



VMware site Recovery Manager et ONTAP

Enterprise applications

NetApp
February 10, 2026

Sommaire

VMware site Recovery Manager et ONTAP	1
Restauration de site en direct VMware avec ONTAP	1
Pourquoi utiliser ONTAP avec VLSR ou SRM ?	1
Comment VLSR exploite ONTAP 9	2
VLSR avec ONTAP et autres cas d'utilisation : cloud hybride et migration	2
Bonnes pratiques de déploiement	3
Utiliser la dernière version des outils ONTAP 10	3
Disposition des SVM et segmentation pour la colocation sécurisée	3
Meilleures pratiques pour la gestion des systèmes ONTAP 9	3
Meilleures pratiques opérationnelles	4
Datastores et protocoles	4
À propos des paires de baies	5
À propos des groupes de réplication	6
À propos des groupes de protection	6
À propos des plans de reprise	7
Tester le basculement	7
Considérations relatives au basculement	7
Reprotéger	8
Du rétablissement	8
Reprotéger le site d'origine	8
Topologies de réplication	9
Dispositions SnapMirror prises en charge	9
Prise en charge de VMFS avec la synchronisation active SnapMirror	11
Mises en page de Array Manager prises en charge	12
Présentations non prises en charge	13
SnapMirror en cascade	14
SnapMirror et SnapVault	15
Utilisation de qtrees dans les environnements site Recovery Manager	17
Environnements FC et iSCSI mixtes	17
Dépannage de VLSRM/SRM lors de l'utilisation de la réplication vVols	18
Informations supplémentaires	19

VMware site Recovery Manager et ONTAP

Restauration de site en direct VMware avec ONTAP

ONTAP est une solution de stockage de premier plan pour VMware vSphere et, plus récemment, Cloud Foundation, depuis l'introduction d'ESX dans les centres de données modernes il y a plus de deux décennies. NetApp continue d'introduire des systèmes innovants, tels que la dernière génération de la série ASA A, ainsi que des fonctionnalités telles que la synchronisation active SnapMirror. Ces avancées simplifient la gestion, améliorent la résilience et réduisent le coût total de possession (TCO) de votre infrastructure informatique.

Ce document présente la solution ONTAP pour VMware Live Site Recovery (VLSR), anciennement connu sous le nom de Site Recovery Manager (SRM), le logiciel de reprise après sinistre (DR) leader du secteur de VMware, y compris les dernières informations sur les produits et les meilleures pratiques pour rationaliser le déploiement, réduire les risques et simplifier la gestion continue.



Cette documentation remplace le rapport technique précédemment publié *TR-4900 : VMware Site Recovery Manager avec 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 porte sur les fonctionnalités des dernières versions de ONTAP 9 utilisées conjointement avec les outils ONTAP pour VMware vSphere 10.4 (notamment NetApp Storage Replication adapter [SRA] et VASA Provider [VP]), ainsi que sur VMware Live site Recovery 9.

Pourquoi utiliser ONTAP avec VLSR ou SRM ?

Les plates-formes de gestion de données NetApp optimisées par ONTAP font partie des solutions de stockage les plus largement adoptées pour VLSR. Les raisons sont nombreuses : une plate-forme de gestion de données sécurisée, hautes performances et unifiée (NAS et SAN ensemble) qui offre une efficacité de stockage définissant le secteur, une multilocation, des contrôles de qualité de service, une protection des données avec des instantanés économes en espace et une réplication avec SnapMirror. Le tout s'appuyant sur l'intégration multicloud hybride native pour la protection des charges de travail VMware et une pléthore d'outils d'automatisation et d'orchestration à portée de main.

Lorsque vous utilisez SnapMirror pour la réplication basée sur une baie, vous bénéficiez de l'une des technologies les plus éprouvées et les plus matures d'ONTAP. SnapMirror vous offre l'avantage de transferts de données sécurisés et très efficaces, en copiant uniquement les blocs de système de fichiers modifiés, et non des machines virtuelles ou des banques de données entières. Même ces blocs bénéficient d'économies d'espace, telles que la déduplication, la compression et le compactage. Les systèmes ONTAP modernes utilisent désormais SnapMirror indépendant de la version, ce qui vous permet de sélectionner vos clusters source et de destination avec flexibilité. SnapMirror est véritablement devenu l'un des outils les plus puissants disponibles pour la reprise après sinistre.

Que vous utilisiez des magasins de données traditionnels NFS, iSCSI ou Fibre Channel (désormais avec prise en charge des magasins de données vVols), VLSR fournit une offre propriétaire robuste qui exploite le

meilleur des fonctionnalités ONTAP pour la reprise après sinistre ou la planification et l'orchestration de la migration du centre de données.

