



Protection des datastores et des machines virtuelles

ONTAP tools for VMware vSphere 10

NetApp

November 17, 2025

Sommaire

Protection des datastores et des machines virtuelles	1
Protégez à l'aide de la protection de cluster hôte	1
Protégez à l'aide de la protection SRA	2
Activez SRA pour protéger les datastores	2
Configurez SRA pour les environnements SAN et NAS	2
Configurez SRA pour les environnements hautement évolutifs	3
Configurez SRA sur l'appliance VMware Live site Recovery	4
Mettez à jour les informations d'identification SRA	5
Configuration des sites protégés et de reprise après incident	6
Configuration des ressources protégées et du site de reprise	7
Vérification des systèmes de stockage répliqués	11

Protection des datastores et des machines virtuelles

Protégez à l'aide de la protection de cluster hôte

Les outils ONTAP pour VMware vSphere gèrent la protection des clusters hôtes. Tous les datastores appartenant au SVM sélectionné et montés sur un ou plusieurs hôtes du cluster sont protégés sous un cluster hôte.

Avant de commencer

Assurez-vous que les conditions préalables suivantes sont remplies :

- Le cluster hôte ne dispose que de datastores d'un SVM.
- Le datastore monté sur le cluster hôte ne doit pas être monté sur un hôte extérieur au cluster.
- Tous les datastores montés sur le cluster hôte doivent être des datastores VMFS avec protocole iSCSI/FC. Les datastores vVols, NFS ou VMFS avec protocoles NVMe/FC et NVMe/TCP ne sont pas pris en charge.
- Les FlexVol/LUN formant des datastores montés sur le cluster hôte ne doivent pas faire partie d'un groupe de cohérence existant.
- Les FlexVol/LUN formant des datastores montés sur le cluster hôte ne doivent pas faire partie d'une relation SnapMirror existante.
- Le cluster hôte doit comporter au moins un datastore.

Étapes

1. Connectez-vous au client vSphere
2. Cliquez avec le bouton droit de la souris sur un cluster hôte et sélectionnez **NetApp ONTAP Tools > Protect Cluster**.
3. Dans la fenêtre protéger le cluster, le type de datastore et les détails de la machine virtuelle de stockage source sont renseignés automatiquement. Sélectionnez le lien datastores pour afficher les datastores protégés.
4. Entrez le **nom du groupe de cohérence**.
5. Sélectionnez **Ajouter une relation**.
6. Dans la fenêtre **Ajouter une relation SnapMirror**, sélectionnez **VM de stockage cible** et le type **Stratégie**.

Le type de règle peut être asynchrone ou automatique FailOverDuplex.

Lorsque vous ajoutez la relation SnapMirror en tant que stratégie de type AutomatedFailOverDuplex, vous devez ajouter la machine virtuelle de stockage cible en tant que back-end de stockage au serveur vCenter sur lequel les outils ONTAP pour VMware vSphere sont déployés.

Dans le type de stratégie AutomatedFailOverDuplex, il existe des configurations hôte uniformes et non uniformes. Lorsque vous sélectionnez le bouton à bascule **uniforme host configuration**, la configuration du groupe initiateur hôte est implicitement répliquée sur le site cible. Pour plus de détails, reportez-vous à "[Concepts et termes clés](#)".

7. Si vous choisissez d'avoir une configuration hôte non uniforme, sélectionnez l'accès hôte (source/cible) pour chaque hôte à l'intérieur de ce cluster.

8. Sélectionnez **Ajouter**.
9. Dans la fenêtre **Protect cluster**, vous ne pouvez pas modifier le cluster protégé pendant l'opération de création. Vous pouvez supprimer et ajouter une protection à nouveau. Pendant l'opération de modification de la protection du cluster hôte, l'option d'édition est disponible. Vous pouvez modifier ou supprimer les relations à l'aide des options du menu points de suspension.
10. Sélectionnez le bouton **protéger**.

Une tâche vCenter est créée avec les détails de l'ID du travail et sa progression est affichée dans le panneau tâches récentes. Il s'agit d'une tâche asynchrone ; l'interface utilisateur affiche uniquement l'état de soumission de la demande et n'attend pas que la tâche soit terminée.
11. Pour afficher les clusters d'hôtes protégés, accédez à **NetApp ONTAP Tools > protection > Host cluster relations**.

