Protection des datastores et des machines virtuelles

ONTAP tools for VMware vSphere 9.10

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-tools-vmware-vsphere-910/protect/task_enable_storage_replication_adapter.html on April 02, 2025. Always check docs.netapp.com for the latest.

Sommaire

Protection des datastores et des machines virtuelles . . . 1
- Activez SRA pour protéger les datastores . . . 1
- Configuration du système de stockage pour la reprise après incident . . . 2
  - Configuration de Storage Replication adapter pour un environnement SAN . . . 2
  - Configurer Storage Replication adapter pour un environnement à grande échelle . . . 3
- Configurez SRA sur l'appliance SRM . . . 4
- Mettez à jour les informations d'identification SRA . . . 5
- Migration de Windows SRM vers l'appliance SRM . . . 5
- Configurez la réplication pour les datastores vvols afin de protéger les machines virtuelles . . . 6
- Configurez la réplication vvols pour les datastores existants . . . 7
- Protection des machines virtuelles non protégées . . . 9
- Configuration des sites protégés et de reprise après incident . . . 9
  - Configurer les règles de stockage des VM . . . 9
  - Configuration des groupes de protection . . . 10
  - Protection par paires et sites de reprise après incident . . . 11
  - Configuration des ressources protégées et du site de reprise . . . 12
  - Vérification des systèmes de stockage répliqués . . . 16

Protection des datastores et des machines virtuelles

Activez SRA pour protéger les datastores

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

Ce dont vous aurez besoin

- Vous devez avoir configuré votre instance vCenter Server et ESXi.
- Vous devez avoir déployé des outils ONTAP.
- Vous devez avoir téléchargé le `.msi` Fichier du plug-in SRA ou `.tar.gz` File pour l'appliance SRM uniquement si vous souhaitez configurer la solution de reprise après incident site Recovery Manager (SRM).

  "Installation et configuration de site Recovery Manager 8.2" a plus d'informations.

À propos de cette tâche

La flexibilité d'activer les fonctionnalités VASA Provider et SRA vous permet d'exécuter uniquement les workflows dont vous avez besoin pour votre entreprise.

Étapes

1. Connectez-vous à l'interface utilisateur Web de VMware vSphere.
2. Dans vSphere client, cliquez sur **Menu** > **ONTAP Tools Console**.
3. Cliquez sur **Paramètres**.
4. Cliquez sur **gérer les fonctionnalités** dans l'onglet **Paramètres d'administration**.
5. Dans la boîte de dialogue **Manage Capabilities**, sélectionnez l'extension SRA à activer.
6. Entrez l'adresse IP des outils ONTAP et le mot de passe administrateur, puis cliquez sur **appliquer**.
7. Vous pouvez utiliser l'une des méthodes suivantes pour déployer SRA :

Pour Windows SRM
Pour l'appareil SRM
a. Double-cliquez sur le téléchargé `.msi` Installateur du plug-in SRA. b. Suivez les instructions à l'écran. c. Entrez l'adresse IP et le mot de passe des outils ONTAP déployés.

a. Accédez à la page de l'appliance SRM, puis à la page Storage Replication Adapters du dispositif SRM.
b. Cliquez sur **Nouvelle carte**.
c. Téléchargez le programme d'installation *.tar.gz* pour le plug-in SRA sur SRM.
d. Relancez l'analyse des cartes pour vérifier que les détails sont mis à jour dans la page SRM Storage Replication Adapters.

Vous devez vous déconnecter de vSphere client, puis vous reconnecter pour vérifier que l'extension sélectionnée est disponible pour la configuration.

Informations connexes

"Configuration de Storage Replication adapter pour la reprise après incident"

Configuration du système de stockage pour la reprise après incident

Configuration de Storage Replication adapter pour un environnement SAN

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

Ce dont vous aurez besoin

Vous devez avoir installé les programmes suivants sur le site protégé et le site de reprise :

- SRM

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

  "Documentation VMware site Recovery Manager"

- SRA

  L'adaptateur est installé sur SRM.

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 qui ont `ostype` Option définie sur *VMware* sur le système de stockage principal.
3. Vérifier que les hôtes ESXi du site de reprise disposent d'une connectivité FC ou iSCSI appropriée vers la machine virtuelle de stockage (SVM).