Comment VLSR exploite ONTAP 9

VLSR 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 des outils ONTAP, précédemment appelé Virtual Storage Console (VSC), simplifie les fonctionnalités d'efficacité et de gestion du stockage, améliore la disponibilité et réduit les coûts de stockage et les coûts d'exploitation, 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 lors de l'utilisation de vSphere avec les systèmes exécutant ONTAP.
- Les outils ONTAP VASA Provider prennent en charge le framework 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. Cela a permis la prise en charge des volumes virtuels VMware (vVols) et la gestion des politiques de stockage des machines virtuelles et des performances des vVols des machines virtuelles individuelles. Il fournit également des alarmes pour la surveillance de la capacité et la conformité avec les profils.
- SRA est utilisée en association avec VLSR pour gérer la réplication des données des machines virtuelles entre les sites de production et de reprise après incident pour les datastores VMFS et NFS traditionnels, et pour les tests non disruptifs des répliques de DR. Il permet d'automatiser les tâches de détection, de restauration et de reprotection. Il comprend à la fois un serveur SRA et des adaptateurs SRA pour le serveur Windows SRM et le dispositif VLSR.

Après avoir installé et configuré les adaptateurs SRA sur le serveur VLSR pour protéger les banques de données non vVols, vous pouvez commencer la tâche de configuration de votre environnement vSphere pour la reprise après sinistre.

SRA est une interface de commande et de contrôle pour le serveur VLSR afin de gérer les volumes ONTAP FlexVol qui contiennent vos machines virtuelles VMware, ainsi que la réplication SnapMirror qui les protège.

VLSR peut tester votre plan DR sans interruption à l'aide de la technologie propriétaire FlexClone de NetApp pour créer des clones quasi instantanés de vos banques de données protégées sur votre site DR. VLSR crée un bac à sable pour effectuer des tests en toute sécurité afin que votre organisation et vos clients soient protégés en cas de véritable sinistre, vous donnant confiance dans la capacité de votre organisation à exécuter un basculement en cas de sinistre.

En cas d'incident véritable ou même de migration planifiée, VLSR 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.



Bien que les systèmes ONTAP vous permettent de coupler des SVM au sein du même cluster pour la réplication SnapMirror, ce scénario n'est pas testé et certifié avec VLSR. Par conséquent, il est recommandé d'utiliser uniquement des SVM provenant de différents clusters lors de l'utilisation de VLSR.

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

L'intégration de votre déploiement VLSR aux fonctionnalités avancées de gestion des données ONTAP permet une évolutivité et des performances considérablement améliorées par rapport aux options de stockage local.

Mais plus que cela, il apporte la flexibilité du cloud hybride. Le cloud hybride vous permet d'économiser de l'argent en hiérarchisant les blocs de données inutilisés de votre baie hautes performances vers votre hyperscaler préféré à l'aide de FabricPool, qui peut être un magasin S3 sur site tel que NetApp StorageGRID. Vous pouvez également utiliser SnapMirror pour les systèmes Edge avec ONTAP Select défini par logiciel ou DR basé sur le cloud à l'aide de ["Stockage NetApp sur Equinix Metal"](#), ou d'autres services ONTAP hébergés.

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.

VLSR 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.

Utiliser la dernière version des outils ONTAP 10

Les outils ONTAP 10 offrent des améliorations significatives par rapport aux versions précédentes, notamment :

- basculement de test 8 fois plus rapide*
- nettoyage et reprotection 2 fois plus rapides*
- basculement 32 % plus rapide*
- Évolutivité accrue
- Prise en charge native des mises en page de sites partagés

*Ces améliorations sont basées sur des tests internes et peuvent varier en fonction de votre environnement.

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.

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 compte SVM. "[Configurer les rôles et privilèges des utilisateurs ONTAP](#)" Utilisation du fichier JSON inclus. Il peut être utilisé pour les comptes évalués au niveau du SVM ou du cluster.
- Comme le plug-in de l'interface utilisateur vCenter, le fournisseur VASA et le serveur SRA sont tous des microservices 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 en cas d'utilisation d'identifiants SVM-scoped, sauf si vous êtes le premier dans ONTAP Tools Manager et si vous "[clusters intégrés](#)" les associez à vCenters. 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 vvol.
- 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 ou iSCSI sur le site A.
- 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. Bien que ce soit toujours la meilleure pratique, 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 fonction de suppression automatique des snapshots sur « essayer ».

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

- La taille automatique du volume doit être définie sur `grow` pour les volumes contenant des datastores SAN et `grow_shrink` pour les datastores NFS. Pour en savoir plus sur ce sujet "[Configurez les volumes pour qu'ils augmentent ou réduisent automatiquement leur taille](#)", rendez-vous sur .
- 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.

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.

vm vSphere Client Menu Search in all environments

ONTAP tools

- Overview
- Storage Systems**
- Storage Capability Profiles
- Storage Mapping
- Settings
- Reports

Storage Systems

ADD REDISCOVER ALL

Name	Type	IP Address
cluster2	Cluster	cluster2.demo.netapp.com

Edit Local Array Manager

Enter a name for the array manager on "vc2.demo.netapp.com":

vc2_array_manager

Storage Array Parameters

Storage Management IP Address or Hostname

cluster2.demo.netapp.com

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

À propos des groupes de réplication

Les groupes de réplication contiennent des ensembles logiques de machines virtuelles qui sont restaurées ensemble. 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 via le réseau, car SnapMirror 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 souhaitez probablement que votre contrôleur de domaine Microsoft Windows démarre avant votre serveur Microsoft SQL, qui doit être en ligne avant votre serveur d'applications, et ainsi de suite. 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 d'effectuer systématiquement un basculement de test lorsqu'une modification est apportée à la configuration du stockage protégé des machines virtuelles. 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 traitée comme une baie unique dans Site Recovery Manager. VLSR prend en charge certaines dispositions de réplication de tableau à tableau (ou SVM à SVM).

