



Protégez les banques de données et les machines virtuelles

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Sommaire

Protégez les banques de données et les machines virtuelles	1
Protéger un cluster hôte dans ONTAP tools	1
Protéger à l'aide de la protection SRA	2
Configurez SRA dans ONTAP tools pour protéger les banques de données	2
Configurer SRA dans ONTAP tools for VMware vSphere pour les environnements SAN et NAS	3
Configurer SRA dans ONTAP tools pour les environnements à grande échelle	4
Configurez SRA sur l'appliance VMware Live Site Recovery à l'aide des ONTAP tools.	5
Mettre à jour les informations d'identification SRA dans ONTAP tools	6
Configurer les sites protégés et de récupération dans ONTAP tools	7
Configurer les ressources du site protégé et du site de récupération	9
Vérifier les systèmes de stockage répliqués dans ONTAP tools	13
Protection contre le fan-out dans ONTAP tools	13

Protégez les banques de données et les machines virtuelles

Protéger un cluster hôte dans ONTAP tools

ONTAP tools for VMware vSphere gèrent la protection des clusters d'hôtes. Toutes les banques de données appartenant à la SVM sélectionnée et montées sur un ou plusieurs hôtes du cluster sont protégées sous un cluster d'hôtes.

Avant de commencer

Assurez-vous de respecter ces exigences avant de protéger un cluster hôte :

- Le cluster hôte contient des banques de données provenant d'une seule SVM.
- Les banques de données du cluster hôte ne sont pas montées sur des hôtes situés en dehors du cluster.
- Les banques de données montées sur le cluster hôte sont des banques de données VMFS utilisant le protocole iSCSI ou FC. Vous ne pouvez pas utiliser vVols, NFS ou des banques de données VMFS avec les protocoles NVMe/FC et NVMe/TCP.
- Les banques de données basées sur des volumes FlexVol/LUN montés sur un hôte ne font partie d'aucun groupe de cohérence.
- Les banques de données basées sur des volumes FlexVol/LUN montés sur un hôte ne font partie d'aucune relation SnapMirror.
- Le cluster hôte contient au moins un datastore.

Étapes

1. Connectez-vous au client vSphere.
2. Cliquez avec le bouton droit sur un cluster hôte et sélectionnez **NetApp ONTAP tools > Protect Cluster**.
3. Dans la fenêtre de protection du cluster, le système renseigne automatiquement le type de datastore et les détails de la machine virtuelle de stockage (VM) source. Sélectionnez le lien des datastores pour afficher les datastores protégés.
4. Sélectionnez **Ajouter une relation**.
5. Dans la fenêtre **Ajouter une relation SnapMirror**, sélectionnez la **VM de stockage cible** et le type de **stratégie**.

Le type de stratégie peut être asynchrone ou AutomatedFailOverDuplex.

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 backend de stockage au même vCenter où ONTAP tools for VMware vSphere est déployé.

Dans le type de stratégie AutomatedFailOverDuplex, il existe des configurations d'hôtes uniformes et non uniformes. Lorsque vous sélectionnez le bouton bascule **Configuration d'hôtes uniforme**, la configuration du groupe d'initiateurs hôtes est implicitement répliquée sur le site cible. Pour plus d'informations, consultez ["Concepts et termes clés"](#).

6. Si vous choisissez une configuration d'hôtes non uniforme, sélectionnez l'accès hôte (source/cible) pour chaque hôte au sein de ce cluster.

7. Sélectionnez **Add**.
8. Vous pouvez modifier la protection du cluster hôte à l'aide de l'opération **Modifier la protection du cluster hôte**. Vous pouvez modifier ou supprimer les relations à l'aide des options du menu à trois points.
9. Sélectionnez le bouton **Protéger**.

Le système crée une tâche vCenter avec les détails de l'ID du travail et affiche sa progression dans le panneau des tâches récentes. Il s'agit d'une tâche asynchrone ; l'interface utilisateur affiche uniquement l'état de soumission de la requête et n'attend pas la fin de la tâche.

10. Pour afficher les clusters d'hôtes protégés, accédez à **NetApp ONTAP tools > Protection > Host cluster relationships**. Sélectionnez un groupe de cohérence pour afficher sa capacité, les banques de données associées et les groupes de cohérence enfants.



Si vous devez supprimer la protection dans l'heure qui suit sa création, effectuez d'abord une découverte du stockage.

Informations connexes

["Cluster de stockage Metro VMware vSphere \(vMSC\)"](#)

Protéger à l'aide de la protection SRA

Configurez SRA dans ONTAP tools pour protéger les banques de données

Les outils ONTAP pour VMware vSphere offrent la possibilité d'activer la fonctionnalité SRA pour configurer la reprise après sinistre.

Avant de commencer

- Vous devez avoir configuré votre instance de serveur vCenter et vos hôtes ESXi.
- Vous devez avoir déployé les outils ONTAP pour VMware vSphere.
- Vous devez avoir téléchargé le fichier SRA Adapter .tar.gz depuis le ["Site de support NetApp"](#).
- Vous devez avoir les mêmes planifications personnalisées SnapMirror sur les clusters ONTAP source et de destination avant d'exécuter les workflows SRA.
- ["Activer les ONTAP tools for VMware vSphere services"](#) pour activer la fonctionnalité SRA.