   Pour ce faire, vous pouvez vérifier que les hôtes ESXi disposent de LUN locales connectées sur la SVM ou à l'aide de `fcp show initiators` commande ou le `iscsi show initiators` Commande sur les SVM.

Configuration de Storage Replication adapter pour un environnement NAS

Ce dont vous aurez besoin

Vous devez avoir installé les programmes suivants sur le site protégé et le site de reprise :

- SRM

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

  "Documentation VMware site Recovery Manager"

- SRA

  L'adaptateur est installé sur SRM et 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 FQDN sur lequel les exportations NFS sont présentes sont spécifiées dans le champ **NFS Addresses** lors de l'utilisation de l'assistant Array Manager pour ajouter des matrices à SRM.
4. Utilisez le `ping` Commande sur chaque hôte ESXi du site de reprise pour vérifier que l'hôte dispose d'un port VMkernel qui peut accéder aux adresses IP utilisées pour servir les exportations NFS à partir du SVM.

"Support NetApp"

Configurer Storage Replication adapter pour un environnement à grande échelle

Vous devez configurer les intervalles d'expiration du stockage en fonction des paramètres recommandés pour Storage Replication adapter (SRA) afin de bénéficier de performances optimales dans les environnements à grande échelle.

Paramètres du fournisseur de stockage

Vous devez définir les valeurs de délai suivantes sur SRM pour l'environnement mis à l'échelle :

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 le `StorageProvider.autoResignatureMode` option.

Pour plus d'informations sur la modification des paramètres du fournisseur de stockage, reportez-vous à la documentation VMware.

"Documentation VMware vSphere : modifiez les paramètres du fournisseur de stockage"

Paramètres de stockage

Vous devez définir la valeur du `storage.commandTimeout` et `storage.maxConcurrentCommandCnt` intervalle d'expiration pour les environnements hautement évolutifs jusqu'à 99,999 secondes.

> 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.

Vous devez également définir le délai maximum pour que SRA effectue une seule opération dans le fichier vvol.properties : offtap.operation.timeout.period.seconds=86400.

"Réponse de la base de connaissances NetApp 1001111 : Guide de dimensionnement de NetApp Storage Replication adapter 4.0/7.X pour ONTAP"

La documentation VMware sur la modification des paramètres du fournisseur de SAN contient davantage d'informations.

"Documentation de VMware site Recovery Manager : modifiez les paramètres de stockage"

Configurez SRA sur l'appliance SRM

Une fois l'appliance SRM déployée, vous devez configurer SRA sur l'appliance SRM. La configuration de SRA permet de communiquer avec SRM Appliance et SRA pour la gestion de la reprise après incident. Vous devez stocker les informations d'identification des outils ONTAP (adresse IP et mot de passe d'administrateur) dans l'appliance SRM pour permettre la communication entre l'appliance SRM et SRA.

Ce dont vous aurez besoin

Vous devriez avoir téléchargé le fichier *tar.gz* à partir de "Site de support NetApp".

À propos de cette tâche

La configuration de SRA sur SRM Appliance stocke les informations d'identification SRA dans l'appliance SRM.

Étapes

1. Sur l'écran SRM Appliance, cliquez sur **Storage Replication adapter** > **New adapter**.
2. Téléchargez le fichier *.tar.gz* vers SRM.
3. Relancez l'analyse des cartes pour vérifier que les détails sont mis à jour dans la page SRM Storage Replication Adapters.
4. Connectez-vous à l'aide du compte administrateur à l'appliance SRM à l'aide de putty.

5. Basculer vers l'utilisateur root à l'aide de la commande : `su root`
6. Dans le journal location, 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 SRM avec l'adresse IP et le mot de passe des outils ONTAP à l'aide de la commande : `perl command.pl -I <va-IP> administrator <va-password>`

   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 SRM communique avec SRA, vous devez mettre à jour les informations d'identification SRA sur le serveur SRM si vous avez modifié les informations d'identification.

Ce dont vous aurez besoin

Vous devriez avoir exécuté les étapes mentionnées dans la rubrique « Configuration de SRA sur l'appliance SRM ».