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

- VLSR 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 VLSR 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

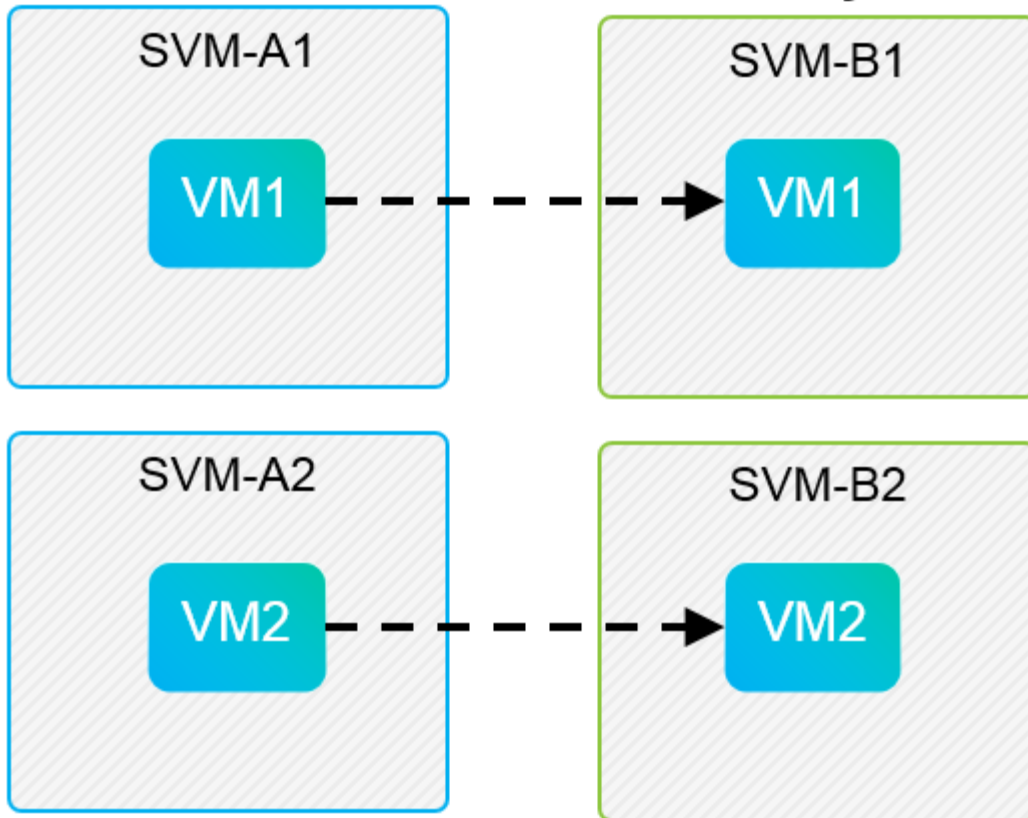
Les figures suivantes présentent les scénarios de disposition des relations SnapMirror pris en charge par VLSR et SRA. Chaque machine virtuelle des volumes répliqués est propriétaire de données sur une seule baie VLSR (SVM) sur chaque site.

