

Administration de Site Recovery Manager

Site Recovery Manager 5.5

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

<https://docs.vmware.com/fr/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2008-2017 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

À propos de l'administration de VMware vCenter Site Recovery Manager 8

Informations mises à jour 9

1 Rôles, privilèges et autorisations Site Recovery Manager 11

Gestion des autorisations par Site Recovery Manager 12

Site Recovery Manager et le rôle d'administrateur vCenter Server 14

Rôles de Site Recovery Manager et devSphere Replication 14

Gestion des autorisations dans une configuration de site de récupération partagé 15

Attribuer des rôles et des autorisations Site Recovery Manager 17

Référence de rôles Site Recovery Manager 19

Référence de rôles vSphere Replication 25

2 Réplication de machines virtuelles 28

Impact de la valeur de l'objectif de point de récupération sur la planification de la réplication 28

Réplication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques 29

Utilisation de vSphere Replication avec le stockage Virtual SAN 30

Configurer la réplication d'une machine virtuelle unique 33

Configurer la réplication de nombreuses machines virtuelles 35

Répliquer des machines virtuelles en utilisant des amorces de réplication 38

Reconfigurer des réplications 39

Arrêter la réplication d'une machine virtuelle 41

3 Création de groupes de protection 42

À propos des groupes de protection basés sur la baie et des groupes de banques de données 43

Comment Site Recovery Manager calcule les groupes de banques de données 44

Créer des groupes de protection basés sur la baie 46

Modifier des groupes de protection basés sur la baie 47

Créer des groupes de protection pour vSphere Replication 47

Modifier des groupes de protection de vSphere Replication 48

Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection 49

4 Création, test, et exécution de plans de récupération 50

Tester un plan de récupération 52

Réseaux de test et réseaux de centre de données 52

Exécution d'une migration planifiée ou d'une récupération d'urgence via un plan de récupération	53
Exécution d'une récupération à l'aide de la fonction de récupération forcée	54
Différences entre tester et exécuter un plan de récupération	55
Interaction de Site Recovery Manager avec DPM et DRS lors d'une récupération	56
Interaction entre Site Recovery Manager et Storage DRS ou Storage vMotion	56
Utilisation de Site Recovery Manager avec la réplication basée sur la baie pour des sites avec Storage DRS ou Storage vMotion	57
Utilisation de Site Recovery Manager avec vSphere Replication sur les sites disposant de Storage DRS ou de Storage vMotion	58
Interaction entre Site Recovery Manager et vSphere High Availability	59
Protection de machines virtuelles MSCS (Microsoft Cluster Server) et tolérantes aux pannes	59
Créer, tester et exécuter un plan de récupération	61
Créer un plan de récupération	62
Modifier un plan de récupération	63
Suspendre les machines virtuelles lors de l'exécution d'un plan de récupération	63
Tester un plan de récupération	64
Nettoyage après l'essai d'un plan de récupération	65
Exécuter un plan de récupération	66
Récupérer un snapshot d'une machine virtuelle à un moment spécifique	67
Étapes pour exporter le plan de récupération	68
Afficher et exporter l'historique du plan de récupération	68
Annuler un test ou une récupération	69
Supprimer un plan de récupération	69
5 Reprotection des machines virtuelles après une récupération	71
Exécution d'une opération de reprotection par Site Recovery Manager	72
Conditions préalables à l'exécution d'une opération de reprotection	73
Reprotéger les machines virtuelles	74
États de reprotection	75
6 Restauration de la configuration du site de pré-récupération par l'exécution d'un retour arrière	77
Effectuer un retour arrière	78
7 Configuration d'un plan de récupération	81
Étapes d'un plan de récupération	82
Spécifier la priorité de récupération d'une machine virtuelle	83
Créer des étapes de récupération personnalisées	83
Types d'étapes de récupération personnalisée	84
Gestion des échecs des étapes de récupération personnalisée par Site Recovery Manager	85
Créer des étapes de commande de niveau supérieur	86

Créer des étapes d'invite de message de niveau supérieur	87
Créer des étapes de commande pour les machines virtuelles individuelles	87
Créer des étapes d'invites de message pour les machines virtuelles individuelles	88
Instructions pour l'écriture des étapes de commande	89
Variables d'environnement pour les étapes de commande	89
Personnaliser la récupération d'une machine virtuelle individuelle	90

8 Personnalisation des propriétés IP des machines virtuelles 92

Personnaliser les propriétés IP pour une machine virtuelle individuelle	93
Signaler les mappages d'adresses IP pour les plans de récupération	94
Personnalisation des propriétés IP pour plusieurs machines virtuelles	95
Syntaxe de l'outil DR IP Customizer	97
Structure du fichier CSV de DR IP Customizer	99
Modification du fichier CSV de DR IP Customizer	102
Exécutez DR IP Customizer pour personnaliser les propriétés IP de plusieurs machines virtuelles	109

9 Configuration avancée Site Recovery Manager 111

Configurer la protection d'une machine virtuelle ou d'un modèle	111
Configurer les mappages de ressources pour une machine virtuelle	113
Spécifier une banque de données non répliquée pour les fichiers d'échange	113
Récupération de machines virtuelles dans plusieurs hôtes sur le site de récupération	114
Redimensionner les fichiers disque de la machine virtuelle pendant la réplication en utilisant des amorces de réplication	115
Redimensionner les fichiers disque de la machine virtuelle pendant la réplication sans utiliser des amorces de réplication	115
Reconfigurer les paramètres de Site Recovery Manager	116
Modifier les paramètres du site local	116
Modifier les paramètres de journalisation	117
Modifier les paramètres de récupération	120
Modifier les paramètres du site distant	122
Modifier le délai d'expiration pour la création de machines virtuelles à espace réservé	122
Modifier les paramètres de stockage	123
Modifier les paramètres du fournisseur de stockage	123
Modifier les paramètres de vSphere Replication	125
Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager	126