"Configuration de SRA sur l'appliance SRM"

Étapes

1. Supprimer le contenu du `/srm/sra/confdirectory` utilisation :
   a. `cd /srm/sra/conf`
   b. `rm -rf *`
2. Exécutez la commande perl pour configurer SRA avec les nouvelles informations d'identification :
   a. `cd /srm/sra/`
   b. `perl command.pl -I <va-IP> administrator <va-password>`

Migration de Windows SRM vers l'appliance SRM

Si vous utilisez Windows site Recovery Manager (SRM) pour la reprise après incident et que vous souhaitez utiliser l'appliance SRM pour la même configuration, vous devez migrer la configuration de la reprise après incident Windows vers la solution SRM basée sur l'appliance.

Les étapes de la migration de la reprise sur incident sont les suivantes :

1. Mise à niveau de vos outils ONTAP existants vers la version 9.7.1.

   "Passez à la dernière version des outils ONTAP"

2. Migration de l'adaptateur de réplication du stockage Windows vers SRA basé sur l'appliance.
3. Migration des données Windows SRM vers l'appliance SRM.

Voir "Migrer de site Recovery Manager for Windows vers site Recovery Manager Virtual Appliance" pour des étapes détaillées

Configurez la réplication pour les datastores vvols afin de protéger les machines virtuelles

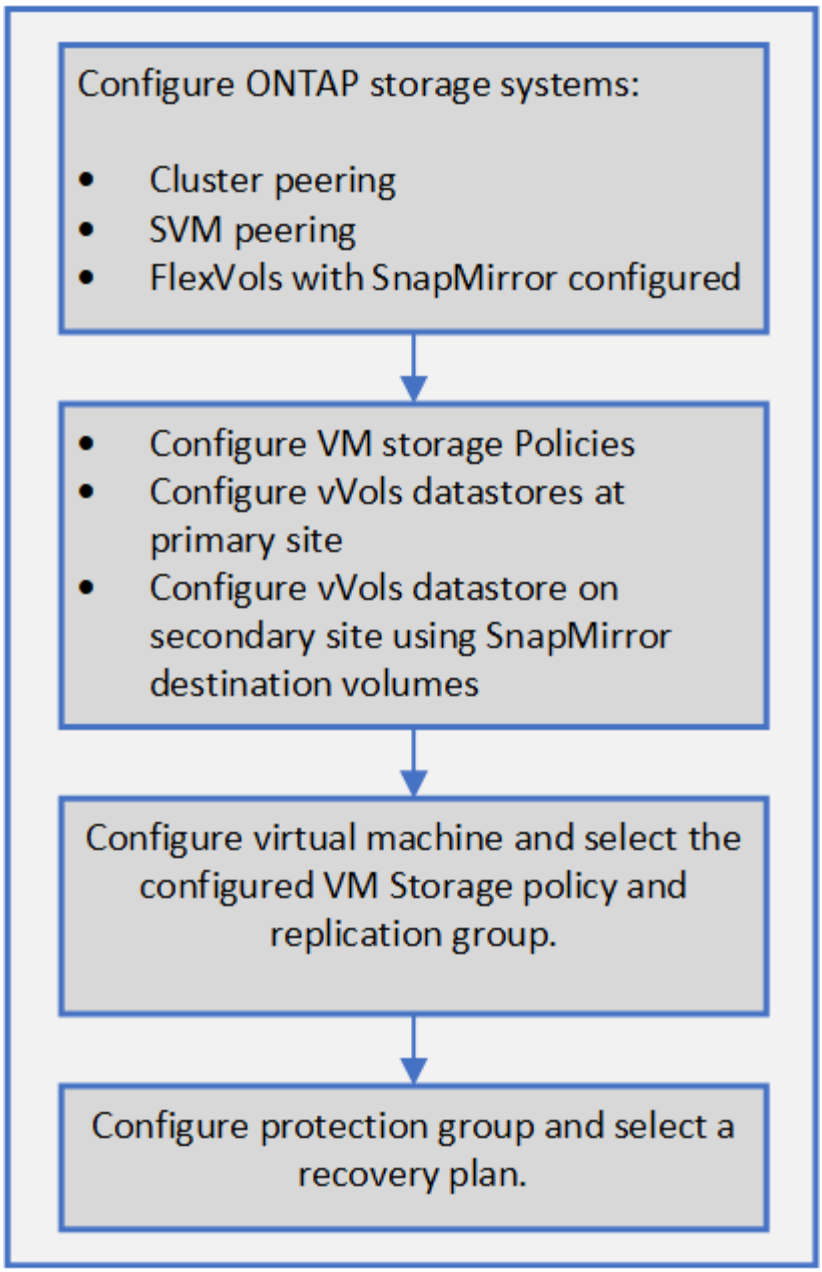
Vous pouvez configurer la réplication de votre datastore vvols à l'aide des outils ONTAP. L'objectif principal de la réplication de vvols est de protéger les ordinateurs virtuels stratégiques lors d'une reprise après incident à l'aide de VMware site Recovery Manager (SRM).