SnapMirror Replication



Protected Site

Recovery Site

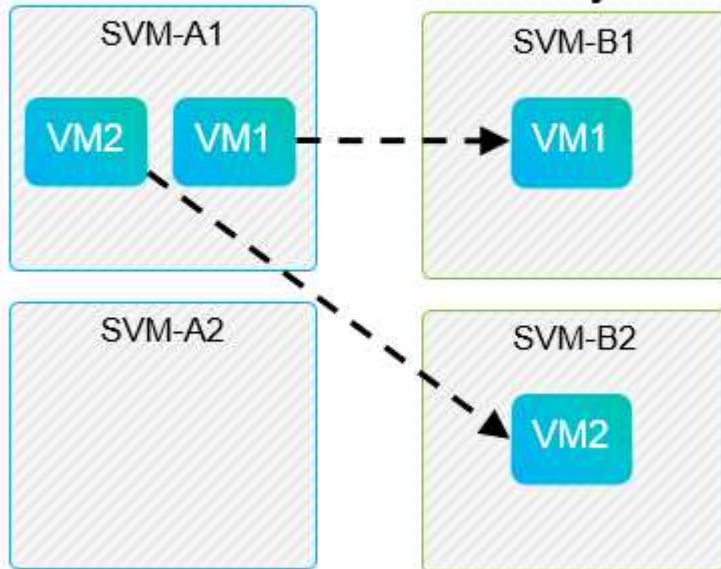


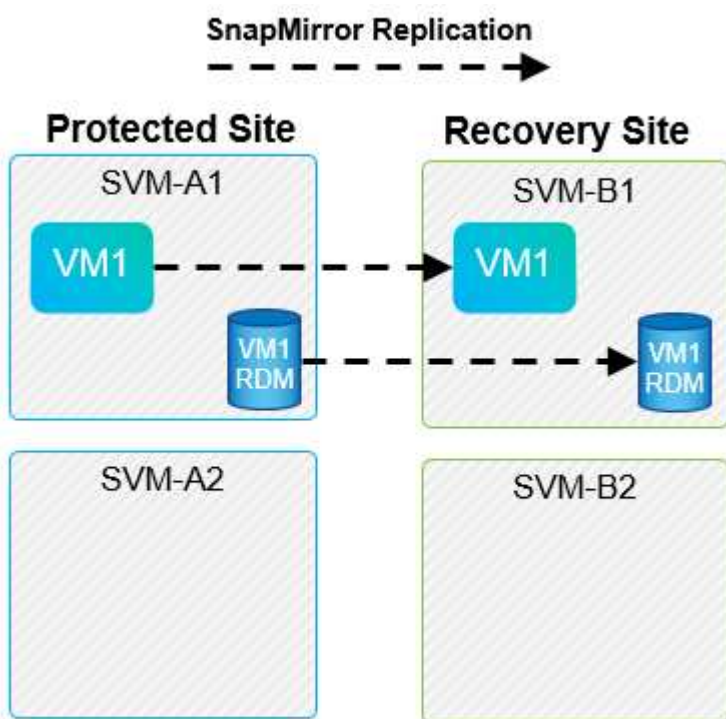
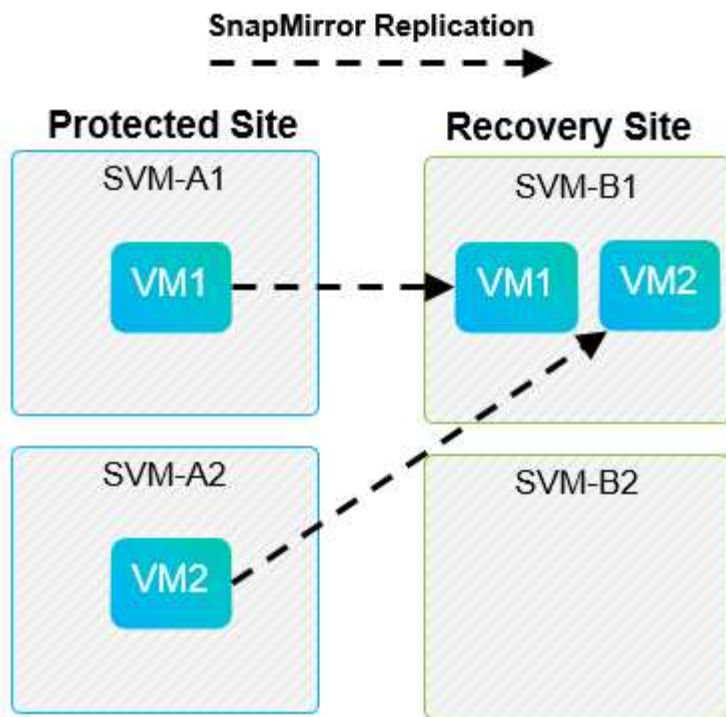
SnapMirror Replication