10 Dépannage de Site Recovery Manager 131

Limitations de la protection et de la récupération des machines virtuelles	131
Limitations de vSphere Replication	135
Événements et alarmes Site Recovery Manager	135
Contrôle des connexions entre sites par Site Recovery Manager	136

Configurer les alarmes Site Recovery Manager	136
Référence d'événements Site Recovery Manager	137
Événements et alarmes de vSphere Replication	148
Configurer des alarmes vSphere Replication	148
Liste des événements de vSphere Replication	148
Recueillir les fichiers de journalisation Site Recovery Manager	152
Recueillir les fichiers journaux de Site Recovery Manager en utilisant l'interface de Site Recovery Manager	153
Recueillir manuellement les fichiers journaux Site Recovery Manager	154
Accéder aux journaux de vSphere Replication	157
Accéder manuellement aux journaux vSphere Replication	158
Résoudre les problèmes de fonctionnement de Site Recovery Manager	158
Site Recovery Manager double le nombre de barres obliques inverses contenues dans la ligne de commande pendant l'exécution des légendes	158
La mise sous tension simultanée de nombreuses machines virtuelles sur le site de récupération peut entraîner des erreurs	159
Le paramètre LVM.enableResignature=1 est conservé après un basculement test Site Recovery Manager	161
L'ajout de machines virtuelles à un groupe de protection échoue avec une erreur de périphériques non résolue	161
La configuration de la protection échoue avec une erreur de création d'un espace réservé	162
La migration planifiée échoue car l'hôte est dans un état incorrect	163
Échec de la récupération avec erreur de délai d'expiration pendant la personnalisation du réseau de certaines machines virtuelles	163
La récupération échoue avec une erreur de non-disponibilité d'hôte et de banque de données	164
Échec de la reprotection avec une erreur de délai d'attente de vSphere Replication	164
Le plan de récupération arrive à expiration lors de l'attente de VMware Tools	165
Échec de la reprotection après le redémarrage de vCenter Server	165
La réanalyse des banques de données échoue car les périphériques de stockage ne sont pas prêts	166
Problèmes d'évolutivité lors de la réplication de nombreuses machines virtuelles avec un RPO court vers une banque de données VMFS partagée sur ESXi Server 5.0	167
La mise au repos au niveau de l'application devient une mise au repos au niveau du système de fichiers lors d'un déplacement vMotion vers un hôte ancien	168
Reconfigurer la réplication sur des machines virtuelles sans mappage de banque de données	169
La configuration de la réplication échoue avec des machines virtuelles comportant deux disques sur des banques de données différentes	170
vSphere Replication - Violation de RPO	170
vSphere Replication ne démarre pas après le déplacement de l'hôte	171
Une défaillance inattendue de vSphere Replication a donné lieu à une erreur générique	172
La génération de bundles de support interrompt la récupération de vSphere Replication	173

La synchronisation complète initiale des fichiers de machine virtuelle vers le stockage VMware Virtual SAN s'exécute lentement 174

La vitesse d'exécution des opérations de vSphere Replication est inversement proportionnelle au nombre de répliques 174

À propos de l'administration de VMware vCenter Site Recovery Manager

VMware vCenter Site Recovery Manager (Site Recovery Manager) est une extension de VMware vCenter Server qui assure une continuité d'activité et constitue une solution de récupération d'urgence qui vous aide à planifier, tester et exécuter la récupération des machines virtuelles de vCenter Server. Site Recovery Manager peut trouver et gérer des banques de données répliquées et automatiser la migration de l'inventaire d'une instance de vCenter vCenter Server à l'autre.

Public cible

Ce guide est destiné aux administrateurs Site Recovery Manager qui connaissent bien vSphere et ses technologies de réplication, telles que la réplication basée sur l'hôte et les banques de données répliquées. Cette solution répond aux besoins des administrateurs qui souhaitent configurer la protection de leur inventaire vSphere. Elle peut également être appropriée pour les autres utilisateurs devant ajouter des machines virtuelles à un inventaire protégé ou vérifier qu'un inventaire existant est correctement configuré pour une utilisation avec Site Recovery Manager.

Informations mises à jour

L'*administration de Site Recovery Manager* est mise à jour lors de la publication de chaque version du produit ou dès que cela s'avère nécessaire.

Ce tableau présente un historique des mises à jour de l'*administration de Site Recovery Manager*.

Révision	Description
05 août 2020	VMware prend l'intégration au sérieux. Pour encourager ce principe auprès de nos clients, nos partenaires et notre communauté interne, nous remplaçons une partie de la terminologie de notre contenu. Nous avons mis à jour ce guide pour supprimer des éléments de langage ne respectant pas le principe de l'intégration.
001112-07	<ul style="list-style-type: none">■ Ajout de précisions sur l'opération de <code>defaultMaxBootAndShutdownOpsPerCluster</code> et <code>defaultMaxBootAndShutdownOpsPerHost</code> dans Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager.■ Mise à jour de la taille maximale du journal de Serveur Site Recovery Manager dans Modifier la taille et le nombre des fichiers journaux de Serveur Site Recovery Manager.■ Mise à jour des informations sur le délai d'expiration de synchronisation pour vSphere Replication dans les rubriques suivantes<ul style="list-style-type: none">■ Modifier les paramètres de vSphere Replication■ Paramètres pour grands environnements Site Recovery Manager■ Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager■ Échec de la reprotection avec une erreur de délai d'attente de vSphere Replication■ Mise à jour de la description du paramètre <code>allowOtherSolutionTagInRecovery</code> dans Modifier les paramètres de vSphere Replication.
001112-06	Reprotéger les machines virtuelles inclut des instructions sur la vérification de l'historique des plans de récupération d'activité pour les erreurs après reprotection.
001112-05	<ul style="list-style-type: none">■ Correction de la syntaxe de l'outil DR IP Reporter dans Signaler les mappages d'adresses IP pour les plans de récupération.■ Reconfigurer les paramètres de Site Recovery Manager indique que les paramètres avancés ne sont pas conservés lors de la mise à niveau ou après la désinstallation et la réinstallation de la même version du produit.
001112-04	Correction de Utilisation de vSphere Replication avec le stockage Virtual SAN , Configurer la réplication d'une machine virtuelle unique et Configurer la réplication de nombreuses machines virtuelles pour indiquer que l'utilisation de vSphere Replication avec le stockage Virtual SAN est prise en charge sur les sites source et cible.
001112-03	<ul style="list-style-type: none">■ Clarification de l'état des privilèges Site Recovery Manager lors de la désinstallation de Site Recovery Manager dans Référence de rôles Site Recovery Manager.■ Clarification de la situation lors de l'échec des étapes de commande par machine virtuelle dans Gestion des échecs des étapes de récupération personnalisée par Site Recovery Manager.■ Correction des noms d'événements dans Événements de récupération et Événements fournisseur de stockage et stockage.