Cependant, pour configurer la réplication de vvols pour les outils ONTAP, la fonctionnalité de VASA Provider et la réplication de vvols doivent être activées. Vasa Provider est activé par défaut dans les outils ONTAP. La réplication basée sur les baies est effectuée au niveau FlexVol. Chaque datastore vvols est mappé à un conteneur de stockage composé d'un ou plusieurs volumes FlexVol. Les volumes FlexVol doivent être préconfigurés avec SnapMirror à partir de ONTAP.

Vous ne devez pas configurer un mélange de machines virtuelles protégées et non protégées dans un seul datastore vvols. Une opération de reprotection après le basculement entraîne la suppression des machines virtuelles non protégées. Assurez-vous que tous les ordinateurs virtuels d'un datastore vVols sont protégés lors de l'utilisation de la réplication.

Des groupes de réplication sont créés lors de la création du workflow de data store vVvols pour chaque volume FlexVol. Pour utiliser la réplication vvols, vous devrez créer des stratégies de stockage de machines virtuelles incluant l'état et la planification de la réplication avec le profil de capacité de stockage. Un groupe de réplication comprend des machines virtuelles répliquées dans le cadre de la reprise sur incident vers le site cible. Vous pouvez configurer des groupes de réplication avec des groupes de protection et des plans de restauration à l'aide de la console SRM, pour les flux de travail de reprise après incident.

Si vous utilisez une reprise après incident pour le datastore vvols, il n'est pas nécessaire de configurer Storage Replication adapter (SRA) séparément puisque la fonctionnalité VASA Provider est améliorée pour disposer d'une réplication vvols.



"Configurez la réplication vvols pour les datastores existants"

Configurez la réplication vvols pour les datastores existants

La fonction de réplication de vvols est améliorée afin de fournir une réplication de vvols pour les machines virtuelles existantes qui ont été créées avant la configuration de SRM. Vous pouvez ainsi restaurer les machines virtuelles existantes et les protéger sur le site de DR.

Ce dont vous aurez besoin

- Le cluster et SVM sont peering.
- Les datastores et les volumes FlexVol sont créés sur des sites source et cible.
- Les sites source et cible ont les mêmes profils de capacité de stockage.

- Les volumes FlexVol ont la même planification SnapMirror.
- La réplication de vvols est activée.

Aucun groupe de réplication n'est créé pour un datastore existant.

Étapes

1. Accéder à l'interface de swagger.
2. Exécutez l'API REST pour configurer le groupe de réplication pour le datastore existant.

