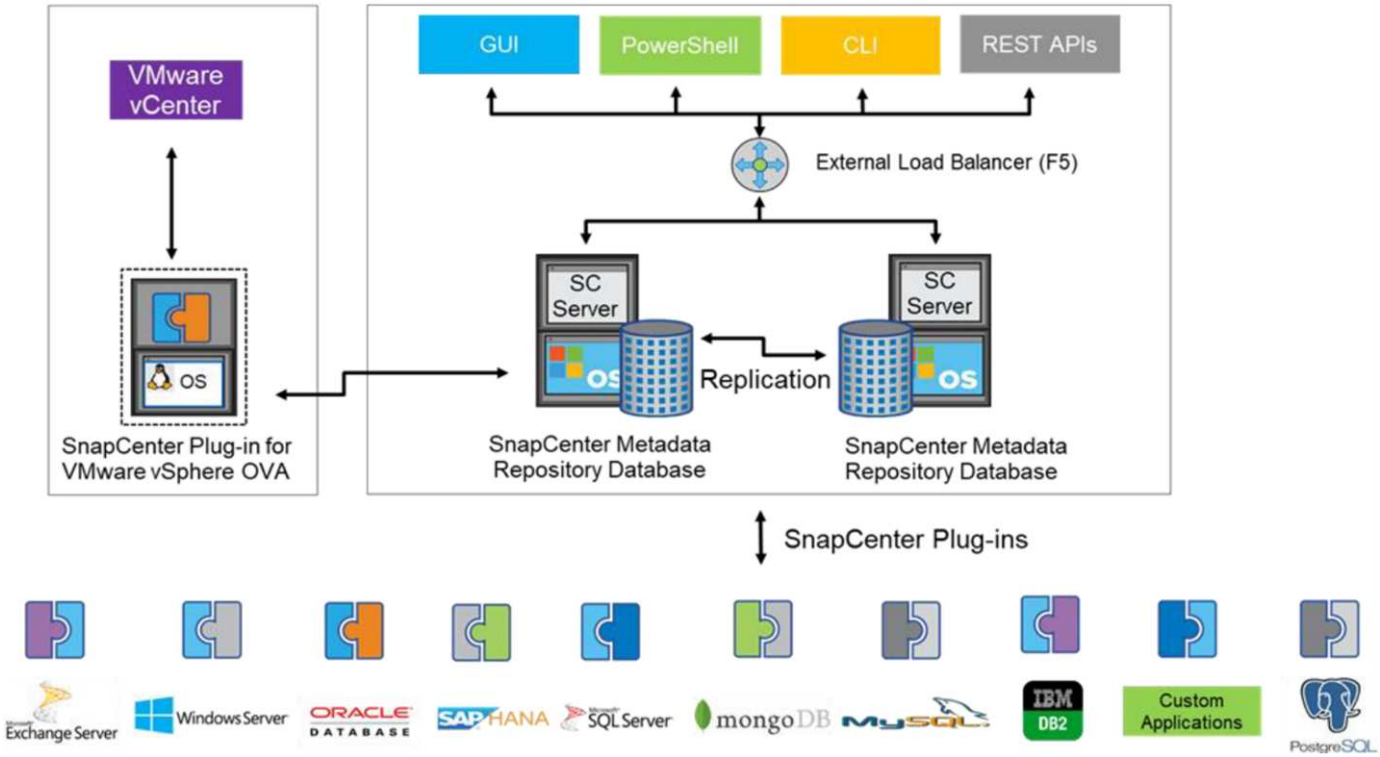
La prise en charge de vSphere 8.0 a été introduite avec SCV 4.7, qui utilisait une architecture de plug-ins locaux isolée. La prise en charge de vSphere 8.0U1 a été ajoutée à SCV 4.8, qui a entièrement migré vers la nouvelle architecture de plug-ins distants.

VVols Backup avec le plug-in SnapCenter pour VMware vSphere

Avec NetApp SnapCenter, vous pouvez désormais créer des groupes de ressources pour les vVols à partir de balises et/ou de dossiers afin de tirer automatiquement parti des snapshots FlexVol d'ONTAP pour les machines virtuelles basées sur vVols. Cela vous permet de définir des services de sauvegarde et de restauration qui protègent automatiquement les machines virtuelles lorsqu'elles sont provisionnées dynamiquement au sein de votre environnement.

Le plug-in SnapCenter pour VMware vSphere est déployé en tant qu'appliance autonome enregistrée en tant qu'extension vCenter, gérée via l'interface utilisateur vCenter ou via les API REST pour l'automatisation des services de sauvegarde et de restauration.

Architecture SnapCenter



Comme les autres plug-ins SnapCenter ne prennent pas encore en charge les vVols au moment de la rédaction de ce document, nous nous concentrerons sur le modèle de déploiement autonome présenté dans ce document.

Étant donné que SnapCenter utilise les copies Snapshot ONTAP FlexVol, il n'y a pas de surcharge placée sur vSphere, ni de réduction des performances comme on peut le voir avec les machines virtuelles traditionnelles

utilisant les snapshots gérés par vCenter. De plus, comme la fonctionnalité de SCV est exposée via les API REST, il est facile de créer des workflows automatisés à l'aide d'outils tels que VMware Aria Automation, Ansible, Terraform et pratiquement tous les autres outils d'automatisation capables d'utiliser des API REST standard.

Pour plus d'informations sur les API REST de SnapCenter, reportez-vous à la section "Présentation des API REST"

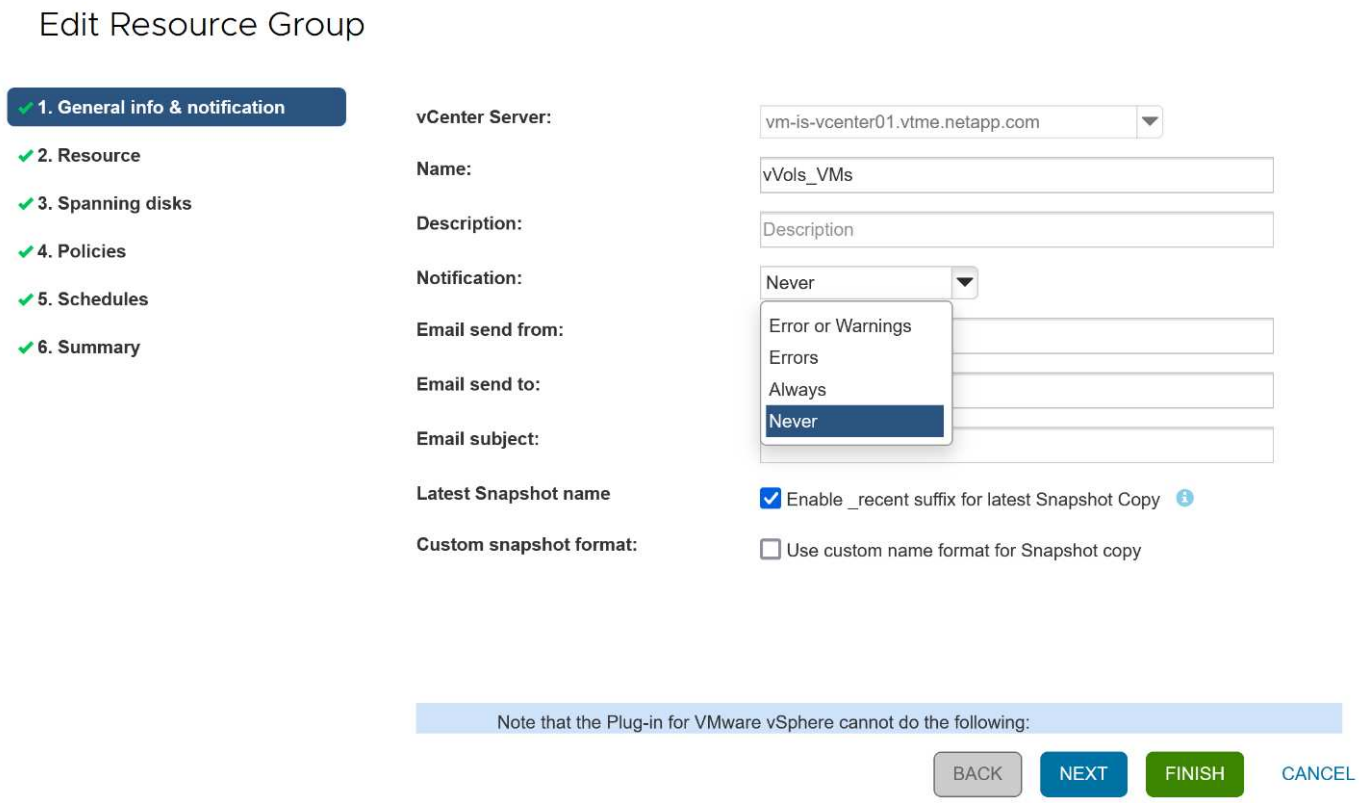
Pour plus d'informations sur le plug-in SnapCenter pour les API REST VMware vSphere, consultez la section "Plug-in SnapCenter pour les API REST VMware vSphere"

Et des meilleures pratiques

Les bonnes pratiques suivantes peuvent vous aider à tirer le meilleur parti de votre déploiement SnapCenter.

- SCV prend en charge les rôles RBAC vCenter Server et ONTAP RBAC et inclut des rôles vCenter prédéfinis qui sont automatiquement créés pour vous lorsque le plug-in est enregistré. Vous pouvez en savoir plus sur les types de RBAC pris en charge "ici."
  - Utilisez l'interface utilisateur de vCenter pour attribuer l'accès au compte le moins privilégié à l'aide des rôles prédéfinis décrits "ici".
  - Si vous utilisez SCV avec le serveur SnapCenter, vous devez attribuer le rôle *SnapCenter_Admin*.
  - ONTAP RBAC fait référence au compte utilisateur utilisé pour ajouter et gérer les systèmes de stockage utilisés par SCV. ONTAP RBAC ne s'applique pas aux sauvegardes basées sur vVols. En savoir plus sur ONTAP RBAC et SCV "ici".
- Répliquez vos jeux de données de sauvegarde sur un second système à l'aide de SnapMirror pour créer des répliques complètes des volumes source. Comme mentionné précédemment, vous pouvez également utiliser des règles de copie miroir pour la conservation à long terme des données de sauvegarde, indépendamment des paramètres de conservation des snapshots du volume source. Les deux mécanismes sont pris en charge avec vVols.
- Étant donné que SCV requiert également les outils ONTAP pour la fonctionnalité VMware vSphere for vVols, vérifiez toujours la compatibilité des versions avec l'outil IMT (Interoperability Matrix Tool) de NetApp
- Si vous utilisez la réplication vVols avec VMware SRM, tenez compte de vos objectifs RPO et de votre planification de sauvegarde
- Concevez vos règles de sauvegarde avec des paramètres de conservation qui répondent aux objectifs de point de restauration (RPO) définis par votre entreprise.
- Configurez les paramètres de notification de vos groupes de ressources pour qu'ils soient informés de l'état lors de l'exécution des sauvegardes (voir la figure 10 ci-dessous).

Options de notification de groupe de ressources



Commencer à utiliser SCV à l'aide de ces documents

"En savoir plus sur le plug-in SnapCenter pour VMware vSphere"

"Déployez le plug-in SnapCenter pour VMware vSphere"

Dépannage

Plusieurs ressources de dépannage sont disponibles avec des informations supplémentaires.

Site de support NetApp

Outre plusieurs articles de la base de connaissances sur les produits de virtualisation NetApp, le site de support NetApp offre également une page d'accueil pratique pour le "Les outils ONTAP pour VMware vSphere" produit. Ce portail propose des liens vers des articles, des téléchargements, des rapports techniques et des discussions sur les solutions VMware sur la communauté NetApp. Il est disponible à l'adresse suivante :

"*Site de support NetApp*"

Vous trouverez une documentation supplémentaire sur les solutions ici :

"*Solutions NetApp pour la virtualisation*"

Dépannage du produit

Les différents composants des outils ONTAP, tels que le plug-in vCenter, VASA Provider et Storage Replication adapter sont tous documentés dans le référentiel de documents NetApp. Cependant, chacun d'entre eux dispose d'une sous-section distincte de la base de connaissances et peut avoir des procédures de dépannage

spécifiques. Ils répondent aux problèmes les plus courants rencontrés avec le fournisseur VASA.

Problèmes liés à l'interface utilisateur de VASA Provider

Il arrive que le client Web vCenter vSphere rencontre des problèmes avec les composants Serenity, ce qui empêche l'affichage des éléments de menu VASA Provider for ONTAP. Consultez la section résolution des problèmes d'enregistrement de VASA Provider dans le Guide de déploiement ou cette base de connaissances "article".

Échec du provisionnement du datastore vVols

Il arrive parfois que les services vCenter prennent du temps lors de la création du datastore vVols. Pour le corriger, redémarrez le service vmware-sps et remontez le datastore vVols à l'aide des menus vCenter (stockage > Nouveau datastore). Ceci est couvert par les échecs de provisionnement du datastore vVols avec vCenter Server 6.5 dans le Guide d'administration.

La mise à niveau d'Unified Appliance ne parvient pas à monter l'ISO

En raison d'un bogue dans vCenter, le montage de l'ISO utilisé pour mettre à niveau l'appliance unifiée d'une version à l'autre peut échouer. Si l'ISO peut être attaché à l'appliance dans vCenter, suivez la procédure de cette base de connaissances "article" à résoudre.

VMware site Recovery Manager et ONTAP

VMware site Recovery Manager et ONTAP

Depuis son introduction dans le data Center moderne en 2002, ONTAP est une solution de stockage leader pour les environnements VMware vSphere. De plus, il continue d'ajouter des fonctionnalités innovantes pour simplifier la gestion tout en réduisant les coûts.

Ce document présente la solution ONTAP pour VMware site Recovery Manager (SRM), le logiciel de reprise après incident de pointe de VMware, qui inclut les dernières informations produit et les meilleures pratiques permettant de rationaliser le déploiement, de réduire les risques et de simplifier la gestion au quotidien.

> ⓘ Cette documentation remplace le rapport technique *TR-4900 : VMware site Recovery Manager with ONTAP*

Les meilleures pratiques complètent d'autres documents, tels que des guides et des outils de compatibilité. Ils sont développés en fonction de tests effectués en laboratoire et d'une vaste expérience sur le terrain par les ingénieurs et les clients NetApp. Dans certains cas, les meilleures pratiques recommandées peuvent ne pas être adaptées à votre environnement. Cependant, ce sont généralement les solutions les plus simples qui répondent aux besoins des plus clients.

Ce document est axé sur les fonctionnalités des dernières versions de ONTAP 9 utilisées conjointement avec les outils ONTAP pour VMware vSphere 9.12 (notamment NetApp Storage Replication adapter [SRA] et VASA Provider [VP]), ainsi que VMware site Recovery Manager 8.7.

Pourquoi utiliser ONTAP avec SRM ?

Les plateformes de gestion des données NetApp optimisées par le logiciel ONTAP constituent certaines des solutions de stockage les plus utilisées pour SRM. Les raisons en sont nombreuses : une plateforme de gestion des données sécurisée, haute performance et multiprotocole unifié (NAS et SAN ensemble) qui fournit

l'efficacité du stockage, la colocation, le contrôle de la qualité de service, la protection des données avec des copies Snapshot compactes et la réplication avec SnapMirror. Exploitez l'intégration native du multicloud hybride pour protéger vos charges de travail VMware et bénéficier de nombreux outils d'automatisation et d'orchestration à portée de main.

Lorsque vous utilisez SnapMirror pour la réplication basée sur les baies, vous tirez parti de l'une des technologies ONTAP les plus éprouvées et les plus matures. SnapMirror vous permet de transférer les données de manière sécurisée et efficace en copiant uniquement les blocs du système de fichiers modifiés, et non les machines virtuelles entières ou les datastores. Même ces blocs tirent parti des économies d'espace, telles que la déduplication, la compression et la compaction. Les systèmes ONTAP modernes utilisent désormais SnapMirror, indépendant de la version, pour vous permettre de sélectionner plus de flexibilité vos clusters source et cible. SnapMirror est véritablement devenu l'un des outils les plus puissants disponibles pour la reprise après incident.

Que vous utilisiez des datastores NFS, iSCSI ou Fibre Channel classiques (désormais avec prise en charge des datastores vvols), SRM constitue une offre commerciale performante qui tire parti des fonctionnalités ONTAP pour la reprise après incident ou la planification et l'orchestration de la migration de data Center.

Comment SRM exploite ONTAP 9

SRM exploite les technologies avancées de gestion des données des systèmes ONTAP en l'intégrant aux outils ONTAP pour VMware vSphere, une appliance virtuelle qui englobe trois composants principaux :

- Le plug-in vCenter, précédemment appelé Virtual Storage Console (VSC), simplifie les fonctionnalités de gestion et d'efficacité du stockage, améliore la disponibilité et réduit les coûts de stockage ainsi que les charges opérationnelles, 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.
- Le fournisseur VASA pour ONTAP prend en charge la structure VMware vStorage APIs for Storage Awareness (VASA). Vasa Provider connecte vCenter Server avec ONTAP pour faciliter le provisionnement et la surveillance du stockage des machines virtuelles. Il assure la prise en charge de VMware Virtual volumes (vvols) et la gestion des profils de capacité de stockage (y compris les fonctionnalités de réplication vvols) ainsi que les performances individuelles de VM vvols. Il fournit également des alarmes pour la surveillance de la capacité et la conformité avec les profils. Utilisé conjointement avec SRM, le fournisseur VASA pour ONTAP permet la prise en charge des machines virtuelles basées sur vvols sans avoir à installer un adaptateur SRA sur le serveur SRM.
- SRA est utilisée en association avec SRM pour gérer la réplication des données des machines virtuelles entre les sites de production et de reprise après incident pour les datastores VMFS et NFS traditionnels, et pour les tests non disruptives des répliques de DR. Il permet d'automatiser les tâches de détection, de restauration et de reprotection. Elle inclut une appliance serveur SRA et des adaptateurs SRA pour le serveur Windows SRM et l'appliance SRM.

Après avoir installé et configuré les adaptateurs SRA sur le serveur SRM pour la protection des datastores non-vvols et/ou la réplication vvols activée dans les paramètres de VASA Provider, vous pouvez commencer la tâche de configuration de votre environnement vSphere pour la reprise après incident.

Les fournisseurs SRA et VASA proposent une interface de commande et de contrôle pour le serveur SRM afin de gérer les volumes FlexVol ONTAP contenant vos machines virtuelles VMware, ainsi que la réplication SnapMirror les protégeant.

À partir de SRM 8.3, un nouveau chemin de contrôle SRM vvols Provider a été introduit dans le serveur SRM, ce qui lui a permis de communiquer avec le serveur vCenter et, par le biais de celui-ci, au VASA Provider sans avoir besoin d'une SRA. Ainsi, le serveur SRM a pu mieux contrôler le cluster ONTAP qu'auparavant. En effet,

VASA fournit une API complète pour une intégration étroitement couplée.

SRM peut tester votre plan de reprise après incident sans interruption grâce à la technologie FlexClone propriétaire de NetApp pour créer des clones quasi instantanés de vos datastores protégés sur votre site de reprise après incident. SRM crée un sandbox afin de tester en toute sécurité afin que votre entreprise et vos clients soient protégés en cas d'incident, vous assurant ainsi la confiance de votre entreprise dans la capacité à exécuter un basculement lors d'un incident.

En cas d'incident véritable ou même de migration planifiée, SRM vous permet d'envoyer les modifications de dernière minute au jeu de données via une mise à jour SnapMirror finale (si vous le souhaitez). Il interrompt ensuite le miroir et monte le datastore sur vos hôtes de reprise après incident. À ce stade, vos machines virtuelles peuvent être automatiquement alimentées dans l'ordre de votre stratégie prédéfinie.

SRM avec ONTAP et autres cas d'utilisation : cloud hybride et migration

En intégrant votre déploiement de SRM aux fonctionnalités avancées de gestion des données de ONTAP, vous pouvez améliorer l'évolutivité et les performances par rapport aux options de stockage local. Elle apporte cependant la flexibilité du cloud hybride. Grâce au cloud hybride, vous pouvez réaliser des économies en transférant les blocs de données non utilisés de votre baie haute performance vers votre hyperscaler préférée, via FabricPool, qui peut être un magasin S3 sur site tel que NetApp StorageGRID. Vous pouvez également utiliser SnapMirror pour les systèmes basés en périphérie avec ONTAP Select l'infrastructure de reprise après incident Software-defined ou basée dans le cloud à l'aide de Cloud Volumes ONTAP (CVO) ou "NetApp Private Storage dans Equinix" Pour créer une pile de services de stockage, de réseau et de calcul entièrement intégrée dans le cloud, Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP)

Vous pouvez ensuite effectuer un basculement de test dans le data Center d'un fournisseur de services clouds avec une empreinte de stockage proche de zéro grâce à FlexClone. La protection de votre entreprise peut à présent être plus économique que jamais.

SRM peut également être utilisé pour exécuter des migrations planifiées en utilisant SnapMirror pour transférer efficacement vos machines virtuelles d'un data Center à un autre ou même au sein d'un même data Center, que vous le soyez propriétaire ou via plusieurs fournisseurs de services partenaires NetApp.

Bonnes pratiques de déploiement

Les sections suivantes présentent les meilleures pratiques de déploiement avec ONTAP et VMware SRM.

Disposition des SVM et segmentation pour la colocation sécurisée

Avec ONTAP, le concept de machine virtuelle de stockage (SVM) offre une segmentation stricte dans les environnements mutualisés sécurisés. Les utilisateurs des SVM situés sur un SVM ne peuvent ni accéder aux ressources d'un autre ni les gérer. De cette façon, vous pouvez exploiter la technologie ONTAP en créant des SVM distincts pour différentes unités commerciales qui gèrent leurs propres flux de travail SRM sur le même cluster, pour une efficacité globale supérieure du stockage.

Envisagez de gérer ONTAP avec des comptes SVM-scoped et des LIF de management SVM pour non seulement améliorer les contrôles de sécurité, mais aussi améliorer les performances. Les performances sont supérieures par nature lorsque des connexions SVM-scoped sont utilisées, car SRA n'est pas nécessaire pour traiter toutes les ressources d'un cluster entier, y compris les ressources physiques. Il ne doit plutôt comprendre que les ressources logiques qui sont extraites vers la SVM particulière.

Si vous utilisez uniquement des protocoles NAS (pas d'accès SAN), vous pouvez même exploiter le nouveau mode optimisé NAS en définissant le paramètre suivant (notez que le nom est tel, car SRA et VASA utilisent

les mêmes services back-end de l'appliance) :

1. Connectez-vous au panneau de commande à `https://<IP address>:9083` Et cliquez sur interface de ligne de commande Web.
2. Lancer la commande `vp updateconfig -key=enable.qtree.discovery -value=true`.
3. Lancer la commande `vp updateconfig -key=enable.optimised.sra -value=true`.
4. Lancer la commande `vp reloadconfig`.

Déployez des outils ONTAP et des considérations pour vvols

Si vous prévoyez d'utiliser SRM avec vvols, vous devez gérer le stockage à l'aide d'identifiants cluster-scoped et d'une LIF de cluster management. En effet, le fournisseur VASA doit comprendre l'architecture physique sous-jacente pour satisfaire aux exigences des règles de stockage des VM. Par exemple, si vous disposez d'une règle exigeant un stockage 100 % Flash, le fournisseur VASA doit pouvoir identifier les systèmes 100 % Flash.

Une autre meilleure pratique de déploiement est de ne jamais stocker votre appliance ONTAP Tools sur un datastore vvols qu'il gère. Cela peut entraîner une situation dans laquelle vous ne pouvez pas mettre le fournisseur VASA sous tension, car vous ne pouvez pas créer le vVol swap pour l'appliance, car l'appliance est hors ligne.

Meilleures pratiques pour la gestion des systèmes ONTAP 9

Comme mentionné précédemment, il est possible de gérer des clusters ONTAP avec des identifiants cluster ou SVM évalués et des LIF de gestion. Pour des performances optimales, il peut être intéressant d'utiliser des identifiants SVM- scoped lorsque vous n'utilisez pas les vVols. Cependant, ce faisant, vous devriez être conscient de certaines exigences, et que vous perdez certaines fonctionnalités.

- Le compte SVM vsadmin par défaut ne dispose pas du niveau d'accès requis pour effectuer les tâches des outils ONTAP Il faut donc créer un nouveau compte SVM.
- Si vous utilisez ONTAP 9.8 ou une version ultérieure, NetApp recommande de créer un compte utilisateur RBAC avec le moins de privilèges à l'aide du menu utilisateurs de ONTAP System Manager ainsi que le fichier JSON disponible sur votre appliance ONTAP Tools à l'adresse `https://<IP address>:9083/vsc/config/`. Utilisez votre mot de passe d'administrateur pour télécharger le fichier JSON. Il peut être utilisé pour les comptes évalués au niveau du SVM ou du cluster.

  Si vous utilisez ONTAP 9.6 ou une version antérieure, vous devez utiliser l'outil Créateur d'utilisateurs RBAC (RUC) disponible dans le "Outils du site de support NetApp".

- Le plug-in de l'interface utilisateur vCenter, VASA Provider et SRA Server étant tous des services entièrement intégrés, vous devez ajouter du stockage à l'adaptateur SRA dans SRM de la même manière que vous ajoutez du stockage dans l'interface utilisateur vCenter pour les outils ONTAP. Sinon, le serveur SRA pourrait ne pas reconnaître les requêtes envoyées depuis SRM via l'adaptateur SRA.
- La vérification du chemin NFS n'est pas effectuée avec les identifiants évalués par SVM. Car l'emplacement physique est logiquement extrait du SVM. Cela ne pose pas de problème, car les systèmes ONTAP modernes ne subissent plus de déclin perceptible des performances lors de l'utilisation de chemins indirects.
- Il est possible que les économies d'espace réalisées grâce à l'efficacité du stockage ne soient pas signalées.
- Lorsqu'ils sont pris en charge, les miroirs de partage de charge ne peuvent pas être mis à jour.

- Il est possible que la connexion EMS ne soit pas effectuée sur des systèmes ONTAP gérés avec des identifiants évalués par SVM.

Meilleures pratiques opérationnelles

Les sections suivantes présentent les meilleures pratiques opérationnelles pour VMware SRM et le stockage ONTAP.

Datastores et protocoles

- Si possible, utilisez toujours les outils ONTAP pour provisionner les datastores et les volumes. Cela vérifie que les volumes, les chemins de jonction, les LUN, les igroups, les règles d'exportation, et d'autres paramètres sont configurés de manière compatible.
- SRM prend en charge iSCSI, Fibre Channel et NFS version 3 avec ONTAP 9 lors de l'utilisation d'une réplication basée sur les baies via SRA. SRM ne prend pas en charge la réplication basée sur la baie pour NFS version 4.1 avec des datastores traditionnels ou vvols.
- Pour confirmer la connectivité, vérifiez toujours que vous pouvez monter et démonter un nouveau datastore test sur le site de reprise sur incident à partir du cluster ONTAP de destination. Testez chaque protocole que vous envisagez d'utiliser pour la connectivité du datastore. L'une des meilleures pratiques est d'utiliser les outils ONTAP pour créer votre datastore de test, car elle effectue toutes les automatisations du datastore telles que dirigées par SRM.
- Les protocoles SAN doivent être homogènes pour chaque site. Vous pouvez combiner les protocoles NFS et SAN, mais les protocoles SAN ne doivent pas être combinés dans un même site. Par exemple, vous pouvez utiliser FCP sur le site A et iSCSI sur le site B. Vous ne devez pas utiliser FCP et iSCSI sur le site A. La raison en est que SRA ne crée pas de groupes initiateurs mixtes sur le site de reprise et SRM ne filtre pas la liste des initiateurs donnée à SRA.
- Les guides précédents ont recommandé de créer la LIF pour la localisation des données. C'est-à-dire toujours monter un datastore à l'aide d'une LIF située sur le nœud qui détient physiquement le volume. Ce n'est plus une exigence dans les versions modernes de ONTAP 9. Dans la mesure du possible, et si des informations d'identification avec périmètre du cluster sont fournies, les outils ONTAP choisissent toujours d'équilibrer la charge entre les LIF locales aux données, mais il ne s'agit pas d'une exigence de haute disponibilité ou de performance.
- ONTAP 9 peut être configuré pour supprimer automatiquement les snapshots afin de préserver la disponibilité en cas de manque d'espace lorsque la taille automatique ne peut pas fournir une capacité d'urgence suffisante. Le paramètre par défaut de cette fonctionnalité ne supprime pas automatiquement les snapshots créés par SnapMirror. Si des snapshots SnapMirror sont supprimés, NetApp SRA ne peut pas inverser et resynchroniser la réplication pour le volume affecté. Pour empêcher ONTAP de supprimer des snapshots SnapMirror, configurez la fonctionnalité de suppression automatique de snapshots.

```
snap autodelete modify -volume -commitment try
```

- La taille automatique du volume doit être définie sur `grow` Pour les volumes contenant les datastores SAN et `grow_shrink` Pour les datastores NFS. En savoir plus sur "configuration des volumes pour l'extension ou la réduction automatique".
- SRM fonctionne mieux lorsque le nombre de datastores et donc les groupes de protection sont limités dans vos plans de reprise d'activité. Par conséquent, vous devez envisager d'optimiser la densité des machines virtuelles dans les environnements protégés par SRM où le RTO est essentiel.
- Utilisez Distributed Resource Scheduler (DRS) pour équilibrer la charge sur vos clusters ESXi protégés et de récupération. N'oubliez pas que si vous prévoyez de revenir en arrière, lorsque vous exécutez une

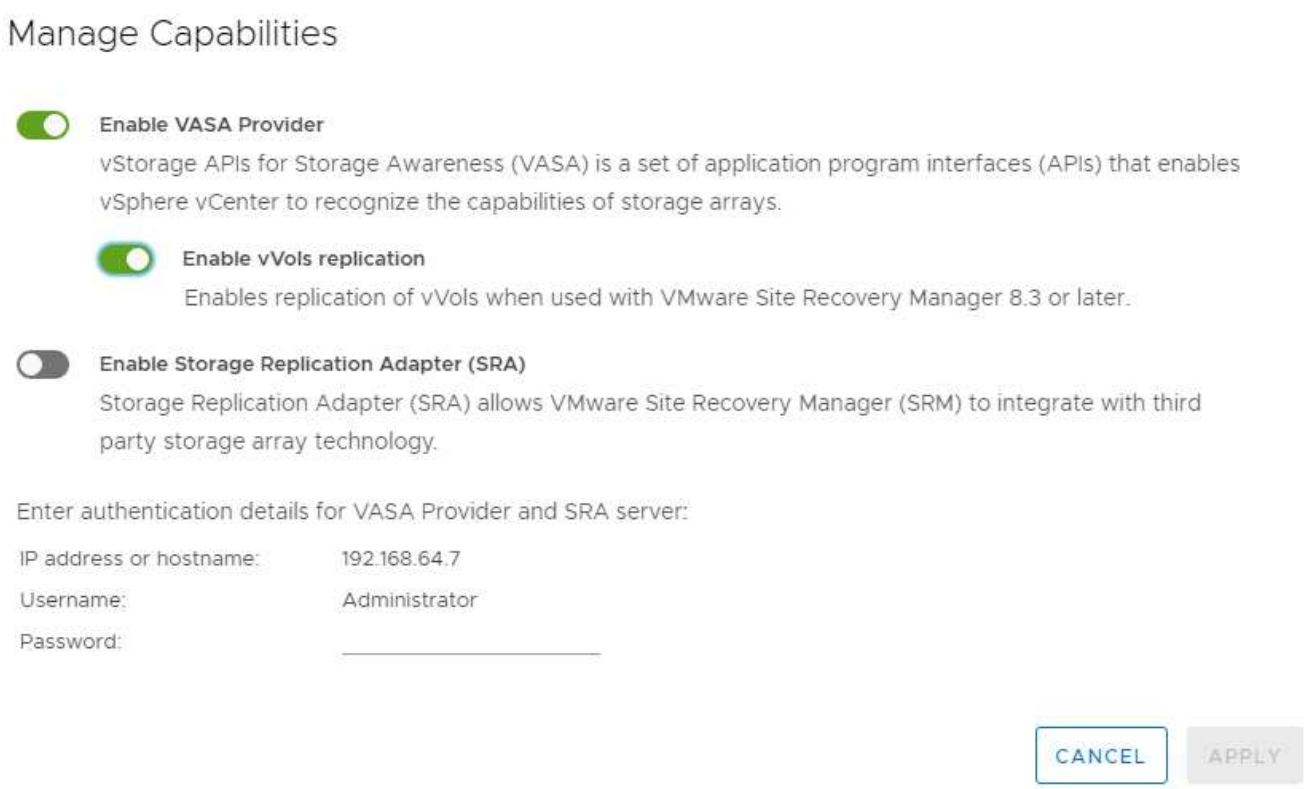
reprotection, les clusters précédemment protégés deviennent les nouveaux clusters de récupération. Le DRS contribue à équilibrer le placement dans les deux sens.

- Dans la mesure du possible, évitez d'utiliser la personnalisation IP avec SRM car cela peut augmenter votre RTO.