Protégez à l'aide de la protection SRA

Activez SRA pour protéger les datastores

Les outils ONTAP pour VMware vSphere permettent d'activer la fonctionnalité SRA pour configurer la reprise après incident.

Avant de commencer

- Vous devez avoir configuré votre instance vCenter Server et votre hôte ESXi.
- Vous devez avoir déployé des outils ONTAP pour VMware vSphere.
- Vous devez avoir téléchargé le `.tar.gz` fichier de l'adaptateur SRA à partir du "[Site de support NetApp](#)".
- Les clusters ONTAP source et destination doivent avoir la même planification SnapMirror personnalisée que celle créée avant d'exécuter les workflows SRA.

Étapes

1. Connectez-vous à l'interface de gestion de l'apppliance VMware Live site Recovery à l'aide de `https://<srm_ip>:5480` l'URL ;, puis accédez à Storage Replication Adapters dans l'interface de gestion de l'apppliance VMware Live site Recovery.
2. Sélectionnez **nouvel adaptateur**.
3. Téléchargez le programme d'installation `.tar.gz` du plug-in SRA vers VMware Live site Recovery.
4. Relancez la recherche des adaptateurs pour vérifier que les détails sont mis à jour sur la page adaptateurs de réplication de stockage de VMware Live site Recovery.

Configurez SRA pour les environnements SAN et NAS

Vous devez configurer les systèmes de stockage avant d'exécuter Storage Replication adapter (SRA) pour VMware Live site Recovery.

Configurez SRA pour les environnements SAN

Avant de commencer

Les programmes suivants doivent être installés sur le site protégé et le site de reprise :

- Restauration de site en direct VMware

La documentation relative à l'installation de VMware Live site Recovery se trouve sur le site VMware.

["À propos de VMware Live site Recovery"](#)

- SRA

L'adaptateur est installé sur VMware Live site Recovery.

Étapes

1. Vérifiez que les hôtes ESXi principaux sont connectés aux LUN du système de stockage principal du site protégé.
2. Vérifiez que les LUN sont dans des igroups dont l' `ostype` option est définie sur *VMware* sur le système de stockage principal.
3. Vérifier que les hôtes ESXi sur le site de reprise disposent d'une connectivité iSCSI appropriée à la machine virtuelle de stockage (SVM). Les hôtes ESXi du site secondaire doivent avoir accès au stockage du site secondaire et les hôtes ESXi du site principal doivent avoir accès au stockage du site principal.

Vous pouvez le faire en vérifiant que les hôtes ESXi disposent de LUN locales connectées au SVM ou bien en vérifiant la `iscsi show initiators` commande sur le SVM. Vérifiez l'accès aux LUN mappées sur l'hôte ESXi pour vérifier la connectivité iSCSI.

Configurez SRA pour les environnements NAS

Avant de commencer

Les programmes suivants doivent être installés sur le site protégé et le site de reprise :

- Restauration de site en direct VMware

La documentation relative à l'installation de VMware Live site Recovery est disponible sur le site VMware.

["À propos de VMware Live site Recovery"](#)

- SRA

L'adaptateur est installé sur VMware Live site Recovery et sur le serveur SRA.

Étapes

1. Vérifiez que les datastores du site protégé contiennent des machines virtuelles enregistrées auprès de vCenter Server.
2. Vérifier que les hôtes ESXi du site protégé ont monté les volumes NFS exportés depuis la machine virtuelle de stockage (SVM).
3. Vérifiez que les adresses valides telles que l'adresse IP, le nom d'hôte ou le nom de domaine complet sur lequel les exportations NFS sont présentes sont spécifiées dans le champ **adresses NFS** lorsque vous utilisez l'assistant Array Manager pour ajouter des baies à VMware Live site Recovery.
4. Utiliser `ping` la commande sur chaque hôte ESXi sur le site de DR pour vérifier que l'hôte dispose d'un port VMkernel qui peut accéder aux adresses IP utilisées pour gérer les exportations NFS à partir du SVM.