Étapes

1. Connectez-vous à l'interface de gestion de l'appliance VMware Live Site Recovery à l'aide de l'URL : `https://<srm_ip>:5480`, puis accédez à Adaptateurs de réplication de stockage dans l'interface de gestion de l'appliance 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. Analysez à nouveau les adaptateurs pour vérifier que les informations sont mises à jour sur la page VMware Live Site Recovery Storage Replication Adapters.



Après un basculement, des actions telles qu'étendre, monter et supprimer peuvent ne pas être disponibles pour les banques de données. Effectuez une découverte des banques de données pour actualiser et afficher les actions appropriées dans le menu contextuel.



Après chaque opération de reprotection, vous devez effectuer une découverte du stockage sur les deux sites.

Lors d'une nouvelle configuration avec protection SRA, effectuez systématiquement un test de basculement. Ignorer le test de basculement pourrait entraîner l'échec de l'opération de reprotection.

Dans une configuration de distribution, après un basculement SnapMirror Active Sync où la source SnapMirror passe au site B pour Automated Failover Duplex et SnapMirror asynchrone, exécutez un test de basculement entre les sites B et C. Ignorer cette étape peut entraîner un échec de l'opération de reprotection.

Informations connexes

["Configurer la reprise après sinistre pour les banques de données NFS à l'aide de VMware Site Recovery Manager"](#)

Configurer SRA dans ONTAP tools for VMware vSphere 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.

Configurer SRA pour les environnements SAN



Les groupes de cohérence dans les flux de travail SRA ne sont pris en charge qu'avec les protocoles SAN (iSCSI et Fibre Channel) sur les systèmes de stockage Unified et ASA r2.

Avant de commencer

Vous devez avoir les programmes suivants installés sur le site protégé et le site de récupération :

- VMware Live Site Recovery : Le site VMware fournit la documentation d'installation de VMware Live Site Recovery.

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

- SRA : Installez l'adaptateur sur VMware Live Site Recovery.

Pour les configurations du protocole iSCSI, notez les points suivants avant d'exécuter les workflows SRA :

- **Site protégé** : les adaptateurs de stockage iSCSI et les détails des LIF de données sont configurés automatiquement lors du provisionnement des banques de données. Aucune configuration manuelle n'est requise.
- Site de reprise d'activité : les adaptateurs de stockage iSCSI doivent être configurés manuellement sur chaque hôte ESXi inclus dans le mappage des ressources pour la reprise d'activité. Pour éviter de configurer les adaptateurs individuellement sur chaque hôte, créez un datastore de type iSCSI sur le site de reprise d'activité à l'aide de la SVM sur laquelle les workflows SRA sont configurés. Cette opération ajoute automatiquement l'adaptateur iSCSI et les adresses IP LIF de données requises à tous les hôtes ESXi mappés. Consultez ["Configurer les magasins de données de substitution dans ONTAP tools"](#) pour plus de détails.

Étapes

1. Vérifiez que les hôtes ESXi principaux sont connectés aux LUN du système de stockage principal sur le site protégé.

2. Vérifiez que les LUN sont dans des igroups qui ont l'option `ostype`` définie sur *VMware* sur le système de stockage principal.
3. Vérifiez que les hôtes ESXi du site de reprise disposent d'une connectivité iSCSI et Fibre Channel 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 procéder soit en vérifiant que les hôtes ESXi disposent de LUN locales connectées sur la SVM, soit en exécutant la commande `iscsi show initiators` sur les SVM. Vérifiez l'accès aux LUN mappées sur l'hôte ESXi pour vérifier la connectivité iSCSI.

Configurer SRA pour les environnements NAS



Les groupes de cohérence ne sont pas pris en charge pour NFS dans les workflows SRA. Si des volumes de datastore NFS sont placés sous un groupe de cohérence et protégés, l'opération Discover Devices échouera. N'utilisez pas de groupes de cohérence lors de la protection des datastores NFS avec SRA.

Avant de commencer

Vous devez avoir les programmes suivants installés sur le site protégé et le site de récupération :

- VMware Live Site Recovery : Vous trouverez la documentation d'installation de VMware Live Site Recovery sur le site de VMware - ["À propos de VMware Live Site Recovery"](#)
- SRA : Installez l'adaptateur sur VMware Live Site Recovery et le serveur SRA.

Étapes

1. Vérifiez que les banques de données du site protégé contiennent des machines virtuelles qui sont enregistrées auprès du serveur vCenter.
2. Vérifiez que les hôtes ESXi du site protégé ont monté les volumes d'export NFS à partir de la machine virtuelle de stockage (SVM).
3. Vérifiez que les adresses IP valides sur lesquelles les exports NFS sont présents sont spécifiées dans le champ **NFS Addresses** lors de l'utilisation de l'assistant Array Manager pour ajouter des baies à VMware Live Site Recovery. N'utilisez pas le nom d'hôte NFS ni le FQDN dans le champ **NFS Addresses**.
4. Utilisez la commande `ping` sur chaque hôte ESXi du site de récupération pour vérifier que l'hôte possède un port VMkernel pouvant accéder aux adresses IP utilisées pour fournir les exports NFS depuis la SVM.