Protected Site

Recovery Site





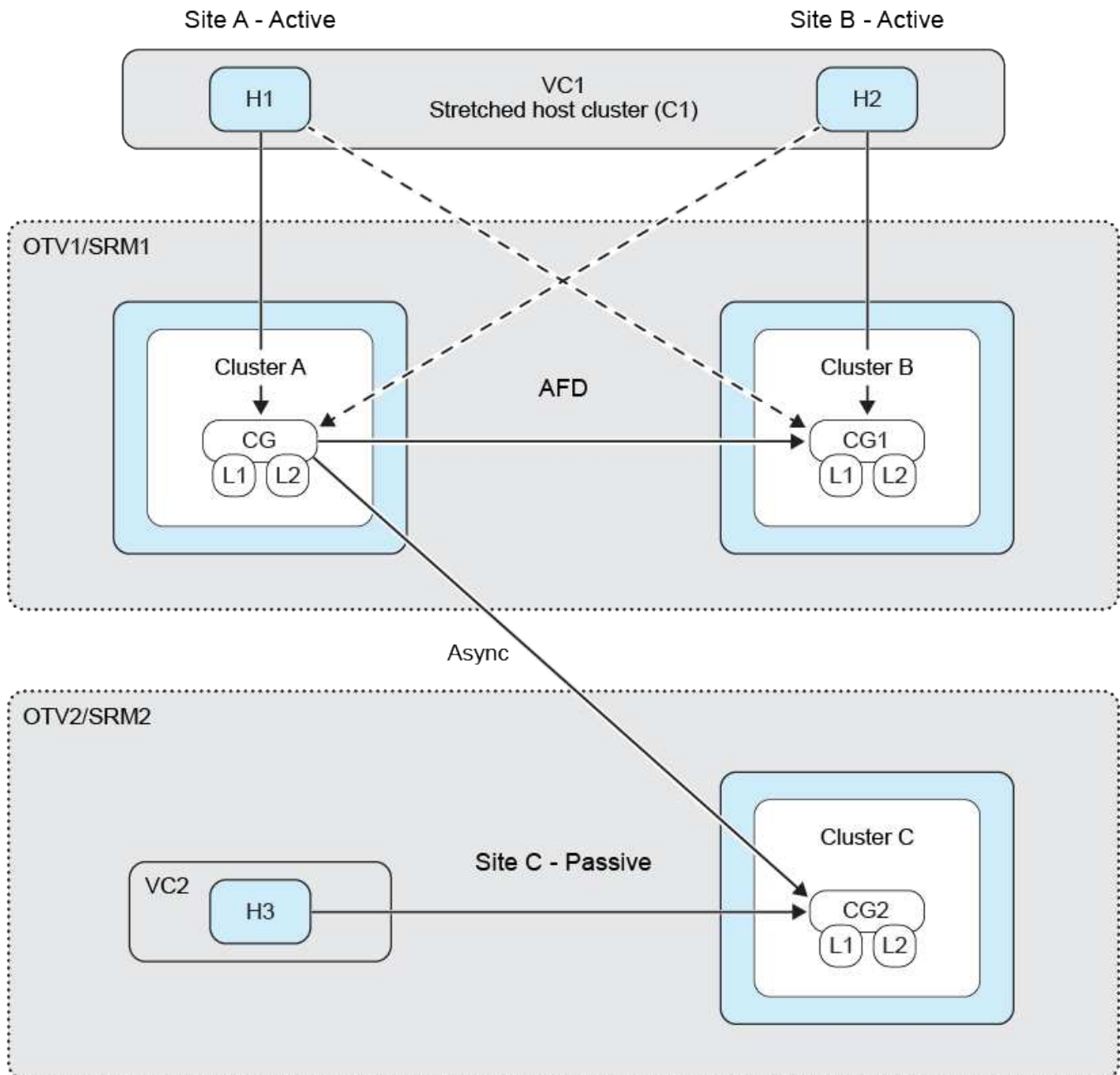
Prise en charge de VMFS avec la synchronisation active SnapMirror

Les outils ONTAP 10.3 et versions ultérieures prennent également en charge la protection de vos banques de données VMFS avec SnapMirror Active Sync (SMas). Cela permet un basculement transparent pour la continuité des activités entre deux centres de données (appelés domaines de défaillance) relativement proches l'un de l'autre. La reprise après sinistre longue distance peut ensuite être orchestrée à l'aide de SnapMirror de manière asynchrone via les outils ONTAP SRA avec VLSR.

"En savoir plus sur la synchronisation active [ONTAP SnapMirror](#)"

Les banques de données sont regroupées dans un groupe de cohérence (CG) et les machines virtuelles de toutes les banques de données resteront toutes cohérentes en termes d'ordre d'écriture en tant que membres du même CG.

Quelques exemples pourraient être d'avoir des sites à Berlin et Hambourg protégés par SMas, et une troisième réplique de site utilisant SnapMirror asynchrone et protégée par VLSR. Un autre exemple pourrait être de protéger des sites à New York et dans le New Jersey en utilisant des SMas, avec un troisième site à Chicago.



Mises en page de Array Manager prises en charge

Lorsque vous utilisez la réplication basée sur la baie (ABR) dans VLSR, 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.

New Protection Group

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

Type

Select the type of protection group you want to create:

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

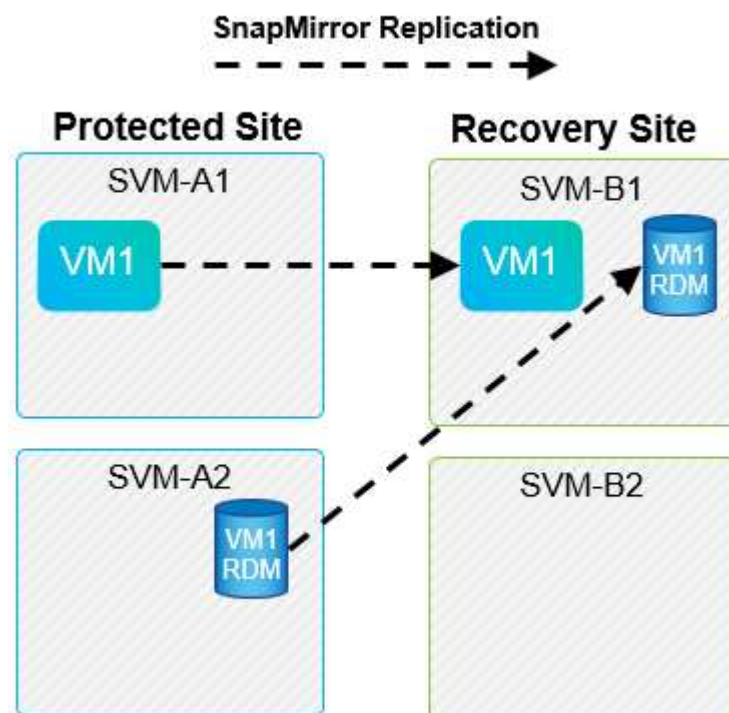
Select array pair

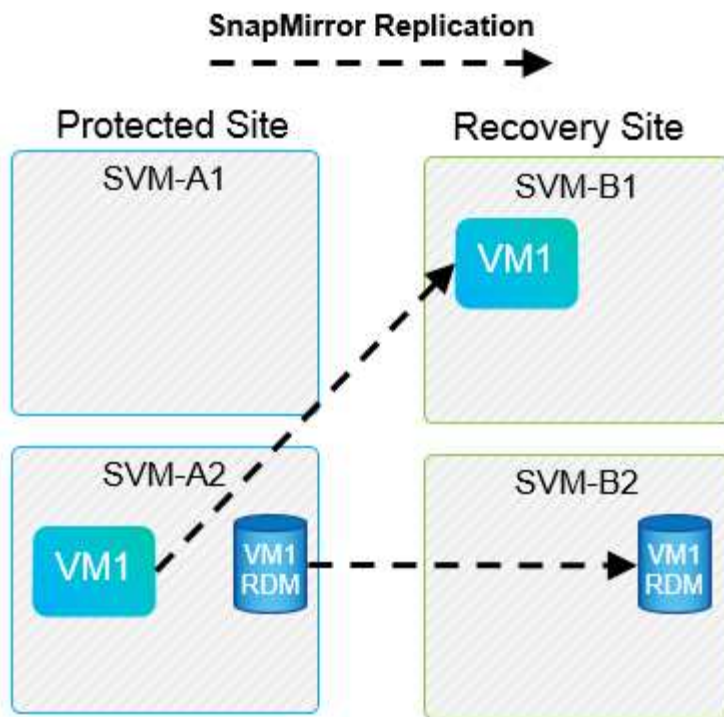
Array Pair	Array Manager Pair
<input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

CANCEL BACK NEXT

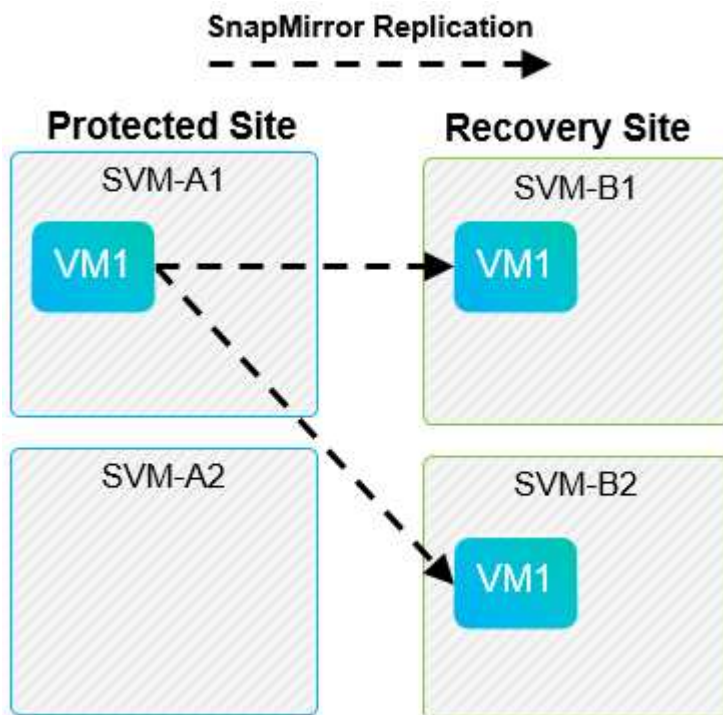
Présentations non prises en charge

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 une protection avec VLSR car VM1 possède des données sur deux SVM.





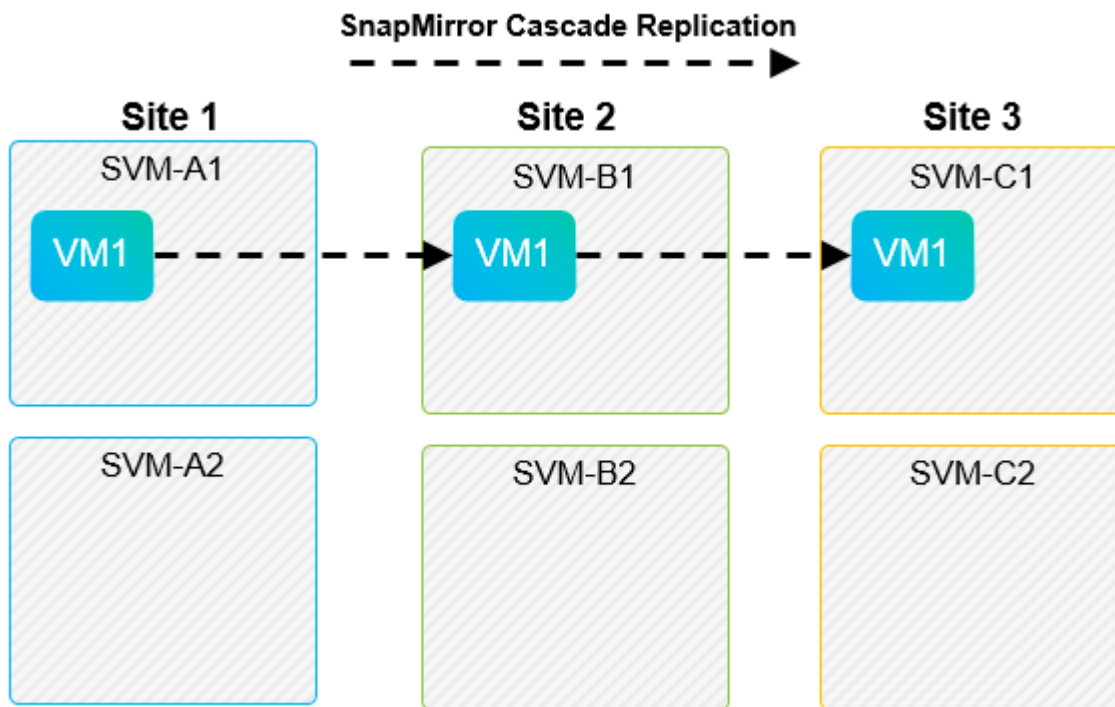
Toute relation de réplication dans laquelle un volume NetApp individuel est répliqué depuis un SVM source vers plusieurs destinations dans un même SVM ou dans différents SVM, est appelée « Fan-Out » de SnapMirror. La réplication « Fan-Out » n'est pas prise en charge par VLSR. Dans l'exemple illustré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