Configurez SRA pour les environnements hautement évolutifs

Vous devez configurer les intervalles de délai d'expiration du stockage conformément aux

paramètres recommandés pour Storage Replication adapter (SRA) afin de garantir des performances optimales dans des environnements hautement évolutifs.

Paramètres du fournisseur de stockage

Vous devez définir les valeurs de temporisation suivantes sur VMware Live site Recovery pour un environnement évolutif :

Paramètres avancés	Valeurs de temporisation
StorageProvider.resignatureTimeout	Augmentez la valeur du réglage de 900 à 12000 secondes.
storageProvider.hostRescanDelaySec	60
storageProvider.hostRescanRepeatCnt	20
storageProvider.hostRescanTimeoutSec	Définir une valeur élevée (par exemple : 99999)

Vous devez également activer `StorageProvider.autoResignatureMode` l'option.

Pour plus d'informations sur la modification des paramètres du fournisseur de stockage, reportez-vous à la section "[Modifier les paramètres du fournisseur de stockage](#)".

Paramètres de stockage

Lorsque vous appuyez sur une temporisation, augmentez les valeurs de `storage.commandTimeout` et `storage.maxConcurrentCommandCnt` à une valeur supérieure.



L'intervalle de temporisation spécifié est la valeur maximale. Il n'est pas nécessaire d'attendre que le délai maximum soit atteint. La plupart des commandes se terminent dans l'intervalle maximal défini de temps d'attente.

Pour modifier les paramètres du fournisseur SAN, reportez-vous à la section "[Modifier les paramètres de stockage](#)".

Configurez SRA sur l'appliance VMware Live site Recovery

Une fois l'appliance VMware Live site Recovery déployée, vous devez configurer SRA sur l'appliance VMware Live site Recovery. La configuration réussie de SRA permet à l'appliance VMware Live site Recovery de communiquer avec SRA pour la gestion de la reprise après incident. Vous devez stocker les outils ONTAP pour les informations d'identification VMware vSphere (adresse IP) sur l'appliance VMware Live site Recovery pour permettre la communication entre l'appliance VMware Live site Recovery et SRA.

Avant de commencer

Vous devez avoir téléchargé le fichier `tar.gz` à partir de "[Site de support NetApp](#)".

À propos de cette tâche

La configuration de SRA sur l'appliance VMware Live site Recovery stocke les informations d'identification SRA sur l'appliance VMware Live site Recovery.

Étapes

1. Sur l'écran de l'appliance VMware Live site Recovery, sélectionnez **Storage Replication adapter > New adapter**.
2. Chargez le fichier **.tar.gz** dans VMware Live site Recovery.
3. Connectez-vous à l'aide d'un compte administrateur à l'appliance VMware Live site Recovery à l'aide de putty.
4. Passez à l'utilisateur root à l'aide de la commande : `su root`
5. Exécutez la commande `cd /var/log/vmware/srm` pour accéder au répertoire de journaux.
6. À l'emplacement du journal, entrez la commande pour obtenir l'ID docker utilisé par SRA : `docker ps -l`
7. Pour vous connecter à l'ID de conteneur, entrez la commande : `docker exec -it -u srm <container id> sh`
8. Configurer VMware Live site Recovery avec les outils ONTAP pour l'adresse IP et le mot de passe VMware vSphere à l'aide de la commande : `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`'



Vous devez fournir la valeur du mot de passe entre guillemets pour vous assurer que le script Perl ne lit pas les caractères spéciaux du mot de passe comme délimiteur de l'entrée.



Le nom d'utilisateur et le mot de passe de l'application sont définis lors du déploiement des outils ONTAP. Cette opération est nécessaire pour l'enregistrement du fournisseur VASA/SRA.

9. Relancez la recherche des adaptateurs pour vérifier que les détails sont mis à jour sur la page adaptateurs de réPLICATION de stockage de VMware Live site Recovery.

Un message de confirmation de la mémorisation des identifiants de stockage s'affiche. SRA peut communiquer avec le serveur SRA à l'aide de l'adresse IP, du port et des informations d'identification fournis.

Mettez à jour les informations d'identification SRA

Pour que VMware Live site Recovery puisse communiquer avec SRA, vous devez mettre à jour les informations d'identification SRA sur le serveur VMware Live site Recovery si vous avez modifié les informations d'identification.