Configurer SRA dans ONTAP tools pour les environnements à grande échelle

Vous devez configurer les intervalles de délai d'expiration du stockage conformément aux paramètres recommandés pour Storage Replication Adapter (SRA) afin d'obtenir des performances optimales dans les environnements à grande échelle.

Paramètres du fournisseur de stockage

Vous devez définir les valeurs de délai d'expiration suivantes sur VMware Live Site Recovery pour un environnement mis à l'échelle :

Paramètres avancés	Valeurs de délai d'attente
--------------------	----------------------------

<code>StorageProvider.resignatureTimeout</code>	Augmentez la valeur du paramètre de 900 secondes à 12000 secondes.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Définissez une valeur élevée (par exemple : 99999)

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

Consultez ["Modifier les paramètres du fournisseur de stockage"](#) pour plus d'informations sur la modification des paramètres du fournisseur de stockage.

Paramètres de stockage

Lorsque vous atteignez un délai d'attente, augmentez les valeurs de `storage.commandTimeout` et `storage.maxConcurrentCommandCnt` à une valeur plus élevée.



Le délai d'attente spécifié correspond à la valeur maximale. Il n'est pas nécessaire d'attendre que le délai d'attente maximal soit atteint. La plupart des commandes s'exécutent dans l'intervalle de délai d'attente maximal défini.

Consultez ["Modifier les paramètres de stockage"](#) pour modifier les paramètres du fournisseur SAN.

Configurez SRA sur l'appliance VMware Live Site Recovery à l'aide des ONTAP tools.

Après avoir déployé l'appliance VMware Live Site Recovery, configurez le Storage Replication Adapter (SRA) pour activer la gestion de la reprise après sinistre.

La configuration de SRA sur l'appliance VMware Live Site Recovery enregistre les informations d'identification des ONTAP tools for VMware vSphere au sein de l'appliance, ce qui permet la communication entre VMware Live Site Recovery et SRA.

Avant de commencer

- Téléchargez le fichier `.tar.gz` depuis le ["Site de support NetApp"](#).
- Activez les services SRA dans ONTAP tools Manager. Pour plus d'informations, consultez la ["Activer les services"](#) section.
- Ajoutez des serveurs vCenter à l'appliance ONTAP tools for VMware vSphere. Pour plus d'informations, consultez la ["Ajouter des serveurs vCenter"](#) section.
- Ajoutez des systèmes de stockage à ONTAP tools for VMware vSphere. Pour plus d'informations, consultez la ["Ajouter des backends de stockage"](#) section.



Si vous avez appliqué le correctif de certificat vCenter à partir des outils ONTAP, mettez à jour la configuration vCenter dans l'appliance VMware Live Site Recovery en utilisant le port (:5480). Pour obtenir des instructions, consultez ["Reconfigurez l'appliance Site Recovery Manager"](#).

Étapes

1. Sur l'écran de l'appliance VMware Live Site Recovery, sélectionnez **Storage Replication Adapter > New Adapter**.
2. Téléversez le fichier `.tar.gz` sur VMware Live Site Recovery.
3. Connectez-vous à l'appliance VMware Live Site Recovery à l'aide d'un compte administrateur via un client SSH tel que 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 des journaux.
6. À l'emplacement du journal, saisissez la commande permettant d'obtenir l'ID Docker utilisé par SRA :
`docker ps -l`
7. Pour vous connecter à l'identifiant du conteneur, saisissez la commande : `docker exec -it -u srm <container id> sh`
8. Configurez VMware Live Site Recovery avec les outils ONTAP pour VMware vSphere, l'adresse IP et le mot de passe 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>`
 - Indiquez le mot de passe entre guillemets simples afin que le script Perl considère les caractères spéciaux comme faisant partie du mot de passe, et non comme des délimiteurs.
 - Vous pouvez définir le nom d'utilisateur et le mot de passe de l'application (VASA Provider/SRA) dans ONTAP tools Manager lors de la première activation de ces services. Utilisez ces informations d'identification pour enregistrer SRA auprès de VMware Live Site Recovery.
 - Pour localiser le GUID vCenter, allez à la page vCenter Server dans ONTAP tools Manager après avoir ajouté votre instance vCenter. Reportez-vous à la section ["Ajouter des serveurs vCenter"](#).
9. Analysez à nouveau les adaptateurs pour confirmer que les informations mises à jour apparaissent sur la page Storage Replication Adapters de VMware Live Site Recovery.

Résultats Un message de confirmation s'affiche, indiquant que les informations d'identification de stockage ont été enregistrées. Vous pouvez désormais utiliser SRA pour communiquer avec le serveur SRA à l'aide de l'adresse IP, du port et des informations d'identification spécifiés.