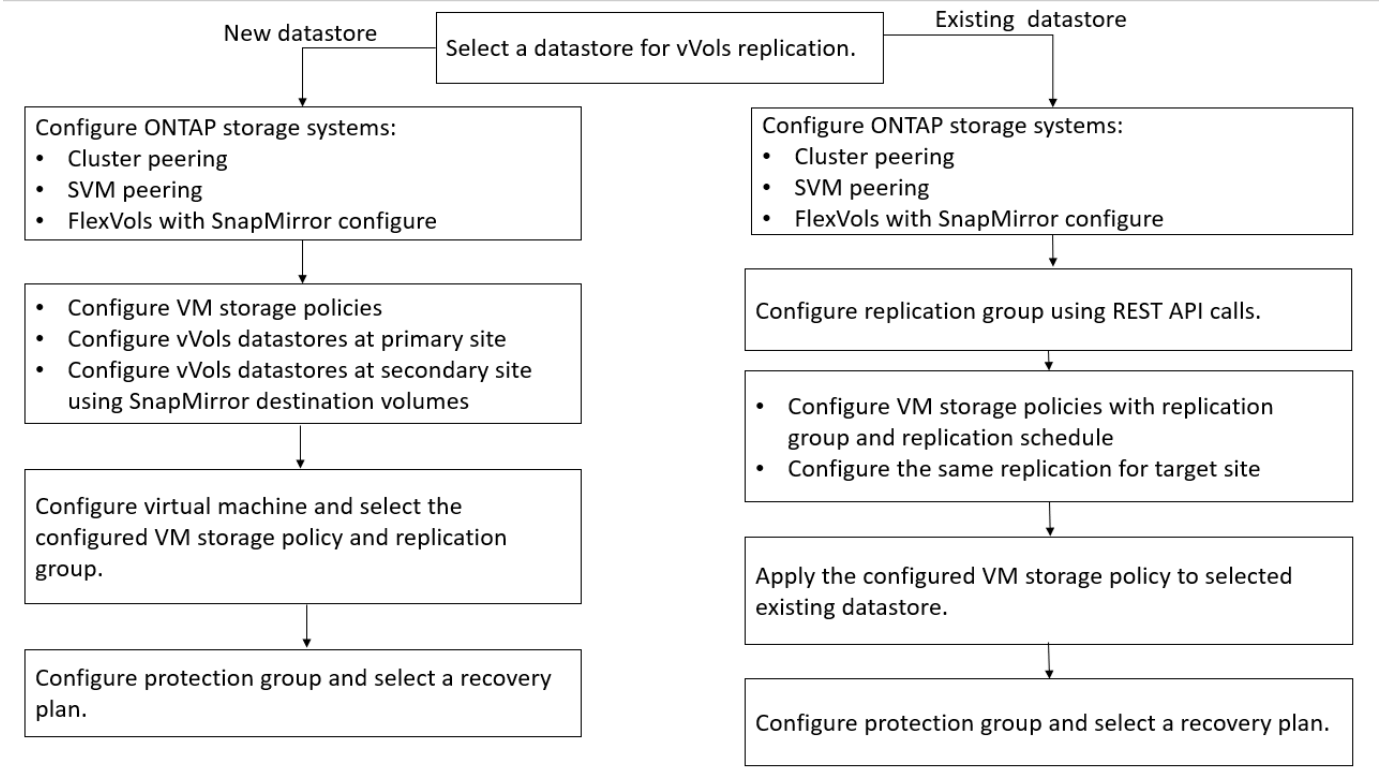
   API : /3.0/admin/{datastore}/Replication-groups

3. Créez la stratégie de stockage de VM pour le datastore vvols existant avec le profil de capacité de stockage utilisé pour créer le datastore.

   Ajoutez la stratégie de réplication, la planification de réplication et le datastore compatible dans la liste disponible.

> Si vous utilisez System Manager pour protéger les volumes FlexVol et le profil de capacité de stockage dispose d'une règle de QoS « aucun », assurez-vous que l'option **appliquer la limite de performances** est désactivée pour la reprise après incident.

1. Accéder à la machine virtuelle non protégée et modifier la stratégie de stockage de la machine virtuelle.
2. Sélectionnez la stratégie de stockage de VM et le datastore.
3. Ajoutez le groupe de réplication à la machine virtuelle non protégée.



REMARQUE :

- Lors de la configuration d'une machine virtuelle afin de permettre la réplication pour les datastores existants, assurez-vous de vérifier le volume FlexVol doté d'une configuration vvols.
- Lorsque vVvols d'une machine virtuelle existante sont répartis entre plusieurs datastores, il est conseillé de déplacer tous les vvols de cette machine virtuelle à l'aide de vMotion vers un seul datastore avant de procéder à la réplication.

Protection des machines virtuelles non protégées

Vous pouvez configurer la protection de vos machines virtuelles non protégées existantes qui ont été créées à l'aide de la stratégie de stockage de la machine virtuelle avec la réplication désactivée. Pour assurer la protection, vous devez modifier la règle de stockage de la machine virtuelle et attribuer un groupe de réplication.

À propos de cette tâche

Si SVM possède à la fois des LIF IPv4 et IPv6, vous devez désactiver les LIF IPv6 et réaliser par la suite des flux de travail de reprise sur incident.