SnapMirror en cascade

VLSR 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, VLSR 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 VLSR 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 reconfigure 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 VLSR.

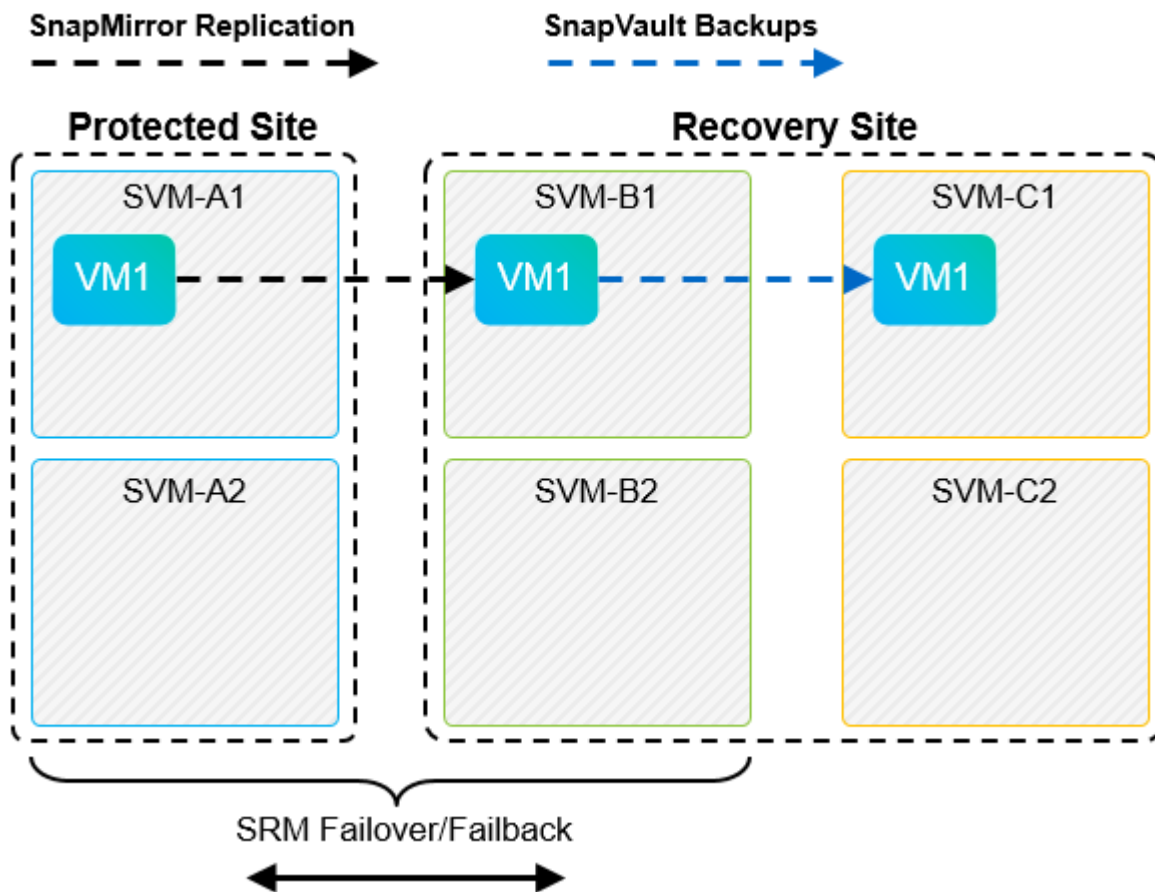
Pour obtenir les informations les plus récentes concernant SnapMirror et SnapVault pour ONTAP 9, consultez ["Tr-4015 Guide des meilleures pratiques en matière de configuration de SnapMirror pour ONTAP 9."](#)

Meilleure pratique

Si SnapVault et VLSR 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.