Mettre à jour les informations d'identification SRA dans ONTAP tools

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 auriez dû exécuter les étapes mentionnées dans le sujet ["Configuration de SRA sur l'appliance VMware Live Site Recovery"](#).

Étapes

1. Exécutez les commandes suivantes pour supprimer les informations d'identification des outils ONTAP mises en cache sur la machine VMware Live Site Recovery :
 - 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 -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`` Vous devez entourer la valeur du mot de passe d'une simple apostrophe.

Un message de confirmation s'affiche indiquant que les informations d'identification de stockage ont bien été enregistrées. SRA peut communiquer avec le serveur SRA en utilisant l'adresse IP, le port et les informations d'identification fournis.

Reconfigurez vCenter dans l'appliance VMware Live Site Recovery après un changement de certificat

Si le certificat vCenter change, par exemple après une mise à niveau vCenter, vous pouvez rencontrer une erreur d'empreinte numérique non concordante dans l'extension Site Recovery. Suivez les étapes ci-dessous pour résoudre ce problème.

Étapes

1. Reconfigurer vCenter dans l'appliance VMware Live Site Recovery

- a. Ouvrez l'interface de gestion de l'appliance VMware Live Site Recovery dans un navigateur :
`https://<SRM_IP>:5480`
- b. Sélectionnez l'onglet **Résumé**.
- c. Sélectionnez **Reconfigurer** pour la connexion au serveur vCenter.

Cette fonction récupère et accepte l'empreinte numérique du certificat la plus récente provenant de vCenter.

2. Reconnecter le site d'appariage (si l'erreur persiste)

Si l'erreur de non-concordance d'empreinte digitale persiste après reconfiguration :

- a. Connectez-vous à l'interface utilisateur vCenter.
- b. Accédez à l'extension **Site Recovery**.
- c. Repérez la section **Appariement de sites**.
- d. Sélectionnez **Reconnect** pour rétablir l'association du site avec le certificat mis à jour.

Configurer les sites protégés et de récupération dans ONTAP tools

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

Lorsque vous ajoutez une nouvelle banque de données, vous pouvez l'intégrer au groupe de banques de données existant ou ajouter une nouvelle banque de données et créer un nouveau volume ou groupe de cohérence pour la protection. Après avoir ajouté une nouvelle banque de données à un groupe de cohérence ou un volume protégé, mettez à jour SnapMirror et effectuez une découverte du stockage sur les sites protégé et de restauration. Vous pouvez exécuter la découverte manuellement ou selon un calendrier afin de garantir

que la nouvelle banque de données soit détectée et protégée.

Associez les sites protégés et de récupération

Vous devez associer les sites protégés et de récupération créés à l'aide de votre vSphere Client pour permettre à l'adaptateur de réplication de stockage (SRA) de découvrir les systèmes de stockage.



L'adaptateur de réplication de stockage (SRA) prend en charge la distribution avec une relation synchrone de type Automated Failover Duplex et une relation asynchrone SnapMirror sur groupe de cohérence. Cependant, la distribution avec deux relations asynchrones SnapMirror sur des groupes de cohérence ou des relations de distribution SnapMirror sur des volumes n'est pas prise en charge. Les relations de type Vault SnapMirror ne sont pas concernées par ces restrictions de distribution. La prise en charge des groupes de cohérence dans SRA est limitée aux protocoles SAN (iSCSI et fibre channel) sur les systèmes de stockage Unified et ASA r2. Les groupes de cohérence ne sont pas pris en charge pour NFS. Si des volumes de datastore NFS sont placés sous un groupe de cohérence, l'opération de découverte des périphériques échouera.

Avant de commencer

- Vous devez avoir installé VMware Live Site Recovery sur les sites protégés et de récupération.
- Vous devez avoir installé SRA sur les sites protégés et de restauration.

Étapes

1. Sur la page d'accueil du client vSphere, double-cliquez sur l'icône **Site Recovery** puis sélectionnez **Sites**.
2. Sélectionnez **Objets > Actions > Associer les sites**.
3. Dans la boîte de dialogue **Associer les serveurs Site Recovery Manager**, saisissez l'adresse du Platform Services Controller du site protégé, puis sélectionnez **Suivant**.
4. Dans la section Sélectionner le serveur vCenter, procédez comme suit :
 - a. Vérifiez que le serveur vCenter du site protégé apparaît comme un candidat correspondant pour l'appariement.
 - b. Saisissez les identifiants d'administrateur SSO, puis sélectionnez **Terminer**.
5. Si le système vous le demande, sélectionnez **Oui** pour accepter les certificats de sécurité.

Résultat

La boîte de dialogue **Objets** affiche à la fois les sites protégés et les sites de récupération.

Configurer les groupes de protection

Avant de commencer

Vous devez vous assurer que les sites source et cible sont configurés comme suit :

- Même version de VMware Live Site Recovery installée
- machines virtuelles
- Sites de protection et de récupération jumelés
- Les banques de données source et de destination doivent être montées sur leurs sites respectifs

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Récupération du site > Groupes de protection**.