Révision	Description
001112-02	<ul style="list-style-type: none"> ■ Instructions de support complet ajoutées pour VMware Virtual SAN dans vSphere 5.5u1 et vSphere Replication 5.5.1. ■ Ajout de l'information précisant que Site Recovery Manager n'applique la personnalisation de l'adresse IP qu'au snapshot à un moment spécifique le plus récent dans la section Replication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques et Récupérer un snapshot d'une machine virtuelle à un moment spécifique. ■ Sections ajoutées sur les limites et les snapshots à un moment spécifique à la section Utilisation de vSphere Replication avec le stockage Virtual SAN. ■ Instruction ajoutée selon laquelle vous devez utiliser Client Web vSphere pour configurer vSphere Replication sur le stockage Virtual SAN à la section Configurer la réplication d'une machine virtuelle unique et Configurer la réplication de nombreuses machines virtuelles. ■ Recommandation ajoutée pour configurer vSphere Replication en lots de 30 machines virtuelles lorsque vous utilisez le stockage Virtual SAN à la section Configurer la réplication de nombreuses machines virtuelles. ■ Information ajoutée sur la latence E/S lorsque vous utilisez vSphere Replication avec le stockage Virtual SAN à la section Tester un plan de récupération. ■ Clarification des descriptions des étapes de récupération de commandes à la section Types d'étapes de récupération personnalisée. ■ Énumération des paramètres appliqués à une machine virtuelle au moment où vous configurez la protection à la section Modifier les paramètres de récupération. ■ Nouveaux paramètres avancés ajoutés pour Site Recovery Manager 5.5.1 à la section Modifier les paramètres du fournisseur de stockage.
001112-01	Informations ajoutées sur le compte d'utilisateur dans lequel les étapes de commande s'exécutent dans Types d'étapes de récupération personnalisée .
001112-00	Version initiale.

Rôles, privilèges et autorisations Site Recovery Manager

1

Site Recovery Manager propose une récupération d'urgence en effectuant des opérations pour les utilisateurs. Ces opérations impliquent la gestion des objets, telle que les plans de récupération ou les groupes de protection, et des opérations d'exécution, telles que la réplication ou la mise hors-tension des machines virtuelles. Site Recovery Manager utilise les rôles et les autorisations de sorte que seuls les utilisateurs disposant de rôles et autorisations appropriés puissent effectuer ces opérations.

Site Recovery Manager ajoute plusieurs rôles à vCenter Server. Chaque rôle comporte des privilèges pour effectuer des tâches Site Recovery Manager et vCenter Server. Vous attribuez des rôles à des utilisateurs afin qu'ils puissent effectuer des tâches dans Site Recovery Manager.

Privilège

Le droit d'accomplir une action, par exemple créer un plan de récupération ou modifier un groupe de protection.

Rôle

Un ensemble de privilèges. Les rôles par défaut offrent les privilèges dont ont besoin certains utilisateurs pour effectuer une série de tâches Site Recovery Manager. Il s'agit, par exemple, pour des utilisateurs de gérer des groupes de protection ou effectuer des récupérations. Un utilisateur peut avoir un rôle au maximum dans un objet, mais plusieurs rôles peuvent être combinés si l'utilisateur appartient à plusieurs groupes disposant tous de rôles dans un objet.

Autorisation

Un rôle accordé à un utilisateur particulier ou à un groupe d'utilisateurs dans un objet spécifique. Un utilisateur ou un groupe d'utilisateurs est également appelé un principal. Une autorisation est une combinaison d'un rôle, d'un objet et d'un principal. Par exemple, une autorisation est un privilège permettant de modifier un groupe de protection spécifique.

Pour plus d'informations sur les rôles que Site Recovery Manager ajoute à vCenter Server et sur les privilèges dont ont besoin les utilisateurs pour accomplir des tâches, consultez [Référence de rôles Site Recovery Manager](#).

- [Gestion des autorisations par Site Recovery Manager](#)

Site Recovery Manager détermine si un utilisateur a l'autorisation d'effectuer une opération, telle que la configuration de la protection ou l'exécution des étapes individuelles d'un plan de récupération. Cette vérification d'autorisation permet de s'assurer que les informations d'authentification de l'utilisateur sont correctes, mais elle ne représente pas le contexte de sécurité dans lequel l'opération est effectuée.

- [Site Recovery Manager et le rôle d'administrateur vCenter Server](#)

Si un utilisateur ou un groupe d'utilisateurs possède le rôle d'administrateur vCenter Server sur une instance de vCenter Server lorsque vous installez Site Recovery Manager, il dispose de tous les privilèges Site Recovery Manager.

- [Rôles de Site Recovery Manager et devSphere Replication](#)

Lorsque vous installez vSphere Replication avec Site Recovery Manager, le rôle d'administrateur de vCenter Server hérite de l'ensemble des privilèges Site Recovery Manager et vSphere Replication.

- [Gestion des autorisations dans une configuration de site de récupération partagé](#)

Vous pouvez configurer Site Recovery Manager pour l'utiliser avec un site de récupération partagé. L'administrateur de vCenter Server sur le site de récupération partagé doit gérer les autorisations afin que chaque client dispose de privilèges suffisants pour configurer et utiliser Site Recovery Manager, mais en veillant également à ce qu'aucun client n'ait accès aux ressources appartenant à un autre client.