Étapes

1. Cliquez sur l'ordinateur virtuel requis et vérifiez qu'il est configuré avec la stratégie de stockage par défaut de l'ordinateur virtuel.
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle sélectionnée, puis cliquez sur **VM Policies** > **Edit VM Storage Policies**.
3. Sélectionnez une stratégie de stockage VM dont la réplication est activée dans la liste déroulante **VM Storage policy**.
4. Sélectionnez un groupe de réplication dans la liste déroulante **Groupe de réplication**, puis cliquez sur **OK**.
5. Vérifiez le récapitulatif de la machine virtuelle pour vérifier que celle-ci est protégée.

- Cette version des outils ONTAP ne prend pas en charge le clonage à chaud des machines virtuelles protégées. Vous devez mettre la machine virtuelle hors tension, puis effectuer l'opération de clonage.
- Si un datastore n'apparaît pas dans les outils ONTAP après une opération de reprotection, vous devez effectuer une détection du système de stockage ou attendre la prochaine opération de détection planifiée.

Configuration des sites protégés et de reprise après incident

Configurer les règles de stockage des VM

Il est recommandé de configurer des stratégies de stockage de machines virtuelles pour gérer les machines virtuelles qui sont configurées sur le datastore vvols et pour activer des services tels que la réplication pour les disques virtuels. Pour les datastores classiques, il est facultatif d'utiliser ces règles de stockage de machines virtuelles.

À propos de cette tâche

Le client web vSphere fournit des règles de stockage par défaut. Mais vous pouvez créer des stratégies et les affecter aux machines virtuelles.

Étapes

1. Sur la page vSphere client, cliquez sur **Menu** > **stratégies et profils**.
2. Cliquez sur **VM Storage Policies** > **Create VM Storage Policy**.
3. Dans la page Créer une stratégie de stockage VM, fournissez les informations suivantes :
   a. Entrez un nom et une description pour la politique de stockage de VM.
   b. Sélectionnez **Activer les règles pour le stockage « NetApp clustered Data ONTAP.VP.vvol »**.
   c. Sélectionnez le profil de capacité de stockage requis dans l'onglet placement.
   d. Sélectionnez l'option **Custom** pour activer la réplication.
   e. Cliquez sur **ADD RULE** pour sélectionner la réplication **asynchrone** et la planification SnapMirror requise, puis cliquez sur **NEXT**.
   f. Vérifiez les datastores compatibles répertoriés, puis cliquez sur **NEXT** dans l'onglet Storage Compatibility.

      Pour les datastores vvols disposant de volumes FlexVol de protection des données, il n'est pas possible de procéder à une vérification des datastores compatibles.
4. Vérifiez la sélection de votre stratégie de stockage VM dans l'onglet **Revue et fin**, puis cliquez sur **Terminer**.

Configuration des groupes de protection

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

Ce dont vous aurez besoin

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

- Même version de SRM installée
- Le datastore vvols est configuré avec une réplication activée et un datastore monté
- Profils de capacité de stockage similaires
- Règles de stockage des serveurs virtuels similaires avec fonctionnalité de réplication qui doit être mappée dans SRM
- 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 votre serveur vCenter, puis cliquez sur **site Recovery** > **protection Groups**.
2. Dans le volet **protection Groups**, cliquez sur **Nouveau**.
3. Spécifiez un nom et une description pour le groupe de protection, la direction, puis cliquez sur **SUIVANT**.

4. Dans le champ **Type**, sélectionnez l'une des options suivantes :

Pour…	Option de champ Type…
Datastore traditionnel	Groupes de datastores (réplication basée sur les baies)
Datastore vVols	Volumes virtuels (réplication vvol)

   Le domaine de panne n'est rien d'autre que les SVM avec la réplication activée. Les SVM qui ont uniquement peering mis en œuvre et sans problèmes sont affichés.

5. Dans l'onglet Replication Groups, sélectionnez la paire Enabled array ou les groupes de réplication possédant la machine virtuelle que vous avez configurée, puis cliquez sur **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 cliquant sur **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 cliquez sur **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 activer Storage Replication adapter (SRA) pour découvrir les systèmes de stockage.

Ce dont vous aurez besoin

- Vous devez avoir installé site Recovery Manager (SRM) sur les sites protégés et de reprise.
- Vous devez avoir installé SRA sur les sites protégés et de reprise.