2. Dans le volet **Groupes de protection**, sélectionnez **Nouveau**.
3. Spécifiez un nom et une description pour le groupe de protection, la direction, puis sélectionnez **Suivant**.
4. Dans le champ **Type**, sélectionnez l'option **Type field option...** comme groupes de banques de données (réplication basée sur des baies) pour les banques de données NFS et VMFS. Le domaine de panne est constitué des SVM dont la réplication est activée. Les SVM qui ont uniquement le peering implémenté et qui ne présentent aucun problème sont affichés.
5. Dans l'onglet Groupes de réplication, sélectionnez soit la paire de baies activée, soit les groupes de réplication contenant la machine virtuelle que vous avez configurée, puis sélectionnez **Suivant**.

Toutes les machines virtuelles du groupe de réplication sont ajoutées au groupe de protection.
6. Vous pouvez sélectionner le plan de récupération existant ou en créer un nouveau en sélectionnant **Ajouter à un nouveau plan de récupération**.
7. Dans l'onglet Prêt à terminer, vérifiez les détails du groupe de protection que vous avez créé, puis sélectionnez **Terminer**.

Configurer les ressources du site protégé et du site de récupération

Configurer les mappages réseau dans ONTAP tools

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 permettre le mappage de chaque ressource du site protégé vers la ressource appropriée sur le site de récupération.

Vous devez effectuer les configurations de ressources suivantes :

- Cartographie des réseaux
- Mappages de dossiers
- Cartographie des ressources
- Magasins de données de substitution

Avant de commencer

Vous devez avoir connecté les sites protégés et de récupération.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Récupération de site > 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 ayant des noms correspondants** et sélectionnez **Suivant**.
 - b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Add Mappings**.
 - c. Sélectionnez **Suivant** après la création réussie des mappages.
 - d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page « Mappages réseau » affiche les ressources du site protégé et celles du site de récupération. Vous pouvez suivre la même procédure pour les autres réseaux de votre environnement.

Configurer les mappages de dossiers dans ONTAP tools

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

Avant de commencer

Vous devez avoir connecté les sites protégés et de récupération.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Récupération de site > 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 dossier.
4. Dans l'assistant Créer un mappage de dossiers, procédez comme suit :
 - a. Sélectionnez **Préparer automatiquement les mappages pour les dossiers aux noms correspondants** et sélectionnez **Suivant**.
 - b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Add Mappings**.
 - c. Sélectionnez **Suivant** après la création réussie des mappages.
 - d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page « Mappage des dossiers » affiche les ressources du site protégé et celles du site de récupération. Vous pouvez suivre la même procédure pour les autres dossiers de votre environnement.

Configurer les mappages de ressources dans ONTAP tools

Vous devez cartographier vos ressources sur le site protégé et le site de récupération afin que les machines virtuelles soient configurées pour basculer vers l'un ou l'autre groupe d'hôtes.

Avant de commencer

Vous devez avoir connecté les sites protégés et de récupération.



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 **Récupération de site > Sites**.
2. Sélectionnez votre site protégé et sélectionnez **Gérer**.
3. Sélectionnez **Mappages de ressources** > **Nouveau** dans l'onglet Gérer pour créer un nouveau mappage de ressources.
4. Dans l'assistant Créer un mappage de ressources, procédez comme suit :

- a. Sélectionnez **Préparer automatiquement les mappages pour les ressources ayant des noms correspondants** et sélectionnez **Suivant**.
- b. Sélectionnez les objets de centre de données requis pour les sites protégés et de récupération, puis sélectionnez **Add Mappings**.
- c. Sélectionnez **Suivant** après la création réussie des mappages.
- d. Sélectionnez l'objet utilisé précédemment pour créer le mappage inverse, puis sélectionnez **Terminer**.

Résultat

La page « Mappages de ressources » affiche les ressources du site protégé et celles du site de récupération. Vous pouvez suivre la même procédure pour les autres ressources de votre environnement.

Configurer les magasins de données de substitution dans ONTAP tools

Configurez un datastore de substitution pour réserver de l'espace dans l'inventaire vCenter du site de récupération pour les machines virtuelles (VM) protégées. Les datastores de substitution nécessitent une capacité minimale, car les machines virtuelles de substitution sont petites et n'utilisent généralement que quelques centaines de kilo-octets.

Avant de commencer

- Assurez-vous que les sites protégés et de restauration sont connectés.
- Vérifiez que les mappages de ressources ont été configurés.

Étapes

1. Connectez-vous à vCenter Server et sélectionnez **Récupération de site > Sites**.
2. Sélectionnez votre site protégé et sélectionnez **Gérer**.
3. Sélectionnez **Magasins de données de substitution > Nouveau** dans l'onglet gérer pour créer un nouveau magasin de données de substitution.
4. Sélectionnez le datastore approprié et cliquez sur **OK**.