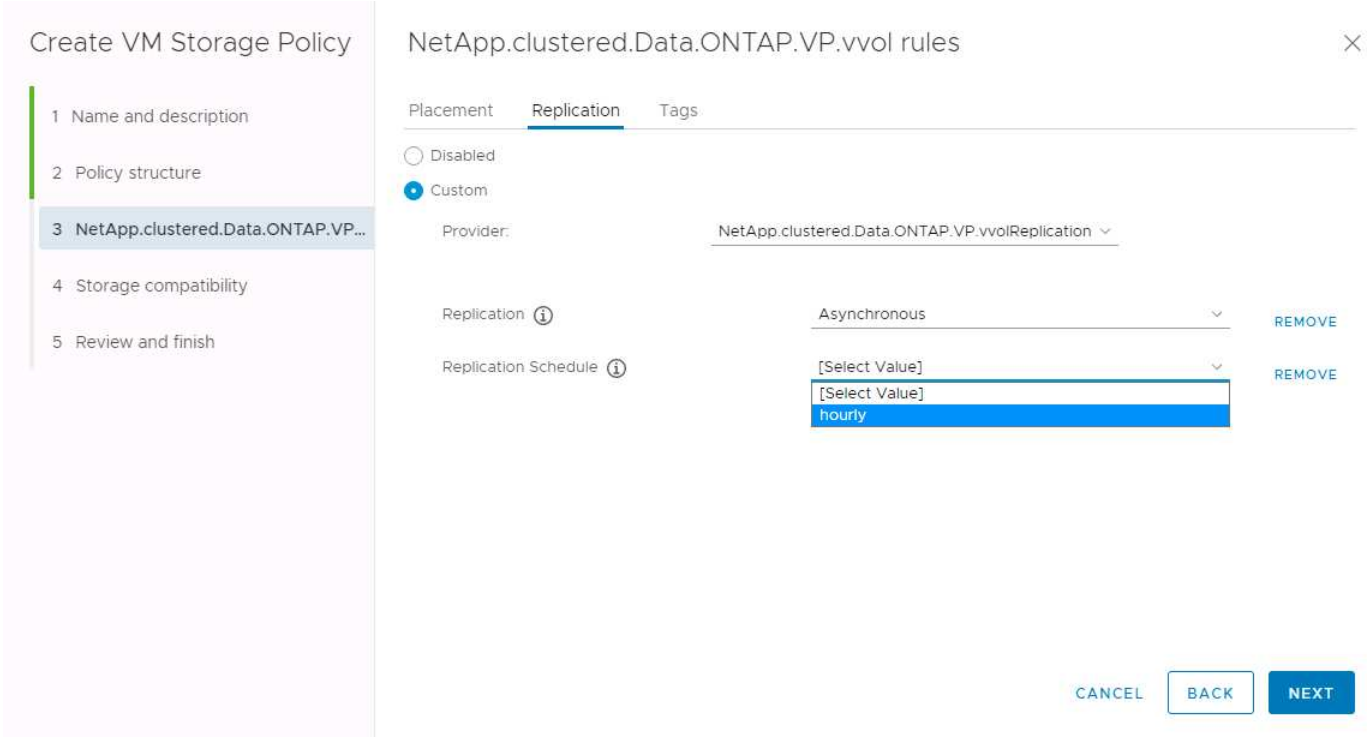
Gestion basée sur des règles de stockage (SPBM) et vVols

À partir de SRM 8.3, la protection des machines virtuelles à l'aide des datastores vVols est prise en charge. Les planifications SnapMirror sont exposées aux règles de stockage de VM par le VASA Provider lorsque la réplication de vvols est activée dans le menu des paramètres des outils ONTAP, comme indiqué dans les captures d'écran suivantes.

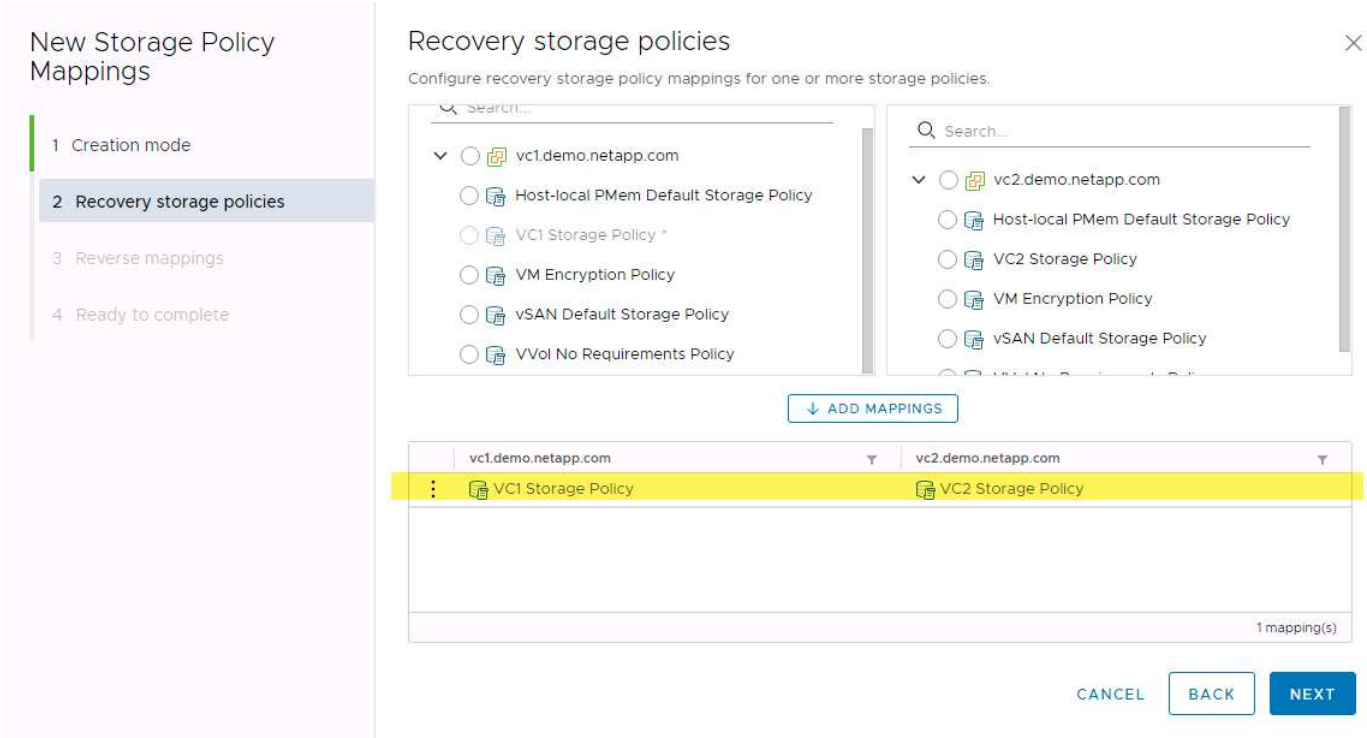
L'exemple suivant montre l'activation de la réplication vVols.



La capture d'écran suivante fournit un exemple de planifications SnapMirror affichées dans l'assistant de création de règles de stockage de machine virtuelle.



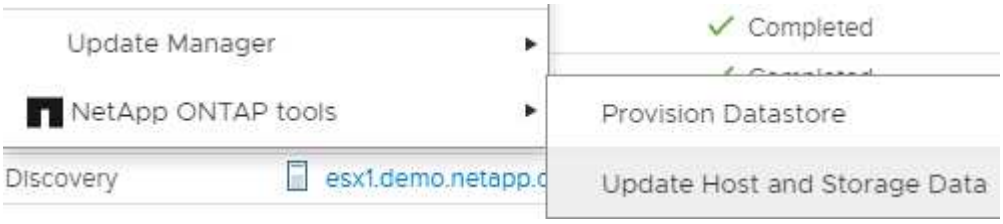
Le fournisseur ONTAP VASA prend en charge le basculement vers des systèmes de stockage différents. Par exemple, le système peut basculer d'un système ONTAP Select à un emplacement de périphérie vers un système AFF dans le data Center central. Indépendamment de la similarité de stockage, vous devez toujours configurer les mappages des règles de stockage et les mappages inversés des règles de stockage de machines virtuelles grâce à la réplication, afin de garantir que les services fournis sur le site de reprise répondent aux attentes et aux exigences de votre entreprise. La capture d'écran suivante met en évidence un exemple de mappage de règles.



Créez des volumes répliqués pour les datastores vvols

À la différence des précédents datastores vvols, les datastores vvols répliqués doivent être créés dès le début avec une réplication activée, et ils doivent utiliser des volumes pré-créés sur les systèmes ONTAP avec des relations SnapMirror. Cela nécessite de pré-configurer des éléments tels que le peering de cluster et de SVM. Ces activités doivent être réalisées par votre administrateur ONTAP, car elles permettent une séparation stricte des responsabilités entre ceux qui gèrent les systèmes ONTAP sur plusieurs sites et ceux qui sont principalement responsables des opérations vSphere.

Cette exigence est nouvelle pour le compte de l'administrateur vSphere. Les volumes étant créés hors du cadre des outils ONTAP, il n'est pas tenu de suivre les modifications apportées par votre administrateur ONTAP tant que la période de redécouverte planifiée n'est pas au moment de la prochaine découverte. C'est pourquoi il est recommandé de toujours exécuter la redécouverte chaque fois que vous créez un volume ou une relation SnapMirror à utiliser avec vvols. Il vous suffit de cliquer avec le bouton droit de la souris sur l'hôte ou le cluster et de sélectionner Outils ONTAP > mettre à jour les données d'hôte et de stockage, comme illustré dans la capture d'écran suivante.

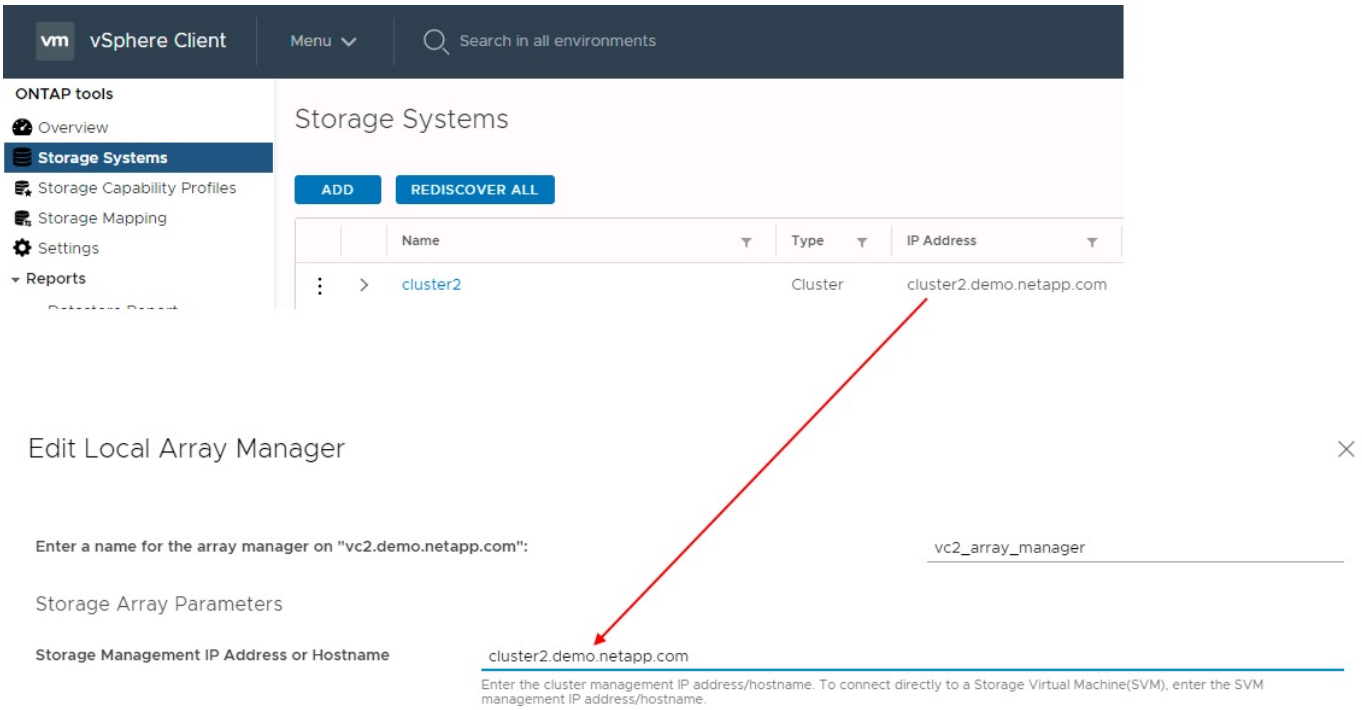


Il faut faire preuve de prudence lorsqu'il s'agit de vVvols et SRM. Ne mélangez jamais des machines virtuelles protégées et non protégées dans le même datastore vVvols. Cela s'explique par le fait que, lorsque vous utilisez SRM pour basculer vers votre site de reprise sur incident, seules les machines virtuelles qui font partie du groupe de protection sont mises en ligne sur le site de reprise sur incident. Par conséquent, lorsque vous reprotégez (repassez de SnapMirror de la reprise sur incident à la production), vous pouvez remplacer les machines virtuelles qui n'étaient pas basculées et qui pouvaient contenir des données précieuses.

À propos des paires de baies

Un gestionnaire de matrices est créé pour chaque paire de matrices. Avec les outils SRM et ONTAP, chaque association de baie s'effectue au sein d'un SVM, même si vous utilisez les identifiants du cluster. Vous pouvez ainsi segmenter les flux de travail de reprise après incident entre des locataires, en fonction des SVM qu'ils ont affectés à la gestion. Vous pouvez créer plusieurs gestionnaires de baies pour un cluster donné, qui peuvent être asymétriques. Vous pouvez « Fan-Out » ou « Fan-In » sur différents clusters ONTAP 9. Par exemple, il peut y avoir des SVM-A et SVM-B dans le Cluster-1 en cours de réplication vers SVM-C dans le Cluster-2, SVM-D dans le Cluster-3 ou vice-versa.

Lors de la configuration des paires de baies dans SRM, vous devez toujours les ajouter à SRM de la même manière que vous les avez ajoutés à ONTAP Tools : autrement dit, ils doivent utiliser le même nom d'utilisateur, mot de passe et LIF de gestion. Cette exigence garantit que SRA communique correctement avec la baie. La copie d'écran suivante montre comment un cluster peut s'afficher dans les outils ONTAP et comment il peut être ajouté à un gestionnaire de baies.



À propos des groupes de réplication

Les groupes de réplication contiennent des ensembles logiques de machines virtuelles qui sont restaurées ensemble. Le fournisseur VASA, un outil de ONTAP, crée automatiquement des groupes de réplication pour vous. Étant donné que la réplication SnapMirror de ONTAP se produit au niveau du volume, toutes les machines virtuelles d'un volume se trouvent dans le même groupe de réplication.

Il existe plusieurs facteurs à prendre en compte dans les groupes de réplication et dans la manière dont vous distribuez les machines virtuelles sur les volumes FlexVol. Le regroupement de machines virtuelles similaires dans un même volume peut améliorer l'efficacité du stockage avec les systèmes ONTAP plus anciens qui n'offrent pas de déduplication au niveau de l'agrégat. Cependant, ce regroupement augmente la taille du volume et réduit la simultanéité E/S du volume. Les systèmes ONTAP modernes offrent un équilibre parfait entre performance et efficacité du stockage en distribuant les machines virtuelles entre les volumes FlexVol au sein d'un même agrégat. La déduplication au niveau de l'agrégat améliore la parallélisation des E/S sur plusieurs volumes. Vous pouvez restaurer des VM dans les volumes simultanément, car un groupe de protection (voir ci-dessous) peut contenir plusieurs groupes de réplication. L'inconvénient de cette disposition est que les blocs peuvent être transmis plusieurs fois sur le réseau, car SnapMirror volume ne prend pas en compte la déduplication dans l'agrégat.

Dernier point à prendre en compte pour les groupes de réplication : chacun d'entre eux est, par nature, un groupe de cohérence logique (à ne pas confondre avec les groupes de cohérence SRM). En effet, toutes les machines virtuelles du volume sont transférées ensemble à l'aide du même snapshot. Ainsi, si vous disposez de machines virtuelles qui doivent être cohérentes les unes avec les autres, envisagez de les stocker dans le même FlexVol.

À propos des groupes de protection

Les groupes de protection définissent les VM et les datastores dans des groupes restaurés à partir du site protégé. Le site protégé est là où existent les VM configurées dans un groupe de protection pendant les opérations stables. Il est important de noter que même si SRM peut afficher plusieurs gestionnaires de baies pour un groupe de protection, un groupe de protection ne peut pas s'étendre sur plusieurs gestionnaires de baies. Pour cette raison, vous ne devez pas couvrir les fichiers de machine virtuelle sur plusieurs datastores

sur différents SVM.

À propos des plans de reprise

Les plans de reprise définissent les groupes de protection qui sont restaurés au cours du même processus. Plusieurs groupes de protection peuvent être configurés dans le même plan de reprise. Par ailleurs, pour activer davantage d'options pour l'exécution des plans de reprise, un seul groupe de protection peut être inclus dans plusieurs plans de restauration.

Les plans de restauration permettent aux administrateurs SRM de définir les flux de travail de restauration en affectant des VM à un groupe de priorité compris entre 1 (le plus élevé) et 5 (le plus faible), dont la valeur par défaut est 3 (moyen). Au sein d'un groupe de priorités, les VM peuvent être configurés pour les dépendances.

Par exemple, votre entreprise peut disposer d'une application stratégique de niveau 1 qui repose sur un serveur Microsoft SQL pour sa base de données. Vous décidez donc de placer vos machines virtuelles dans le groupe de priorité 1. Au sein du groupe de priorité 1, vous commencez à planifier la commande afin d'obtenir des services. Vous devez probablement démarrer votre contrôleur de domaine Microsoft Windows avant votre serveur Microsoft SQL, qui devra être en ligne avant votre serveur d'applications, etc. Vous devez ajouter toutes ces machines virtuelles au groupe de priorité, puis définir les dépendances, car elles ne s'appliquent qu'à un groupe de priorité donné.

NetApp recommande fortement de travailler avec vos équipes en charge des applications pour comprendre l'ordre des opérations requises dans un scénario de basculement et pour élaborer vos plans de reprise en conséquence.

Tester le basculement

Il est recommandé de toujours effectuer un basculement de test dès que la configuration d'un stockage protégé d'ordinateurs virtuels modifie. Ainsi, en cas d'incident, vous avez l'assurance que site Recovery Manager peut restaurer les services au sein de la cible de délai de restauration prévue.

NetApp recommande également de confirmer occasionnellement les fonctionnalités des applications chez l'invité, en particulier après la reconfiguration du stockage des machines virtuelles.

Lors de l'exécution d'une opération de restauration test, un réseau de bulles de test privé est créé sur l'hôte ESXi pour les machines virtuelles. Cependant, ce réseau n'est pas automatiquement connecté à aucune carte réseau physique et ne fournit donc pas de connectivité entre les hôtes ESXi. Pour permettre la communication entre les machines virtuelles s'exécutant sur différents hôtes ESXi lors du test de reprise après incident, un réseau privé physique est créé entre les hôtes ESXi du site de reprise après incident. Pour vérifier que le réseau de test est privé, le réseau de bulles de test peut être séparé physiquement ou à l'aide de VLAN ou de balisage VLAN. Ce réseau doit être isolé du réseau de production car les machines virtuelles sont restaurées. En effet, ils ne peuvent pas être placés sur le réseau de production avec des adresses IP qui pourraient entrer en conflit avec les systèmes de production réels. Lors de la création d'un plan de reprise d'activité dans SRM, le réseau test créé peut être sélectionné comme réseau privé afin de connecter les VM à pendant le test.

Une fois le test validé et n'est plus nécessaire, effectuez une opération de nettoyage. Le nettoyage en cours d'exécution renvoie l'état initial des machines virtuelles protégées à leur état initial et réinitialise le plan de restauration en mode prêt.

Considérations relatives au basculement

Il y a plusieurs autres considérations lorsqu'il s'agit de basculer sur un site en plus de l'ordre des opérations mentionné dans ce guide.

Vous devrez peut-être résoudre ce problème en tenant compte des différences de réseau entre les sites.

Certains environnements peuvent utiliser les mêmes adresses IP réseau à la fois sur le site primaire et sur le site de reprise après incident. Cette fonctionnalité est appelée VLAN (Virtual LAN) étendu ou configuration réseau étendu. Dans d'autres environnements, il est parfois nécessaire d'utiliser différentes adresses IP réseau (par exemple, sur différents VLAN) sur le site primaire par rapport au site de reprise.

VMware offre plusieurs moyens de résoudre ce problème. Pour la première, des technologies de virtualisation de réseau comme VMware NSX-T Data Center extraient la pile réseau des couches 2 à 7 de l'environnement d'exploitation, afin d'offrir des solutions plus portables. En savoir plus sur "Options NSX-T avec SRM".

SRM vous permet également de modifier la configuration réseau d'une machine virtuelle lors de sa restauration. Cette reconfiguration inclut des paramètres tels que les adresses IP, les adresses de passerelle et les paramètres du serveur DNS. Différents paramètres réseau, qui sont appliqués aux machines virtuelles individuelles au fur et à mesure qu'elles sont restaurées, peuvent être spécifiés dans les paramètres de propriété d'une machine virtuelle dans le plan de reprise.

Pour configurer SRM de façon à appliquer différents paramètres réseau à plusieurs machines virtuelles sans devoir modifier les propriétés de chacune d'entre elles dans le plan de reprise, VMware fournit un outil appelé dr-ip-customizer. Pour savoir comment utiliser cet utilitaire, reportez-vous à la section "Documentation de VMware".

Reprotéger

Après une restauration, le site de reprise devient le nouveau site de production. Comme l'opération de reprise a rompue la réplication SnapMirror, le nouveau site de production n'est pas protégé contre un futur incident. Il est recommandé de protéger le nouveau site de production sur un autre site immédiatement après une restauration. Si le site de production d'origine est opérationnel, l'administrateur VMware peut utiliser le site de production d'origine comme nouveau site de reprise pour protéger le nouveau site de production, ce qui inversera efficacement la direction de la protection. La reprotection est disponible uniquement en cas de défaillance majeure. Par conséquent, les serveurs vCenter d'origine, les serveurs ESXi, les serveurs SRM et les bases de données correspondantes doivent être récupérables. S'ils ne sont pas disponibles, un nouveau groupe de protection et un nouveau plan de récupération doivent être créés.

Du rétablissement

Une opération de retour arrière est fondamentalement un basculement dans une direction différente de celle précédente. Il est recommandé de vérifier que le site d'origine fonctionne à un niveau de fonctionnalité acceptable avant de tenter un retour arrière ou, en d'autres termes, un basculement vers le site d'origine. Si le site d'origine est toujours compromis, vous devez reporter la restauration jusqu'à ce que la défaillance soit suffisamment remédiée.

Une autre meilleure pratique de restauration consiste à toujours effectuer un basculement de test après avoir terminé la reprotection et avant de procéder à la restauration finale. Cela vérifie que les systèmes en place sur le site initial peuvent mener à bien l'opération.

Reprotéger le site d'origine

Après la restauration, vous devez confirmer auprès de toutes les parties prenantes que leurs services ont été renvoyés à la normale avant d'exécuter à nouveau reprotéger.

La reprotection après le retour arrière reprend l'état où il était au début, avec la réplication SnapMirror à nouveau en cours d'exécution depuis le site de production vers le site de reprise.

Topologies de réplication

Dans ONTAP 9, les composants physiques d'un cluster sont visibles pour les administrateurs du cluster, mais ils ne sont pas directement visibles pour les applications et les hôtes qui utilisent le cluster. Les composants physiques offrent un pool de ressources partagées à partir duquel les ressources logiques du cluster sont créées. Les applications et les hôtes accèdent aux données uniquement au moyen de SVM qui contiennent des volumes et des LIF.

Chaque SVM NetApp est traité comme une baie dans VMware vCenter site Recovery Manager. SRM prend en charge certaines dispositions de réplication baie à baie (ou SVM à SVM).

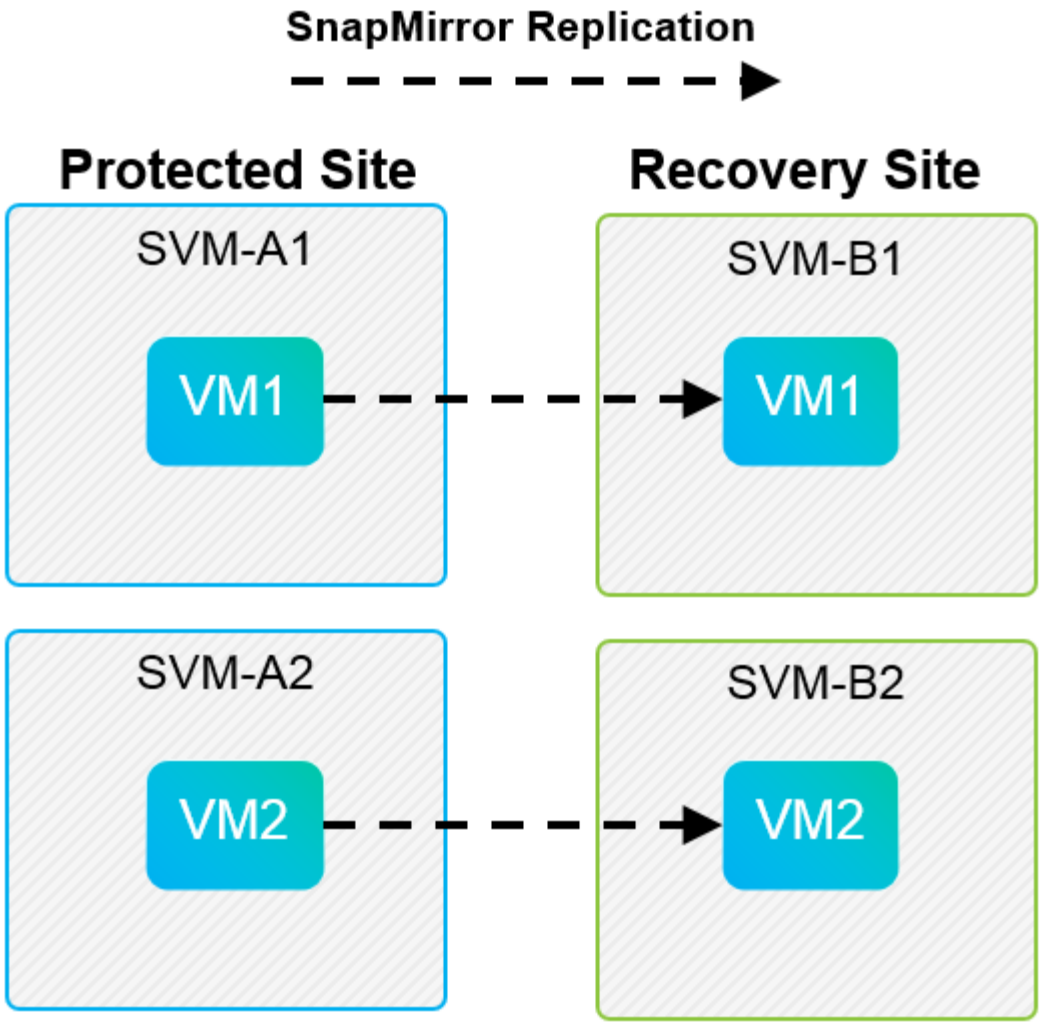
Une seule machine virtuelle ne peut pas héberger de données (Virtual machine Disk (VMDK) ou RDM) sur plusieurs baies SRM pour les raisons suivantes :

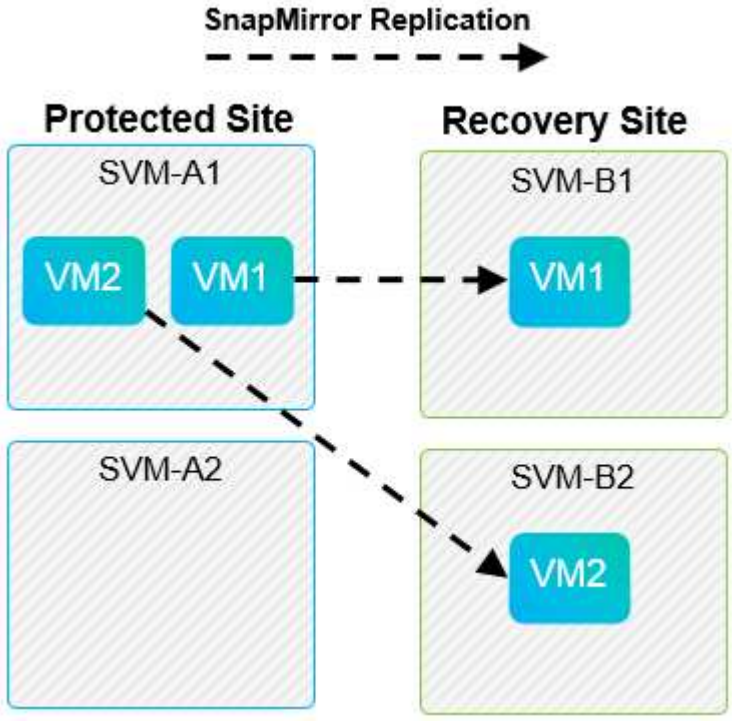
- SRM ne voit que la SVM, pas un contrôleur physique individuel.
- Un SVM peut contrôler les LUN et les volumes répartis sur plusieurs nœuds dans un cluster.

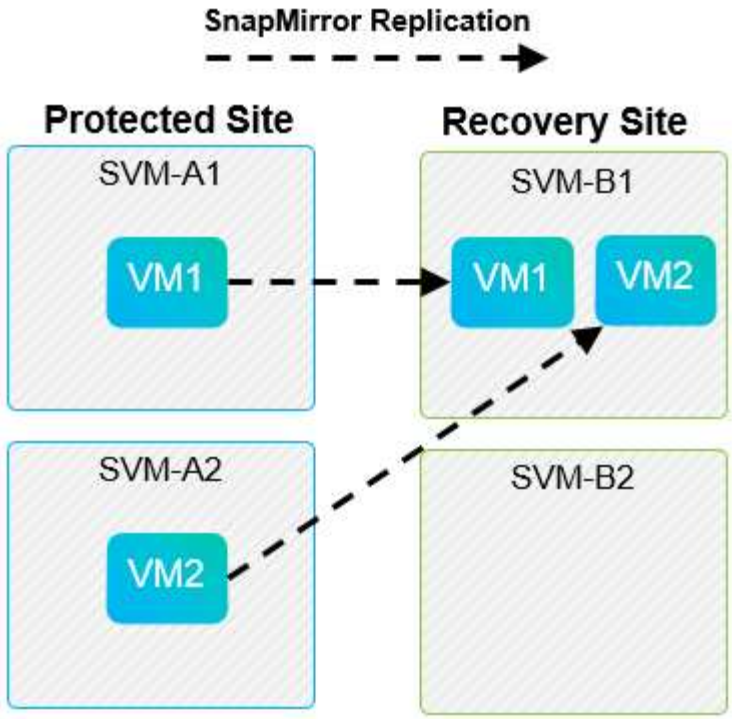
Meilleure pratique
Pour déterminer la prise en charge, conservez cette règle à l'esprit : pour protéger une machine virtuelle via SRM et NetApp SRA, tous les composants de la machine virtuelle doivent exister sur un seul SVM. Cette règle s'applique aussi bien au site protégé que au site de reprise.

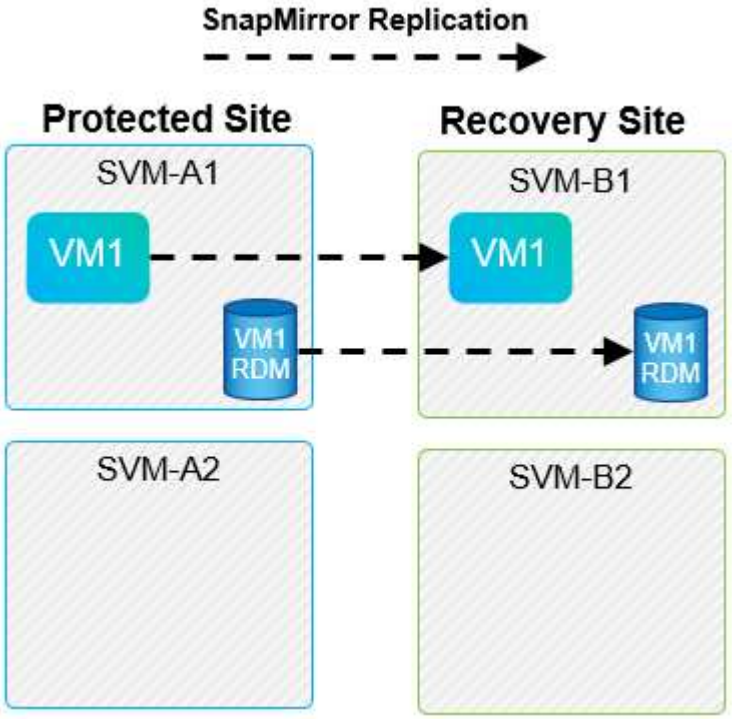
Dispositions SnapMirror prises en charge

Les figures suivantes présentent les scénarios de disposition des relations SnapMirror pris en charge par SRM et SRA. Chaque machine virtuelle des volumes répliqués est propriétaire de données sur une seule baie SRM (SVM) sur chaque site.