- [Attribuer des rôles et des autorisations Site Recovery Manager](#)

Pendant l'installation, des droits d'administrateur Site Recovery Manager sont attribués au rôle d'administrateur de vCenter Server. À ce stade, seuls les administrateurs de vCenter Server peuvent se connecter à Site Recovery Manager, sauf s'ils octroient explicitement un droit d'accès à d'autres utilisateurs.

- [Référence de rôles Site Recovery Manager](#)

Site Recovery Manager inclut un ensemble de rôles. Chaque rôle comporte un ensemble de privilèges qui autorisent les utilisateurs disposant de ce rôle à effectuer différentes actions.

Gestion des autorisations par Site Recovery Manager

Site Recovery Manager détermine si un utilisateur a l'autorisation d'effectuer une opération, telle que la configuration de la protection ou l'exécution des étapes individuelles d'un plan de récupération. Cette vérification d'autorisation permet de s'assurer que les informations d'authentification de l'utilisateur sont correctes, mais elle ne représente pas le contexte de sécurité dans lequel l'opération est effectuée.

Site Recovery Manager effectue les opérations dans le contexte de sécurité de l'ID d'utilisateur utilisé pour la connexion aux sites, ou dans le contexte de l'ID sous lequel le service Site Recovery Manager s'exécute, par exemple, l'ID du système local.

Après que Site Recovery Manager a vérifié qu'un utilisateur dispose des autorisations appropriées sur les ressources vSphere cibles, Site Recovery Manager effectue les opérations pour le compte des utilisateurs en utilisant le rôle d'administrateur de vSphere.

Pour les opérations de configuration de la protection sur des machines virtuelles, Site Recovery Manager valide les autorisations de l'utilisateur lorsque ce dernier demande l'opération. Les opérations nécessitent deux phases de validation.

- 1 Pendant la configuration, Site Recovery Manager vérifie que l'utilisateur configurant le système dispose des autorisations appropriées pour effectuer la configuration sur l'objet vCenter Server. Par exemple, un utilisateur doit disposer d'une autorisation pour protéger une machine virtuelle et utiliser les ressources sur l'instance secondaire de vCenter Server que la machine virtuelle récupérée utilise.
- 2 L'utilisateur exécutant la configuration doit disposer des autorisations adéquates pour terminer la tâche qu'il configure. Par exemple, un utilisateur doit avoir les autorisations nécessaires à l'exécution d'un plan de récupération. Site Recovery Manager termine ensuite la tâche pour le compte de l'utilisateur en tant qu'administrateur de vCenter Server.

Comme résultat, un utilisateur qui termine une tâche particulière, comme un récupération, n'a pas nécessairement besoin d'autorisations pour agir sur les ressources vSphere. L'utilisateur a uniquement besoin de l'autorisation d'exécuter une récupération dans Site Recovery Manager. Le rôle autorise l'action, mais l'action est effectuée par Site Recovery Manager, agissant comme administrateur. Site Recovery Manager effectue les opérations en utilisant les informations d'identification d'administrateur fournies lors de la connexion aux sites protégés et de récupération.

Site Recovery Manager maintient une base de données des autorisations pour les objets Site Recovery Manager internes utilisant un modèle similaire à celui employé par vCenter Server. Site Recovery Manager vérifie ses propres privilèges Site Recovery Manager même sur les objets vCenter Server. Par exemple, Site Recovery Manager vérifie l'autorisation **Ressource.Utilisation de reprise** sur la banque de données cible plutôt que de vérifier plusieurs autorisations de bas niveau, par exemple **Allouer espace**. Site Recovery Manager vérifie également les autorisations sur l'instance distante de vCenter Server.

Pour utiliser Site Recovery Manager avec vSphere Replication, vous devez attribuer des rôles vSphere Replication à des utilisateurs ainsi que des rôles Site Recovery Manager. Pour plus d'informations sur les rôles vSphere Replication, reportez-vous à *Administration de vSphere Replication*.

Site Recovery Manager et le rôle d'administrateur vCenter Server

Si un utilisateur ou un groupe d'utilisateurs possède le rôle d'administrateur vCenter Server sur une instance de vCenter Server lorsque vous installez Site Recovery Manager, il dispose de tous les privilèges Site Recovery Manager.

Site Recovery Manager n'effectue pas la vérification des rôles ou des autorisations après l'installation. Si vous attribuez le rôle d'administrateur vCenter Server à des utilisateurs ou des groupes d'utilisateurs après avoir installé Site Recovery Manager, vous devez leur attribuer manuellement les rôles Site Recovery Manager.

Vous pouvez attribuer des rôles Site Recovery Manager à des utilisateurs ou des groupes d'utilisateurs qui ne possèdent pas le rôle d'administrateur vCenter Server. Dans ce cas, ils sont autorisés à effectuer les opérations de Site Recovery Manager, mais pas toutes les opérations de vCenter Server.

Rôles de Site Recovery Manager et vSphere Replication

Lorsque vous installez vSphere Replication avec Site Recovery Manager, le rôle d'administrateur de vCenter Server hérite de l'ensemble des privilèges Site Recovery Manager et vSphere Replication.

Si vous attribuez manuellement un rôle Site Recovery Manager à un utilisateur ou un groupe d'utilisateurs, ou si vous attribuez un rôle Site Recovery Manager à un utilisateur ou un groupe d'utilisateurs qui n'est pas un administrateur de vCenter Server, ces utilisateurs n'héritent pas des privilèges vSphere Replication. Les rôles Site Recovery Manager n'incluent pas les privilèges des rôles vSphere Replication. Par exemple, le rôle d'administrateur de récupération Site Recovery Manager comporte le privilège permettant d'exécuter des plans de récupération, notamment des plans de récupération contenant des groupes de protection vSphere Replication, mais pas celui permettant de configurer vSphere Replication sur une machine virtuelle. La séparation des rôles Site Recovery Manager et des rôles vSphere Replication vous permet de répartir les responsabilités entre différents utilisateurs. Par exemple, un utilisateur possédant le rôle d'administrateur de VRM est responsable de la configuration de vSphere Replication sur des machines virtuelles et un autre utilisateur possédant le rôle d'administrateur de récupération Site Recovery Manager est chargé d'exécuter des récupérations.