Les banques de données temporaires peuvent résider sur un stockage local ou distant, mais elles ne nécessitent pas de réplication.

5. Répétez les étapes 3 à 5 pour configurer un datastore de substitution pour le site de restauration.

Configurez SRA à l'aide du gestionnaire de baies dans ONTAP tools

Vous pouvez configurer l'adaptateur de réplication de stockage (SRA) en utilisant l'assistant Array Manager de VMware Live Site Recovery pour permettre les interactions entre VMware Live Site Recovery et les machines virtuelles de stockage (SVM).

Avant de commencer

- Vous devez avoir associé les sites protégés et les sites de récupération 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 récupération.

- Vous devez avoir activé les LIF de gestion SVM pour permettre la multitenance.

SRA prend en charge la gestion au niveau du cluster et au niveau des SVM. Si vous ajoutez du stockage au niveau du cluster, vous pouvez découvrir et effectuer des opérations sur toutes les SVM du cluster. Si vous ajoutez du stockage au niveau d'une SVM, vous ne pouvez gérer que cette SVM spécifique.

Étapes

1. Dans VMware Live Site Recovery, sélectionnez **Gestionnaires de baies > Ajouter un gestionnaire de baies**.

2. Saisissez les informations suivantes pour décrire la baie dans VMware Live Site Recovery :

a. Saisissez un nom pour identifier le gestionnaire de la baie dans le champ **Nom d'affichage**.

b. Dans le champ **Type de SRA**, sélectionnez **NetApp Storage Replication Adapter for ONTAP**.

c. Saisissez les informations pour vous connecter au cluster ou à la SVM :

- Si vous vous connectez à un cluster, vous devez saisir la LIF de gestion du cluster.
- Si vous vous connectez directement à une SVM, vous devez saisir l'adresse IP de l'interface LIF de gestion de la SVM.



Lors de la configuration du gestionnaire de baies, vous devez utiliser la même connexion (adresse IP) pour le système de stockage que celle utilisée pour intégrer le système de stockage dans ONTAP tools for VMware vSphere. Par exemple, si la configuration du gestionnaire de baies est au niveau SVM, alors le stockage sous ONTAP tools for VMware vSphere doit être ajouté au niveau SVM.

d. Si vous vous connectez à un cluster, spécifiez le nom de la SVM dans le champ **SVM name**, ou laissez-le vide pour gérer toutes les SVM du cluster.

e. Saisissez les volumes à découvrir dans le champ **Volume include list**.

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

Par exemple, si vous souhaitez découvrir le volume *src_vol1* qui est en 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 récupération.

f. **(Facultatif)** Saisissez les volumes à exclure de la découverte dans le champ **Volume exclude list**.

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

Par exemple, si vous souhaitez exclure le volume *src_vol1* qui est en SnapMirror relation avec le volume *dst_vol1*, vous devez spécifier *src_vol1* dans le champ du site protégé et *dst_vol1* dans le champ du site de récupération.

3. Sélectionnez **Suivant**.

4. Vérifiez que le tableau est détecté et affiché en bas de la fenêtre Ajouter un gestionnaire de tableaux, puis sélectionnez **Terminer**.

Vous pouvez suivre les mêmes étapes pour le site de récupération en utilisant les adresses IP de gestion SVM et les identifiants appropriés. Sur l'écran « Activer les paires de baies » de l'assistant « Ajouter un gestionnaire de baies », vous devez vérifier que la paire de baies correcte est sélectionnée et qu'elle est indiquée comme

prête à être activée.

Vérifier les systèmes de stockage répliqués dans ONTAP tools

Après avoir configuré Storage Replication Adapter (SRA), vous devez vérifier que le site protégé et le site de récupération sont correctement appariés. Le système de stockage répliqué doit être détectable à la fois par le site protégé et le site de récupération.

Avant de commencer

- Vous devez avoir configuré votre système de stockage.
- Vous devez avoir associé le site protégé et le site de récupération à l'aide du gestionnaire de baies VMware Live Site Recovery.
- Vous devez avoir activé la licence FlexClone et la licence SnapMirror avant d'effectuer l'opération de basculement de test et l'opération de basculement pour SRA.
- Vous devez avoir les mêmes politiques SnapMirror et les mêmes calendriers sur les sites source et de destination.
- Si vous utilisez des stratégies SnapMirror personnalisées avec une planification personnalisée, vous devez configurer la même planification et la même stratégie sur les sites protégés et de récupération.
- Si vous utilisez des stratégies SnapMirror personnalisées (avec une planification par défaut ou personnalisée), vous devez effectuer une découverte du stockage à partir des outils ONTAP afin que la nouvelle stratégie soit reconnue. Sans cela, les workflows SRA, y compris le test de basculement et le basculement, échoueront. Effectuez la découverte du stockage aux points suivants :
 - Après avoir créé la politique personnalisée sur le site de récupération.
 - Après une opération de reprotection, qui recrée la policy sur le site protégé.

Étapes

1. Connectez-vous à votre serveur vCenter.
2. Accédez à **Récupération de site > Réplication basée sur des baies**.
3. Sélectionnez la paire de tableaux requise et vérifiez les détails correspondants.