Avant de commencer

Vous devez avoir exécuté les étapes mentionnées dans la rubrique "[Configuration de SRA sur l'appliance VMware Live site Recovery](#)".

Étapes

1. Exécutez les commandes suivantes pour supprimer le dossier de la machine de restauration de site direct VMware Outils ONTAP mis en cache nom d'utilisateur mot de passe :
 - a. `sudo su <enter root password>`

- b. docker ps
 - c. docker exec -it <container_id> sh
 - d. cd conf/
 - e. rm -rf *
2. Exécutez la commande Perl pour configurer SRA avec les nouvelles informations d'identification :
- a. cd ..
 - b. perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID> Vous devez avoir un devis unique autour de la valeur du mot de passe.
- Un message de confirmation de la mémorisation des identifiants de stockage s'affiche. SRA peut communiquer avec le serveur SRA à l'aide de l'adresse IP, du port et des informations d'identification fournis.

Configuration des sites protégés et de reprise après incident

Vous devez créer des groupes de protection pour protéger un groupe de machines virtuelles sur le site protégé.

Configuration des groupes de protection

Avant de commencer

Vous devez vous assurer que les sites source et cible sont configurés pour les sites suivants :

- La même version de VMware Live site Recovery est installée
- Ordinateurs virtuels
- Sites protégés et de reprise par paires
- Les datastores source et de destination doivent être montés sur les sites respectifs

Étapes

1. Connectez-vous à vCenter Server, puis sélectionnez **site Recovery > protection Groups**.
2. Dans le volet **groupes de protection**, sélectionnez **Nouveau**.
3. Spécifiez un nom et une description pour le groupe de protection, Direction et sélectionnez **Suivant**.
4. Dans le champ **Type**, sélectionnez l'option de champ **Type...** en tant que groupes de datastores (réplication basée sur la baie) pour les datastores NFS et VMFS. Le domaine de panne n'est rien d'autre que les SVM avec la réplication activée. Les SVM qui ont uniquement mis en œuvre le peering et qui ne présentent aucun problème sont affichés.
5. Dans l'onglet **Replication Groups**, sélectionnez la paire de matrices activée ou les groupes de réplication sur lesquels la machine virtuelle est configurée, puis sélectionnez **Next**.

Toutes les machines virtuelles du groupe de réplication sont ajoutées au groupe de protection.

6. Sélectionnez le plan de reprise existant ou créez un nouveau plan en sélectionnant **Ajouter au nouveau plan de reprise**.
7. Dans l'onglet prêt à terminer, vérifiez les détails du groupe de protection que vous avez créé, puis

sélectionnez **Terminer**.

Protection par paires et sites de reprise après incident

Vous devez coupler les sites protégés et de reprise créés à l'aide de votre client vSphere pour permettre à Storage Replication adapter (SRA) de détecter les systèmes de stockage.

Avant de commencer

- VMware Live site Recovery doit être installé sur les sites protégés et de reprise.
- SRA doit être installée sur les sites protégés et de reprise.

Étapes

1. Double-cliquez sur **site Recovery** sur la page d'accueil du client vSphere et sélectionnez **sites**.
2. Sélectionnez **objets > actions > associer sites**.
3. Dans la boîte de dialogue **pair site Recovery Manager Servers**, entrez l'adresse du Platform Services Controller du site protégé, puis sélectionnez **Next**.
4. Dans la section Select vCenter Server, procédez comme suit :
 - a. Vérifiez que le serveur vCenter du site protégé apparaît comme candidat correspondant au couplage.
 - b. Entrez les informations d'identification d'administration SSO, puis sélectionnez **Terminer**.
5. Si vous y êtes invité, sélectionnez **Oui** pour accepter les certificats de sécurité.

Résultat

Les sites protégés et de restauration s'affichent dans la boîte de dialogue objets.

Configuration des ressources protégées et du site de reprise

Configurer les mappages du réseau

Vous devez configurer vos mappages de ressources tels que les réseaux de machines virtuelles, les hôtes ESXi et les dossiers sur les deux sites afin de pouvoir mapper chaque ressource du site protégé à la ressource appropriée sur le site de reprise.