Dans certains cas, un utilisateur qui n'est pas un administrateur de vCenter Server peut nécessiter des privilèges pour effectuer des opérations Site Recovery Manager et des opérations vSphere Replication. Pour attribuer une combinaison de rôles Site Recovery Manager et de rôles vSphere Replication à un utilisateur, vous pouvez ajouter ce dernier à deux groupes d'utilisateurs.

Exemple : Attribuer des rôles Site Recovery Manager et des rôles vSphere Replication à un utilisateur

La création de deux groupes d'utilisateurs vous permet d'accorder à un utilisateur les privilèges d'un rôle Site Recovery Manager et d'un rôle vSphere Replication, sans qu'il soit un administrateur de vCenter Server.

- 1 Créez deux groupes d'utilisateurs.
- 2 Attribuez un rôle Site Recovery Manager à un groupe d'utilisateurs, par exemple le rôle d'administrateur de Site Recovery Manager.
- 3 Attribuez un rôle vSphere Replication à l'autre groupe d'utilisateurs (par exemple, administrateur VRM).
- 4 Ajoutez l'utilisateur aux deux groupes d'utilisateurs.

L'utilisateur dispose de l'ensemble des privilèges du rôle d'administrateur de Site Recovery Manager et du rôle d'administrateur de VRM.

Gestion des autorisations dans une configuration de site de récupération partagé

Vous pouvez configurer Site Recovery Manager pour l'utiliser avec un site de récupération partagé. L'administrateur de vCenter Server sur le site de récupération partagé doit gérer les autorisations afin que chaque client dispose de privilèges suffisants pour configurer et utiliser Site Recovery Manager, mais en veillant également à ce qu'aucun client n'ait accès aux ressources appartenant à un autre client.

Dans le contexte d'un site de récupération partagé, un client est le propriétaire d'une paire d'instances de Serveur Site Recovery Manager. Les clients disposant d'autorisations adéquates doivent pouvoir accéder au site de récupération partagé pour créer, tester et exécuter les plans de récupération de leur propre site protégé. L'administrateur de vCenter Server sur le site de récupération partagé doit créer un groupe d'utilisateurs distinct pour chaque client. Aucun compte utilisateur ne peut être membre du groupe Administrateurs de vCenter Server. La seule configuration d'un site de récupération partagé prise en charge permet à une organisation de gérer tous les sites protégés et le site de récupération.

Attention Dans la mesure où certains rôles Site Recovery Manager permettent aux utilisateurs d'exécuter des commandes sur le Serveur Site Recovery Manager, vous devez les attribuer uniquement à des utilisateurs de niveau administrateur de confiance. Reportez-vous à [Référence de rôles Site Recovery Manager](#) pour la liste des rôles Site Recovery Manager qui exécutent des commandes sur le Serveur Site Recovery Manager.

Sur un site de récupération partagé, plusieurs clients partagent une même instance de vCenter Server. Dans certains cas, plusieurs clients peuvent partager un même hôte ESXi sur le site de récupération. Vous pouvez mapper les ressources des sites protégés aux ressources partagées du site de récupération partagé. Vous pouvez partager des ressources sur le site de récupération si vous n'avez pas besoin de conserver toutes les machines virtuelles des clients séparées, dans le cas par exemple où tous les clients appartiennent à une même organisation.

Vous pouvez également créer des ressources isolées sur le site de récupération partagé et mapper les ressources des sites protégés à leurs propres ressources sur le site de récupération partagé. Vous pouvez utiliser cette configuration si vous devez conserver toutes les machines virtuelles des clients séparées les unes des autres, dans le cas par exemple où tous les clients appartiennent à des organisations différentes.

Instructions de partage des ressources des clients

Suivez ces instructions lors de la configuration d'autorisations pour le partage de ressources des clients sur le site de récupération partagé :

- Tous les clients doivent disposer d'un accès en lecture à tous les dossiers du système vCenter Server sur le site de récupération partagé.
- N'accordez pas à un client l'autorisation de renommer, de déplacer ou de supprimer le centre de données ou l'hôte.
- N'accordez pas à un client l'autorisation de créer des machines virtuelles en dehors des dossiers et des pools de ressources qui lui sont dédiés.
- N'autorisez pas un client à modifier des rôles ou à attribuer des autorisations pour des objets qui ne sont pas dédiés à son propre usage.
- Pour empêcher la propagation non désirée d'autorisations entre différentes ressources d'organisation, ne propagez pas les autorisations dans le dossier racine, les centres de données et les hôtes du système vCenter Server sur le site de récupération partagé.

Instructions d'isolement des ressources des clients

Lors de la configuration d'autorisations dans le but d'isoler les ressources des clients sur le site de récupération partagé, procédez comme suit :

- Attribuez à chaque client un dossier de machine virtuelle distinct dans l'inventaire vCenter Server.
 - Définissez des autorisations sur ce dossier de manière à empêcher tout autre client d'y placer ses machines virtuelles. Par exemple, définissez le rôle Administrateur et activez l'option de propagation d'un client sur ce dossier. Cette configuration permet d'empêcher les erreurs de noms dupliqués susceptibles de se produire si plusieurs clients protègent des machines virtuelles portant des noms identiques.
 - Placez dans ce dossier toutes les machines virtuelles à espace réservé du client, afin qu'elles puissent hériter de ses autorisations.

- N'attribuez pas à d'autres clients des autorisations d'accès à ce dossier.
- Attribuez des pools de ressources, des banques de données et des réseaux dédiés à chaque client, et configurez les autorisations de la même manière que pour des dossiers.