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2

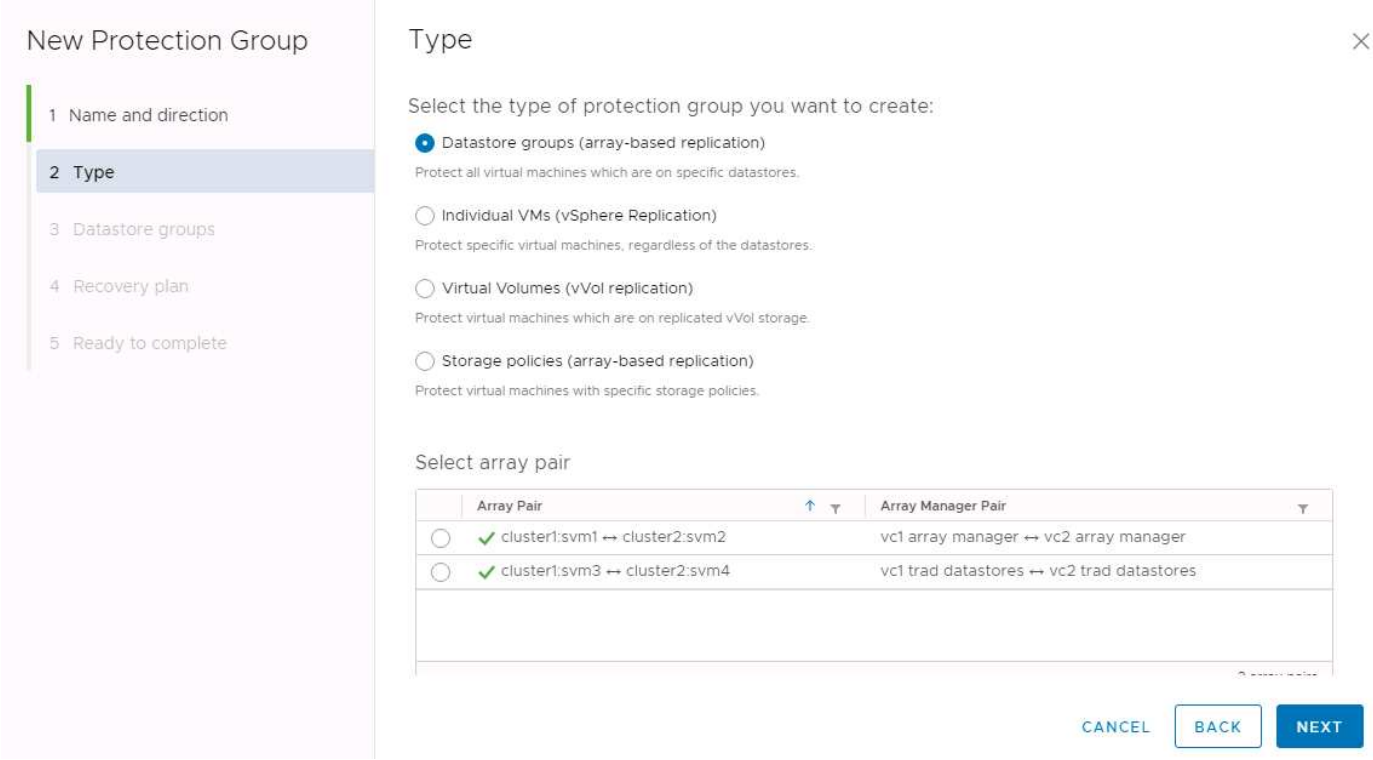

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2





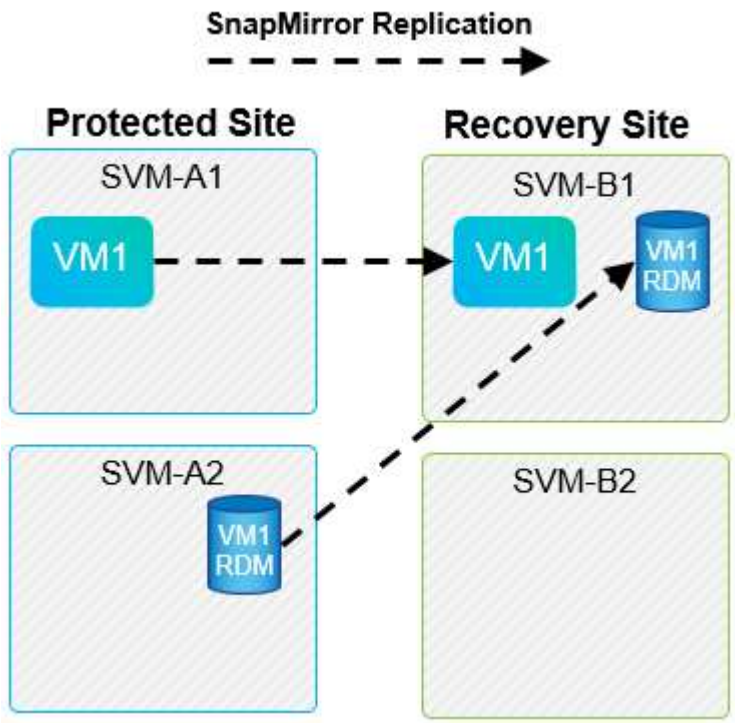
Mises en page de Array Manager prises en charge

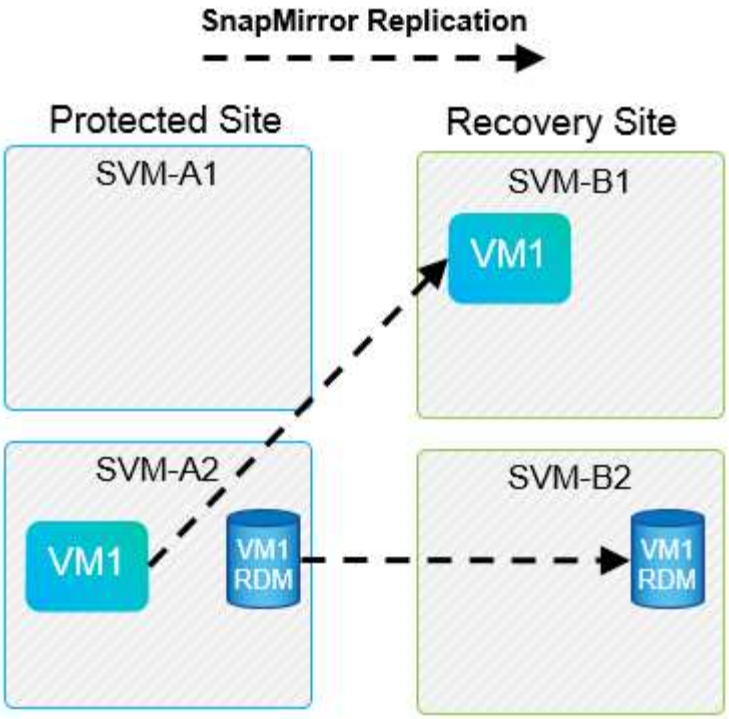
Lorsque vous utilisez la réplication basée sur la baie (ABR) dans SRM, les groupes de protection sont isolés vers une seule paire de baies, comme l'illustre la capture d'écran suivante. Dans ce scénario, `SVM1` et `SVM2` sont associés à `SVM3` et `SVM4` sur le site de reprise. Cependant, vous ne pouvez sélectionner qu'une des deux paires de matrices lorsque vous créez un groupe de protection.



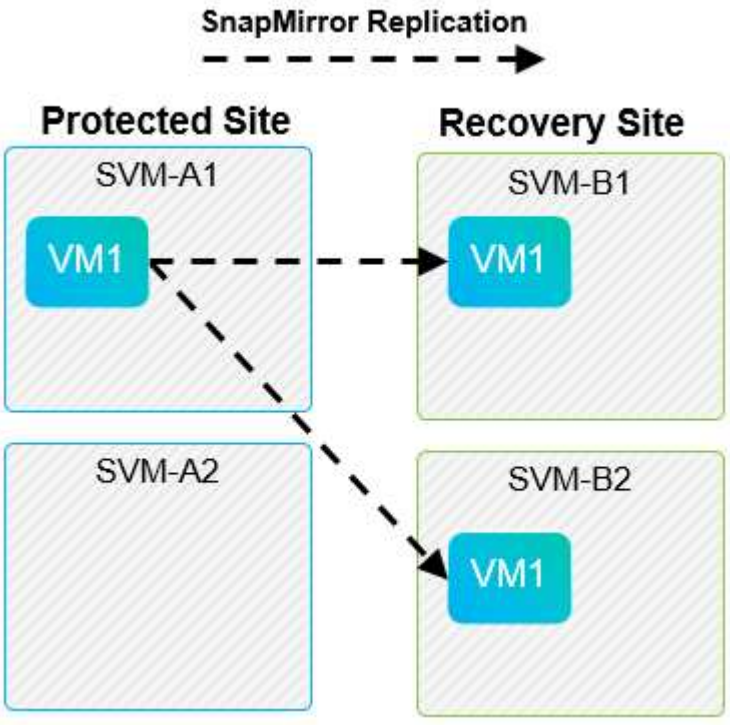
Présentations non prises en charge

Les configurations non prises en charge possèdent des données (VMDK ou RDM) sur plusieurs SVM appartenant à une machine virtuelle individuelle. Dans les exemples présentés dans les figures suivantes, `VM1` Ne peut pas être configuré pour la protection avec SRM car `VM1` Possède des données sur deux SVM.





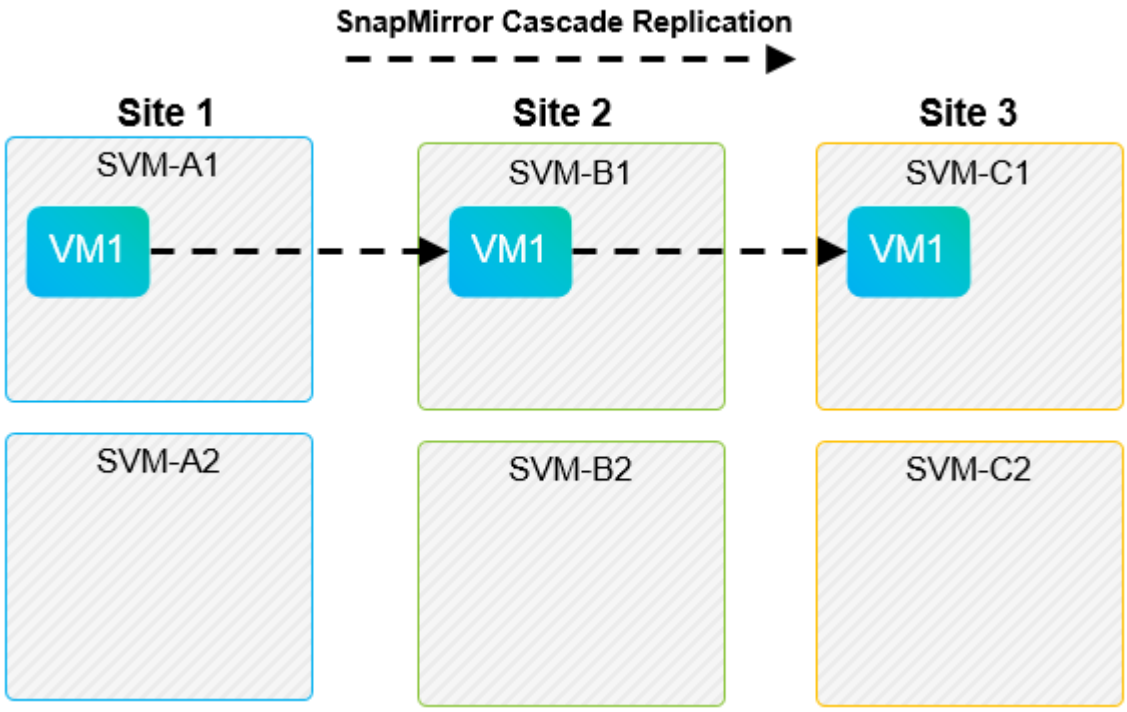
Toute relation de réplication dans laquelle un volume NetApp individuel est répliqué depuis un SVM source vers plusieurs destinations dans un même SVM ou dans différents SVM, est appelée « Fan-Out » de SnapMirror. La réplication « Fan-Out » n'est pas prise en charge par SRM. Dans l'exemple illustré dans la figure suivante, `VM1` Ne peut pas être configuré pour la protection dans SRM car elle est répliquée avec SnapMirror dans deux emplacements différents.



SnapMirror en cascade

SRM ne prend pas en charge le cascade des relations SnapMirror, dans lesquelles un volume source est répliqué sur un volume de destination, et ce volume de destination est également répliqué avec SnapMirror

vers un autre volume de destination. Dans le scénario illustré dans la figure suivante, SRM ne peut pas être utilisé pour le basculement entre des sites.



SnapMirror et SnapVault

Le logiciel NetApp SnapVault permet de sauvegarder les données d'entreprise sur disque entre les systèmes de stockage NetApp. SnapVault et SnapMirror peuvent coexister dans un même environnement, mais SRM prend en charge le basculement de uniquement les relations SnapMirror.

L'adaptateur NetApp SRA prend en charge le `mirror-vault` type de règle.

SnapVault a été entièrement reconstruit pour ONTAP 8.2. Bien que les anciens utilisateurs de Data ONTAP 7-mode trouvent des similarités, des améliorations majeures ont été apportées dans cette version d'SnapVault. Une avancée majeure est la capacité à préserver l'efficacité du stockage sur les données primaires au cours des transferts SnapVault.

L'architecture SnapVault de ONTAP 9 réplique au niveau du volume et non au niveau du qtree, comme c'est le cas avec 7-mode SnapVault. Dans ce cas, la source d'une relation SnapVault doit être un volume, et ce volume doit être répliqué sur son propre volume sur le système secondaire SnapVault.

Dans un environnement dans lequel SnapVault est utilisé, des snapshots nommés spécifiques sont créés sur le système de stockage principal. Selon la configuration implémentée, les snapshots nommés peuvent être créés sur le système principal par une planification SnapVault ou par une application telle que NetApp Active IQ Unified Manager. Les snapshots nommés créés sur le système primaire sont ensuite répliqués sur la destination SnapMirror, puis stockés sur la destination SnapVault.

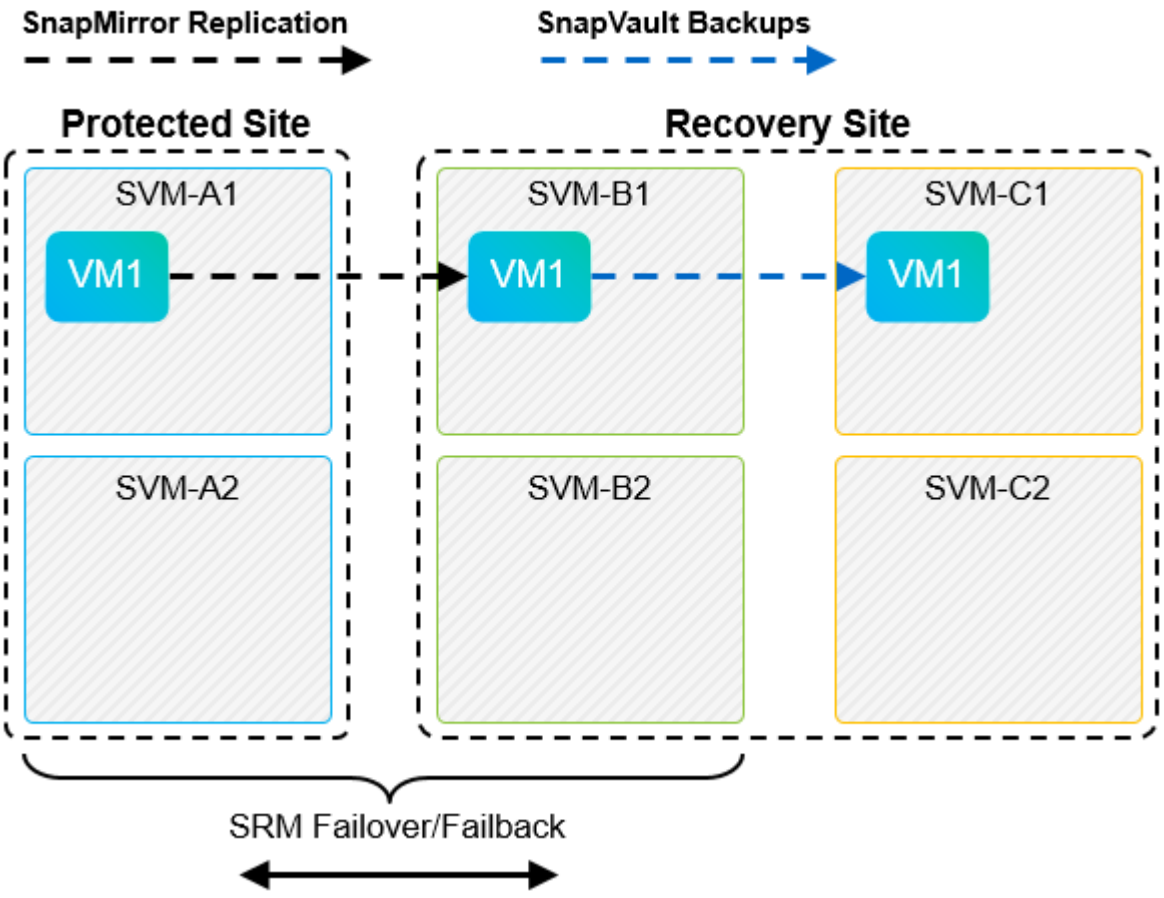
Un volume source peut être créé dans une configuration en cascade, dans laquelle un volume est répliqué vers une destination SnapMirror dans le site de reprise après incident, et depuis ce volume est copié vers une destination SnapVault. Un volume source peut également être créé au sein d'une relation « fan-out » où une destination est une destination SnapMirror et l'autre destination est une destination SnapVault. Toutefois, SRA ne reconfigurez pas automatiquement la relation SnapVault pour utiliser le volume de destination SnapMirror comme source du coffre-fort en cas de basculement ou d'inversion de réplication SRM.

Pour connaître les dernières informations concernant SnapMirror et SnapVault pour ONTAP 9, consultez "Tr-4015 Guide des meilleures pratiques en matière de configuration de SnapMirror pour ONTAP 9."

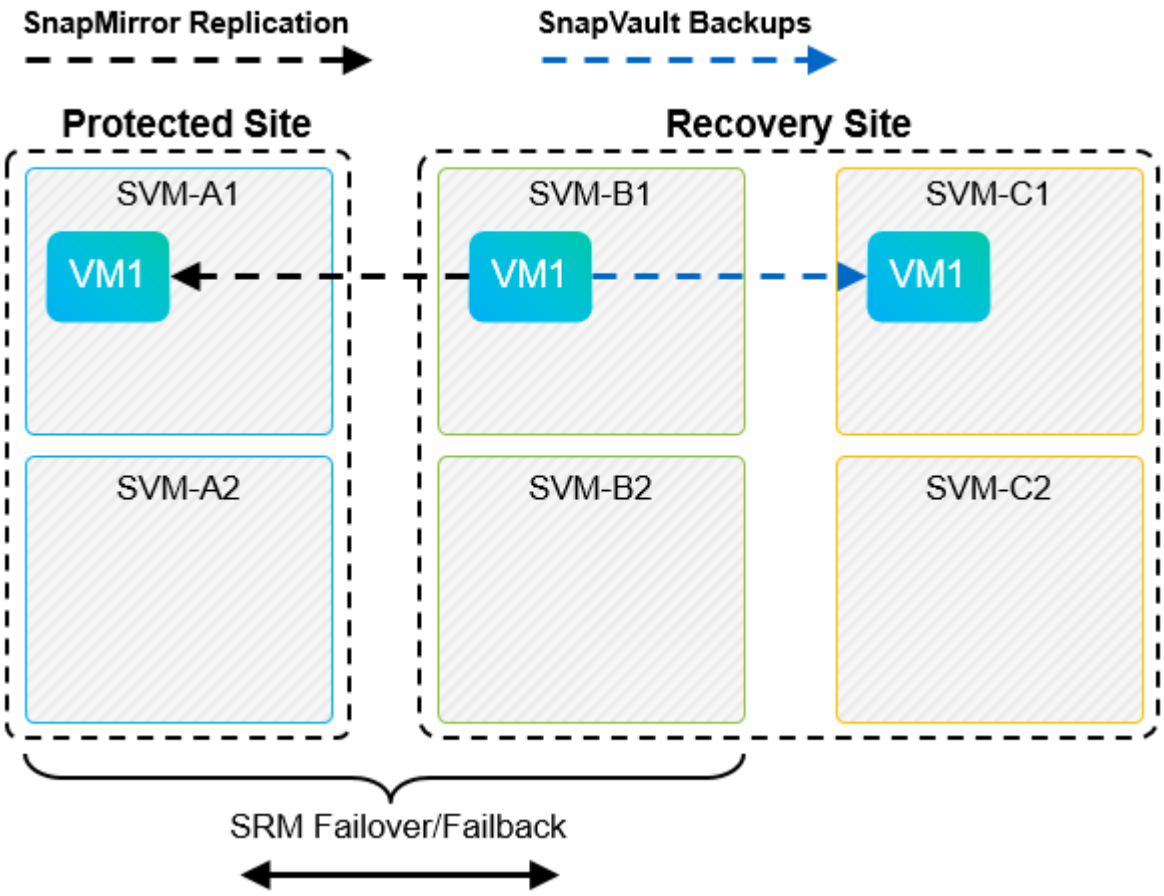
Meilleure pratique
Si SnapVault et SRM sont utilisés dans le même environnement, NetApp recommande d'utiliser une configuration SnapMirror vers SnapVault en cascade dans laquelle les sauvegardes SnapVault sont normalement exécutées à partir de la destination SnapMirror sur le site de reprise après incident. En cas d'incident, cette configuration rend le site principal inaccessible. Le fait de conserver la destination SnapVault sur le site de reprise permet de reconfigurer les sauvegardes SnapVault après le basculement, de sorte que les sauvegardes SnapVault puissent continuer sur le site de reprise.

Dans un environnement VMware, chaque datastore dispose d'un identifiant unique universel (UUID) et chaque machine virtuelle possède un ID d'objet géré unique (MOID). Ces identifiants ne sont pas gérés par SRM lors du basculement ou de la restauration. Étant donné que les UID et les MOID de machine virtuelle ne sont pas maintenus lors du basculement par SRM, toutes les applications qui dépendent de ces ID doivent être reconfigurées après le basculement SRM. NetApp Active IQ Unified Manager, qui coordonne la réplication SnapVault avec l'environnement vSphere, est un exemple d'application.

La figure suivante décrit une configuration SnapMirror vers SnapVault en cascade. Si la destination SnapVault se trouve sur le site de reprise après incident ou sur un site tertiaire non affecté par une panne sur le site primaire, l'environnement peut être reconfiguré afin de permettre la continuité des sauvegardes après le basculement.



La figure suivante décrit la configuration après l'utilisation de SRM pour renvoyer la réplication SnapMirror vers le site primaire. L'environnement a également été reconfiguré de façon à ce que les sauvegardes SnapVault s'effectuent à partir d'une source SnapMirror. Cette configuration est « Fan-Out » de SnapMirror SnapVault.



Une fois que SRM a effectué une restauration et une seconde inversion des relations SnapMirror, les données de production sont de nouveau sur le site principal. Ces données sont désormais protégées de la même manière qu'avant le basculement vers le site de reprise après incident, via les sauvegardes SnapMirror et SnapVault.

Utilisation de qtrees dans les environnements site Recovery Manager

Les qtrees sont des répertoires spéciaux qui permettent l'application de quotas de système de fichiers pour NAS. ONTAP 9 permet la création de qtrees et peut exister dans les volumes répliqués avec SnapMirror. Toutefois, SnapMirror ne permet pas la réplication de qtrees individuels ni de réplication au niveau qtree. Toute la réplication SnapMirror se fait au niveau du volume uniquement. C'est pour cette raison que NetApp ne recommande pas l'utilisation de qtrees avec SRM.

Environnements FC et iSCSI mixtes

Grâce à la prise en charge des protocoles SAN (FC, FCoE et iSCSI), ONTAP 9 propose des services LUN, à savoir la création de LUN et leur mappage vers les hôtes associés. Dans la mesure où le cluster compte plusieurs contrôleurs, il existe plusieurs chemins logiques gérés par les E/S multivoies vers une LUN individuelle. L'accès ALUA (Asymmetric Logical Unit Access) est utilisé sur les hôtes pour que le chemin optimisé vers un LUN soit sélectionné et activé pour le transfert de données. Si ce chemin change (par exemple, en raison du déplacement du volume qui y est associé), ONTAP 9 reconnaît automatiquement cette modification et s'ajuste de façon non disruptive. S'il devient indisponible, ONTAP peut également basculer sans interruption sur un autre chemin.

VMware SRM et NetApp SRA prennent en charge l'utilisation du protocole FC sur un site et le protocole iSCSI sur l'autre site. Il ne prend pas en charge la combinaison de datastores FC et de datastores iSCSI dans le même hôte ESXi ou d'hôtes différents dans le même cluster. Cette configuration n'est pas prise en charge

avec SRM car, pendant le basculement SRM ou le basculement de test, SRM inclut tous les initiateurs FC et iSCSI des hôtes ESXi dans la demande.

Meilleure pratique
SRM et SRA prennent en charge les protocoles FC et iSCSI mixtes entre les sites protégés et de reprise. Cependant, chaque site ne doit pas être configuré avec un seul protocole, FC ou iSCSI, et non avec les deux protocoles sur le même site. Si il est nécessaire de configurer les protocoles FC et iSCSI sur le même site, NetApp recommande que certains hôtes utilisent iSCSI et d'autres hôtes utilisent FC. Dans ce cas, NetApp recommande également de configurer les mappages de ressources SRM de sorte que les VM soient configurés pour basculer vers un groupe d'hôtes ou un autre.

Dépannage de SRM lors de l'utilisation de la réplication de vvols

Le flux de travail de SRM est significativement différent lors de l'utilisation de la réplication vvols à partir de ce qui est utilisé avec SRA et les datastores traditionnels. Par exemple, il n'existe pas de concept de gestionnaire de baie. Comme c'est le cas, `discoverarrays` et `discoverdevices` les commandes ne sont jamais vues.

Lors du dépannage, il est utile de comprendre les nouveaux flux de travail répertoriés ci-dessous :

1. QueryReplicationPeer : détecte les accords de réplication entre deux domaines de défaillance.
2. QueryFaultDomain : détecte la hiérarchie du domaine de pannes.
3. QueryReplicationGroup : détecte les groupes de réplication présents dans les domaines source ou cible.
4. SyncReplicationGroup : synchronise les données entre la source et la cible.
5. QueryPointInTimeReplica : détecte le point dans le temps des répliques sur une cible.
6. TestFailoverReplicationGroupStart : démarre le basculement de test.
7. TestFailoverReplicationGroupStop : met fin au basculement de test.
8. PromoteReplicationGroup : promeut un groupe actuellement en cours de test à la production.
9. PreparFailoverReplicationTM : prépare une reprise après sinistre.
10. FailoverReplicationGroup : exécute la reprise après incident.
11. ReverseReplicateGroup : lance la réplication inverse.
12. QueryMatchingContainer : recherche les conteneurs (ainsi que les hôtes ou les groupes de réplication) susceptibles de satisfaire une demande de provisionnement avec une règle donnée.
13. QueryResourceMetadata : recherche les métadonnées de toutes les ressources du fournisseur VASA, l'utilisation des ressources peut être renvoyée comme réponse à la fonction queryMatchingContainer.

L'erreur la plus courante lors de la configuration de la réplication vvols est une incapacité à découvrir les relations SnapMirror. En effet, les volumes et les relations SnapMirror sont créés en dehors de la purView des outils ONTAP. Il est donc recommandé de toujours s'assurer que votre relation SnapMirror est totalement initialisée et que vous avez exécuté une redécouverte dans les outils ONTAP sur les deux sites avant de tenter de créer un datastore vvols répliqué.

Informations supplémentaires

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

- Tr-4597 : VMware vSphere pour ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- Tr-4400 : volumes virtuels VMware vSphere avec ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- Tr-4015 Guide des meilleures pratiques en matière de configuration de SnapMirror pour ONTAP 9
  https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- Créateur d'utilisateurs RBAC pour ONTAP
  "https://mysupport.netapp.com/site/tools/tool-eula/rbac"
- Outils ONTAP pour les ressources VMware vSphere
  "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- Documentation VMware site Recovery Manager
  "https://docs.vmware.com/en/Site-Recovery-Manager/index.html"

Reportez-vous à la "Matrice d'interopérabilité (IMT)" Le site de support NetApp vous assure que les versions de produits et de fonctionnalités mentionnées dans le présent document sont prises en charge par votre environnement. NetApp IMT définit les composants et versions de produits qu'il est possible d'utiliser pour créer des configurations prises en charge par NetApp. Les résultats dépendent des installations de chaque client et de leur conformité aux spécifications publiées.

Cluster de stockage vSphere Metro avec ONTAP

Cluster de stockage vSphere Metro avec ONTAP

L'hyperviseur vSphere de pointe de VMware peut être déployé en tant que cluster étendu appelé vMSC (vSphere Metro Storage Cluster).

Les solutions VMSC sont prises en charge avec NetApp® MetroCluster™ et la synchronisation active SnapMirror (anciennement appelée SnapMirror Business Continuity ou SMBC) et assurent une continuité de l'activité avancée si un ou plusieurs domaines à défaillance subissent une panne totale. La résilience aux différents modes de défaillance dépend des options de configuration que vous choisissez.

Disponibilité continue pour les environnements vSphere

L'architecture ONTAP est une plateforme de stockage flexible et évolutive qui fournit des services SAN (FCP, iSCSI et NVMe-of) et NAS (NFS v3 et v4.1) pour les datastores. Les systèmes de stockage NetApp AFF, ASA et FAS utilisent le système d'exploitation ONTAP pour offrir des protocoles supplémentaires pour l'accès au stockage invité comme S3 et SMB/CIFS.

NetApp MetroCluster utilise la fonction HA (basculement du contrôleur ou CFO) de NetApp pour se protéger contre les défaillances du contrôleur. Elle inclut également la technologie SyncMirror locale, le basculement de cluster en cas d'incident (basculement du contrôleur à la demande ou CFOD), la redondance matérielle et la séparation géographique pour atteindre des niveaux élevés de disponibilité. SyncMirror met en miroir les données de manière synchrone sur les deux moitiés de la configuration MetroCluster en écrivant les données sur deux plexes : le plex local (sur le tiroir local) assure activement le service des données et le plex distant (sur le tiroir distant) n'assure généralement pas le service des données. La redondance matérielle est mise en place pour tous les composants MetroCluster, tels que les contrôleurs, le stockage, les câbles, les commutateurs (utilisés avec Fabric MetroCluster) et les adaptateurs.

La synchronisation active NetApp SnapMirror offre une protection granulaire des datastores avec les protocoles SAN FCP et iSCSI, ce qui vous permet de protéger de manière sélective uniquement les workloads

prioritaires. Il offre un accès actif/actif aux sites locaux et distants, contrairement à NetApp MetroCluster, qui est une solution de secours actif. Actuellement, la synchronisation active est une solution asymétrique où l'un des côtés est préféré à l'autre, offrant de meilleures performances. Pour ce faire, la fonctionnalité ALUA (Asymmetric Logical Unit Access) informe automatiquement l'hôte ESXi des contrôleurs qui lui préfèrent. Cependant, NetApp a annoncé qu'une synchronisation active permettra bientôt un accès totalement symétrique.

Pour créer un cluster VMware HA/DRS sur deux sites, les hôtes ESXi sont utilisés et gérés par une appliance vCenter Server (VCSA). Les réseaux de gestion vSphere, vMotion® et machine virtuelle sont connectés via un réseau redondant entre les deux sites. Le serveur vCenter gérant le cluster HA/DRS peut se connecter aux hôtes ESXi sur les deux sites et doit être configuré à l'aide de vCenter HA.

Reportez-vous à la section "Comment créer et configurer des clusters dans le client vSphere" Pour configurer vCenter HA.

Reportez-vous également à la section "Bonnes pratiques pour VMware vSphere Metro Storage Cluster".

Qu'est-ce que le cluster de stockage vSphere Metro ?

VSphere Metro Storage Cluster (vMSC) est une configuration certifiée qui protège les machines virtuelles et les conteneurs contre les défaillances. Pour y parvenir, les concepts de stockage étendus ainsi que les clusters d'hôtes ESXi sont répartis sur différents domaines à défaillance, tels que les racks, les bâtiments, les campus ou même les villes. Les technologies de stockage avec synchronisation active NetApp MetroCluster et SnapMirror assurent respectivement une protection RPO=0 ou RPO=0 aux clusters hôtes. La configuration vMSC est conçue pour assurer la disponibilité continue des données, même en cas de défaillance d'un « site » physique ou logique complet. Un périphérique de stockage faisant partie de la configuration vMSC doit être certifié après avoir suivi un processus de certification vMSC réussi. Tous les périphériques de stockage pris en charge sont disponibles dans le "Guide de compatibilité du stockage VMware".

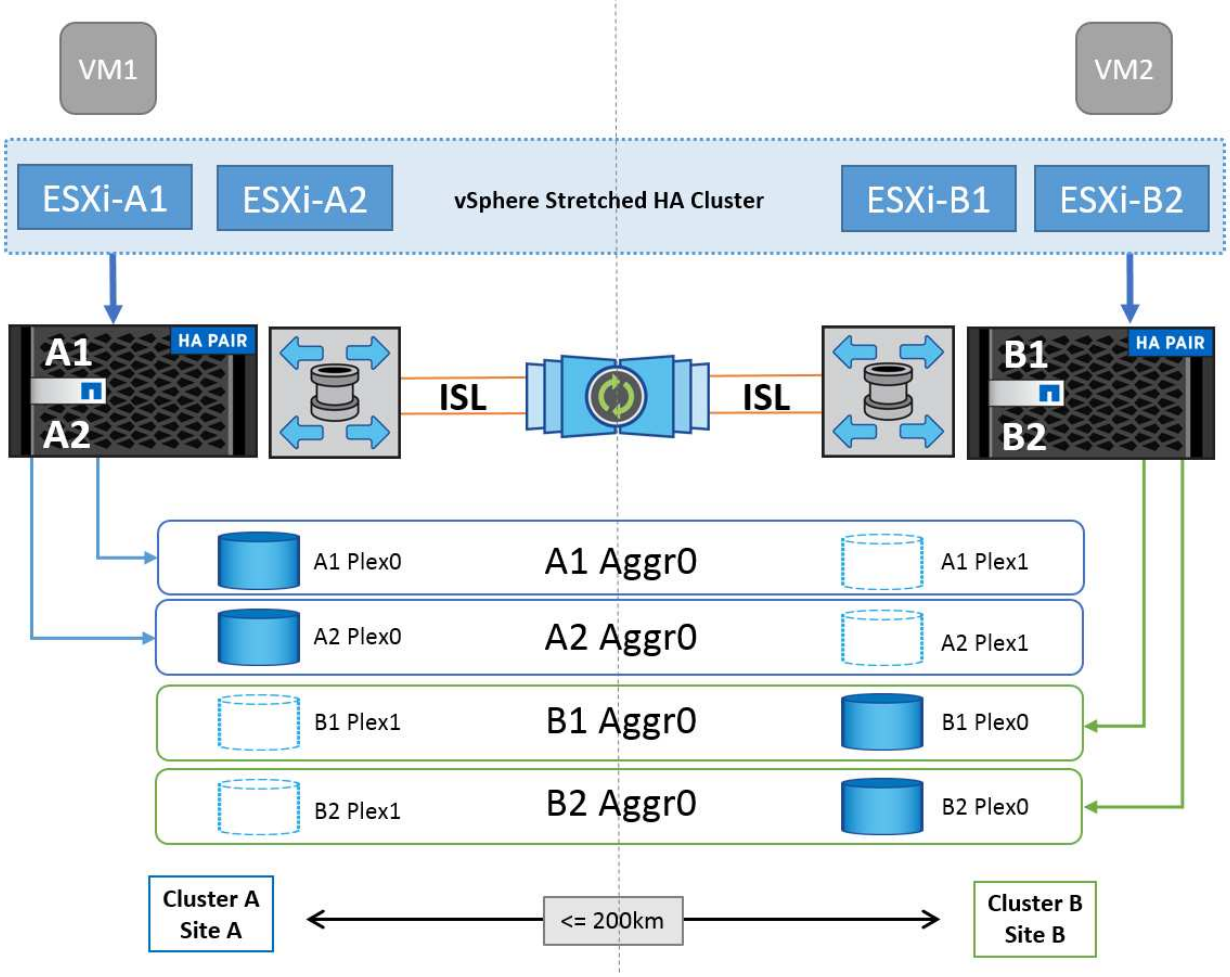
Pour plus d'informations sur les conseils de conception pour vSphere Metro Storage Cluster, reportez-vous à la documentation suivante :

- "Prise en charge de VMware vSphere avec NetApp MetroCluster"
- "Prise en charge de VMware vSphere avec la continuité de l'activité NetApp SnapMirror" (Maintenant appelé synchronisation active SnapMirror)

Selon les considérations relatives à la latence, NetApp MetroCluster peut être déployé dans deux configurations différentes pour une utilisation avec vSphere :

- MetroCluster extensible
- MetroCluster de structure

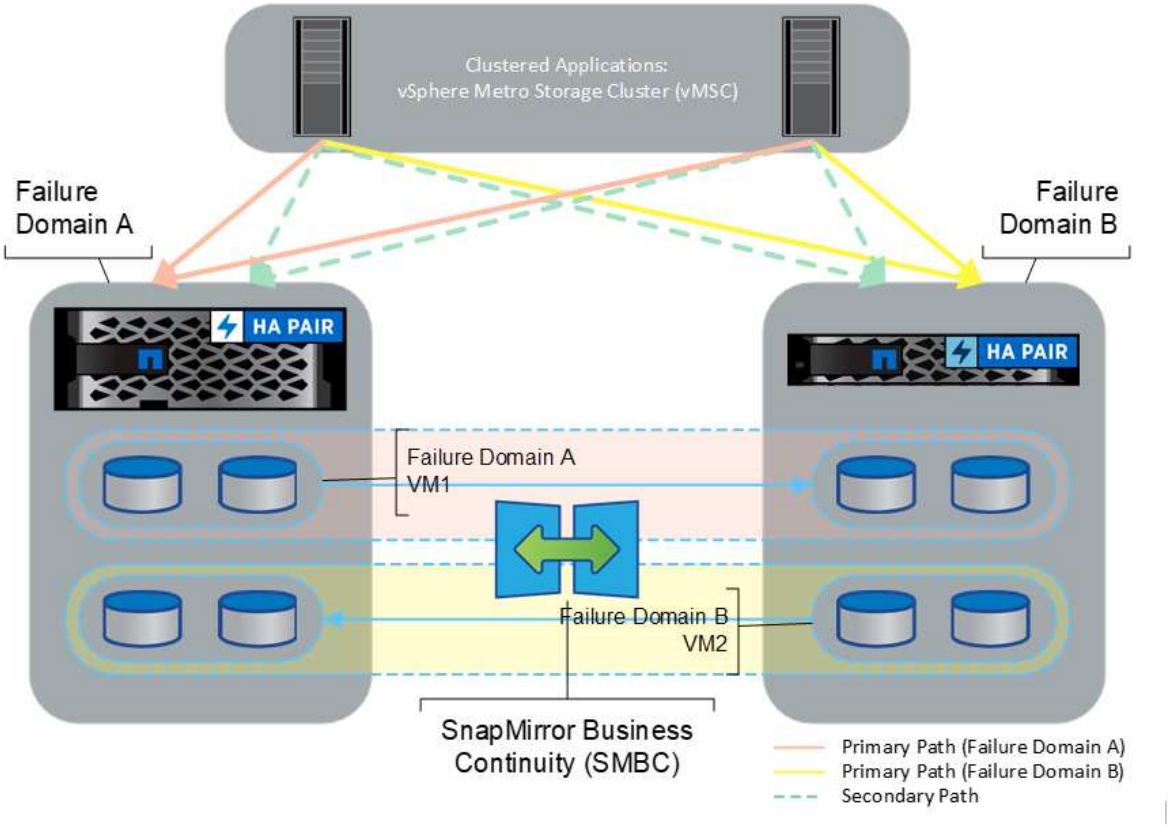
Voici une illustration de la topologie générale d'Stretch MetroCluster.