Les systèmes de stockage doivent être détectés sur le site protégé et le site de récupération avec le statut **Enabled**.

Protection contre le fan-out dans ONTAP tools

Dans un scénario de protection par répartition, le groupe de cohérence est doublement protégé avec une relation synchrone sur le premier cluster ONTAP de destination et avec une relation asynchrone sur le second cluster ONTAP de destination. Les workflows de création, de modification et de suppression de la protection active SnapMirror maintiennent la protection synchrone. Les workflows de basculement et de reprotection de l'appliance VMware Live Site Recovery maintiennent la protection asynchrone.



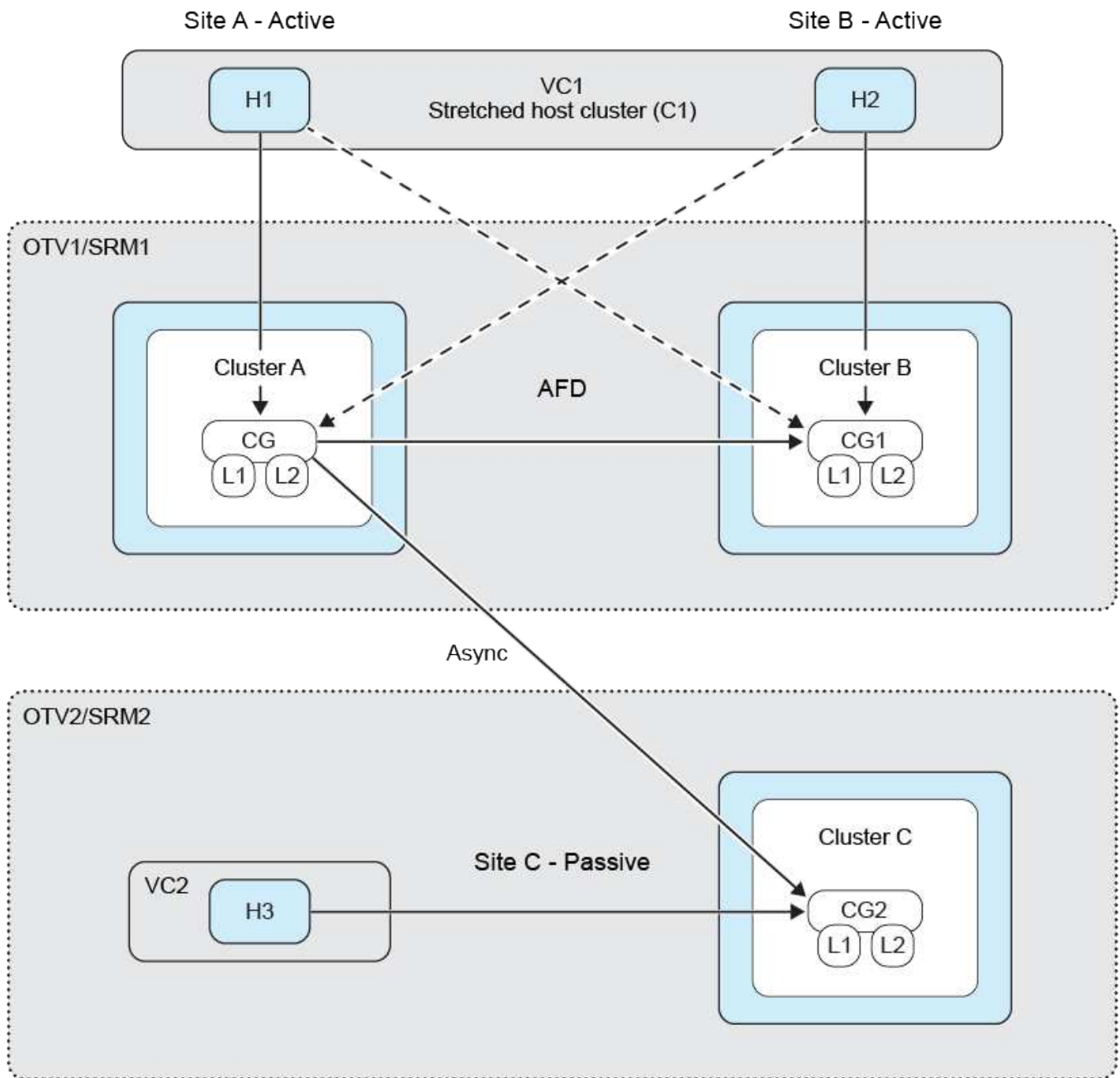
La fonction de diffusion n'est pas prise en charge pour les utilisateurs de SVM.