Affichage de tâches et d'événements dans une configuration de site de récupération partagé

Dans le panneau Tâches récentes de vSphere Client, les utilisateurs autorisés à afficher un objet peuvent voir les tâches que d'autres utilisateurs démarrent sur cet objet. Tous les clients peuvent voir toutes les tâches que d'autres utilisateurs effectuent sur une ressource partagée. Par exemple, tous les utilisateurs peuvent voir les tâches qui s'exécutent sur un hôte partagé, un centre de données ou le dossier racine de vCenter Server.

Les événements que toutes les instances du Serveur Site Recovery Manager génèrent sur un site de récupération partagé ont des autorisations identiques. Tous les utilisateurs qui peuvent voir les événements d'une instance du Serveur Site Recovery Manager peuvent voir les événements de toutes les instances du Serveur Site Recovery Manager qui s'exécutent sur le site de récupération partagé.

Attribuer des rôles et des autorisations Site Recovery Manager

Pendant l'installation, des droits d'administrateur Site Recovery Manager sont attribués au rôle d'administrateur de vCenter Server. À ce stade, seuls les administrateurs de vCenter Server peuvent se connecter à Site Recovery Manager, sauf s'ils octroient explicitement un droit d'accès à d'autres utilisateurs.

Afin d'autoriser les autres utilisateurs à accéder à Site Recovery Manager, les administrateurs vCenter Server doivent leur accorder les autorisations sur l'interface Site Recovery Manager. Les attributions d'autorisation s'appliquent par site. Vous devez ajouter les autorisations correspondantes sur les deux sites.

Site Recovery Manager exige des autorisations sur les objets vCenter Server ainsi que sur les objets Site Recovery Manager. Pour configurer des autorisations sur l'installation à distance de vCenter Server, démarrez une autre instance de vSphere Client. Après avoir connecté le site protégé et le site de récupération, vous pouvez modifier les autorisations Site Recovery Manager dans la même interface sur les deux sites.

Site Recovery Manager augmente les rôles et autorisations de vCenter Server avec des autorisations supplémentaires qui permettent un contrôle détaillé des tâches et opérations propres à Site Recovery Manager. Pour plus d'informations sur les autorisations de chaque rôle Site Recovery Manager, consultez [Référence de rôles Site Recovery Manager](#).

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, puis sélectionnez le site auquel attribuer les autorisations.

- 2 Cliquez sur l'onglet **Autorisations**.
- 3 Cliquez avec le bouton droit de la souris à n'importe quel endroit du panneau pour le site local ou le site distant et sélectionnez **Ajouter autorisation**.
- 4 Cliquez sur **Ajouter**.
- 5 Identifier un utilisateur ou un groupe pour le rôle.
 - a Dans le menu déroulant **Domaine**, sélectionnez le domaine qui contient l'utilisateur ou le groupe.
 - b Entrez un nom d'utilisateur ou de groupe d'utilisateurs dans la zone de texte **Rechercher** ou sélectionnez un nom dans la liste **Nom**.
 - c Cliquez sur **Ajouter** et cliquez sur **OK**.
- 6 Dans le menu déroulant **Rôle assigné**, sélectionnez un rôle à attribuer à l'utilisateur ou au groupe d'utilisateurs que vous avez sélectionné.

Le menu déroulant **Rôle assigné** inclut l'ensemble des rôles rendus disponibles par vCenter Server et ses plug-ins. Site Recovery Manager ajoute plusieurs rôles à vCenter Server.

Option	Action
Autoriser un utilisateur ou un groupe d'utilisateurs à effectuer toutes les opérations de configuration et d'administration de Site Recovery Manager.	Attribuer le rôle Administrateur Site Recovery Manager.
Autoriser un utilisateur ou un groupe d'utilisateurs à gérer et modifier des groupes de protection et à configurer la protection sur des machines virtuelles.	Attribuer le rôle Administrateur de groupes de protection Site Recovery Manager.
Autoriser un utilisateur ou un groupe d'utilisateurs à effectuer des récupérations et à tester des récupérations.	Attribuer le rôle Administrateur de récupération Site Recovery Manager.
Autoriser un utilisateur ou un groupe d'utilisateurs à créer, modifier et tester des plans de récupération.	Attribuer le rôle Administrateur de plans de récupération Site Recovery Manager.
Autoriser un utilisateur ou un groupe d'utilisateurs à tester des plans de récupération.	Attribuer le rôle Administrateur de tests de récupération Site Recovery Manager.

Lorsque vous sélectionnez un rôle, une liste hiérarchique affiche les privilèges de ce rôle. Cliquez sur un privilège de la liste hiérarchique pour voir sa description. Vous ne pouvez pas modifier la liste des privilèges de ce rôle.

- 7 Sélectionnez **Propager vers les objets enfants** pour appliquer le rôle sélectionné à tous les objets enfants des objets d'inventaire susceptibles d'être affectés par ce rôle.

Par exemple, si un rôle contient des privilèges pour modifier des dossiers, la sélection de cette option permet d'étendre les privilèges à toutes les machines virtuelles d'un dossier. Vous pouvez désactiver cette option pour créer une hiérarchie d'autorisations plus complexe. Par exemple, désactivez cette option pour remplacer les autorisations propagées à partir de la racine d'un certain nœud dans l'arborescence de la hiérarchie, mais sans remplacer les autorisations des objets enfants de ce nœud.

- 8 Cliquez sur **OK** pour attribuer le rôle et ses privilèges associés à l'utilisateur ou au groupe d'utilisateurs.
- 9 Répétez les étapes [Étape 1](#) à [Étape 8](#) pour attribuer des rôles et des privilèges aux utilisateurs ou groupes d'utilisateurs sur l'autre site Site Recovery Manager.

Résultats

Vous avez attribué un rôle Site Recovery Manager donné à un utilisateur ou à un groupe d'utilisateurs. Cet utilisateur ou ce groupe d'utilisateurs dispose de privilèges pour effectuer les actions définies par le rôle sur les objets du site Site Recovery Manager que vous avez configuré.