Reportez-vous à la section "Documentation MetroCluster" Pour obtenir des informations spécifiques sur la conception et le déploiement de MetroCluster.

La synchronisation active SnapMirror peut également être déployée de deux manières différentes.

- Asymétrique
- Symétrique (préversion privée dans ONTAP 9.14.1)



Reportez-vous à la section "Documents NetApp" Pour des informations spécifiques sur le design et le déploiement de SnapMirror active Sync.

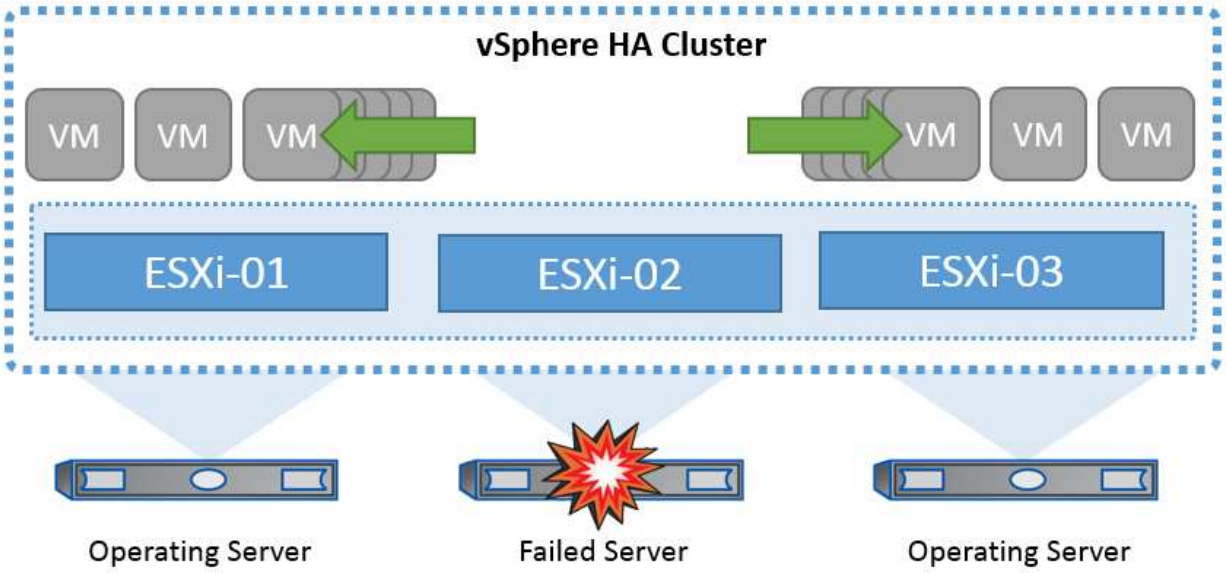
Présentation de la solution VMware vSphere

VCenter Server Appliance (VCSA) est le puissant système de gestion centralisée et une interface unique pour vSphere qui permet aux administrateurs d'exploiter efficacement les clusters ESXi. Cet outil facilite les fonctions clés telles que le provisionnement des machines virtuelles, les opérations vMotion, la haute disponibilité (HA), Distributed Resource Scheduler (DRS), Tanzu Kubernetes Grid et bien plus encore. Elle constitue un composant essentiel des environnements clouds VMware et doit être conçue en tenant compte de la disponibilité du service.

Haute disponibilité vSphere

La technologie de cluster de VMware regroupe les serveurs ESXi en pools de ressources partagées pour les machines virtuelles et fournit la haute disponibilité (HA) vSphere. VSphere HA offre une haute disponibilité et une simplicité d'utilisation pour les applications qui s'exécutent sur des machines virtuelles. Lorsque la fonction de haute disponibilité est activée sur le cluster, chaque serveur ESXi maintient la communication avec les autres hôtes de sorte que si un hôte ESXi ne répond plus ou est isolé, le cluster de haute disponibilité peut négocier la restauration des machines virtuelles qui s'exécutaient sur cet hôte ESXi parmi les hôtes survivants du cluster. En cas de défaillance d'un système d'exploitation invité, vSphere HA redémarre la machine virtuelle concernée sur le même serveur physique. La haute disponibilité vSphere permet de réduire les temps d'indisponibilité planifiés, d'éviter les temps d'indisponibilité non planifiés et de restaurer rapidement les données en cas de panne.

Cluster vSphere HA qui récupère les machines virtuelles à partir d'un serveur défaillant.



Il est important de comprendre que VMware vSphere ne connaît pas la synchronisation active NetApp MetroCluster ou SnapMirror et que tous les hôtes ESXi du cluster vSphere sont identifiés comme des hôtes éligibles pour les opérations de cluster haute disponibilité selon les configurations d'affinité de l'hôte et du groupe de machines virtuelles.

Détection de défaillance de l'hôte

Dès la création du cluster HA, tous les hôtes du cluster participent à des élections et l'un des hôtes devient maître. Chaque esclave exécute une pulsation réseau vers le maître, et le maître effectue à son tour une pulsation réseau sur tous les hôtes esclaves. L'hôte maître d'un cluster vSphere HA est responsable de la détection de la défaillance des hôtes esclaves.

En fonction du type de défaillance détecté, les machines virtuelles exécutées sur les hôtes peuvent avoir besoin d'être basculées.

Dans un cluster vSphere HA, trois types de défaillance d'hôte sont détectés :

- Défaillance - Un hôte cesse de fonctionner.
- Isolation - Un hôte devient isolé du réseau.
- Partition : Un hôte perd la connectivité réseau avec l'hôte maître.

L'hôte maître surveille les hôtes esclaves du cluster. Cette communication s'effectue par échange de battements de cœur réseau toutes les secondes. Lorsque l'hôte maître cesse de recevoir ces battements de cœur d'un hôte esclave, il vérifie la livenité de l'hôte avant de déclarer l'échec de l'hôte. La vérification de la livenité effectuée par l'hôte maître consiste à déterminer si l'hôte esclave échange des pulsations avec l'un des datastores. En outre, l'hôte maître vérifie si l'hôte répond aux requêtes ping ICMP envoyées à ses adresses IP de gestion pour détecter s'il est simplement isolé de son nœud maître ou complètement isolé du réseau. Pour ce faire, il exécute une commande ping sur la passerelle par défaut. Une ou plusieurs adresses d'isolement peuvent être spécifiées manuellement pour améliorer la fiabilité de la validation de l'isolement.

Meilleure pratique

NetApp recommande de spécifier au moins deux adresses d'isolement supplémentaires, et que chacune de ces adresses soit site-local. Cela améliorera la fiabilité de la validation de l'isolement.

Réponse d'isolation de l'hôte

Isolation Response est un paramètre de vSphere HA qui détermine l'action déclenchée sur les machines virtuelles lorsqu'un hôte d'un cluster vSphere HA perd ses connexions réseau de gestion mais continue à s'exécuter. Il existe trois options pour ce paramètre, « Désactivé », « Arrêter et redémarrer les machines virtuelles » et « Arrêter et redémarrer les machines virtuelles ».

Il est préférable d'arrêter le système plutôt que de le mettre hors tension, qui ne vide pas les dernières modifications apportées au disque ou ne commet pas les transactions. Si les machines virtuelles ne s'arrêtent pas dans les 300 secondes, elles sont éteintes. Pour modifier le temps d'attente, utilisez l'option avancée das.isolashutdowntimeout.

Avant que la haute disponibilité ne lance la réponse d'isolation, elle vérifie d'abord si l'agent principal vSphere HA possède le datastore qui contient les fichiers de configuration de la machine virtuelle. Si ce n'est pas le cas, l'hôte ne déclenchera pas la réponse d'isolation, car il n'y a pas de maître pour redémarrer les machines virtuelles. L'hôte vérifie régulièrement l'état du datastore pour déterminer s'il est demandé par un agent vSphere HA qui détient le rôle principal.

Meilleure pratique

NetApp recommande de définir la « réponse d'isolation de l'hôte » sur Désactivé.

Une condition de split-brain peut se produire si un hôte est isolé ou partitionné à partir de l'hôte maître vSphere HA et que le maître ne peut pas communiquer via des datastores heartbeat ou par ping. Le maître déclare l'hôte isolé comme étant mort et redémarre les machines virtuelles sur les autres hôtes du cluster. Une condition de split-brain existe maintenant parce qu'il y a deux instances de la machine virtuelle en cours d'exécution, dont une seule peut lire ou écrire les disques virtuels. Il est désormais possible d'éviter les conditions de split-brain en configurant VM Component protection (VMCP).

Protection des composants VM (VMCP)

L'une des améliorations de vSphere 6, concernant la haute disponibilité, est VMCP. VMCP offre une protection améliorée contre les conditions de tous les chemins d'accès (APD) et de perte permanente de périphérique (PDL) pour le stockage bloc (FC, iSCSI, FCoE) et de fichiers (NFS).

Perte permanente de périphérique (PDL)

PDL est une condition qui se produit lorsqu'un périphérique de stockage tombe en panne de manière permanente ou est supprimé administrativement et ne devrait pas revenir. La baie de stockage NetApp émet un code de détection SCSI pour ESXi déclarant que le périphérique est définitivement perdu. Dans la section Conditions de défaillance et réponse de la machine virtuelle de vSphere HA, vous pouvez configurer la réponse après la détection d'une condition PDL.

Meilleure pratique

NetApp recommande de définir la "réponse du datastore avec PDL" sur "**éteindre et redémarrer les machines virtuelles**". Lorsque cette condition est détectée, une machine virtuelle est redémarrée instantanément sur un hôte sain dans le cluster vSphere HA.

Tous les chemins en panne (APD)

L'APD est une condition qui se produit lorsqu'un périphérique de stockage devient inaccessible à l'hôte et qu'aucun chemin vers la matrice n'est disponible. ESXi considère cela comme un problème temporaire avec le périphérique et s'attend à ce qu'il redevienne disponible.

Lorsqu'une condition APD est détectée, une minuterie démarre. Au bout de 140 secondes, la condition APD est officiellement déclarée et le périphérique est marqué comme étant hors délai APD. Lorsque les 140 secondes sont écoulées, la haute disponibilité commence à compter le nombre de minutes spécifié dans le délai d'attente pour le basculement de machine virtuelle. Une fois le délai spécifié écoulé, la haute disponibilité redémarre les machines virtuelles impactées. Vous pouvez configurer VMCP pour qu'il réponde différemment si vous le souhaitez (désactivé, événements de problème ou mise hors tension et redémarrage des machines virtuelles).

Meilleure pratique

NetApp recommande de configurer la « réponse pour le datastore avec APD » sur « * mettre hors tension et redémarrer les machines virtuelles (conservatrices)* ».

Conservateur fait référence à la probabilité que la haute disponibilité soit capable de redémarrer les machines virtuelles. Si elle est définie sur conservateur, la haute disponibilité ne redémarrera la machine virtuelle concernée par l'APD que si elle sait qu'un autre hôte peut la redémarrer. Dans le cas d'un environnement agressif, la haute disponibilité essaiera de redémarrer la machine virtuelle même si elle ne connaît pas l'état des autres hôtes. Cela peut entraîner le redémarrage des machines virtuelles si aucun hôte n'a accès au datastore sur lequel elles se trouvent.

Si le statut APD est résolu et que l'accès au stockage est restauré avant le délai d'expiration, la haute disponibilité ne redémarrera pas inutilement la machine virtuelle, sauf si vous la configurez explicitement pour le faire. Si une réponse est souhaitée, même lorsque l'environnement a récupéré de la condition APD, la réponse pour la restauration APD après le délai APD doit être configurée pour réinitialiser les machines virtuelles.

Meilleure pratique

NetApp recommande de configurer la réponse pour la récupération APD après le délai APD sur Désactivé.

Implémentation de VMware DRS pour NetApp MetroCluster

VMware DRS est une fonctionnalité qui regroupe les ressources hôtes dans un cluster et est principalement utilisée pour équilibrer la charge au sein d'un cluster dans une infrastructure virtuelle. VMware DRS calcule principalement les ressources CPU et mémoire pour effectuer l'équilibrage de charge dans un cluster. Étant donné que vSphere ne connaît pas la mise en cluster étendue, il prend en compte tous les hôtes des deux sites lors de l'équilibrage de charge. Pour éviter le trafic intersite, NetApp recommande de configurer des règles d'affinité DRS pour gérer une séparation logique des machines virtuelles. Cela permet de garantir que, sauf en cas de défaillance complète du site, les systèmes HA et DRS n'utilisent que les hôtes locaux.

Si vous créez une règle d'affinité DRS pour votre cluster, vous pouvez spécifier comment vSphere applique cette règle lors du basculement d'une machine virtuelle.

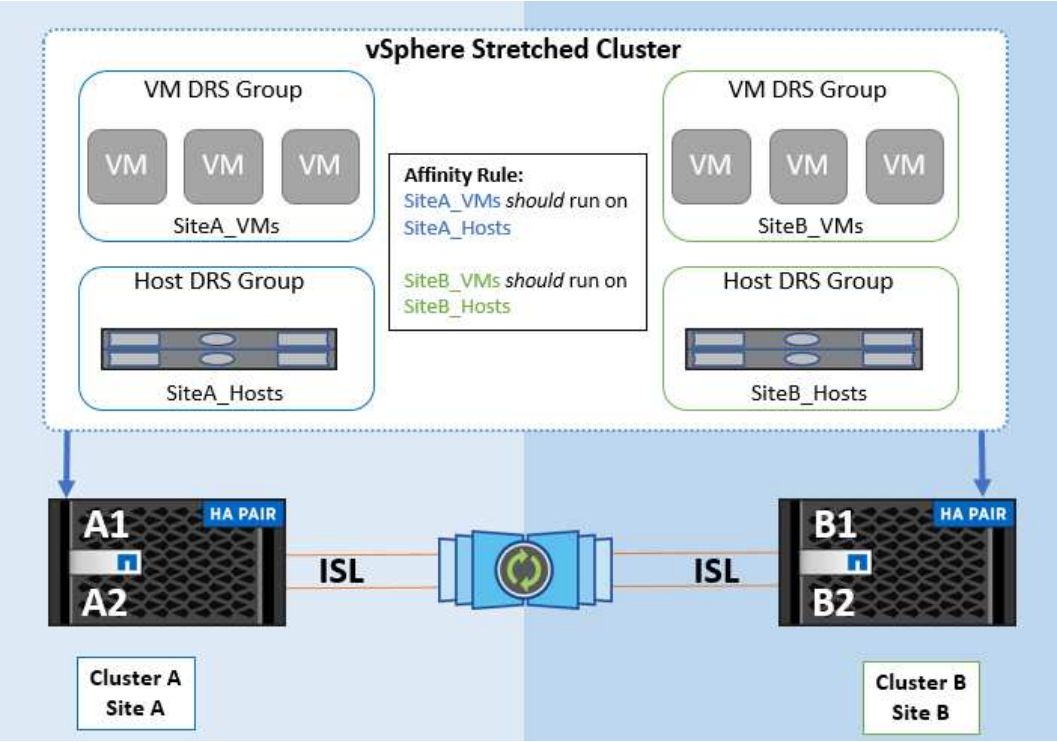
Vous pouvez spécifier deux types de règles pour le basculement de vSphere HA :

- Les règles d'anti-affinité pour les machines virtuelles forcent les machines virtuelles spécifiées à rester séparées pendant les opérations de basculement.
- Les règles d'affinité des hôtes VM placent les machines virtuelles spécifiées sur un hôte particulier ou un membre d'un groupe défini d'hôtes lors des actions de basculement.

En utilisant les règles d'affinité pour les hôtes de machine virtuelle dans VMware DRS, il est possible d'avoir une séparation logique entre le site A et le site B, de sorte que la machine virtuelle s'exécute sur l'hôte au même site que la baie configurée comme contrôleur de lecture/écriture principal pour un datastore donné. De plus, les règles d'affinité des hôtes de VM permettent aux machines virtuelles de rester locales au stockage, ce

qui à son tour ascert la connexion de la machine virtuelle en cas de défaillances réseau entre les sites.

Voici un exemple de groupes d'hôtes de machine virtuelle et de règles d'affinité.



Meilleure pratique

NetApp recommande de mettre en place des règles « a » plutôt que des règles « a », car elles sont violées par vSphere HA en cas de défaillance. L'utilisation de règles « must » peut entraîner des interruptions de service.

La disponibilité des services doit toujours prévaloir sur les performances. Lorsqu'un data Center complet tombe en panne, les règles « must » doivent choisir les hôtes du groupe d'affinité des hôtes de la machine virtuelle et, lorsque le data Center n'est pas disponible, les machines virtuelles ne redémarrent pas.

Implémentation de VMware Storage DRS avec NetApp MetroCluster

La fonction VMware Storage DRS permet l'agrégation de datastores en une seule unité et équilibre les disques de la machine virtuelle lorsque les seuils de contrôle d'E/S du stockage sont dépassés.

Le contrôle des E/S du stockage est activé par défaut sur les clusters DRS compatibles avec Storage DRS. Le contrôle des E/S du stockage permet à un administrateur de contrôler la quantité d'E/S de stockage allouée aux serveurs virtuels pendant les périodes d'encombrement des E/S. Ainsi, les serveurs virtuels plus importants sont préfénables aux serveurs virtuels moins importants pour l'allocation des ressources d'E/S.

Storage DRS utilise Storage vMotion pour migrer les machines virtuelles vers différents datastores au sein d'un cluster de datastores. Dans un environnement NetApp MetroCluster, la migration des machines virtuelles doit être contrôlée dans les datastores de ce site. Par exemple, la machine virtuelle A, qui s'exécute sur un hôte du site A, doit idéalement migrer au sein des datastores du SVM sur le site A. Si ce n'est pas le cas, la machine virtuelle continue à fonctionner mais avec des performances dégradées, puisque la lecture/l'écriture du disque virtuel se fera à partir du site B via des liens inter-sites.

Meilleure pratique

NetApp recommande de créer des clusters de datastores en fonction de l'affinité avec les sites de stockage. En d'autres termes, les datastores avec affinité pour le site A ne doivent pas être associés à des clusters de datastores avec affinité pour le site B.

Lorsqu'une machine virtuelle est nouvellement provisionnée ou migrée à l'aide de Storage vMotion, NetApp recommande de mettre à jour manuellement toutes les règles VMware DRS spécifiques à ces machines virtuelles en conséquence. Cela permet de vérifier l'affinité de la machine virtuelle au niveau du site pour l'hôte et le datastore et de réduire ainsi la surcharge réseau et stockage.

Directives de conception et de mise en œuvre VMSC

Ce document présente les lignes directrices en matière de conception et d'implémentation pour vMSC avec systèmes de stockage ONTAP.

Configuration du stockage NetApp

Les instructions d'installation de NetApp MetroCluster (appelées « configuration MCC ») sont disponibles à l'adresse "Documentation MetroCluster". Des instructions pour la synchronisation active SnapMirror sont également disponibles à l'adresse "Présentation de la continuité de l'activité SnapMirror".

Une fois que vous avez configuré MetroCluster, son administration revient à gérer un environnement ONTAP traditionnel. Vous pouvez configurer des machines virtuelles de stockage (SVM) à l'aide de divers outils tels que l'interface de ligne de commande (CLI), System Manager ou Ansible. Une fois les SVM configurés, créez des interfaces logiques (LIF), des volumes et des LUN sur le cluster qui seront utilisés pour les opérations normales. Ces objets seront automatiquement répliqués sur l'autre cluster à l'aide du réseau de peering de cluster.

Si vous n'utilisez pas MetroCluster, vous pouvez utiliser la synchronisation active SnapMirror qui offre une protection granulaire du datastore et un accès actif-actif sur plusieurs clusters ONTAP dans différents domaines de défaillance. La synchronisation active SnapMirror utilise des groupes de cohérence pour assurer la cohérence de l'ordre d'écriture dans un ou plusieurs datastores. Vous pouvez également créer plusieurs groupes de cohérence selon les besoins de vos applications et de vos datastores. Les groupes de cohérence sont particulièrement utiles pour les applications qui nécessitent une synchronisation des données entre plusieurs datastores. La synchronisation active SnapMirror prend également en charge les mappages de périphériques Raw Device (RDM) et le stockage connecté par l'invité avec les initiateurs iSCSI invités. Pour en savoir plus sur les groupes de cohérence, consultez la page "Présentation des groupes de cohérence".

La gestion d'une configuration vMSC avec SnapMirror Active Sync est différente de celle d'un MetroCluster. Tout d'abord, il s'agit d'une configuration SAN uniquement. Les datastores NFS ne peuvent pas être protégés avec la synchronisation active SnapMirror. Ensuite, vous devez mapper les deux copies des LUN sur vos hôtes ESXi afin qu'elles puissent accéder aux datastores répliqués dans les deux domaines de défaillance.

Haute disponibilité VMware vSphere

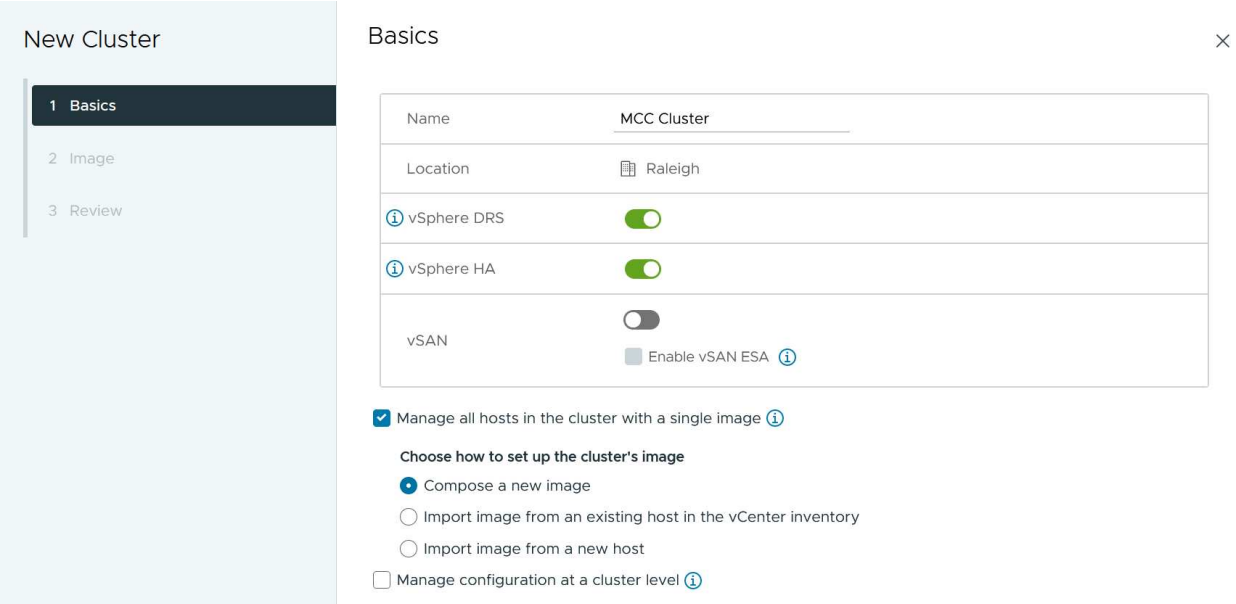
Créer un cluster haute disponibilité vSphere

La création d'un cluster vSphere HA est un processus en plusieurs étapes entièrement documenté à l'adresse "Comment créer et configurer des clusters dans vSphere client sur docs.vmware.com". En bref, vous devez d'abord créer un cluster vide, puis, à l'aide de vCenter, vous devez ajouter des hôtes et spécifier les paramètres vSphere HA et autres du cluster.

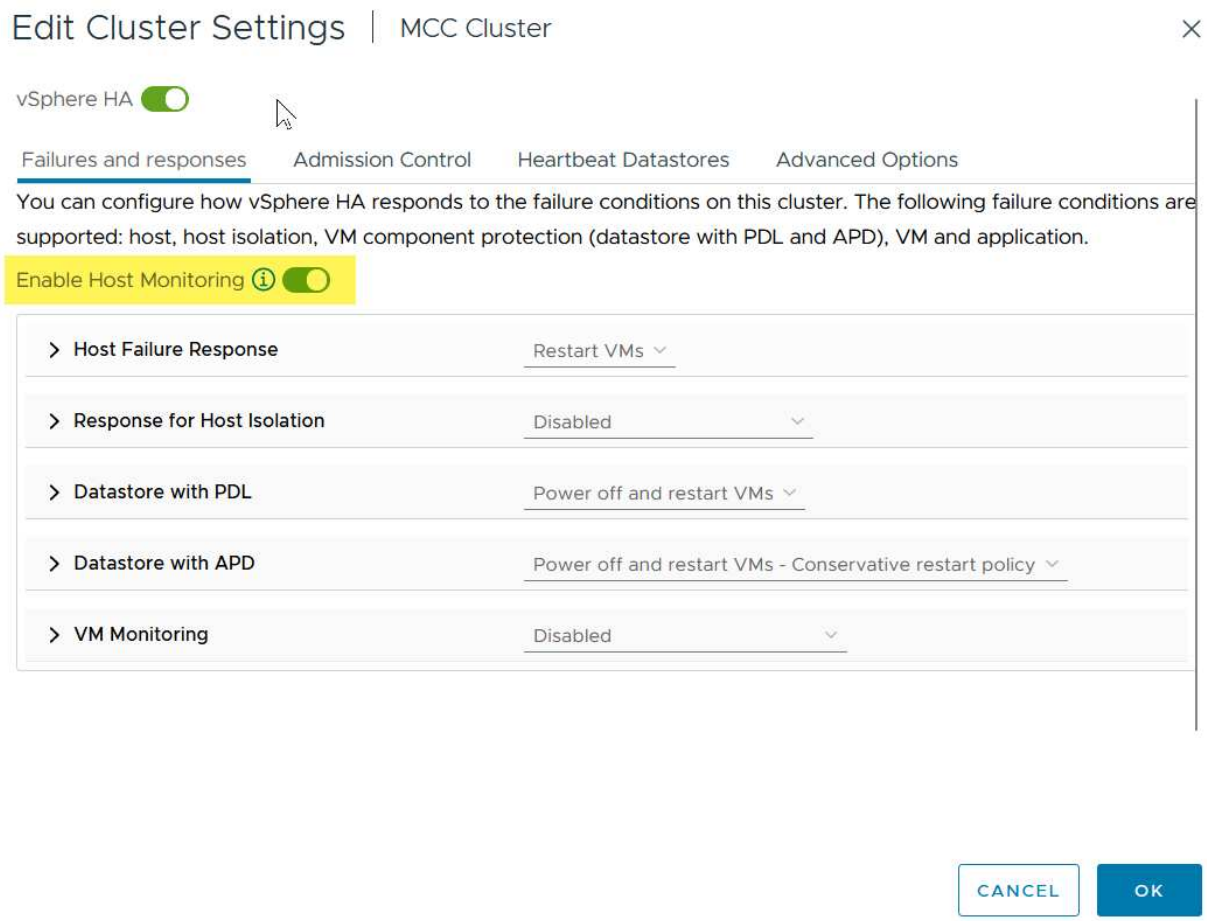
Note: rien dans ce document ne remplace "Bonnes pratiques pour VMware vSphere Metro Storage Cluster"

Pour configurer un cluster HA, effectuez les étapes suivantes :

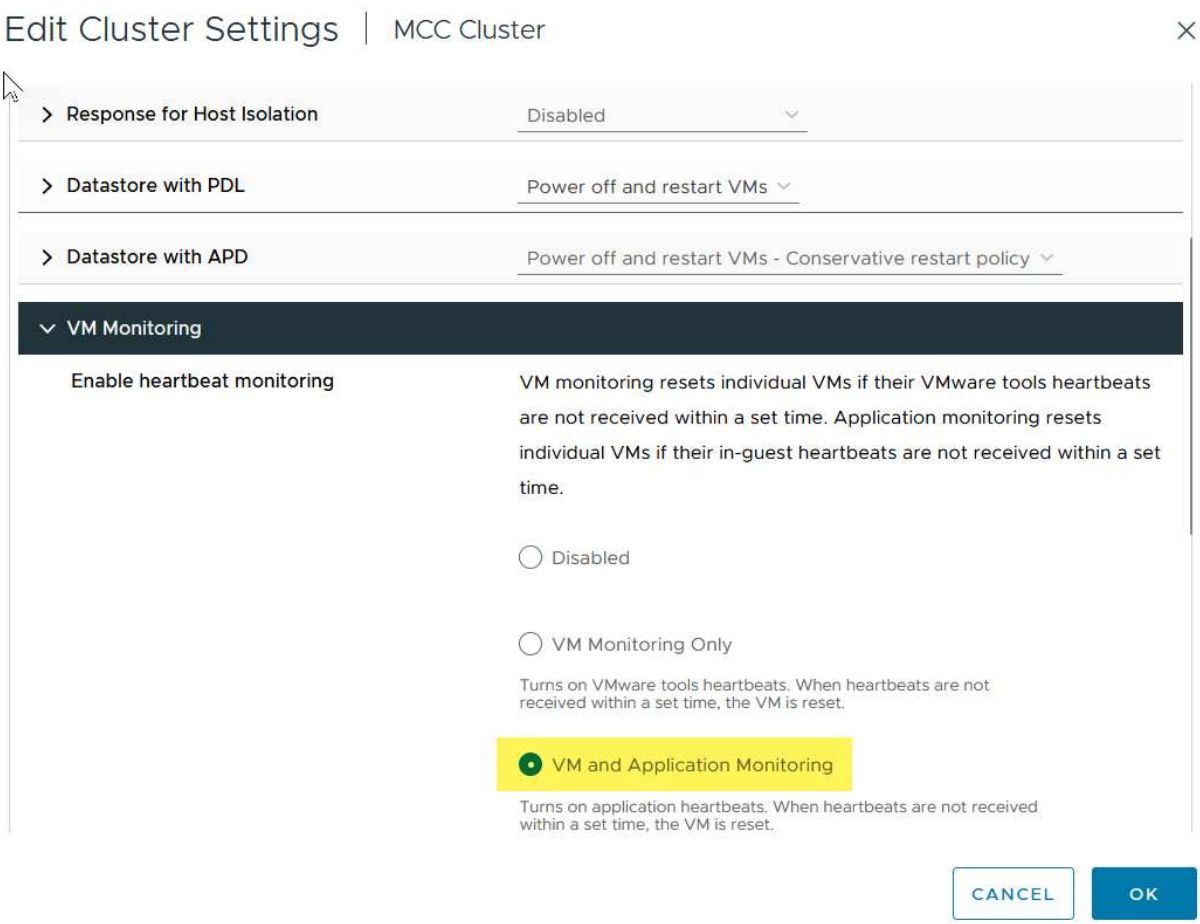
1. Connectez-vous à l'interface utilisateur vCenter.
2. Dans hôtes et clusters, accédez au data Center où vous souhaitez créer votre cluster haute disponibilité.
3. Cliquez avec le bouton droit de la souris sur l'objet de data Center et sélectionnez Nouveau cluster. Dans les notions de base, assurez-vous d'avoir activé vSphere DRS et vSphere HA. Suivez l'assistant.