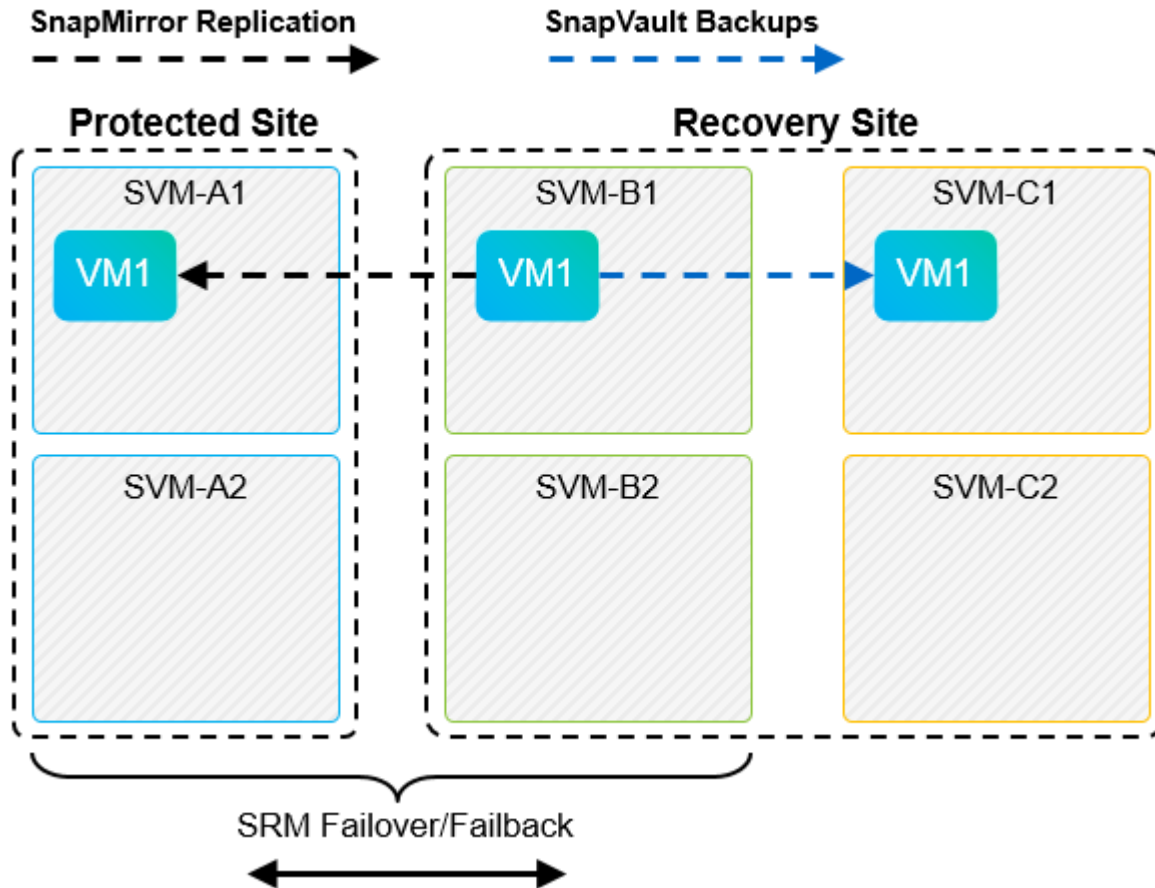
Dans un environnement VMware, chaque datastore dispose d'un identifiant unique universel (UUID) et chaque machine virtuelle possède un ID d'objet géré unique (MOID). Ces identifiants ne sont pas gérés par VLSR lors du basculement ou de la restauration. Étant donné que les UUID et les MOID de machine virtuelle ne sont pas maintenus lors du basculement par VLSR, toutes les applications qui dépendent de ces ID doivent être reconfigurées après le basculement VLSR. 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 VLSR 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 vsrm a effectué le retour arrière 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 VLSR.

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

Meilleure pratique

VLSR 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 VLSR de sorte que les VM soient configurés pour basculer vers un groupe d'hôtes ou un autre.

Dépannage de VLSRM/SRM lors de l'utilisation de la réplication vVols

Lors de l'utilisation des outils ONTAP 9.13P2, le workflow au sein de VLSR et de SRM est très différent lors de l'utilisation de la réplication vVols par rapport à l'utilisation de SRA et des datastores traditionnels. Par exemple, il n'existe pas de concept de gestionnaire de baie. Ainsi, `discoverarrays` les commandes et `discoverdevices` 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 :

- Ressources relatives aux outils ONTAP pour VMware vSphere 10.x.
["https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"](https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab)
- Ressources relatives aux outils ONTAP pour VMware vSphere 9.x.
["https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"](https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab)
- Tr-4597 : VMware vSphere pour ONTAP
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"](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"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html)
- TR-4015 Guide des bonnes pratiques de configuration de SnapMirror pour ONTAP 9
<https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf>
- Documentation de VMware Live site Recovery ["https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"](https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html)

Reportez-vous à la "[Matrice d'interopérabilité \(IMT\)](#)" sur le site de support NetApp pour vous assurer 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.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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