Vous devez effectuer les configurations de ressources suivantes :

- Mappages de réseau
- Mappages de dossiers
- Mappages de ressources
- Datastores à espace réservé

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery > sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages réseau > Nouveau** dans l'onglet gérer pour créer un nouveau mappage réseau.

4. Dans l'assistant Créer un mappage réseau, procédez comme suit :
 - a. Sélectionnez **préparer automatiquement les mappages pour les réseaux avec des noms correspondants** et sélectionnez **Suivant**.
 - b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Ajouter des mappages**.
 - c. Sélectionnez **Suivant** une fois les mappages créés.
 - d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page Network mappings affiche les ressources du site protégé et les ressources du site de reprise. Vous pouvez suivre les mêmes étapes pour les autres réseaux de votre environnement.

Configurer les mappages de dossiers

Vous devez mapper vos dossiers sur le site protégé et le site de reprise pour permettre la communication entre eux.

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery > sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages de dossiers** > icône **dossier** dans l'onglet gérer pour créer un nouveau mappage de dossiers.
4. Dans l'assistant Créer un mappage de dossier, effectuez les opérations suivantes :
 - a. Sélectionnez **préparer automatiquement les mappages pour les dossiers avec des noms correspondants** et sélectionnez **Suivant**.
 - b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Ajouter des mappages**.
 - c. Sélectionnez **Suivant** une fois les mappages créés.
 - d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page mappages des dossiers affiche les ressources du site protégé et les ressources du site de reprise. Vous pouvez suivre les mêmes étapes pour les autres réseaux de votre environnement.

Configurer les mappages de ressources

Vous devez mapper vos ressources sur le site protégé et le site de reprise de manière à ce que les machines virtuelles soient configurées pour basculer vers un groupe d'hôtes ou vers un autre.

Avant de commencer

Vous devez avoir connecté les sites protégés et de reprise.



Dans VMware Live site Recovery, les ressources peuvent être des pools de ressources, des hôtes ESXi ou des clusters vSphere.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery > sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **mappages de ressources > Nouveau** dans l'onglet gérer pour créer un mappage de ressources.
4. Dans l'assistant Créer un mappage de ressources, effectuez les opérations suivantes :
 - a. Sélectionnez **préparer automatiquement les mappages pour la ressource avec les noms correspondants** et sélectionnez **Suivant**.
 - b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Ajouter des mappages**.
 - c. Sélectionnez **Suivant** une fois les mappages créés.
 - d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page mappages des ressources affiche les ressources protégées du site et les ressources du site de reprise. Vous pouvez suivre les mêmes étapes pour les autres réseaux de votre environnement.

Configurez les datastores à espace réservé

Vous devez configurer un datastore de marque de réservation pour qu'il garde un emplacement dans l'inventaire vCenter sur le site de reprise pour la machine virtuelle protégée (VM). Le datastore réservé n'a pas besoin d'être volumineux car les machines virtuelles de substitution sont petites et n'utilisent que quelques centaines de kilo-octets ou moins.

Avant de commencer

- Vous devez avoir connecté les sites protégés et de reprise.
- Vous devez avoir configuré vos mappages de ressources.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **site Recovery > sites**.
2. Sélectionnez votre site protégé et sélectionnez **gérer**.
3. Sélectionnez **Placeholder datastores > New** dans l'onglet gérer pour créer un nouveau datastore de marque de réservation.
4. Sélectionnez le datastore approprié et sélectionnez **OK**.



Les datastores à espace réservé peuvent être locaux ou distants et ne doivent pas être répliqués.

5. Répétez les étapes 3 à 5 pour configurer un datastore de marque de réservation pour le site de reprise.

Configurez SRA à l'aide du gestionnaire de baies

Vous pouvez configurer Storage Replication adapter (SRA) à l'aide de l'assistant Array Manager de VMware Live site Recovery pour activer les interactions entre VMware Live site Recovery et les machines virtuelles de stockage (SVM).

Avant de commencer

- Vous devez avoir couplé les sites protégés et les sites de reprise dans VMware Live site Recovery.
- Vous devez avoir configuré votre stockage intégré avant de configurer le gestionnaire de baie.
- Vous devez avoir configuré et répliqué les relations SnapMirror entre les sites protégés et les sites de reprise.
- Vous devez avoir activé les LIF de gestion du SVM pour permettre la colocation.