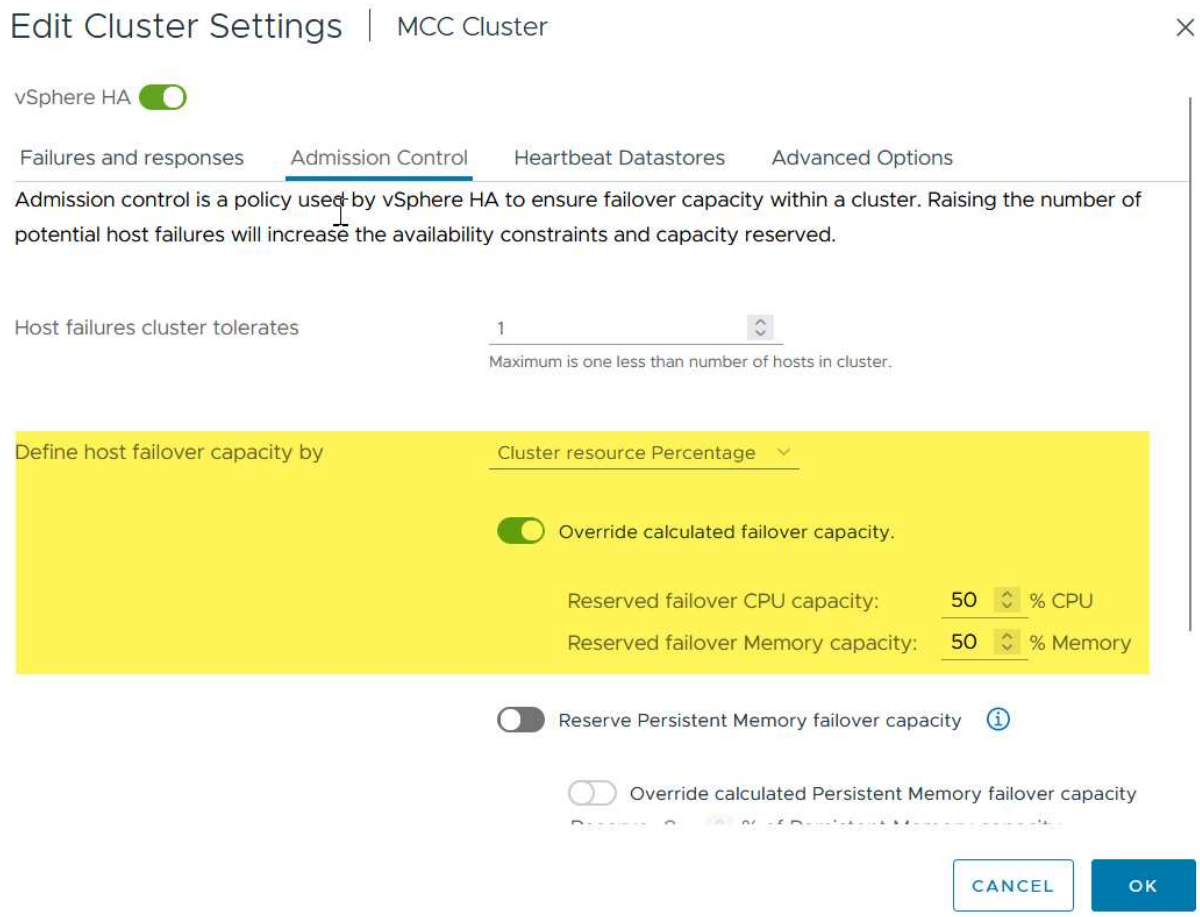
1. Sélectionnez le cluster et accédez à l'onglet configure. Sélectionnez vSphere HA et cliquez sur Edit.
2. Sous surveillance de l'hôte, sélectionnez l'option Activer la surveillance de l'hôte.



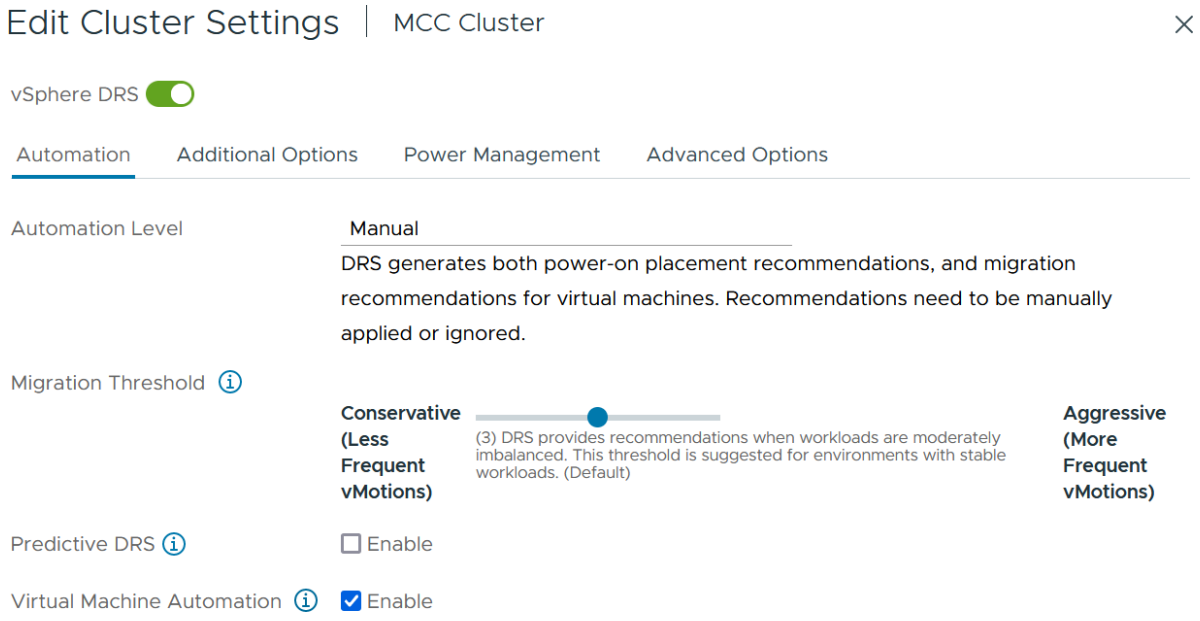
1. Toujours sous l'onglet défaillances et réponses, sous surveillance VM, sélectionnez l'option VM Monitoring Only ou VM and application Monitoring.



1. Sous contrôle d'admission, définissez l'option de contrôle d'admission HA sur réserve de ressources de cluster ; utilisez 50 % CPU/MEM.



1. Cliquez sur OK.
2. Sélectionnez DRS et cliquez sur EDIT.
3. Définissez le niveau d'automatisation sur manuel, sauf si vos applications en ont besoin.



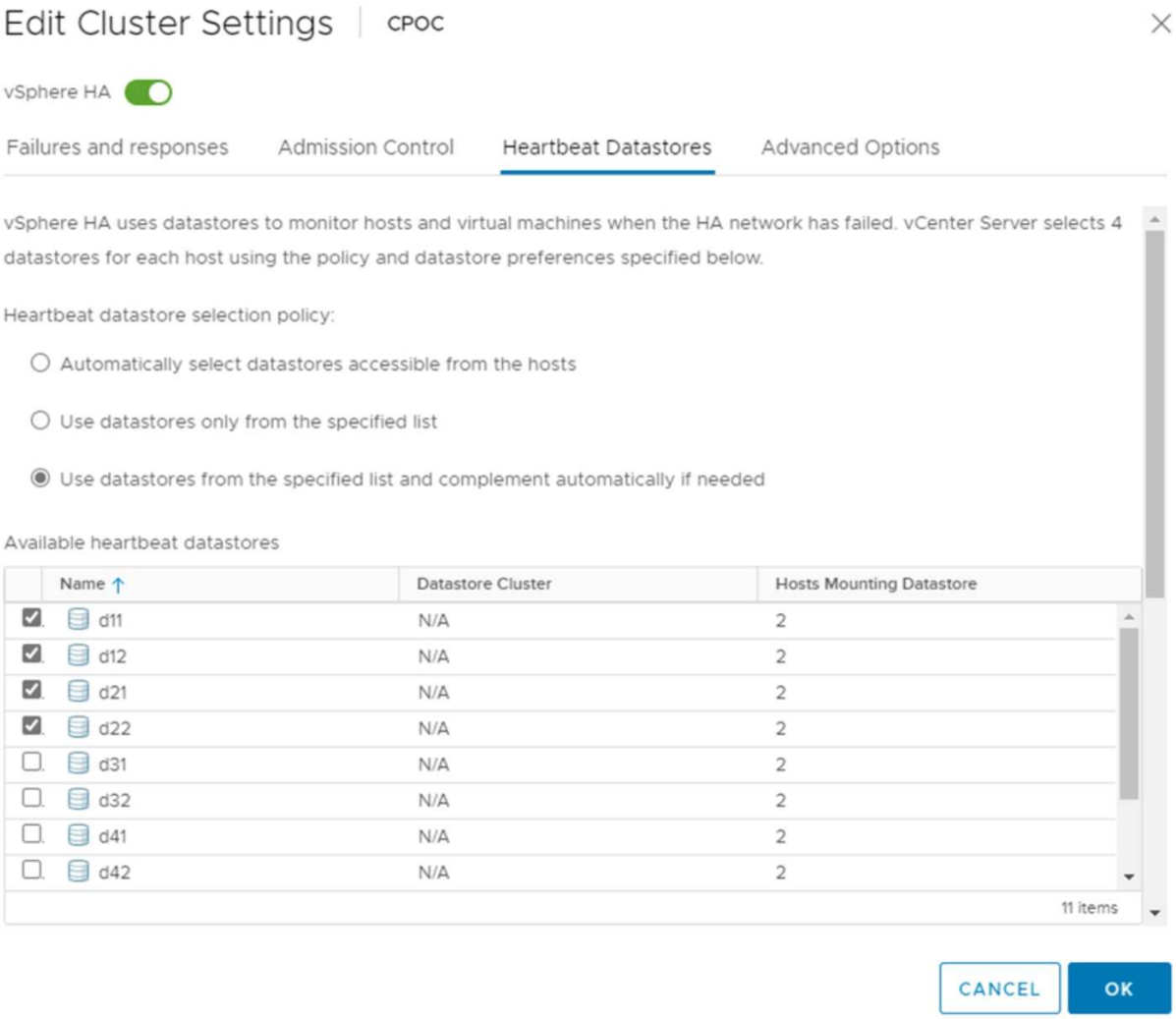
1. Activer la protection des composants VM, voir "docs.vmware.com".
2. Les paramètres vSphere HA supplémentaires suivants sont recommandés pour vMSC avec MCC :

Panne	Réponse
Défaillance d'hôte	Redémarrage des machines virtuelles
Isolation de l'hôte	Désactivé
Datastore avec perte de périphérique permanente (PDL)	Mettez les machines virtuelles hors tension et redémarrez-les
Datastore avec tous les chemins en panne (APD)	Mettez les machines virtuelles hors tension et redémarrez-les
Client qui ne bat pas	Réinitialiser les VM
Règle de redémarrage de machine virtuelle	Déterminé par l'importance de la machine virtuelle
Réponse pour l'isolation de l'hôte	Arrêtez et redémarrez les machines virtuelles
Réponse pour datastore avec PDL	Mettez les machines virtuelles hors tension et redémarrez-les
Réponse pour le datastore avec APD	Mise hors tension et redémarrage des machines virtuelles (prudent)
Délai de basculement de machine virtuelle pour APD	3 minutes
Réponse pour la restauration APD avec délai d'expiration APD	Désactivé
Sensibilité de surveillance des machines virtuelles	Présélection haute

Configurez les datastores pour Heartbeat

VSphere HA utilise les datastores pour surveiller les hôtes et les machines virtuelles en cas de panne du réseau de gestion. Vous pouvez configurer la façon dont vCenter sélectionne les datastores Heartbeat. Pour configurer des datastores pour les pulsations, procédez comme suit :

1. Dans la section pulsation du datastore, sélectionnez utiliser les datastores dans la liste spécifiée et complétez automatiquement si nécessaire.
2. Sélectionnez les datastores que vCenter doit utiliser sur les deux sites et appuyez sur OK.

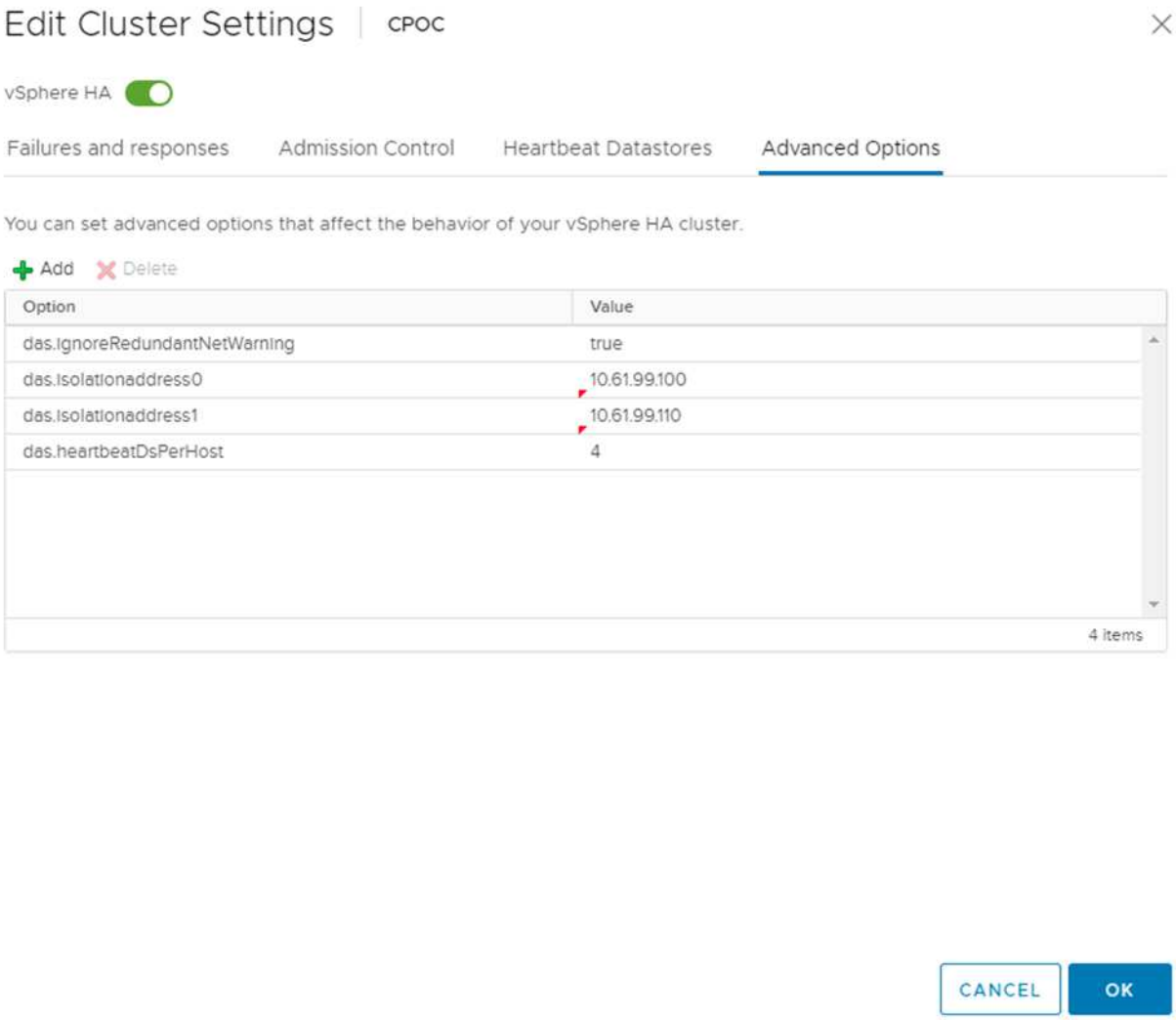


Configurer les options avancées

Détection de défaillance de l'hôte

Les événements d'isolation se produisent lorsque les hôtes d'un cluster haute disponibilité perdent la connectivité au réseau ou à d'autres hôtes du cluster. Par défaut, vSphere HA utilise la passerelle par défaut de son réseau de gestion comme adresse d'isolation par défaut. Toutefois, vous pouvez spécifier des adresses d'isolement supplémentaires pour que l'hôte puisse envoyer une requête ping afin de déterminer si une réponse d'isolement doit être déclenchée. Ajoutez deux adresses IP d'isolation pouvant être ping, une par site. N'utilisez pas l'adresse IP de la passerelle. Le paramètre avancé de vSphere HA utilisé est das.isolaaddress. Vous pouvez utiliser des adresses IP ONTAP ou Mediator à cette fin.

Reportez-vous à la section "core.vmware.com" pour plus d'informations_.__



L'ajout d'un paramètre avancé appelé das.heartbeatDsPerHost peut augmenter le nombre de datastores de pulsation. Utilisez quatre datastores de pulsation (DSS HB)—deux par site. Utilisez l'option « Sélectionner dans la liste mais compléter ». Ceci est nécessaire car si un site tombe en panne, vous avez toujours besoin de deux DSS HB. Toutefois, ceux-ci n'ont pas à être protégés avec la synchronisation active MCC ou SnapMirror.

Reportez-vous à la section "core.vmware.com" pour plus d'informations_.__

Affinité avec VMware DRS pour NetApp MetroCluster

Dans cette section, nous créons des groupes DRS pour les machines virtuelles et les hôtes pour chaque site/cluster dans l'environnement MetroCluster. Ensuite, nous configurons les règles VM/Host pour aligner l'affinité des hôtes VM avec les ressources de stockage locales. Par exemple, les machines virtuelles du site A appartiennent au groupe de machines virtuelles sitea_VM et les hôtes du site A appartiennent au groupe d'hôtes sitea_hosts. Ensuite, dans VM\Host Rules, nous faisons état que sitea_vm doit s'exécuter sur les hôtes de sitea_hosts.

Meilleure pratique

- NetApp recommande vivement la spécification **devrait s'exécuter sur les hôtes du groupe** plutôt que la spécification **doit s'exécuter sur les hôtes du groupe**. En cas de défaillance d'un hôte sur un site, les machines virtuelles Du site A doivent être redémarrées sur les hôtes du site B via vSphere HA, mais cette

dernière spécification ne permet pas à HA de redémarrer les machines virtuelles sur le site B, car il s'agit d'une règle stricte. Il s'agit d'une règle souple qui ne sera pas respectée en cas de haute disponibilité, garantissant ainsi la disponibilité plutôt que la performance.

Remarque : vous pouvez créer une alarme basée sur des événements qui est déclenchée lorsqu'une machine virtuelle viole une règle d'affinité VM-Host. Dans le client vSphere, ajoutez une nouvelle alarme pour la machine virtuelle et sélectionnez « VM viole VM-Host Affinity Rule » comme déclencheur d'événement. Pour plus d'informations sur la création et la modification d'alarmes, reportez-vous à la section "Surveillance et performances vSphere" documentation :

Créer des groupes d'hôtes DRS

Pour créer des groupes d'hôtes DRS spécifiques au site A et au site B, procédez comme suit :

1. Dans le client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster dans l'inventaire et sélectionnez Paramètres.
2. Cliquez sur VM\Host Groups.
3. Cliquez sur Ajouter.
4. Saisissez le nom du groupe (par exemple, sitea_hosts).
5. Dans le menu Type, sélectionnez Groupe d'hôtes.
6. Cliquez sur Ajouter et sélectionnez les hôtes souhaités sur le site A, puis cliquez sur OK.
7. Répétez ces étapes pour ajouter un autre groupe d'hôtes pour le site B.
8. Cliquez sur OK.

Créer des groupes VM DRS

Pour créer des groupes VM DRS spécifiques au site A et au site B, procédez comme suit :

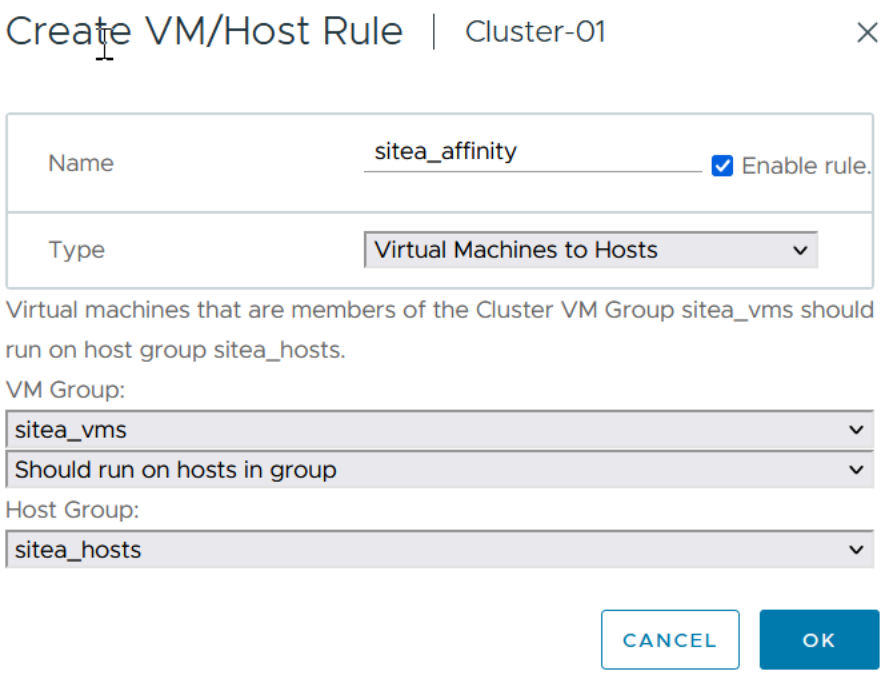
1. Dans le client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster dans l'inventaire et sélectionnez Paramètres.
2. Cliquez sur VM\Host Groups.
3. Cliquez sur Ajouter.
4. Saisissez le nom du groupe (par exemple, sitea_vm).
5. Dans le menu Type, sélectionnez VM Group.
6. Cliquez sur Ajouter, sélectionnez les machines virtuelles souhaitées sur le site A, puis cliquez sur OK.
7. Répétez ces étapes pour ajouter un autre groupe d'hôtes pour le site B.
8. Cliquez sur OK.

Créer des règles d'hôte VM

Pour créer des règles d'affinité DRS spécifiques au site A et au site B, procédez comme suit :

1. Dans le client Web vSphere, cliquez avec le bouton droit de la souris sur le cluster dans l'inventaire et sélectionnez Paramètres.
2. Cliquez sur VM\Host Rules.
3. Cliquez sur Ajouter.
4. Tapez le nom de la règle (par exemple, sitea_affinité).

5. Vérifiez que l'option Activer la règle est cochée.
6. Dans le menu Type, sélectionnez ordinateurs virtuels vers hôtes.
7. Sélectionnez le groupe VM (par exemple, sitea_vm).
8. Sélectionnez le groupe Host (par exemple, sitea_hosts).
9. Répétez ces étapes pour ajouter une autre règle VM\Host pour le site B.
10. Cliquez sur OK.



VMware vSphere Storage DRS pour NetApp MetroCluster

Créer des clusters de datastores

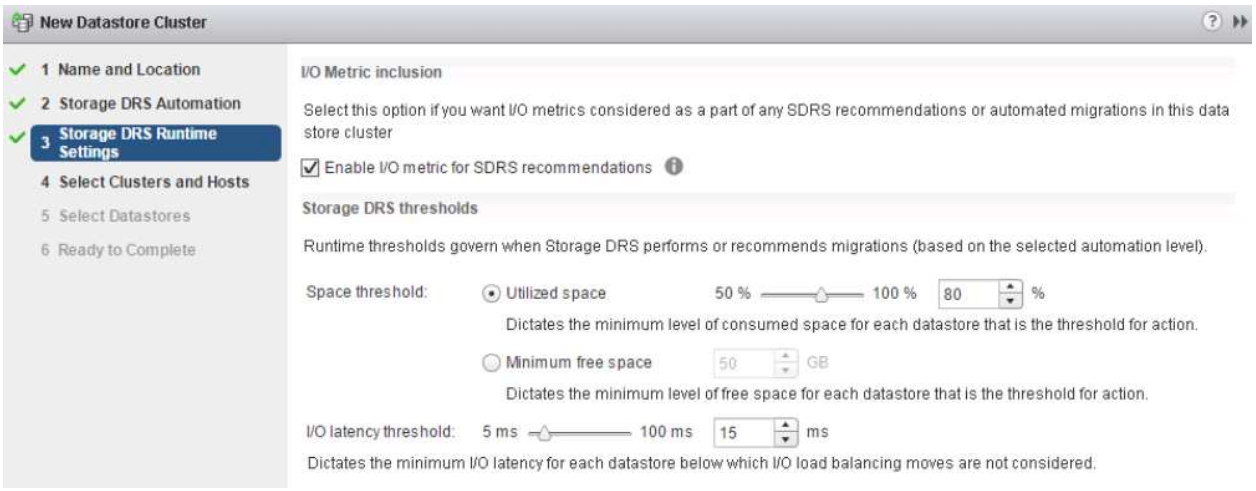
Pour configurer un cluster de datastore pour chaque site, procédez comme suit :

1. À l'aide du client web vSphere, accédez au data Center où réside le cluster HA sous Storage.
2. Cliquez avec le bouton droit de la souris sur l'objet datacenter et sélectionnez Storage > New datastore Cluster.
3. Sélectionnez l'option ACTIVER Storage DRS et cliquez sur Suivant.
4. Définissez toutes les options sur pas d'automatisation (mode manuel) et cliquez sur Suivant.

Meilleure pratique

- NetApp recommande de configurer Storage DRS en mode manuel, afin que l'administrateur puisse décider et contrôler les opérations de migration.

1. Vérifiez que la case Activer les mesures d'E/S pour les recommandations SDRS est cochée ; les paramètres de mesure peuvent être laissés avec les valeurs par défaut.



1. Sélectionnez le cluster HA et cliquez sur Next.

1. Sélectionnez les datastores appartenant au site A et cliquez sur Suivant.

1. Vérifiez les options et cliquez sur Terminer.
2. Répétez ces étapes pour créer le cluster de datastore du site B et vérifier que seuls les datastores du site B sont sélectionnés.

Disponibilité du serveur vCenter

Vos appliances vCenter Server (VCSA) doivent être protégées avec vCenter HA. VCenter HA vous permet de

déployer deux VCSA dans une paire haute disponibilité actif-passif. Un dans chaque domaine de défaillance. Pour en savoir plus sur vCenter HA, rendez-vous sur "docs.vmware.com".

Résilience pour les événements planifiés et non planifiés

NetApp MetroCluster et la synchronisation active SnapMirror sont des outils puissants qui améliorent la haute disponibilité et la continuité de l'activité du matériel NetApp et du logiciel ONTAP®.

Ces outils assurent une protection à l'échelle du site pour l'ensemble de l'environnement de stockage, garantissant ainsi la disponibilité permanente de vos données. Que vous utilisiez des serveurs autonomes, des clusters à haute disponibilité, des conteneurs Docker ou des serveurs virtualisés, la technologie NetApp assure la disponibilité du stockage de manière transparente en cas de panne totale due à une coupure d'alimentation, à des problèmes de climatisation, de connectivité réseau, à l'arrêt des baies de stockage ou à une erreur de fonctionnement.

La synchronisation active MetroCluster et SnapMirror propose trois méthodes de base pour la continuité des données en cas d'événements planifiés ou non :

- Des composants redondants pour une protection contre les défaillances d'un seul composant
- Basculement de haute disponibilité locale en cas d'événements affectant un contrôleur unique
- Protection complète du site – reprise rapide du service en déplaçant le stockage et l'accès client du cluster source vers le cluster de destination

Cela signifie que les opérations se poursuivent en toute transparence en cas de défaillance d'un seul composant et reviennent automatiquement au fonctionnement redondant lorsque le composant défectueux est remplacé.

Tous les clusters ONTAP, à l'exception des clusters à un seul nœud (en général, les versions Software-defined, telles que ONTAP Select, par exemple), disposent de fonctionnalités haute disponibilité intégrées appelées Takeover et giveback. Chaque contrôleur du cluster est couplé à un autre contrôleur, formant une paire haute disponibilité. Ces paires garantissent que chaque nœud est connecté localement au stockage.

Le basculement est un processus automatisé qui consiste à prendre le contrôle du stockage d'un nœud pour assurer les services de données. Le rétablissement est le processus inverse qui restaure le fonctionnement normal. Le basculement peut être planifié, par exemple lors de la maintenance matérielle ou des mises à niveau ONTAP, ou non planifié, suite à une panne matérielle ou de panique sur un nœud.

Lors d'un basculement, les interfaces logiques NAS dans les configurations MetroCluster basculent automatiquement. Toutefois, les LIF SAN (Storage Area Network) ne basculent pas ; elles continuent d'utiliser le chemin direct vers les LUN (Logical Unit Numbers).

Pour plus d'informations sur le basculement et le rétablissement HA, reportez-vous au "Présentation de la gestion des paires HAUTE DISPONIBILITÉ". Notez que cette fonctionnalité n'est pas spécifique à la synchronisation active MetroCluster ou SnapMirror.

Le basculement de site avec MetroCluster a lieu lorsqu'un site est hors ligne ou lors d'une activité planifiée pour la maintenance à l'échelle du site. Le site restant assume la propriété des ressources de stockage (disques et agrégats) du cluster hors ligne, et les SVM sur le site en panne sont mis en ligne et redémarrés sur le site en cas de sinistre, tout en préservant leur identité complète pour l'accès des clients et des hôtes.

Avec la synchronisation active SnapMirror, dans la mesure où les deux copies sont activement utilisées simultanément, vos hôtes existants continueront de fonctionner. Le médiateur NetApp est nécessaire pour

garantir que le basculement de site se produit correctement.

Scénarios de panne pour vMSC avec MCC

Les sections suivantes décrivent les résultats attendus de différents scénarios de défaillance avec les systèmes vMSC et NetApp MetroCluster.

Défaillance d'un seul chemin de stockage

Dans ce scénario, si des composants tels que le port HBA, le port réseau, le port du commutateur de données frontal ou un câble FC ou Ethernet échouent, ce chemin particulier vers le périphérique de stockage est marqué comme mort par l'hôte ESXi. Si plusieurs chemins sont configurés pour le périphérique de stockage en fournissant la résilience au niveau du port HBA/réseau/commutateur, ESXi effectue idéalement un basculement de chemin. Pendant cette période, les ordinateurs virtuels restent en fonctionnement sans être affectés, car la disponibilité du stockage est assurée par plusieurs chemins vers le périphérique de stockage.

Note: il n'y a pas de changement dans le comportement de MetroCluster dans ce scénario, et tous les datastores continuent d'être intacts de leurs sites respectifs.

Meilleure pratique

Dans les environnements dans lesquels les volumes NFS/iSCSI sont utilisés, NetApp recommande de configurer au moins deux liaisons montantes réseau pour le port vmkernel NFS dans le vSwitch standard et la même pour le groupe de ports où l'interface vmkernel NFS est mappée pour le vSwitch distribué. Le regroupement de cartes réseau peut être configuré en mode actif-actif ou actif-veille.

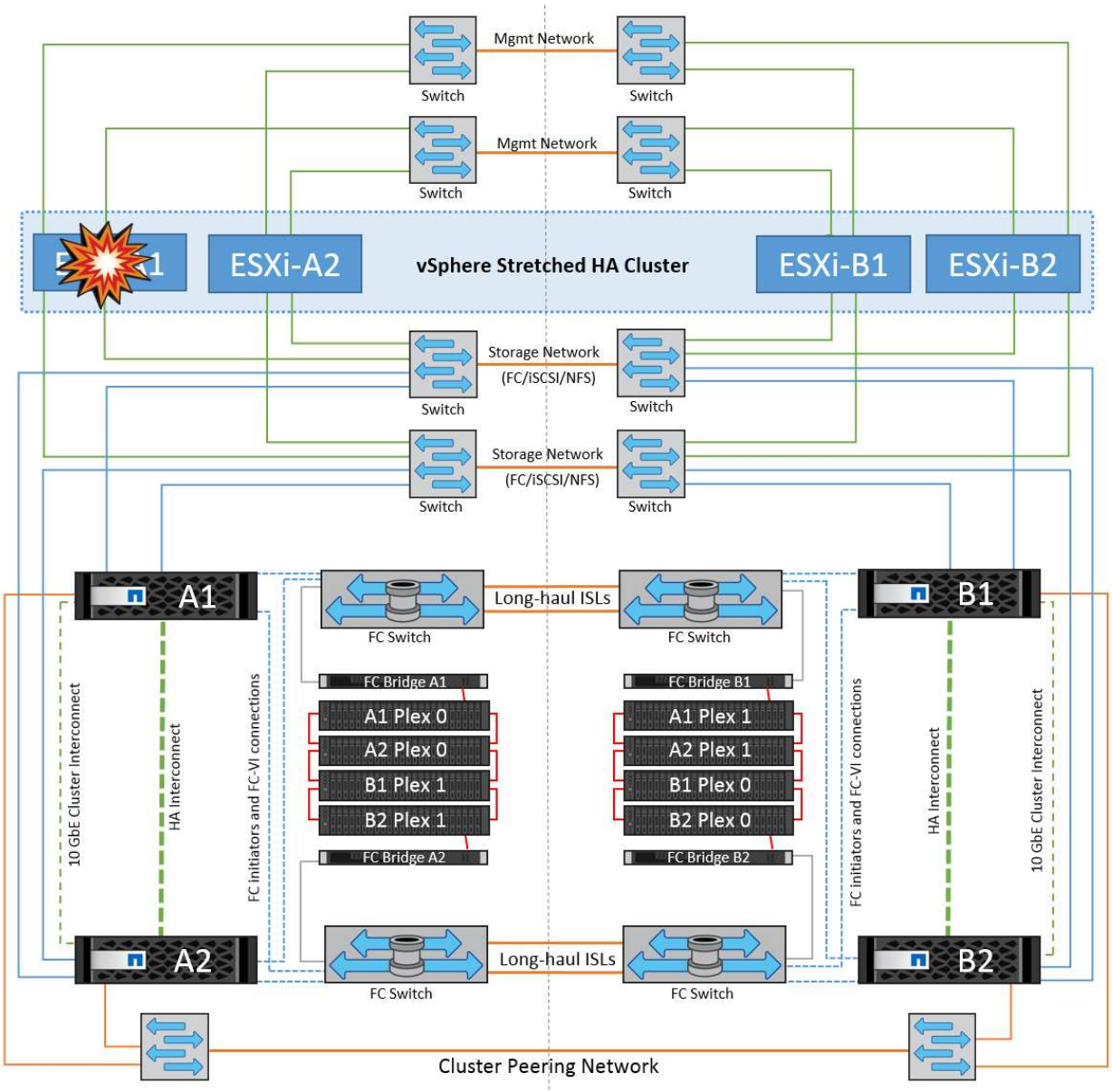
En outre, pour les LUN iSCSI, les chemins d'accès multiples doivent être configurés en liant les interfaces vmkernel aux adaptateurs réseau iSCSI. Pour plus d'informations, reportez-vous à la documentation sur le stockage vSphere.

Meilleure pratique

Dans les environnements dans lesquels des LUN Fibre Channel sont utilisées, NetApp recommande d'avoir au moins deux HBA, ce qui garantit la résilience au niveau des HBA/ports. NetApp recommande également la segmentation entre un initiateur unique et une seule cible comme meilleure pratique pour la configuration de la segmentation.

Virtual Storage Console (VSC) doit être utilisé pour définir des règles de chemins d'accès multiples, car il définit des règles pour tous les périphériques de stockage NetApp, nouveaux ou existants.