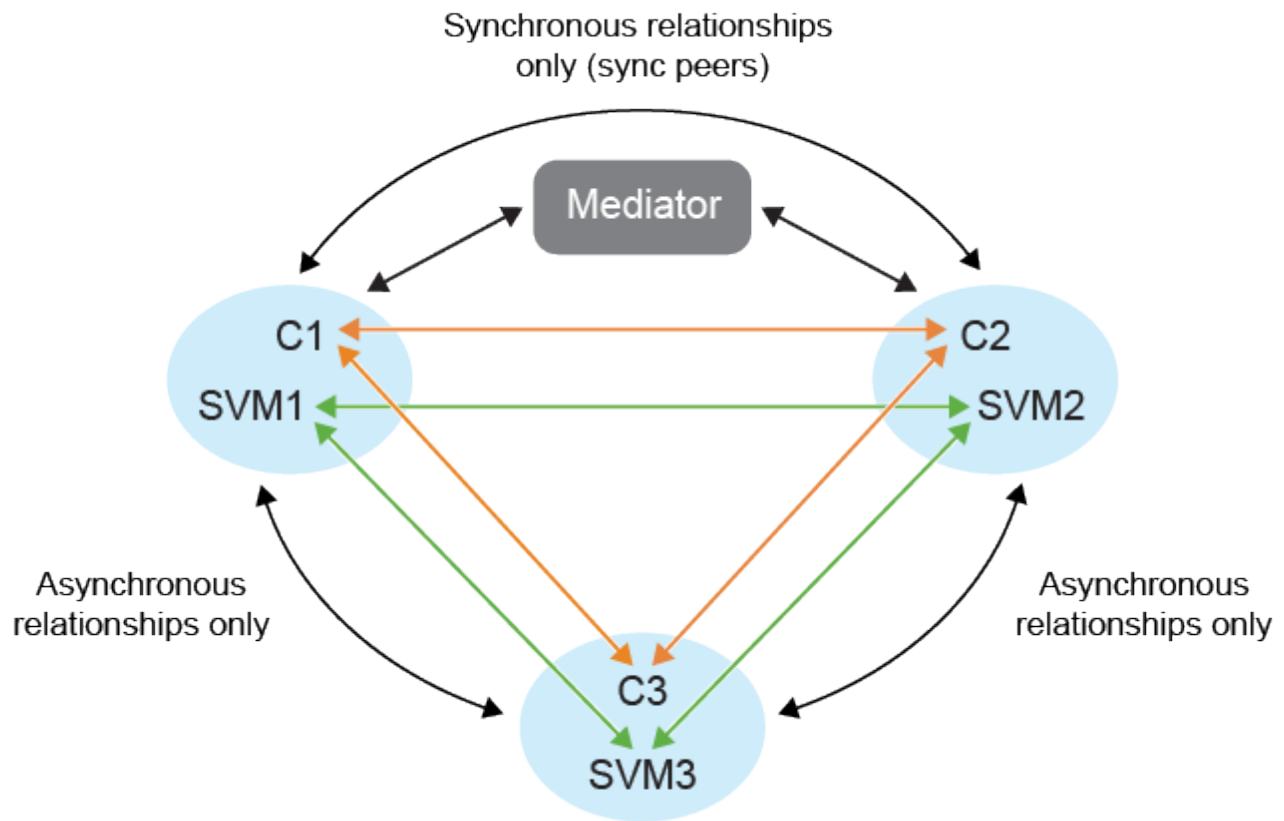
Pour configurer la protection par diffusion, mettez en peering les trois clusters de sites et les SVM.

Exemple :

Si	alors
• Le groupe de cohérence source se trouve sur le cluster c1 et le SVM svm1 • Le premier groupe de cohérence se trouve sur le cluster c2 et le SVM svm2 et • Le deuxième groupe de cohérence de destination se trouve sur le cluster c3 et la SVM svm3	• Le cluster peering sur le cluster ONTAP source sera (C1, C2) et (C1, C3). • Le cluster peering sur le premier cluster ONTAP de destination sera (C2, C1) et (C2, C3) et • Le cluster peering sur le deuxième cluster ONTAP de destination sera (C3, C1) et (C3, C2). • L'appairage SVM sur la SVM source sera (svm1, svm2) et (svm1, svm3). • L'appairage SVM sur le premier SVM de destination sera (svm2, svm1) et (svm2, svm3) et • Le peering SVM sur la deuxième destination svm sera (svm3, svm1) et (svm3, svm2).

Le schéma suivant illustre la configuration de protection par dérivation :





Étapes

1. Sélectionnez un nouveau magasin de données de substitution. Les critères de sélection du magasin de données de substitution pour la protection progressive sont les suivants :
 - Ne placez pas le datastore de substitution dans le cluster hôte que vous protégez.
 - Si vous devez inclure le datastore de substitution dans le cluster hôte, ajoutez-le à l'appliance VMware Live Site Recovery avant de configurer la protection SnapMirror active sync. Avec cette configuration, vous pouvez laisser le datastore de substitution en dehors de la protection.

Pour plus d'informations, consultez ["Sélectionnez un datastore de remplacement"](#)

2. Ajoutez des banques de données à la protection du cluster hôte en suivant ["Modifier le cluster d'hôtes protégé"](#). Ajoutez des types de stratégies asynchrones et synchrones.

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.