À propos de cette tâche

Les configurations « fan-out » SnapMirror sont celles où un volume source est répliqué vers deux destinations différentes. Ces opérations créent un problème lors de la restauration lorsque SRM a besoin de restaurer la machine virtuelle à partir de la destination.

Storage Replication adapter (SRA) ne prend pas en charge les configurations SnapMirror « Fan-Out ».

Étapes

1. Double-cliquez sur **site Recovery** sur la page d'accueil de vSphere client, puis cliquez sur **sites**.
2. Cliquez sur **objets** > **actions** > **paire de sites**.
3. Dans la boîte de dialogue paire de serveurs de Gestionnaire de récupération de site, entrez l'adresse du contrôleur des services de plate-forme du site protégé, puis cliquez sur **Suivant**.
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 administrateur SSO, puis cliquez sur **Terminer**.

5. Si vous y êtes invité, cliquez sur **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 des deux sites afin de permettre le mappage de chaque ressource du site protégé vers la ressource appropriée du site de reprise.

Vous devez effectuer les configurations de ressources suivantes :

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

Ce dont vous aurez besoin

Vous devez avoir connecté les sites protégés et de restauration.

Étapes

1. Connectez-vous à votre serveur vCenter et cliquez sur **site Recovery** > **sites**.
2. Sélectionnez votre site protégé, puis cliquez sur **gérer**.
3. Dans l'onglet gérer, sélectionnez **mappages réseau**.
4. Cliquez sur le bouton pour créer un nouveau mappage réseau.

   L'assistant de création de mappage réseau s'affiche.

5. Dans l'assistant de création de mappage réseau, effectuez les opérations suivantes :
   a. Sélectionnez **préparer automatiquement les mappages pour les réseaux avec des noms correspondants**, puis cliquez sur **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de reprise, puis cliquez sur **Ajouter des mappages**.
   c. Cliquez sur **Suivant** une fois les mappages créés.
   d. Sélectionnez l'objet utilisé précédemment pour créer un mappage inversé, puis cliquez sur **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 sur le site de restauration pour permettre la communication entre eux.

Ce dont vous aurez besoin

Vous devez avoir connecté les sites protégés et de restauration.

Étapes

1. Connectez-vous à votre serveur vCenter et cliquez sur **site Recovery** > **sites**.
2. Sélectionnez votre site protégé, puis cliquez sur **gérer**.
3. Dans l'onglet gérer, sélectionnez **mappages de dossiers**.
4. Cliquez sur le bouton pour créer un nouveau mappage de dossier.

   L'assistant de création de mappage de dossier s'affiche.

5. Dans l'assistant Créer un mappage de dossier, effectuez les opérations suivantes :
   a. Sélectionnez **préparer automatiquement les mappages pour les dossiers avec des noms de correspondance**, puis cliquez sur **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de reprise, puis cliquez sur **Ajouter des mappages**.
   c. Cliquez sur **Suivant** une fois les mappages créés.
   d. Sélectionnez l'objet utilisé précédemment pour créer un mappage inversé, puis cliquez sur **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 afin que les ordinateurs virtuels puissent basculer vers un groupe d'hôtes ou un autre.

Ce dont vous aurez besoin

Vous devez avoir connecté les sites protégés et de restauration.

Dans site Recovery Manager (SRM), les ressources peuvent être des pools de ressources, des hôtes ESXi ou des clusters vSphere.

Étapes

1. Connectez-vous à votre serveur vCenter et cliquez sur **site Recovery** > **sites**.
2. Sélectionnez votre site protégé, puis cliquez sur **gérer**.
3. Dans l'onglet gérer, sélectionnez **mappages de ressources**.
4. Cliquez sur le bouton pour créer un mappage de ressources.

L’assistant de création de mappage de ressources s’affiche.

5. 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**, puis cliquez sur **Suivant**.
   b. Sélectionnez les objets de centre de données requis pour les sites protégés et de reprise, puis cliquez sur **Ajouter des mappages**.
   c. Cliquez sur **Suivant** une fois les mappages créés.
   d. Sélectionnez l’objet utilisé précédemment pour créer un mappage inversé, puis cliquez sur **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.

Mappage des règles de stockage

Vous devez mapper les stratégies de stockage du site protégé vers les stratégies de stockage du site de reprise pour que votre plan de reprise place les serveurs virtuels récupérés sur les datastores appropriés, en fonction de vos mappages. Après la restauration de la machine virtuelle sur le site de reprise, la stratégie de stockage des machines virtuelles mappées sera attribuée à la machine virtuelle.