Défaillance d'un hôte ESXi unique



Dans ce scénario, en cas de défaillance de l'hôte ESXi, le nœud maître du cluster VMware HA détecte la panne de l'hôte, car il ne reçoit plus de pulsations réseau. Pour déterminer si l'hôte est réellement en panne ou uniquement une partition réseau, le nœud maître surveille les pulsations du datastore et, s'il est absent, il effectue une vérification finale en envoyant une requête ping aux adresses IP de gestion de l'hôte en panne. Si toutes ces vérifications sont négatives, le nœud maître déclare cet hôte comme étant en panne et toutes les machines virtuelles qui s'exécutaient sur cet hôte en panne sont redémarrées sur l'hôte survivant du cluster.

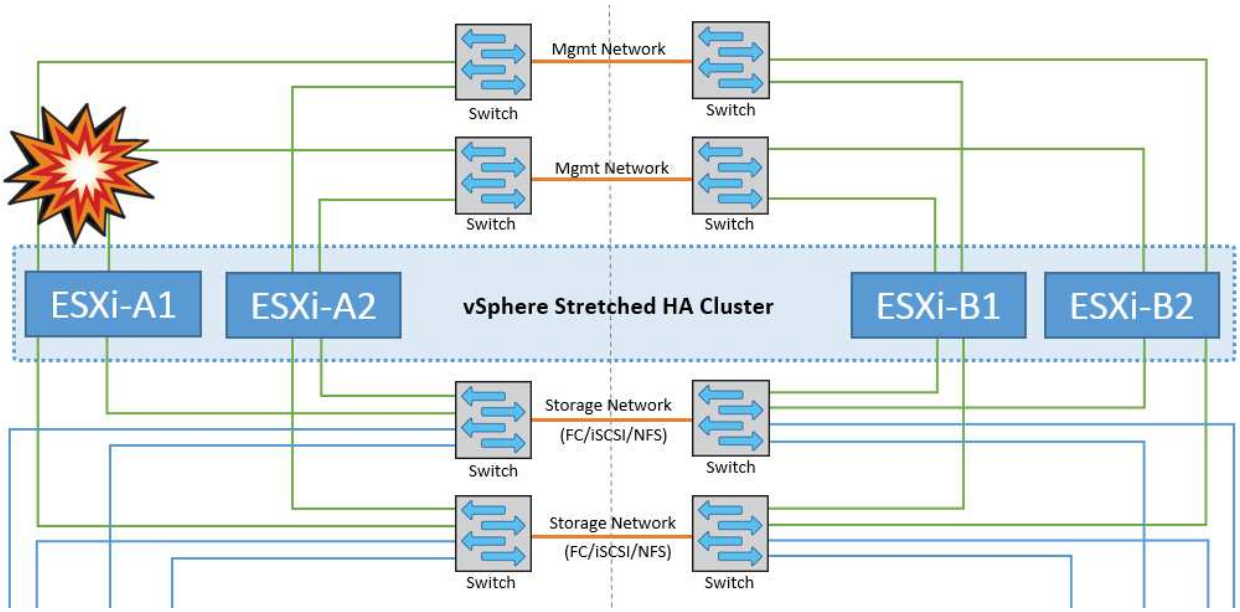
Si les règles d'affinité des machines virtuelles DRS et des hôtes ont été configurées (les machines virtuelles du groupe de machines virtuelles sitea_vm doivent exécuter des hôtes dans le groupe d'hôtes sitea_hosts), le maître haute disponibilité vérifie d'abord les ressources disponibles sur le site A. Si aucun hôte n'est disponible sur le site A, le maître tente de redémarrer les machines virtuelles sur les hôtes du site B.

Il est possible que les machines virtuelles soient démarrées sur les hôtes ESXi de l'autre site s'il existe une contrainte de ressource sur le site local. Cependant, les règles d'affinité VM et hôte DRS définies seront correctes si des règles sont enfreintes en migrant les machines virtuelles vers des hôtes ESXi survivants sur le site local. Dans les cas où DRS est défini sur manuel, NetApp recommande d'invoquer DRS et d'appliquer les recommandations pour corriger le positionnement de la machine virtuelle.

Dans ce scénario, le comportement de MetroCluster n'a pas changé et tous les datastores sont toujours

intacts sur leurs sites respectifs.

Isolation de l'hôte ESXi

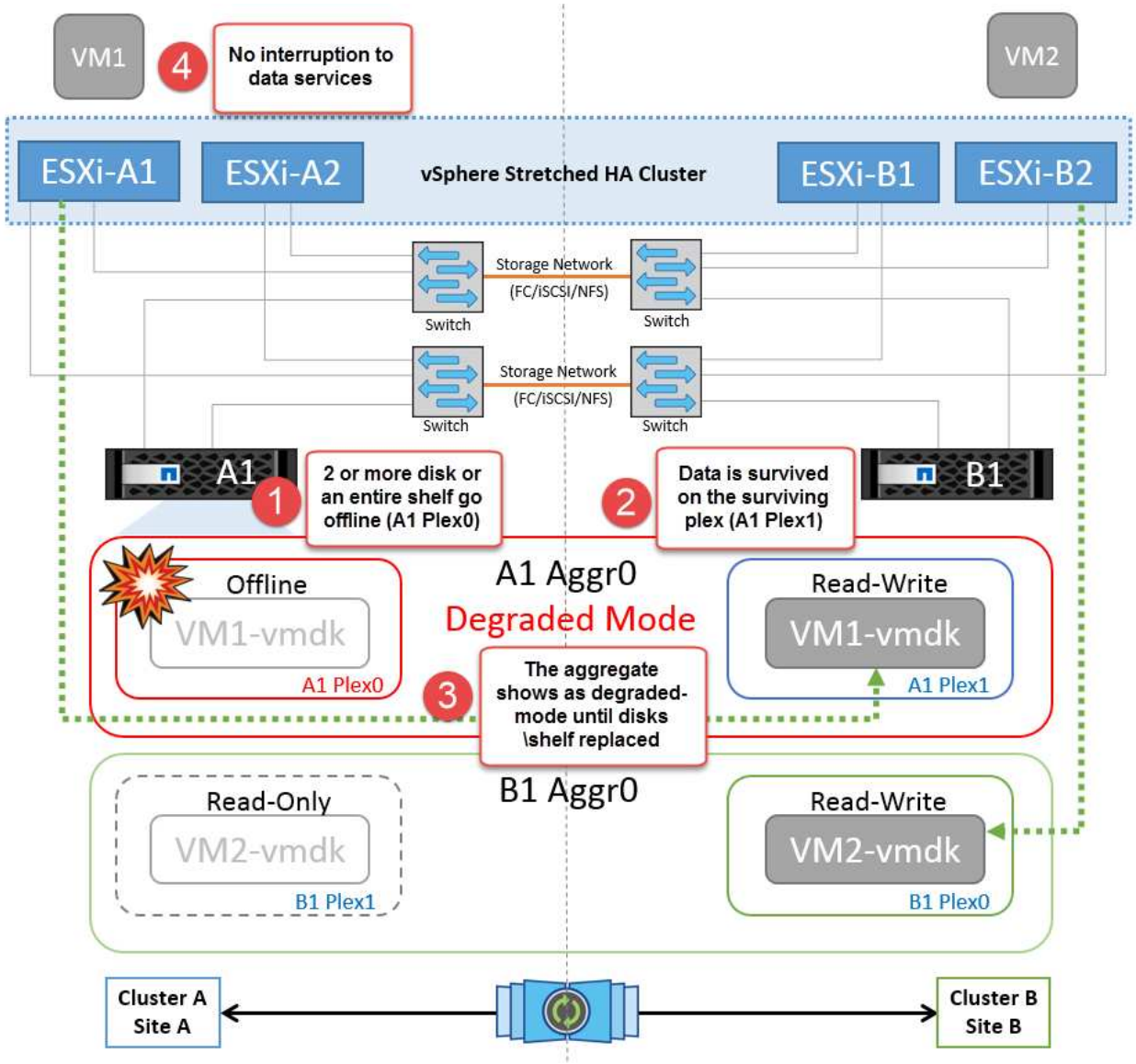


Dans ce scénario, si le réseau de gestion de l'hôte ESXi est en panne, le nœud principal du cluster HA ne recevra aucun battement de cœur. Cet hôte est donc isolé dans le réseau. Pour déterminer s'il a échoué ou s'il est isolé uniquement, le nœud maître commence à surveiller le battement de cœur du datastore. S'il est présent, l'hôte est déclaré isolé par le nœud maître. Selon la réponse d'isolement configurée, l'hôte peut choisir de mettre hors tension, d'arrêter les machines virtuelles ou même de laisser les machines virtuelles sous tension. L'intervalle par défaut pour la réponse d'isolement est de 30 secondes.

Dans ce scénario, le comportement de MetroCluster n'a pas changé et tous les datastores sont toujours intacts sur leurs sites respectifs.

Panne de tiroir disque

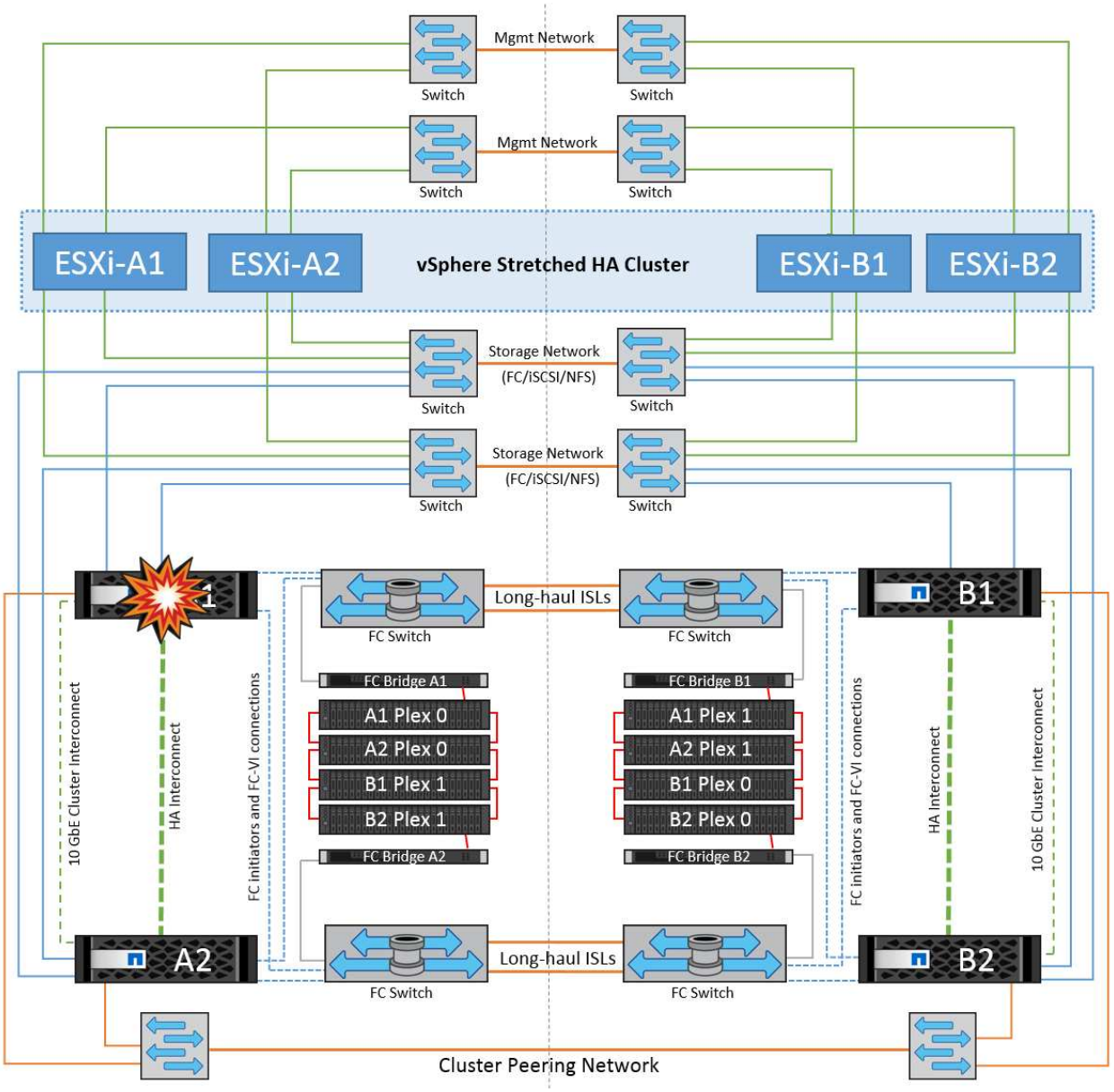
Dans ce scénario, il y a une panne de plus de deux disques ou d'un tiroir entier. Les données sont servies depuis le plex opérationnel sans interruption des services de données. La défaillance de disque peut affecter un plex local ou distant. Les agrégats s'affichent en mode dégradé, car un seul plex est actif. Une fois les disques défaillants remplacés, les agrégats affectés resynchroniseront automatiquement pour reconstruire les données. Après la resynchronisation, les agrégats reviennent automatiquement en mode miroir normal. Si plus de deux disques au sein d'un même groupe RAID sont défaillants, le plex doit être reconstruit à partir de zéro.



Remarque : au cours de cette période, il n'y a pas d'impact sur les opérations d'E/S de la machine virtuelle, mais les performances sont dégradées car les données sont accessibles depuis le tiroir disque distant via les liaisons ISL.

Panne d'un seul contrôleur de stockage

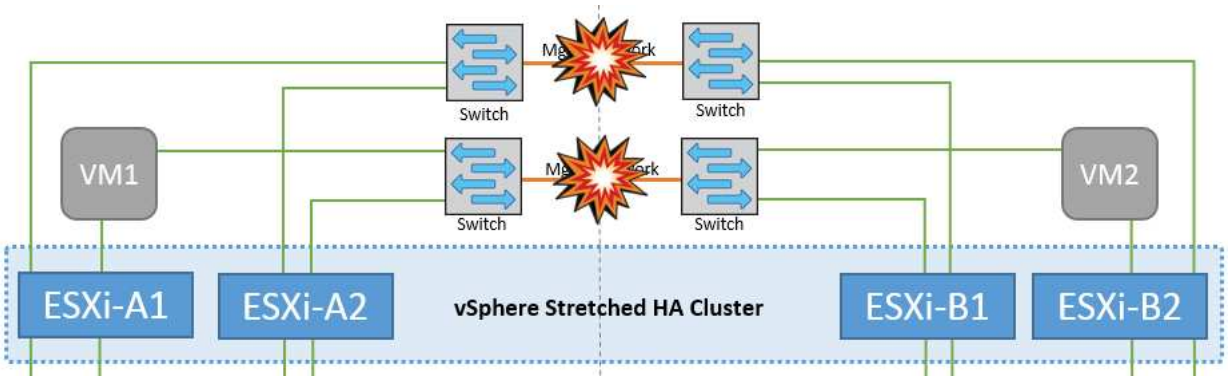
Dans ce scénario, l'un des deux contrôleurs de stockage tombe en panne sur un site. Comme il existe une paire haute disponibilité sur chaque site, la panne d'un nœud entraîne le basculement vers l'autre nœud de manière transparente et automatique. Par exemple, si le nœud A1 tombe en panne, son stockage et ses charges de travail sont automatiquement transférés vers le nœud A2. Les machines virtuelles ne seront pas affectées, car tous les plexes restent disponibles. Les nœuds du second site (B1 et B2) ne sont pas affectés. En outre, vSphere HA ne prendra aucune action, car le nœud maître du cluster recevra toujours les battements de cœur du réseau.



Si le basculement fait partie d'un incident en cours (le nœud A1 bascule vers A2) et qu'il y a une panne ultérieure de A2, ou la panne complète du site A, le basculement après un incident peut se produire sur le site B.

Défaillances de liaison entre commutateurs

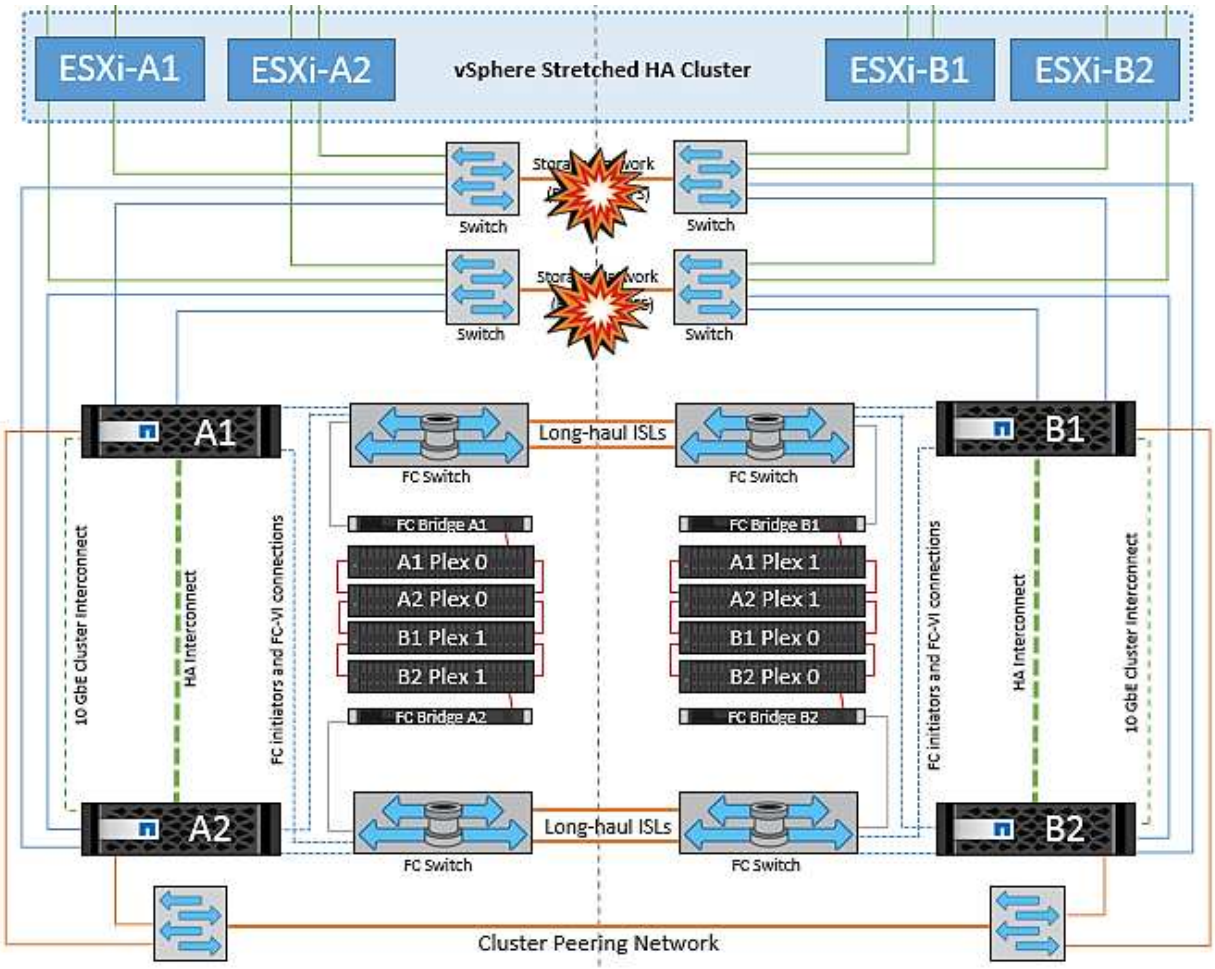
Défaillance de la liaison inter-commutateur sur le réseau de gestion



Dans ce scénario, si les liaisons ISL du réseau de gestion de l'hôte frontal tombent en panne, les hôtes ESXi du site A ne pourront pas communiquer avec les hôtes ESXi du site B. Cela entraîne une partition réseau, car les hôtes ESXi d'un site particulier ne peuvent pas envoyer les battements de cœur du réseau au nœud maître du cluster HA. Ainsi, il y aura deux segments de réseau en raison de la partition et il y aura un nœud maître dans chaque segment qui protégera les machines virtuelles des défaillances de l'hôte au sein du site particulier.

Remarque : pendant cette période, les machines virtuelles restent en cours d'exécution et il n'y a pas de changement dans le comportement de MetroCluster dans ce scénario. Tous les datastores sont toujours intacts sur leurs sites respectifs.

Défaillance de la liaison intercommutateur sur le réseau de stockage

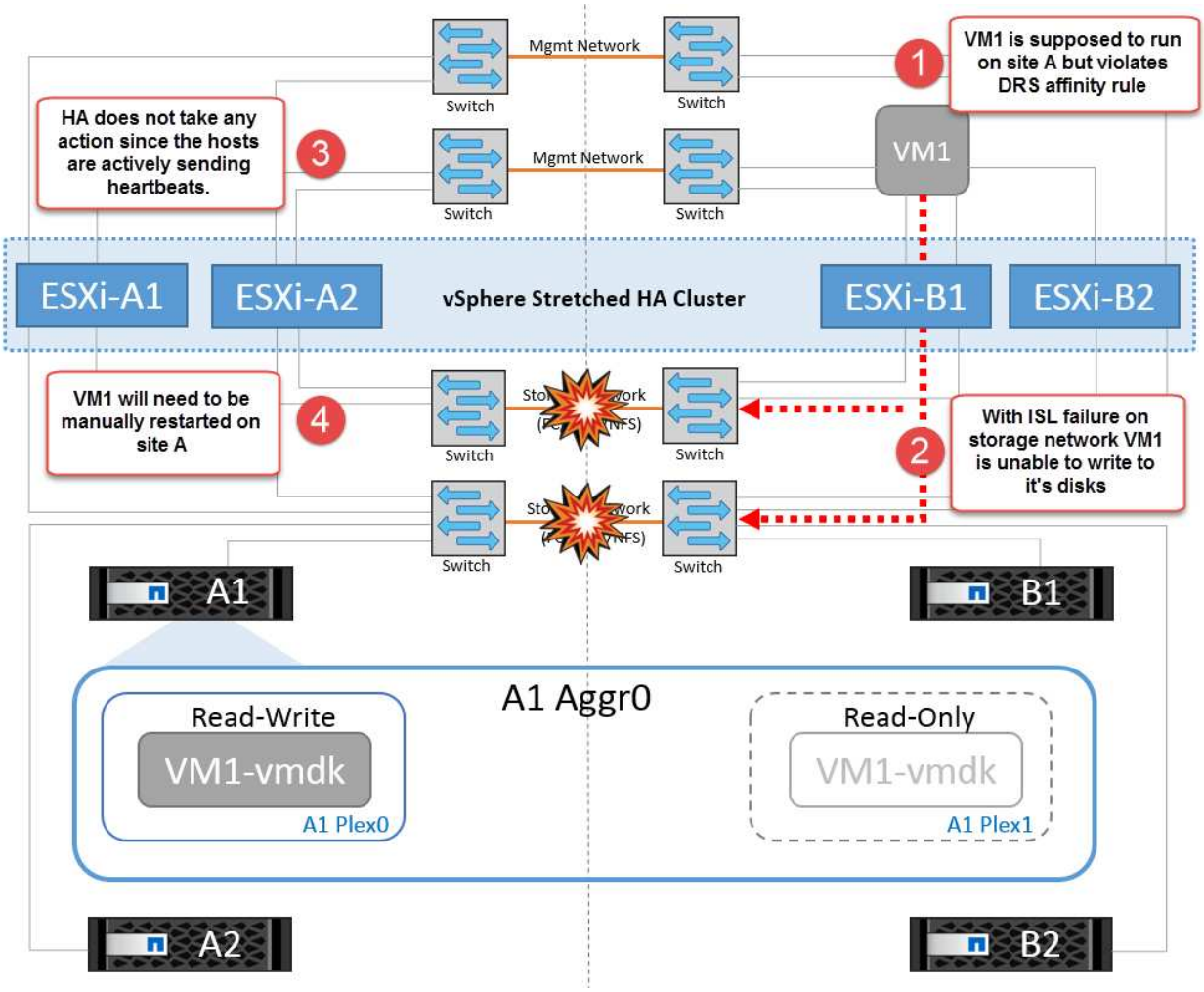


Dans ce scénario, si les liaisons ISL du réseau de stockage back-end tombent en panne, les hôtes du site A perdront l'accès aux volumes de stockage ou aux LUN du cluster B sur le site B et vice versa. Les règles VMware DRS sont définies de manière à ce que l'affinité entre l'hôte et le site de stockage facilite l'exécution des machines virtuelles sans impact sur le site.

Pendant cette période, les machines virtuelles restent en cours d'exécution sur leurs sites respectifs et le comportement de MetroCluster n'a pas changé dans ce scénario. Tous les datastores sont toujours intacts sur leurs sites respectifs.

Si, pour une raison quelconque, la règle d'affinité a été enfreinte (par exemple, VM1, qui était censé s'exécuter à partir du site A où ses disques résident sur les nœuds du cluster A local, s'exécute sur un hôte du site B), le disque de la machine virtuelle est accessible à distance via des liens ISL. En raison d'une défaillance de la liaison ISL, VM1 exécuté sur le site B ne pouvait pas écrire sur ses disques, car les chemins vers le volume de

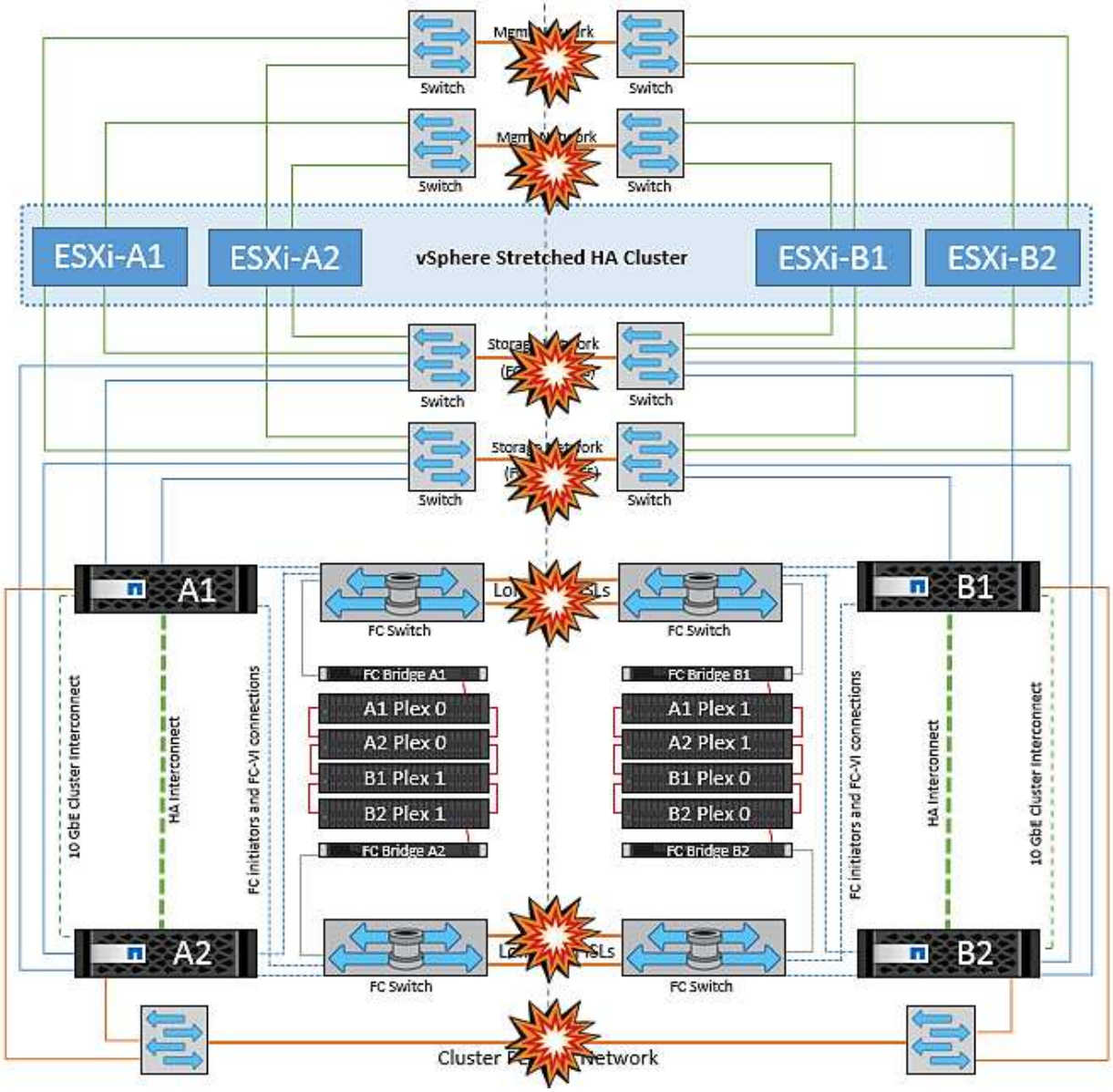
stockage sont en panne et cette machine virtuelle est en panne. Dans ce cas, VMware HA ne prend aucune action, car les hôtes envoient activement des battements du cœur. Ces machines virtuelles doivent être manuellement désactivées et activées sur leurs sites respectifs. La figure suivante illustre une machine virtuelle violant une règle d'affinité DRS.



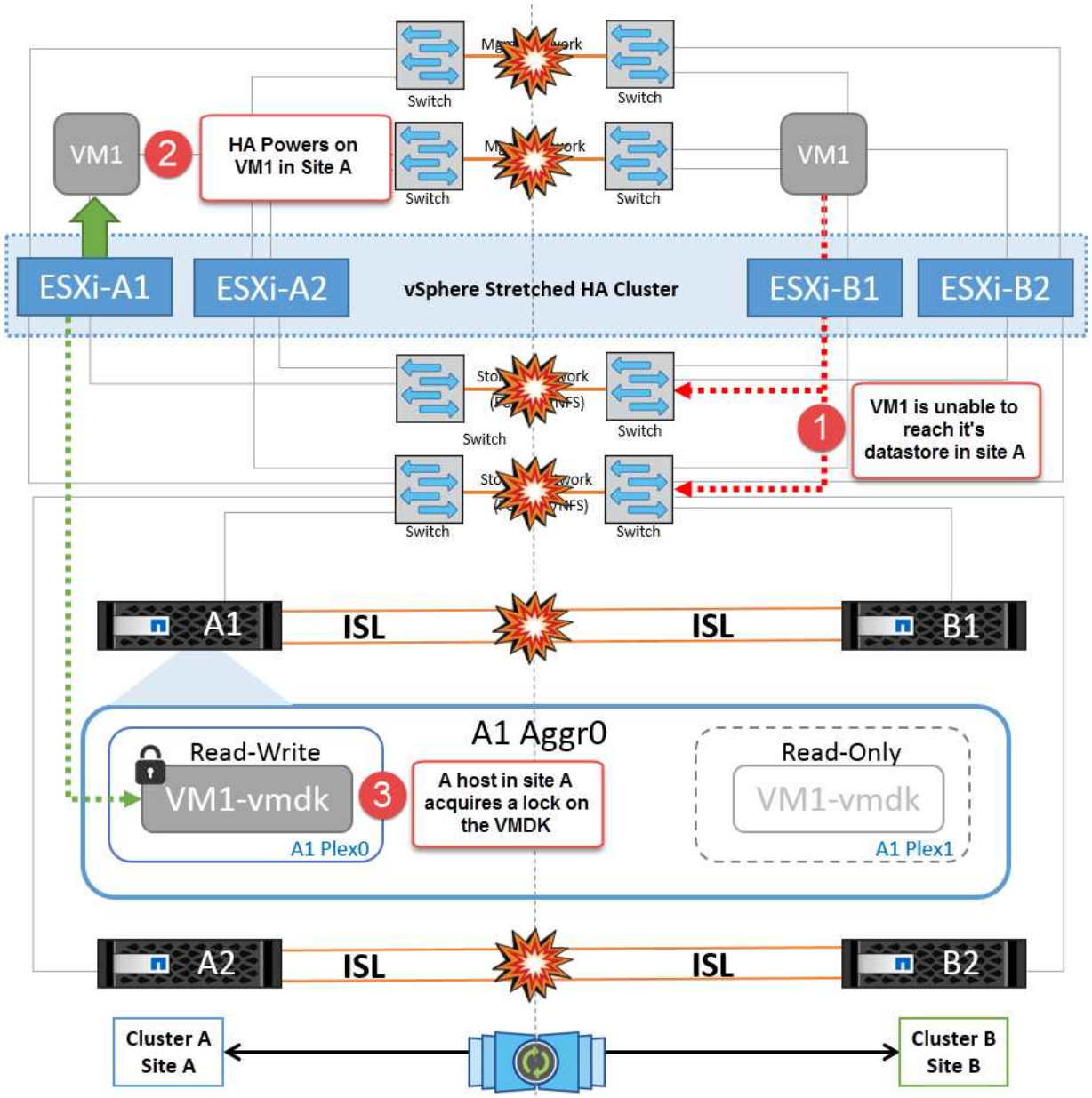
Défaillance de tous les commutateurs ou partition complète du centre de données

Dans ce scénario, toutes les liaisons ISL entre les sites sont en panne et les deux sites sont isolés les uns des autres. Comme nous l'avons vu dans les scénarios précédents, tels que la défaillance des liens ISL au niveau du réseau de gestion et du réseau de stockage, les machines virtuelles ne sont pas affectées par la défaillance complète des liens ISL.

Une fois les hôtes ESXi partitionnés entre les sites, l'agent vSphere HA vérifie la présence de battements de cœur du datastore et, sur chaque site, les hôtes ESXi locaux pourront mettre à jour les battements de cœur du datastore vers leur volume/LUN de lecture/écriture respectif. Les hôtes du site A partent du principe que les autres hôtes ESXi du site B ont échoué car il n'y a pas de pulsations réseau/datastore. VSphere HA sur le site A tentera de redémarrer les machines virtuelles du site B, ce qui finira par échouer car les datastores du site B ne seront pas accessibles en raison d'une panne de lien ISL du stockage. Une situation similaire est répétée sur le site B.