Exemple : Combinaison de rôles Site Recovery Manager

Vous ne pouvez attribuer qu'un seul rôle à un utilisateur ou à un groupe d'utilisateurs. Si un utilisateur, qui n'est pas administrateur de vCenter Server, doit disposer des privilèges de plusieurs rôles Site Recovery Manager, vous pouvez créer plusieurs groupes d'utilisateurs. Par exemple, un utilisateur peut avoir besoin des privilèges permettant de gérer et d'exécuter des plans de récupération.

- 1 Créez deux groupes d'utilisateurs.
- 2 Attribuez le rôle Administrateur de plans de récupération Site Recovery Manager à un groupe.
- 3 Attribuez le rôle Administrateur de récupération Site Recovery Manager à l'autre groupe.
- 4 Ajoutez l'utilisateur aux deux groupes d'utilisateurs.

En étant membre des groupes qui disposent tous les deux des rôles Administrateur de plans de récupération Site Recovery Manager et Administrateur de récupération Site Recovery Manager, l'utilisateur peut gérer des plans de récupération et exécuter des récupérations.

Référence de rôles Site Recovery Manager

Site Recovery Manager inclut un ensemble de rôles. Chaque rôle comporte un ensemble de privilèges qui autorisent les utilisateurs disposant de ce rôle à effectuer différentes actions.

Les rôles peuvent avoir des groupes de privilèges et d'actions qui se chevauchent. Par exemple, le rôle d'administrateur de Site Recovery Manager et l'administrateur de groupes de protection de Site Recovery Manager disposent du privilège **Créer** pour des groupes de protection. L'utilisateur disposant de ce privilège peut effectuer une partie du groupe de tâches qui constituent la gestion des groupes de protection.

Attribuez uniformément des rôles aux utilisateurs sur les objets Site Recovery Manager sur les deux sites, afin que les objets protégés et les objets de récupération disposent des mêmes autorisations.

Tous les utilisateurs doivent disposer au minimum du privilège **Système.Lecture** sur les dossiers racine de vCenter Server et les nœuds racine Site Recovery Manager sur les deux sites.

Note Si vous désinstallez Serveur Site Recovery Manager, Site Recovery Manager supprime les rôles Site Recovery Manager par défaut, mais les privilèges Site Recovery Manager sont conservés. Vous pouvez toujours consulter les privilèges Site Recovery Manager et les attribuer à d'autres rôles après la désinstallation de Site Recovery Manager. Il s'agit du comportement standard de vCenter Server. Les privilèges ne sont pas supprimés lorsque vous désinscrivez une extension dans vCenter Server.

Tableau 1-1. Rôles Site Recovery Manager

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
Administrateur de Site Recovery Manager	<p>L'administrateur de Site Recovery Manager accorde l'autorisation d'effectuer toutes les opérations d'administration et de configuration de Site Recovery Manager.</p> <ul style="list-style-type: none"> ■ Configurer les paramètres avancés. ■ Configurer les connexions. ■ Configurer des préférences d'inventaire. ■ Configurer les banques de données à espace réservé. ■ Configurez les gestionnaires de baies. ■ Gérer les groupes de protection. ■ Gérer les plans de récupération. ■ Effectuer des opérations de reprotection. ■ Configurer la protection sur les machines virtuelles. ■ Modifier les groupes de protection. ■ Supprimer des groupes de protection. <p>Les utilisateurs disposant de ce rôle ne peuvent pas exécuter des récupérations. Seuls les utilisateurs disposant du rôle Administrateur de récupération Site Recovery Manager peuvent effectuer des récupérations.</p>	<p>Site Recovery Manager.Paramètres avancés.Modifier</p> <p>Site Recovery Manager.Gestionnaire de baies.Configurer</p> <p>Site Recovery Manager.Diagnostics.Exporter</p> <p>Site Recovery Manager.Préférences d'inventaire.Modifier</p> <p>Site Recovery Manager.Banques de données réservée.Configurer</p> <p>Site Recovery Manager.Diagnostics Exporter</p> <p>Site Recovery Manager.Groupe de protection.Attribuer au plan</p> <p>Site Recovery Manager.Groupe de protection.Créer</p> <p>Site Recovery Manager.Groupe de protection.Modifier</p> <p>Site Recovery Manager.Groupe de protection.Supprimer</p> <p>Site Recovery Manager.Groupe de protection.Supprimer du plan</p> <p>Site Recovery Manager.Historique de récupération.Afficher les plans supprimés</p> <p>Site Recovery Manager.Plan de récupération.Configurer</p> <p>Site Recovery Manager.Plan de récupération.Créer</p>	<ul style="list-style-type: none"> ■ Machines virtuelles ■ Banques de données ■ Dossiers vCenter Server ■ Pools de ressources ■ Instances de service Site Recovery Manager ■ Réseaux ■ Dossiers Site Recovery Manager ■ Groupes de protection ■ Plans de récupération ■ Gestionnaire des baies

Tableau 1-1. Rôles Site Recovery Manager (suite)

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
		Site Recovery Manager.Plan de récupération.Modifier Site Recovery Manager.Plan de récupération.Supprimer Site Recovery Manager.Plan de récupération.Reprotéger Site Recovery Manager.Plan de récupération.Tester Site Recovery Manager.Site distant.Modifier Banque de données.Réplication.Protéger Banque de données.Réplication.Ôter la protection Ressource.Utilisation de la récupération Machine virtuelle.Protection SRM.Protéger Machine virtuelle.Protection SRM.Arrêter	
Administrateur de groupes de protection Site Recovery Manager	Le rôle de l'administrateur de groupes de protection Site Recovery Manager permet aux utilisateurs de gérer des groupes de protection. <ul style="list-style-type: none"> ■ Créez des groupes de protection. ■ Modifier des groupes de protection. ■ Ajouter des machines virtuelles aux groupes de protection. ■ Supprimer des groupes de protection. ■ Configurer la protection sur les machines virtuelles. ■ Supprimer la protection des machines virtuelles. 	Site Recovery Manager.Groupe de protection.Créer Site Recovery Manager.Groupe de protection.Modifier Site Recovery Manager.Groupe de protection.Supprimer Banque de données.Réplication.Protéger Banque de données.Réplication.Ôter la protection Ressource.Utilisation de la récupération	<ul style="list-style-type: none"> ■ Dossiers Site Recovery Manager ■ Groupes de protection