Étapes

1. Dans vSphere client, cliquez sur **site Recovery** > **Open site Recovery**.
2. Dans l’onglet paire de sites, cliquez sur **configurer** > **mappages de stratégie de stockage**.
3. Sélectionnez le site requis, puis cliquez sur **Nouveau** pour créer un nouveau mappage.
4. Sélectionnez l’option **préparer automatiquement les mappages pour les stratégies de stockage avec les noms correspondants**, puis cliquez sur **SUIVANT**.

   SRM sélectionne les stratégies de stockage sur le site protégé pour lequel une stratégie de stockage portant le même nom existe sur le site de reprise. Vous pouvez également sélectionner l’option de mappage manuel pour sélectionner plusieurs règles de stockage.

5. Cliquez sur **Ajouter des mappages**, puis sur **SUIVANT**.
6. Dans la section **Reverse Mapping**, cochez les cases requises pour le mappage, puis cliquez sur **NEXT**.
7. Dans la section **prêt à compléter**, vérifiez vos sélections et cliquez sur **TERMINER**.

Configurez les datastores à espace réservé

Vous devez configurer un datastore réservé afin qu’il puisse placer 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.

Ce dont vous aurez besoin

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

Étapes

1. Connectez-vous à votre serveur vCenter et cliquez sur **site Recovery** > **sites**.
2. Sélectionnez votre site protégé, puis cliquez sur **gérer**.
3. Dans l'onglet gérer, sélectionnez **espace de stockage réservé**.
4. Cliquez sur le bouton pour créer un datastore de marque de réservation.
5. Sélectionnez le datastore approprié, puis cliquez sur **OK**.

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

6. 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

La configuration de Storage Replication adapter (SRA) peut être configurée à l'aide de l'assistant Array Manager de site Recovery Manager (SRM) pour activer les interactions entre SRM et les SVM (Storage Virtual machines).

Ce dont vous aurez besoin

- Vous devez avoir apparié les sites protégés et les sites de reprise dans SRM.
- Vous devez avoir configuré votre stockage avant de configurer le gestionnaire de baies.
- 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.

VMware ne prend pas en charge le protocole NFS4.1 pour SRM.

Étapes

1. Dans SRM, cliquez sur **Array Managers**, puis sur **Add Array Manager**.
2. Entrez les informations suivantes pour décrire la matrice dans SRM :

   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 et les mêmes informations d'identification pour le système de stockage utilisé pour ajouter le système de stockage dans le menu systèmes de stockage de Virtual Storage Console. Par exemple, si la configuration Array Manager est prévue au niveau du SVM, le stockage sous VSC 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. Vous pouvez entrer le nom du volume complet ou le nom du volume partiel.

   Par exemple, si vous souhaitez 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. Vous pouvez entrer le nom du volume complet ou le nom du volume partiel.

Par exemple, si vous souhaitez 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 récupération.

a. **(Facultatif)** Entrez le nom d'utilisateur du compte au niveau du cluster ou du compte au niveau du SVM dans le champ **Nom d'utilisateur**.
b. Saisissez le mot de passe du compte utilisateur dans le champ **Mot de passe**.

3. Cliquez sur **Suivant**.
4. Vérifiez que la matrice est découverte et affichée en bas de la fenêtre Add Array Manager.
5. Cliquez sur **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 appariés avec succès après la configuration de Storage Replication adapter (SRA). Le système de stockage répliqué doit être localisé vers le site protégé et vers le site de reprise.

Ce dont vous aurez besoin

- Vous devez avoir configuré votre système de stockage.
- Vous devez avoir associé le site protégé et le site de reprise à l'aide du gestionnaire de baies SRM.
- Vous devez avoir activé la licence FlexClone et la licence SnapMirror avant d'effectuer l'opération de test

de basculement et de basculement pour SRA.

Étapes

1. Connectez-vous à votre serveur vCenter.
2. Accédez à **site Recovery** > **Array Based Replication**.
3. Sélectionner la SVM requise, puis vérifier les détails correspondants dans les Array paires.

   Les systèmes de stockage doivent être découverts sur le site protégé et sur le site de reprise avec l'état « 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 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 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.