SRA prend en charge la gestion au niveau du cluster et de la SVM. Si vous ajoutez du stockage au niveau du cluster, vous pouvez détecter et exécuter des opérations sur tous les SVM du cluster. Si vous ajoutez du stockage au niveau d'un SVM, vous ne pouvez gérer que ce SVM spécifique.

Étapes

1. Dans VMware Live site Recovery, sélectionnez **Array Managers > Add Array Manager**.
2. Entrez les informations suivantes pour décrire la baie dans VMware Live site Recovery :
 - a. Entrez un nom pour identifier le gestionnaire de matrice dans le champ **Nom d'affichage**.
 - b. Dans le champ **SRA Type**, sélectionnez **NetApp Storage Replication adapter pour ONTAP**.
 - c. Entrer les informations pour se connecter au cluster ou au SVM :
 - Si vous vous connectez à un cluster, vous devez saisir la LIF de gestion du cluster.
 - Si vous vous connectez directement à un SVM, vous devez saisir l'adresse IP de la LIF de management du SVM.



Lors de la configuration du gestionnaire de baies, vous devez utiliser la même connexion (adresse IP) pour le système de stockage utilisé pour intégrer le système de stockage dans les outils ONTAP pour VMware vSphere. Par exemple, si la configuration de Array Manager est étendue au SVM, le stockage sous ONTAP Tools for VMware vSphere doit être ajouté au niveau du SVM.

- d. Si vous vous connectez à un cluster, entrez le nom du SVM dans le champ **SVM name**.

Vous pouvez également laisser ce champ vide.

- e. Entrez les volumes à découvrir dans le champ **liste d'inclure le volume**.

Vous pouvez saisir le volume source sur le site protégé et le volume de destination répliqué sur le site de reprise.

Par exemple, si vous voulez découvrir le volume src_vol1 qui se trouve dans une relation SnapMirror avec le volume dst_vol1, vous devez spécifier src_vol1 dans le champ site protégé et dst_vol1 dans le champ site de reprise.

- f. **(Facultatif)** Entrez les volumes à exclure de la découverte dans le champ **liste d'exclusion de volume**.

Vous pouvez saisir le volume source sur le site protégé et le volume de destination répliqué sur le site de reprise.

Par exemple, si vous voulez exclure le volume *src_vol1* qui se trouve dans une relation SnapMirror avec le volume *dst_vol1*, vous devez spécifier *src_vol1* dans le champ site protégé et *dst_vol1* dans le champ site de reprise.

3. Sélectionnez **Suivant**.

4. Vérifiez que la matrice est découverte et affichée en bas de la fenêtre Ajouter un gestionnaire de matrice et sélectionnez **Terminer**.

Vous pouvez suivre les mêmes étapes pour le site de reprise à l'aide des adresses IP et des identifiants de gestion des SVM appropriés. Dans l'écran Activer les paires de matrices de l'assistant Ajouter un gestionnaire de matrice, vérifiez que la paire de matrices correcte est sélectionnée et qu'elle indique prête à être activée.

Vérification des systèmes de stockage répliqués

Vous devez vérifier que le site protégé et le site de reprise sont correctement couplés après avoir configuré Storage Replication adapter (SRA). Le système de stockage répliqué doit être détectable par le site protégé et le site de reprise.

Avant de commencer

- Vous devez avoir configuré votre système de stockage.
- Vous devez avoir couplé le site protégé et le site de reprise à l'aide du gestionnaire de baie VMware Live site Recovery.
- Vous devez avoir activé la licence FlexClone et la licence SnapMirror avant d'effectuer l'opération de basculement et l'opération de basculement pour SRA.
- Vous devez disposer des mêmes stratégies et plannings SnapMirror sur les sites source et de destination.

Étapes

1. Connectez-vous à votre serveur vCenter.
2. Accédez à **site Recovery > Array Based Replication**.
3. Sélectionnez la paire de matrices requise et vérifiez les détails correspondants.

Les systèmes de stockage doivent être découverts sur le site protégé et le site de reprise dont le statut est « activé ».

Informations sur le copyright

Copyright © 2025 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 JOUSSANCE, 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 DÉLICTUELLE (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.