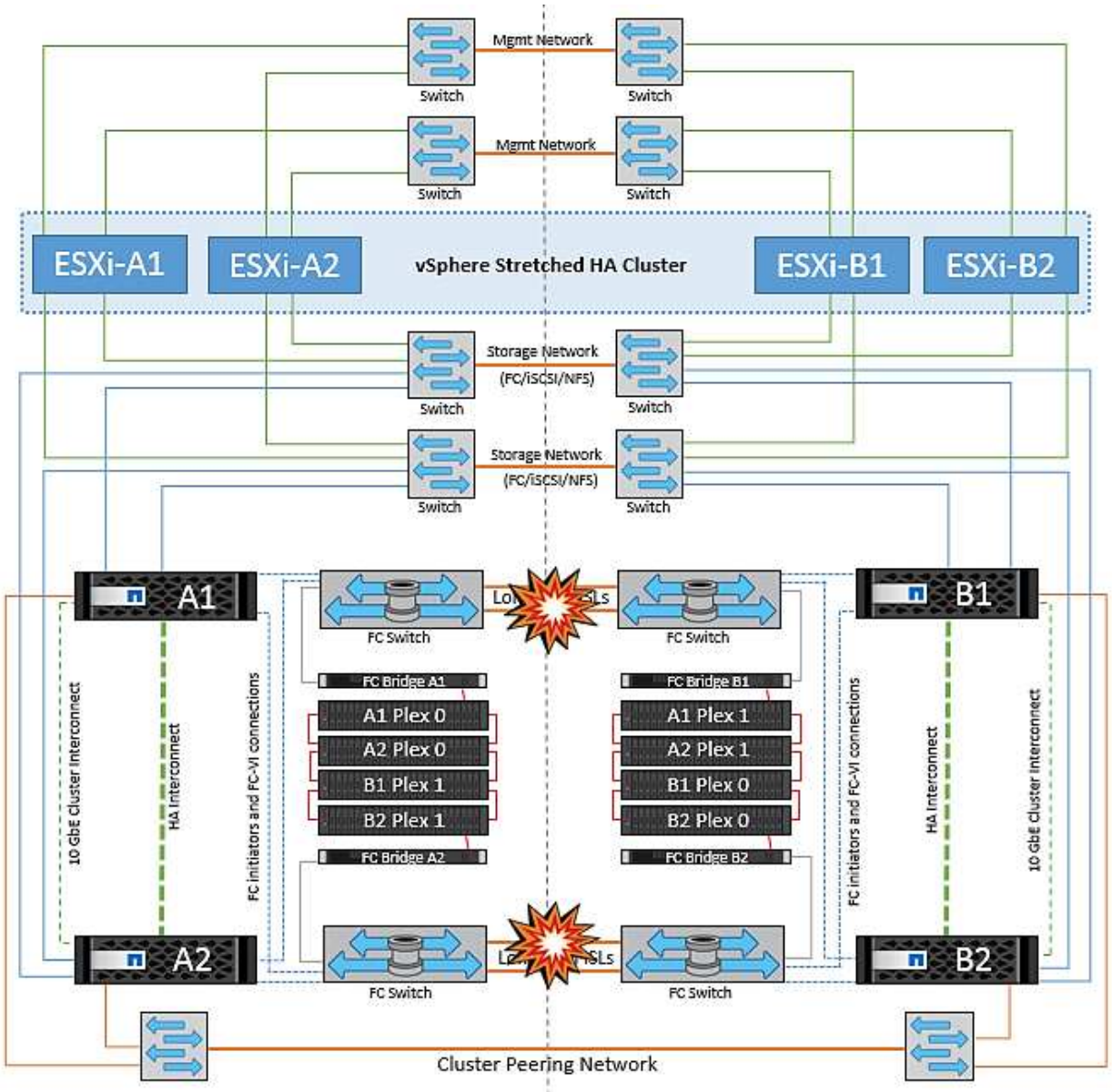
NetApp recommande de déterminer si une machine virtuelle a enfreint les règles DRS. Toutes les machines virtuelles exécutées à partir d'un site distant sont en panne, car elles ne pourront pas accéder au datastore. VSphere HA redémarrera cette machine virtuelle sur le site local. Une fois les liens ISL de nouveau en ligne, la machine virtuelle qui s'exécutait sur le site distant est arrêtée, car il ne peut pas y avoir deux instances de machines virtuelles fonctionnant avec les mêmes adresses MAC.



Défaillance de la liaison inter-commutateur sur les deux fabriques dans NetApp MetroCluster

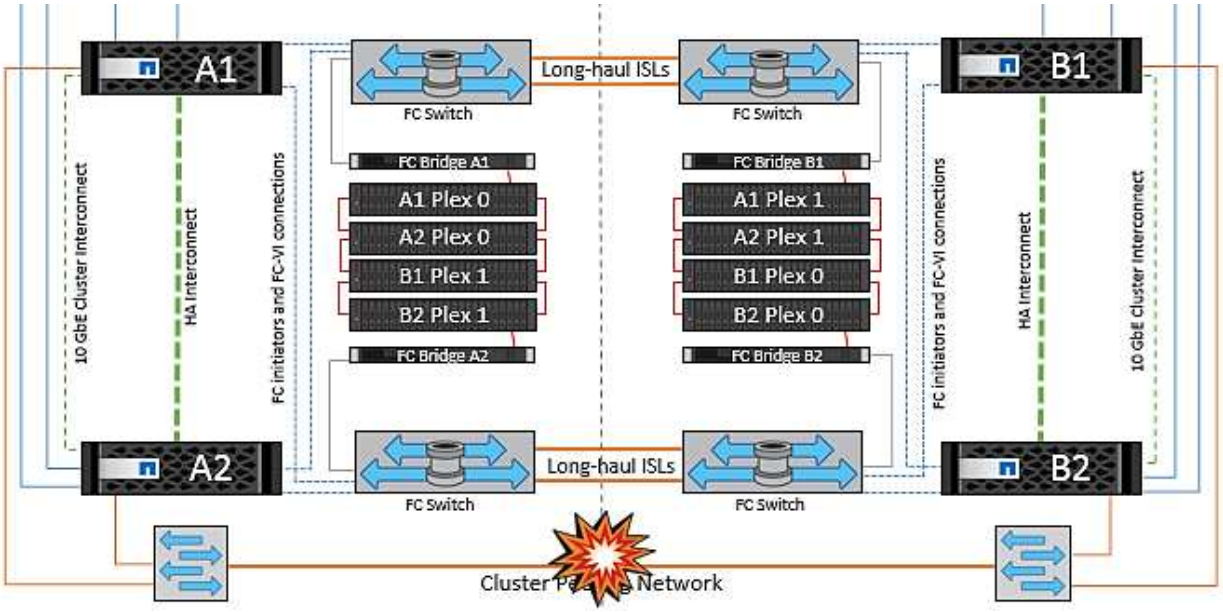
Dans le cas d'une défaillance d'un ou de plusieurs liens ISL, le trafic continue à travers les liens restants. Si toutes les liaisons ISL des deux structures échouent, de sorte qu'il n'y ait pas de liaison entre les sites pour le stockage et la réplication NVRAM, chaque contrôleur continue de transmettre ses données locales. Lors de la restauration d'un ISL au moins, la resynchronisation de tous les plexes se fera automatiquement.

Toute écriture effectuée après l'arrêt de toutes les ISL ne sera pas mise en miroir sur l'autre site. Un basculement sur incident, dans cet état, entraînerait la perte des données non synchronisées. Dans ce cas, une intervention manuelle est requise pour la restauration après le basculement. S'il est probable qu'aucune ISL ne soit disponible pendant une période prolongée, l'administrateur peut choisir de fermer tous les services de données afin d'éviter tout risque de perte de données en cas de basculement en cas d'incident. L'exécution de cette action doit être comparée à la probabilité d'un incident nécessitant un basculement avant qu'au moins un lien ISL ne soit disponible. Sinon, si les liens ISL échouent dans un scénario en cascade, un administrateur peut déclencher un basculement planifié vers l'un des sites avant que tous les liens n'aient échoué.



Défaillance du lien de peering de cluster

Dans le cas d'une défaillance de liaison de cluster peering, les liens ISL de la structure sont toujours actifs, les services de données (lectures et écritures) continuent sur les deux sites vers les deux plexes. Toute modification de la configuration du cluster (par exemple, ajout d'un SVM, provisionnement d'un volume ou d'une LUN dans un SVM existant) ne peut pas être propagée à l'autre site. Ils sont conservés dans les volumes de métadonnées CRS locaux et automatiquement propagés à l'autre cluster lors de la restauration du lien du cluster peering. Si un basculement forcé est nécessaire avant la restauration de la liaison de cluster peering, les modifications de la configuration du cluster en attente seront automatiquement lues à partir de la copie répliquée à distance des volumes de métadonnées sur le site survivant dans le cadre du processus de basculement.



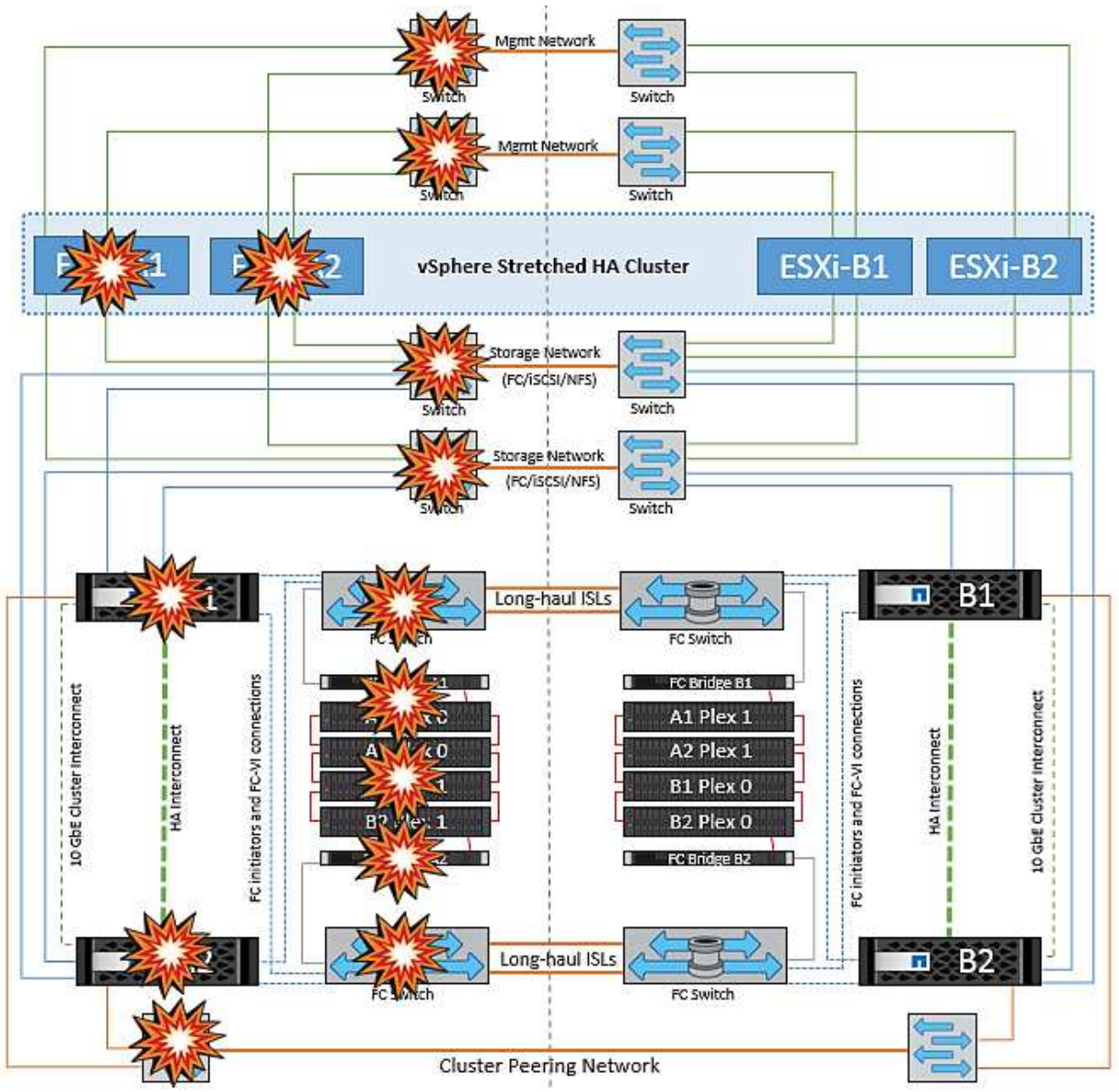
Défaillance complète du site

Dans un scénario de défaillance de site complet A, les hôtes ESXi du site B n'obtiennent pas la pulsation réseau des hôtes ESXi du site A car ils sont en panne. Le maître haute disponibilité sur le site B vérifie que les pulsations du datastore ne sont pas présentes, déclare que les hôtes du site A sont en panne et tente de redémarrer le site A des machines virtuelles sur le site B. Pendant cette période, l'administrateur du stockage effectue un basculement pour reprendre les services des nœuds défaillants sur le site survivant, ce qui restaure tous les services de stockage du site A sur le site B. Une fois que les volumes ou les LUN du site A sont disponibles sur le site B, l'agent principal de haute disponibilité tente de redémarrer le site A des machines virtuelles sur le site B.

Si la tentative de redémarrage d'une machine virtuelle par l'agent principal vSphere HA (qui implique son enregistrement et sa mise sous tension) échoue, le redémarrage est relancé après un délai. Le délai entre les redémarrages peut être configuré jusqu'à un maximum de 30 minutes. VSphere HA tente ces redémarrages au maximum pour un nombre maximal de tentatives (six tentatives par défaut).

Remarque : le maître HA ne lance pas les tentatives de redémarrage tant que le gestionnaire de placement n'a pas trouvé le stockage approprié, donc dans le cas d'une défaillance complète du site, ce serait une fois le basculement effectué.

Si le site A été basculé, la panne suivante de l'un des nœuds du site B survivant peut être gérée de manière transparente par le basculement vers le nœud survivant. Dans ce cas, le travail de quatre nœuds est désormais effectué par un seul nœud. Dans ce cas, la restauration consiste à effectuer un rétablissement vers le nœud local. Ensuite, lorsque le site A est restauré, une opération de rétablissement est effectuée pour restaurer le fonctionnement en état stable de la configuration.



Sécurité des produits

Les outils ONTAP pour VMware vSphere

L'ingénierie logicielle avec les outils ONTAP pour VMware vSphere utilise les activités de développement sécurisé suivantes :

- **Modélisation des menaces.** le but de la modélisation des menaces est de découvrir des défauts de sécurité dans une fonction, un composant ou un produit au début du cycle de vie du développement logiciel. Un modèle de menace est une représentation structurée de toutes les informations qui affectent la sécurité d'une application. En substance, c'est une vision de l'application et de son environnement par le biais du principe de sécurité.
- **Dynamic application Security Testing (DAST).** cette technologie est conçue pour détecter les conditions vulnérables sur les applications dans leur état d'exécution. DAST teste les interfaces HTTP et HTML exposées des applications Web-enable.
- **Devise de code tierce.** dans le cadre du développement de logiciels avec des logiciels open-source (OSS), vous devez corriger les vulnérabilités de sécurité qui pourraient être associées à tout OSS intégré à

votre produit. Il s'agit d'un effort continu car une nouvelle version OSS peut avoir une nouvelle vulnérabilité découverte signalée à tout moment.

- **Analyse des vulnérabilités** l'analyse des vulnérabilités a pour but de détecter les vulnérabilités de sécurité courantes et connues dans les produits NetApp avant leur publication auprès des clients.
- * Tests de pénétration.* le test de pénétration est le processus d'évaluation d'un système, d'une application Web ou d'un réseau pour trouver des vulnérabilités de sécurité qui pourraient être exploitées par un attaquant. Les tests d'intrusion chez NetApp sont réalisés par un groupe d'entreprises tierces de confiance et approuvées. Leur domaine de test comprend le lancement d'attaques contre une application ou un logiciel similaire à des intrus hostiles ou des pirates informatiques à l'aide de méthodes ou d'outils d'exploitation sophistiqués.

Fonctionnalités de sécurité du produit

Les outils ONTAP pour VMware vSphere comprennent les fonctions de sécurité suivantes dans chaque version.

- **Bannière de connexion.** SSH est désactivé par défaut et n'autorise que les connexions à une seule fois si elles sont activées à partir de la console VM. La bannière de connexion suivante s'affiche une fois que l'utilisateur a saisi un nom d'utilisateur dans l'invite de connexion :

  AVERTISSEMENT: l'accès non autorisé à ce système est interdit et sera poursuivi par la loi. En accédant à ce système, vous convenez que vos actions peuvent être surveillées si vous soupçonnez une utilisation non autorisée.

  Une fois la connexion établie par l'utilisateur via le canal SSH, le texte suivant s'affiche :

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Contrôle d'accès basé sur les rôles (RBAC).** deux types de contrôles RBAC sont associés aux outils ONTAP :
  - Privilèges de serveur vCenter natif
  - Privilèges spécifiques au plug-in vCenter. Pour plus de détails, voir "ce lien".
- **Canaux de communication cryptés.** toutes les communications externes se produisent sur HTTPS en utilisant la version 1.2 de TLS.
- **Exposition minimale au port.** seuls les ports nécessaires sont ouverts sur le pare-feu.

  Le tableau suivant décrit les détails du port ouvert.

N° de port TCP v4/v6	Direction	Fonction
8143	entrant	Connexions HTTPS pour l'API REST
8043	entrant	Connexions HTTPS

N° de port TCP v4/v6	Direction	Fonction
9060	entrant	Connexions HTTPS Utilisé pour les connexions SOAP sur https Ce port doit être ouvert pour permettre à un client de se connecter au serveur d'API des outils ONTAP.
22	entrant	SSH (désactivé par défaut)
9080	entrant	Connexions HTTPS - VP et SRA - connexions internes à partir du bouclage uniquement
9083	entrant	Connexions HTTPS - VP et SRA Utilisé pour les connexions SOAP sur https
1162	entrant	Paquets de déroutement SNMP VP
1527	diffusion interne uniquement	Port de base de données Derby, uniquement entre cet ordinateur et lui-même, connexions externes non acceptées — connexions internes uniquement
443	bidirectionnel	Utilisé pour les connexions aux clusters ONTAP

- **Prise en charge des certificats signés de l'autorité de certification (CA).** les outils ONTAP pour VMware vSphere prennent en charge les certificats signés de l'autorité de certification. Voir ceci "article de la base de connaissances" pour en savoir plus.
- **Audit Logging.** les offres de support peuvent être téléchargées et sont extrêmement détaillées. Les outils ONTAP consigne toutes les activités de connexion et de déconnexion de l'utilisateur dans un fichier journal distinct. Les appels d'API VASA sont connectés à un journal d'audit VASA dédié (local cxf.log).
- **Stratégies de mot de passe.** les stratégies de mot de passe suivantes sont respectées :
  - Les mots de passe ne sont pas enregistrés dans des fichiers journaux.
  - Les mots de passe ne sont pas communiqués en texte brut.
  - Les mots de passe sont configurés lors du processus d'installation lui-même.
  - L'historique des mots de passe est un paramètre configurable.
  - L'âge minimum du mot de passe est défini sur 24 heures.
  - La saisie automatique des champs de mot de passe est désactivée.
  - Les outils ONTAP crypte toutes les informations d'identification stockées à l'aide de la fonction de hachage SHA256.

Plug-in SnapCenter VMware vSphere

Le plug-in NetApp SnapCenter pour l'ingénierie logicielle VMware vSphere exploite les activités de développement sécurisées suivantes :

- **Modélisation des menaces.** le but de la modélisation des menaces est de découvrir des défauts de sécurité dans une fonction, un composant ou un produit au début du cycle de vie du développement logiciel. Un modèle de menace est une représentation structurée de toutes les informations qui affectent la sécurité d'une application. En substance, c'est une vision de l'application et de son environnement par le biais du principe de sécurité.
- **Test dynamique de sécurité des applications (DAST).** technologies conçues pour détecter les conditions vulnérables des applications dans leur état d'exécution. DAST teste les interfaces HTTP et HTML exposées des applications Web-enable.
- **Devise de code tierce.** dans le cadre du développement de logiciels et de l'utilisation de logiciels open-source (OSS), il est important de traiter les vulnérabilités de sécurité qui pourraient être associées à OSS qui a été intégré à votre produit. Il s'agit d'un effort continu car la version du composant OSS peut avoir une vulnérabilité nouvellement découverte signalée à tout moment.
- **Analyse des vulnérabilités** l'analyse des vulnérabilités a pour but de détecter les vulnérabilités de sécurité courantes et connues dans les produits NetApp avant leur publication auprès des clients.
- * Tests de pénétration.* le test de pénétration est le processus d'évaluation d'un système, d'une application Web ou d'un réseau pour trouver des vulnérabilités de sécurité qui pourraient être exploitées par un attaquant. Les tests d'intrusion chez NetApp sont réalisés par un groupe d'entreprises tierces de confiance et approuvées. Leur domaine de test comprend le lancement d'attaques contre une application ou un logiciel comme des intrus hostiles ou des pirates informatiques à l'aide de méthodes ou d'outils d'exploitation sophistiqués.
- **Activité de réponse aux incidents de sécurité des produits.** les vulnérabilités de sécurité sont découvertes à la fois en interne et en externe dans l'entreprise et peuvent constituer un risque sérieux pour la réputation de NetApp si elles ne sont pas traitées dans les délais impartis. Pour faciliter ce processus, l'équipe d'intervention en cas d'incident de sécurité des produits (PSIRT) signale et effectue le suivi des vulnérabilités.

Fonctionnalités de sécurité du produit

Le plug-in NetApp SnapCenter pour VMware vSphere inclut les fonctionnalités de sécurité suivantes dans chaque version :

- **Accès limité au shell.** SSH est désactivé par défaut, et les connexions à une seule fois ne sont autorisées que si elles sont activées à partir de la console VM.
- **Avertissement d'accès dans la bannière de connexion.** la bannière de connexion suivante s'affiche après que l'utilisateur ait entré un nom d'utilisateur dans l'invite de connexion :

  AVERTISSEMENT: l'accès non autorisé à ce système est interdit et sera poursuivi par la loi. En accédant à ce système, vous convenez que vos actions peuvent être surveillées si vous soupçonnez une utilisation non autorisée.

  Une fois que l'utilisateur a terminé sa connexion via le canal SSH, les valeurs de sortie suivantes s'affichent :

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Contrôle d'accès basé sur les rôles (RBAC).** deux types de contrôles RBAC sont associés aux outils ONTAP :
  - Privilèges de serveur vCenter natif.
  - Privilèges spécifiques au plug-in VMware vCenter. Pour plus d'informations, voir "Contrôle d'accès basé sur des rôles (RBAC)".
- **Canaux de communication cryptés.** toutes les communications externes sont effectuées via HTTPS en utilisant TLS.
- **Exposition minimale au port.** seuls les ports nécessaires sont ouverts sur le pare-feu.

Le tableau suivant fournit les détails du port ouvert.

Numéro de port TCP v4/v6	Fonction
8144	Connexions HTTPS pour l'API REST
8080	Connexions HTTPS pour interface graphique OVA
22	SSH (désactivé par défaut)
3306	MySQL (connexions internes uniquement, connexions externes désactivées par défaut)
443	Nginx (services de protection des données)

- **Prise en charge des certificats signés par l'autorité de certification (CA).** le plug-in SnapCenter pour VMware vSphere prend en charge la fonctionnalité des certificats signés par l'autorité de certification. Voir "Comment créer et/ou importer un certificat SSL dans le plug-in SnapCenter pour VMware vSphere (SCV)".
- **Stratégies de mot de passe.** les stratégies de mot de passe suivantes sont en vigueur :
  - Les mots de passe ne sont pas enregistrés dans des fichiers journaux.
  - Les mots de passe ne sont pas communiqués en texte brut.
  - Les mots de passe sont configurés lors du processus d'installation lui-même.
  - Toutes les informations d'identification sont stockées à l'aide d'un hachage SHA256.
- **Image du système d'exploitation de base.** le produit est fourni avec le système d'exploitation de base Debian pour OVA avec accès restreint et accès au shell désactivé. Cela réduit l'empreinte d'attaque. Chaque système d'exploitation de base SnapCenter est mis à jour avec les derniers correctifs de sécurité disponibles pour une protection maximale.

NetApp développe des fonctionnalités logicielles et des correctifs de sécurité en ce qui concerne le plug-in SnapCenter pour l'appliance VMware vSphere, puis les publie auprès de ses clients sous la forme d'un pack logiciel. Étant donné que ces dispositifs intègrent des dépendances spécifiques au système d'exploitation Linux et à notre logiciel propriétaire, NetApp vous recommande de ne pas modifier le système sous-exploitation, car il présente un potentiel important d'affecter l'appliance NetApp. Cela pourrait affecter la capacité de NetApp à prendre en charge l'appliance. NetApp recommande de tester et de déployer la dernière version de code pour les appliances, car elles sont publiées pour corriger les problèmes de sécurité.

Guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere

Guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere

Le guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere fournit un ensemble complet d'instructions pour configurer les paramètres les plus sécurisés.

Ces guides s'appliquent à la fois aux applications et au système d'exploitation invité de l'appliance elle-même.

Vérification de l'intégrité des outils ONTAP pour les packages d'installation VMware vSphere

Deux méthodes sont disponibles pour vérifier l'intégrité des packages d'installation des outils ONTAP.

1. Vérification des checksums
2. Vérification de la signature

Les sommes de contrôle sont fournies sur les pages de téléchargement des paquets d'installation d'OTV. Les utilisateurs doivent vérifier les sommes de contrôle des paquets téléchargés par rapport à la somme de contrôle fournie sur la page de téléchargement.

Vérification de la signature des outils ONTAP OVA

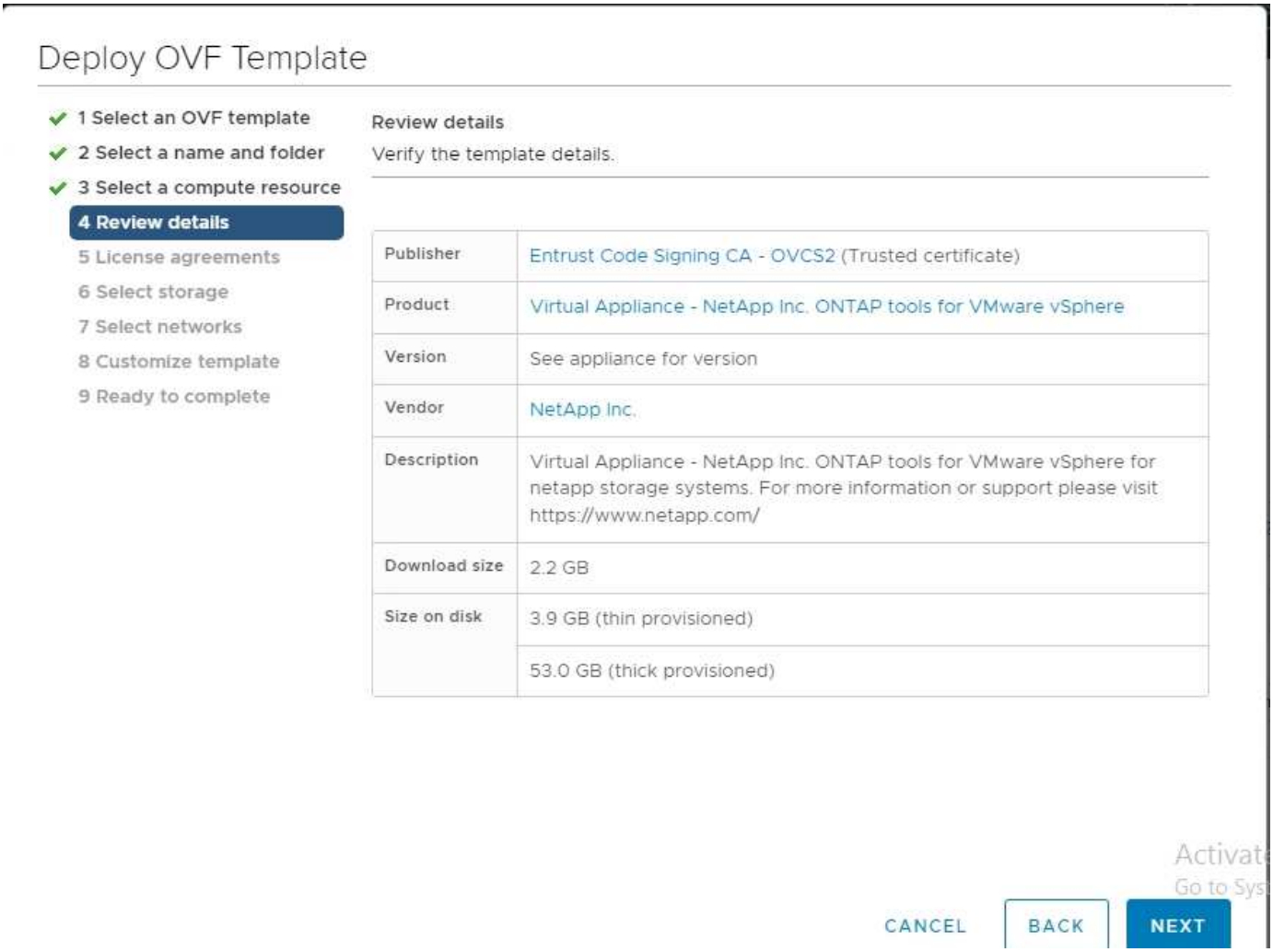
Le paquet d'installation de vApp est livré sous la forme d'une boule de commande. Ce tarball contient des certificats intermédiaires et racine pour l'appliance virtuelle, ainsi qu'un fichier README et un package OVA. Le fichier README guide les utilisateurs sur la façon de vérifier l'intégrité du progiciel VApp OVA.

Les clients doivent également télécharger les certificats racine et intermédiaire fournis sur vCenter version 7.0U3E et ultérieure. Pour les versions vCenter comprises entre 7.0.1 et 7.0.U3E, la fonctionnalité de vérification du certificat n'est pas prise en charge par VMware. Les clients n'ont pas besoin de télécharger de certificat pour vCenter versions 6.x.

Téléchargement du certificat racine sécurisé vers vCenter

1. Connectez-vous à vCenter Server à l'aide du client VMware vSphere.
2. Spécifiez le nom d'utilisateur et le mot de passe de laman@vspher.locl ou d'un autre membre du groupe administrateurs d'authentification unique vCenter. Si vous avez spécifié un domaine différent lors de l'installation, connectez-vous en tant qu'administrateur@mondomaine.
3. Accédez à l'interface utilisateur de la gestion des certificats : a. Dans le menu Accueil, sélectionnez Administration. b. Sous certificats, cliquez sur gestion des certificats.
4. Si le système vous y invite, entrez les informations d'identification de votre serveur vCenter.
5. Sous certificats racine approuvés, cliquez sur Ajouter.
6. Cliquez sur Parcourir et sélectionnez l'emplacement du fichier .pem du certificat (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).
7. Cliquez sur Ajouter. Le certificat est ajouté au magasin.

Reportez-vous à la section "Ajoutez un certificat racine de confiance au magasin de certificats" pour en savoir plus. Lors du déploiement d'une vApp (à l'aide du fichier OVA), la signature numérique du package vApp peut être vérifiée sur la page « Review details » (vérifier les détails). Si le package vApp téléchargé est authentique, la colonne « Éditeur » affiche « certificat de confiance » (comme dans la capture d'écran suivante).



Vérification de la signature des outils ONTAP ISO et SRA tar.gz

NetApp partage son certificat de signature de code avec les clients sur la page de téléchargement du produit, ainsi que les fichiers zip du produit pour OTV-ISO et SRA.tgz.

À partir du certificat de signature de code, les utilisateurs peuvent extraire la clé publique comme suit :

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Ensuite, la clé publique doit être utilisée pour vérifier la signature
pour iso et tgz produit zip comme ci-dessous :
```

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
Exemple :
```

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

Ports et protocoles

La liste ci-dessous répertorie les ports et les protocoles requis permettant la communication entre les outils ONTAP pour le serveur VMware vSphere et d'autres entités telles que les systèmes de stockage géré, les serveurs et d'autres composants.

Ports entrants et sortants requis pour OTV

Veuillez noter le tableau ci-dessous qui répertorie les ports entrants et sortants requis pour le bon fonctionnement des outils ONTAP. Il est important de s'assurer que seuls les ports mentionnés dans le tableau sont ouverts pour les connexions à partir de machines distantes, tandis que tous les autres ports doivent être bloqués pour les connexions à partir de machines distantes. Cela permet d'assurer la sécurité de votre système.

Le tableau suivant décrit les détails du port ouvert.

Port TCP v4/v6 #	Direction	Fonction
8143	entrant	Connexions HTTPS pour l'API REST
8043	entrant	Connexions HTTPS
9060	entrant	Connexions HTTPS Utilisé pour les connexions SOAP sur HTTPS Ce port doit être ouvert pour permettre à un client de se connecter au serveur d'API des outils ONTAP.
22	entrant	SSH (désactivé par défaut)
9080	entrant	Connexions HTTPS - VP et SRA - connexions internes à partir du bouclage uniquement
9083	entrant	Connexions HTTPS - VP et SRA Utilisé pour les connexions SOAP sur HTTPS
1162	entrant	Paquets de déroutement SNMP VP
8443	entrant	Plug-in distant
1527	diffusion interne uniquement	Port de base de données Derby, uniquement entre cet ordinateur et lui-même, connexions externes non acceptées — connexions internes uniquement
8150	diffusion interne uniquement	Le service d'intégrité des journaux s'exécute sur le port
443	bidirectionnel	Utilisé pour les connexions aux clusters ONTAP

Contrôle de l'accès à distance à la base de données Derby

Les administrateurs peuvent accéder à la base de données derby à l'aide des commandes suivantes. Il est accessible via la machine virtuelle locale des outils ONTAP ainsi qu'un serveur distant en procédant comme suit :

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

exemple:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                   |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                   |
SYS                 |SYSCHECKS                    |
SYS                 |SYSCOLPERMS                  |
SYS                 |SYSCOLUMNS                   |
SYS                 |SYSCONGLOMERATES             |
SYS                 |SYSCONSTRAINTS               |
SYS                 |SYSDEPENDS                   |
SYS                 |SYSFILES                     |
SYS                 |SYSFOREIGNKEYS               |
SYS                 |SYSKEYS                      |
SYS                 |SYSPERMS                     |
```

Outils ONTAP pour les points d'accès VMware vSphere (utilisateurs)

L'installation des outils ONTAP pour VMware vSphere crée et utilise trois types d'utilisateurs :

1. Utilisateur système : compte utilisateur root
2. Utilisateur de l'application : l'utilisateur administrateur, l'utilisateur maint et les comptes utilisateur db
3. Utilisateur de support : compte utilisateur diag

1. Utilisateur du système

L'utilisateur System(root) est créé par l'installation des outils ONTAP sur le système d'exploitation sous-jacent (Debian).

- Un utilisateur système par défaut "root" est créé sur Debian par l'installation des outils ONTAP. Sa valeur par défaut est désactivée et peut être activée ad hoc via la console « maint ».

2. Utilisateur de l'application

L'utilisateur de l'application est nommé en tant qu'utilisateur local dans les outils ONTAP. Il s'agit d'utilisateurs créés dans l'application Outils ONTAP. Le tableau ci-dessous répertorie les types d'utilisateurs d'applications :

Utilisateur	Description
Utilisateur administrateur	Il est créé lors de l'installation des outils ONTAP et l'utilisateur fournit les informations d'identification lors du déploiement des outils ONTAP. Les utilisateurs ont la possibilité de modifier le mot de passe dans la console « maint ». Le mot de passe expirera dans 90 jours et les utilisateurs devraient changer de mot de passe.
Utilisateur de maintenance	Il est créé lors de l'installation des outils ONTAP et l'utilisateur fournit les informations d'identification lors du déploiement des outils ONTAP. Les utilisateurs ont la possibilité de modifier le mot de passe dans la console « maint ». Il s'agit d'un utilisateur de maintenance créé pour exécuter les opérations de la console de maintenance.
Utilisateur de la base de données	Il est créé lors de l'installation des outils ONTAP et l'utilisateur fournit les informations d'identification lors du déploiement des outils ONTAP. Les utilisateurs ont la possibilité de modifier le mot de passe dans la console « maint ». Le mot de passe expirera dans 90 jours et les utilisateurs devraient changer de mot de passe.

3. Support user(diag user)

Lors de l'installation des outils ONTAP, un utilisateur du support est créé. Cet utilisateur peut accéder aux outils ONTAP en cas de problème ou de panne du serveur et collecter les journaux. Par défaut, cet utilisateur est désactivé, mais il peut être activé sur une base ad hoc via la console « maint ». Il est important de noter que cet utilisateur sera automatiquement désactivé après une certaine période.

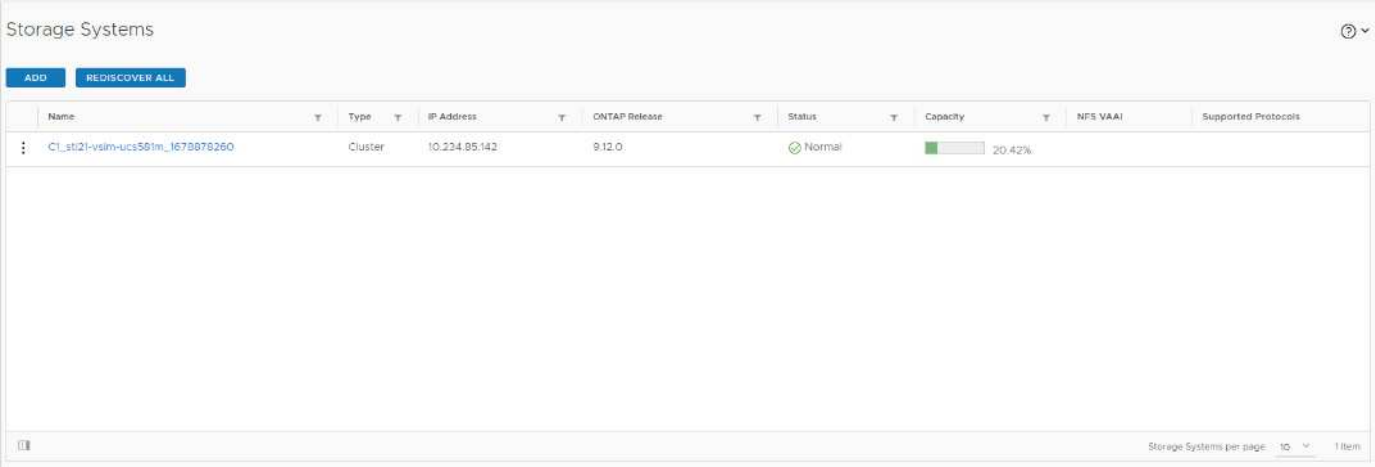
Authentification mutuelle TLS (basée sur un certificat)

Les versions 9.7 et ultérieures de ONTAP prennent en charge les communications TLS mutuelles. Depuis les outils ONTAP pour VMware et vSphere 9.12, le protocole TLS mutuel est utilisé pour la communication avec les nouveaux clusters ajoutés (selon la version de ONTAP).

ONTAP

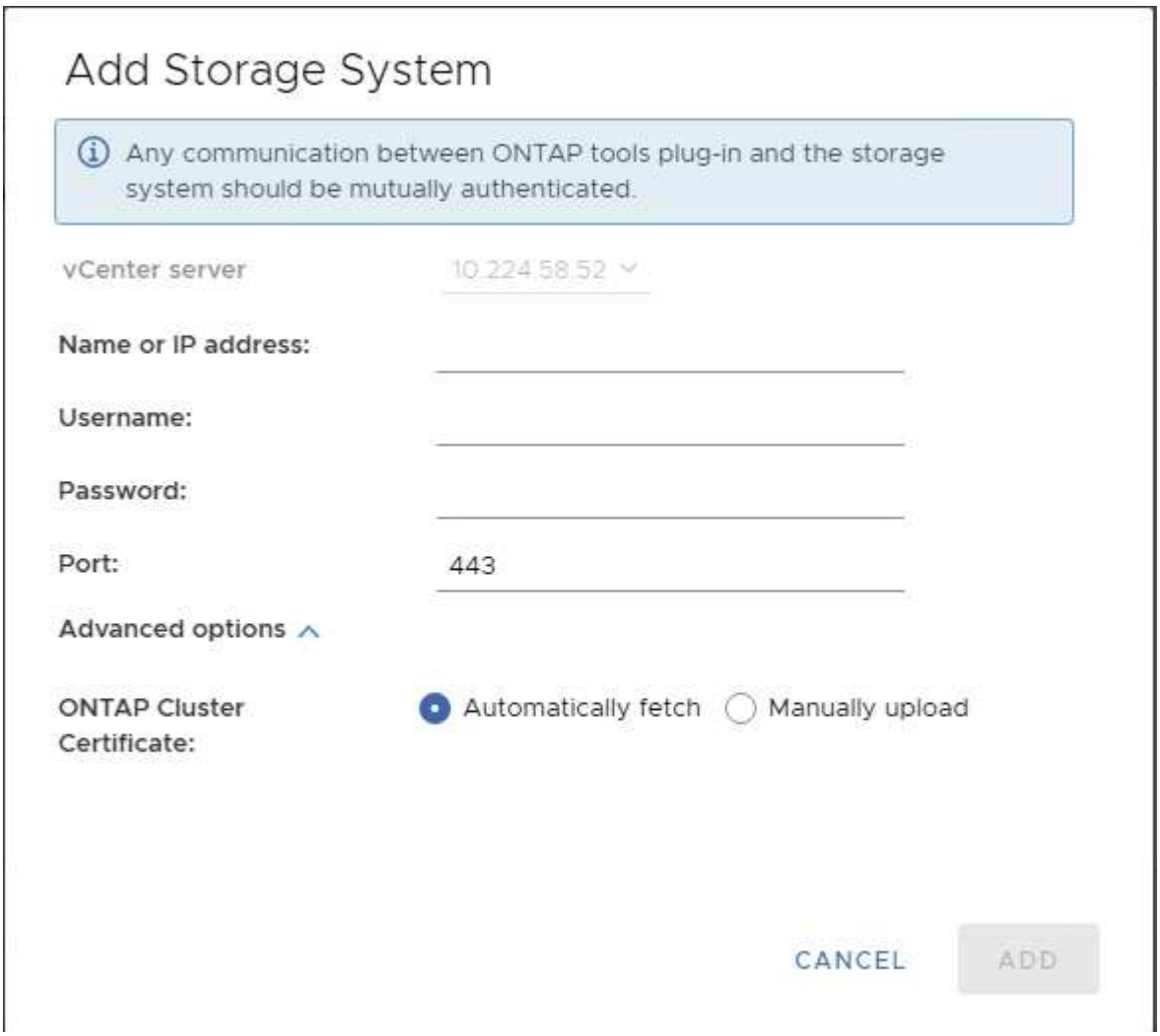
Pour tous les systèmes de stockage précédemment ajoutés : lors d'une mise à niveau, tous les systèmes de stockage ajoutés font l'objet d'une fiabilité automatique et les mécanismes d'authentification basés sur des certificats sont configurés.

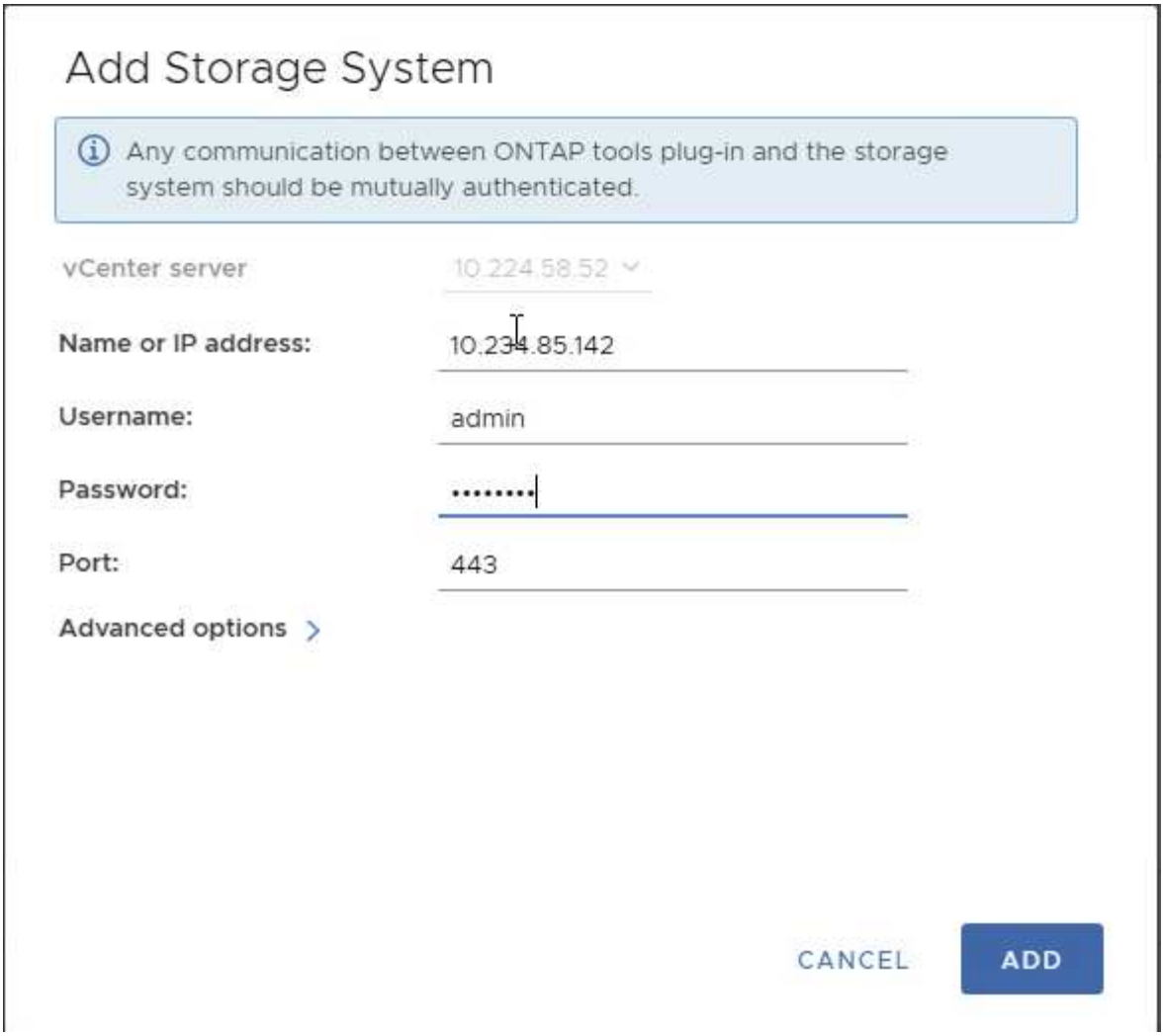
Comme dans la capture d'écran ci-dessous, la page de configuration du cluster affiche l'état d'authentification mutuelle TLS (Certificate Based Authentication), configurée pour chaque cluster.

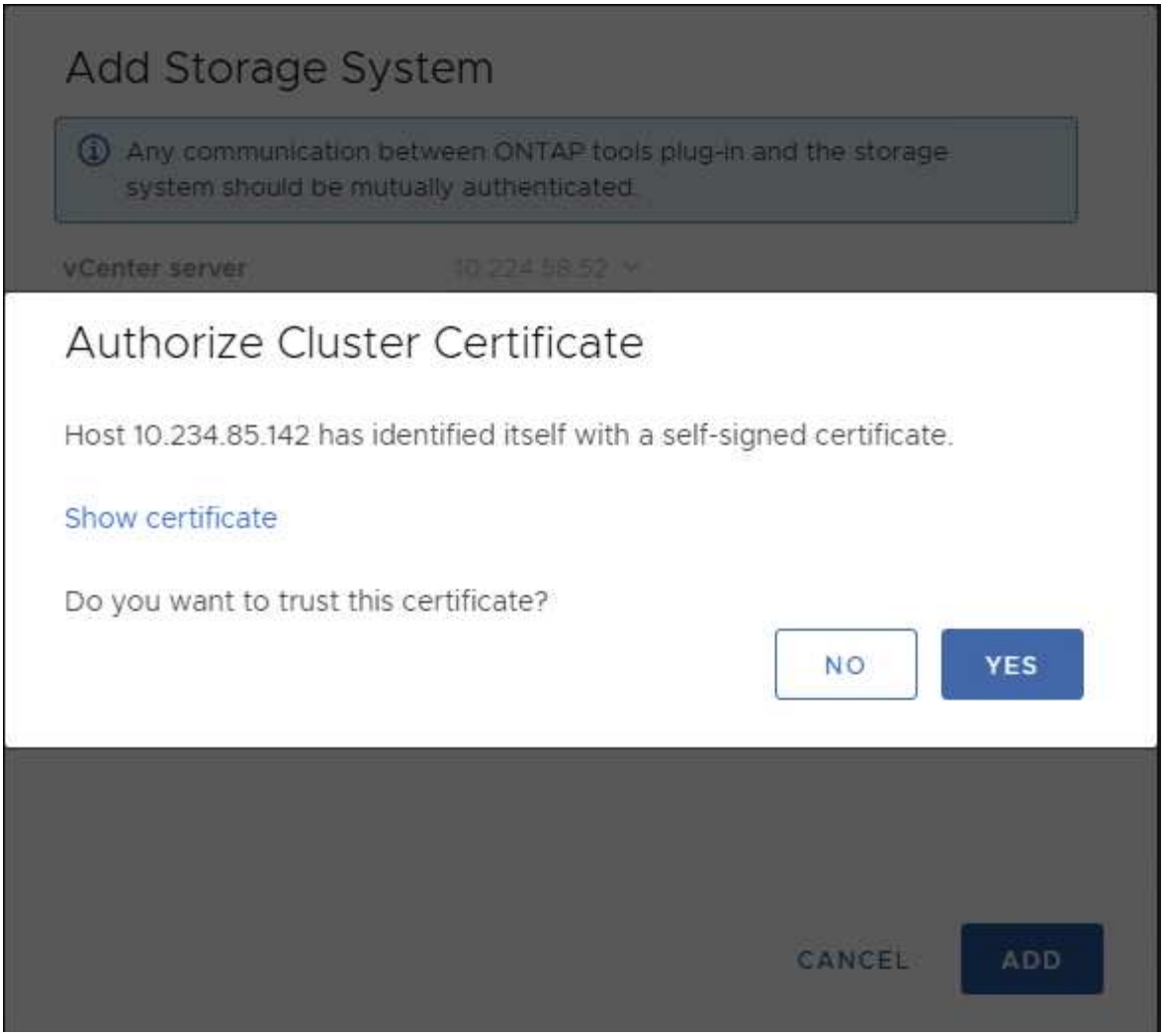


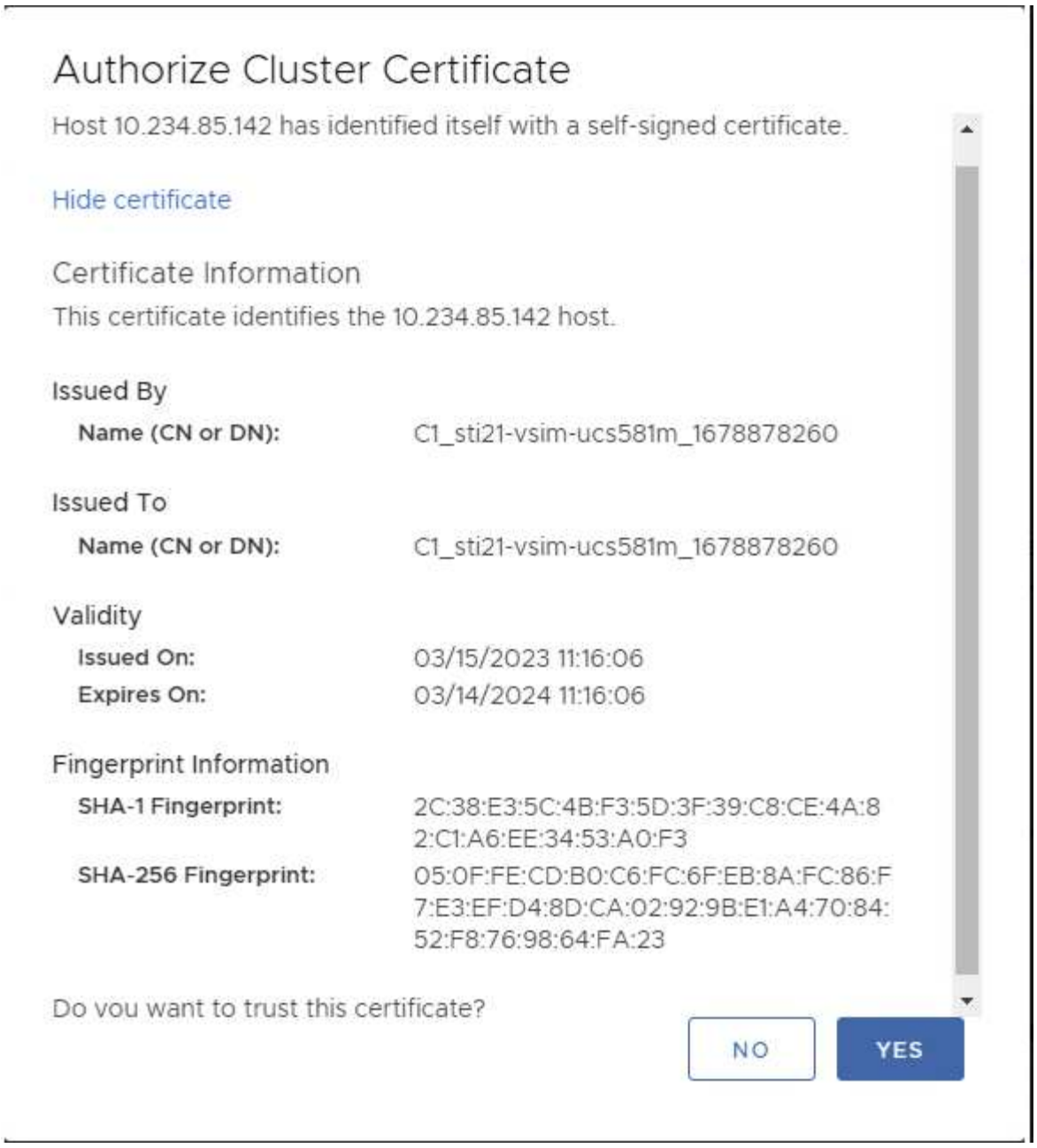
Cluster Add

Lors du workflow d'ajout de cluster, si le cluster ajouté prend en charge MTLS, MTLS sera configuré par défaut. L'utilisateur n'a pas besoin d'effectuer de configuration pour cela. La capture d'écran ci-dessous présente l'écran présenté à l'utilisateur lors de l'ajout d'un cluster.




Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

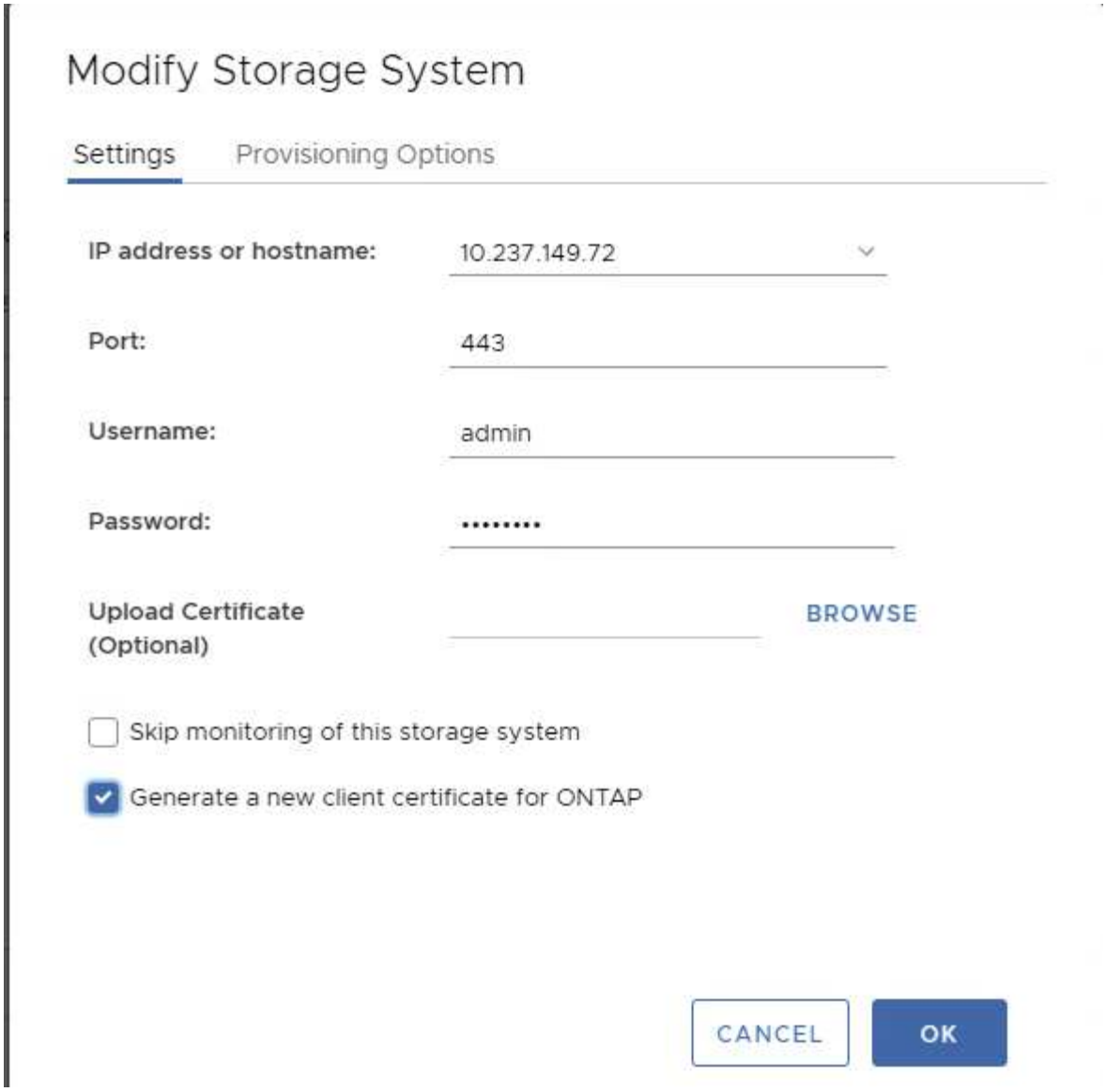

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

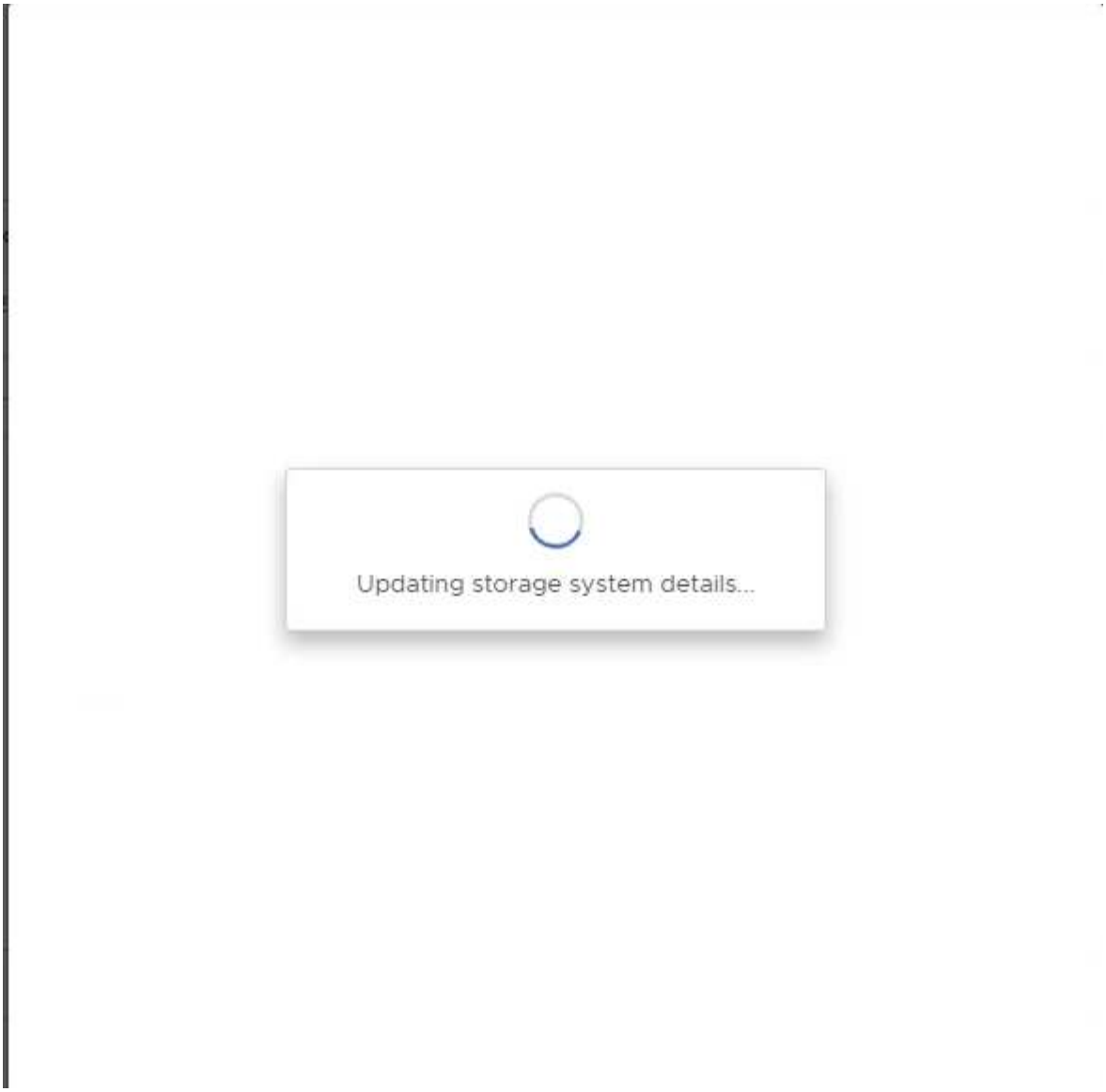


Modification du cluster

Lors de l'opération d'édition de cluster, il existe deux scénarios :

- Si le certificat ONTAP expire, l'utilisateur devra obtenir le nouveau certificat et le télécharger.
- Si le certificat OTV expire, l'utilisateur peut le régénérer en cochant la case.
  - *Générer un nouveau certificat client pour ONTAP.*


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK



Certificat HTTPS des outils ONTAP

Par défaut, les outils ONTAP utilisent un certificat auto-signé automatiquement créé lors de l'installation pour sécuriser l'accès HTTPS à l'interface utilisateur Web. Les outils ONTAP offrent les fonctionnalités suivantes :

1. Régénérer le certificat HTTPS

Lors de l'installation des outils ONTAP, un certificat d'autorité de certification HTTPS est installé et le certificat est stocké dans le magasin de clés. L'utilisateur a la possibilité de régénérer le certificat HTTPS via la console maint.

Les options ci-dessus sont accessibles dans *maint* console en accédant à *'Configuration de l'application'* → *'régénérer les certificats'*.

Bannière de connexion

La bannière de connexion suivante s'affiche lorsque l'utilisateur saisit un nom d'utilisateur

dans l'invite de connexion. Notez que SSH est désactivé par défaut et n'autorise que les connexions uniques lorsqu'elles sont activées à partir de la console de la machine virtuelle.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Une fois que l'utilisateur a terminé sa connexion via le canal SSH, le texte suivant s'affiche :

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Délai d'inactivité

Pour empêcher tout accès non autorisé, un délai d'inactivité est défini, ce qui déconnecte automatiquement les utilisateurs inactifs pendant une certaine période pendant l'utilisation des ressources autorisées. Cela permet de garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources et contribue à maintenir la sécurité.

- Par défaut, les sessions du client vSphere se ferment après 120 minutes d'inactivité, ce qui oblige l'utilisateur à se reconnecter pour reprendre à l'aide du client. Vous pouvez modifier la valeur du délai d'attente en modifiant le fichier webclient.properties. Vous pouvez configurer le délai d'expiration du client vSphere "Configurez la valeur du délai d'expiration du client vSphere"
- Les outils ONTAP ont un délai de déconnexion de session de l'interface de ligne de commande Web de 30 minutes.

Nombre maximal de requêtes simultanées par utilisateur (protection de sécurité réseau :: Attaque DOS)

Par défaut, le nombre maximal de requêtes simultanées par utilisateur est de 48. L'utilisateur root des outils ONTAP peut modifier cette valeur en fonction des besoins de son environnement. **Cette valeur ne doit pas être définie sur une valeur très élevée car cela fournit un mécanisme contre les attaques par déni de service (DOS).**

Les utilisateurs peuvent modifier le nombre maximal de sessions simultanées et d'autres paramètres pris en

charge dans le fichier */opt/netapp/vscserver/etc/dofilterParams.json*.

Nous pouvons configurer le filtre en utilisant les paramètres suivants :

- ***delayMS***: Le délai en millisecondes donné à toutes les demandes au-delà de la limite de taux avant qu'elles ne soient prises en compte. Donnez -1 pour rejeter simplement la demande.
- ***étrangletMs***: Combien de temps pour attendre le sémaphore en mode asynchrone.
- ***maxRequestMS*** : durée d'exécution de cette requête.
- ***ipWhitelist***: Une liste d'adresses IP séparées par des virgules qui ne seront pas à débit limité. (Il peut s'agir d'adresses IP vCenter, ESXi et SRA)
- ***maxRequestsPerSec*** : nombre maximal de requêtes provenant d'une connexion par seconde.

Valeurs par défaut dans le fichier *dofilterParams*:

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

Configuration du protocole NTP (Network Time Protocol)

Des problèmes de sécurité peuvent parfois se produire en raison de différences dans les configurations de l'heure du réseau. Il est important de s'assurer que tous les périphériques d'un réseau disposent de paramètres d'heure précis pour éviter de tels problèmes.

Appareil virtuel

Vous pouvez configurer le ou les serveurs NTP à partir de la console de maintenance de l'appliance virtuelle. Les utilisateurs peuvent ajouter les détails du serveur NTP sous *System Configuration* ⇒ *Add New NTP Server* option

Par défaut, le service NTP est ntpd. Il s'agit d'un service hérité qui ne fonctionne pas bien pour les machines virtuelles dans certains cas.

Debian

Sous Debian, l'utilisateur peut accéder au fichier /etc/ntp.conf pour obtenir des détails sur le serveur ntp.

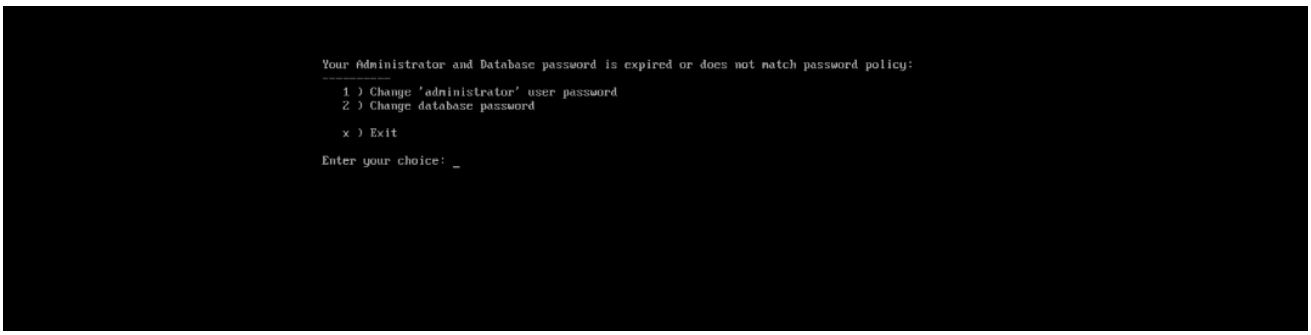
Stratégies de mot de passe

Les utilisateurs qui déploient des outils ONTAP pour la première fois ou qui effectuent une mise à niveau vers la version 9.12 ou ultérieure devront suivre la stratégie de mot de passe robuste pour l'administrateur et les utilisateurs de base de données. Au cours du processus de déploiement, les nouveaux utilisateurs seront invités à entrer leurs mots de passe. Pour les utilisateurs de brownfield qui effectuent une mise à niveau vers la version 9.12 ou ultérieure, l'option de suivre la stratégie de mot de passe fort sera disponible

dans la console de maintenance.

- Une fois que l'utilisateur se connecte à la console maint, les mots de passe sont vérifiés par rapport au jeu de règles complexes et s'il n'est pas suivi, l'utilisateur est invité à les réinitialiser.
- La validité par défaut du mot de passe est de 90 jours et après 75 jours, l'utilisateur commence à recevoir la notification de modification du mot de passe.
- Il est nécessaire de définir un nouveau mot de passe à chaque cycle, le système ne prendra pas le dernier mot de passe comme nouveau mot de passe.
- Chaque fois qu'un utilisateur se connecte à la console maint, il vérifie les stratégies de mot de passe comme les captures d'écran ci-dessous avant de charger le menu principal :

- S'il n'est pas trouvé en suivant la stratégie de mot de passe ou sa configuration de mise à niveau à partir des outils ONTAP 9.11 ou antérieurs. L'utilisateur verra alors l'écran suivant pour réinitialiser le mot de passe :



- Si l'utilisateur tente de définir un mot de passe faible ou donne à nouveau le dernier mot de passe, l'erreur suivante s'affiche :