Tableau 1-1. Rôles Site Recovery Manager (suite)

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
	Les utilisateurs disposant de ce rôle ne peuvent ni effectuer ou tester des récupérations, ni créer ou modifier des plans de récupération.	Machine virtuelle. Protection SRM.Protéger Machine virtuelle. Protection SRM.Arrêter	
Administrateur de récupération Site Recovery Manager	<p>Le rôle de l'administrateur de récupération Site Recovery Manager permet aux utilisateurs d'effectuer des opérations de reprotection et de récupération.</p> <ul style="list-style-type: none"> ■ Supprimer des groupes de protection des plans de récupération. ■ Tester les plans de récupération. ■ Exécuter des plans de récupération. ■ Exécuter des opérations de reprotection. ■ Configurer des étapes de commande personnalisée sur des machines virtuelles. ■ Afficher les plans de récupération supprimés. ■ Modifier les propriétés de récupération des machines virtuelles. <p>Les utilisateurs disposant de ce rôle ne peuvent ni configurer la protection sur les machines virtuelles, ni créer ou modifier des plans de récupération.</p>	<p>Site Recovery Manager.Groupe de protection.Supprimer du plan</p> <p>Site Recovery Manager.Plan de récupération.Modifier</p> <p>Site Recovery Manager.Plan de récupération.Tester</p> <p>Site Recovery Manager.Plan de récupération.Récupération</p> <p>Site Recovery Manager.Plan de récupération.Reprotéger</p> <p>Site Recovery Manager.Plan de récupération.Configurer les commandes</p> <p>Site Recovery Manager.Historique de récupération.Afficher les plans supprimés</p>	<ul style="list-style-type: none"> ■ Groupes de protection ■ Plans de récupération ■ Instances de service Site Recovery Manager

Tableau 1-1. Rôles Site Recovery Manager (suite)

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
Administrateur de plans de récupération Site Recovery Manager	<p>Le rôle Administrateur de plans de récupération Site Recovery Manager autorise les utilisateurs à créer et tester des plans de récupération.</p> <ul style="list-style-type: none"> ■ Ajouter des groupes de protection aux plans de récupération. ■ Supprimer des groupes de protection des plans de récupération. ■ Configurer des étapes de commande personnalisée sur des machines virtuelles. ■ Créez des plans de récupération. ■ Tester les plans de récupération. ■ Annuler des tests de plans de récupération. ■ Modifier les propriétés de récupération des machines virtuelles. <p>Les utilisateurs disposant de ce rôle ne peuvent ni configurer la protection sur les machines virtuelles, ni effectuer des opérations de récupération ou de reprotction.</p>	<p>Site Recovery Manager.Groupe de protection.Attribuer au plan</p> <p>Site Recovery Manager.Groupe de protection.Supprimer du plan</p> <p>Site Recovery Manager.Plan de récupération.Configurer les commandes</p> <p>Site Recovery Manager.Plan de récupération.Créer</p> <p>Site Recovery Manager.Plan de récupération.Modifier</p> <p>Site Recovery Manager.Plan de récupération.Supprimer</p> <p>Site Recovery Manager.Plan de récupération.Tester</p> <p>Ressource.Utilisation de la récupération</p>	<ul style="list-style-type: none"> ■ Groupes de protection ■ Plans de récupération ■ Dossiers vCenter Server ■ Banques de données ■ Pools de ressources ■ Réseaux
Administrateur de test Site Recovery Manager	<p>Le rôle Administrateur de tests Site Recovery Manager autorise uniquement les utilisateurs à tester des plans de récupération.</p> <ul style="list-style-type: none"> ■ Tester les plans de récupération. ■ Annuler des tests de plans de récupération. ■ Modifier les propriétés de récupération des machines virtuelles. <p>Les utilisateurs disposant de ce rôle ne peuvent ni configurer la protection sur les machines virtuelles, ni créer des groupes</p>	<p>Site Recovery Manager.Plan de récupération.Modifier</p> <p>Site Recovery Manager.Plan de récupération.Tester</p>	Plans de récupération

Tableau 1-1. Rôles Site Recovery Manager (suite)

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
	de protection ou des plans de récupération, ni effectuer des opérations de récupération ou de reprotection.		

Référence de rôles vSphere Replication

vSphere Replication inclut un ensemble de rôles. Chaque rôle inclut un groupe de privilèges qui permettent aux utilisateurs disposant de ces rôles d'exécuter des actions différentes.

Note Lorsque vous attribuez des autorisations sans propagation, assurez-vous de disposer au moins de l'autorisation de lecture seule pour tous les objets parents.

Tableau 1-2. Rôles de vSphere Replication

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
Visionneuse de réplication VRM	<ul style="list-style-type: none"> Afficher les réplifications. Impossible de changer les paramètres de réplication. 	VRM distant.Afficher VR VRM distant.Afficher VRM Mappeur de banque de données VRM.Affichage Hôte.vSphere Replication.Gérer la réplication Machine virtuelle.vSphere Replication.Surveiller la réplication	Dossier racine de vCenter Server avec propagation, sur le site source (réplifications sortantes) et le site cible (réplifications entrantes). Ou dossier racine de vCenter Server sans propagation sur les deux sites et machine virtuelle sans propagation sur le site source.
Utilisateur de réplication de machine virtuelle VRM	<ul style="list-style-type: none"> Afficher les réplifications. Gérer les banques de données. Configurer et annuler la configuration des réplifications. Gérer et surveiller les réplifications. <p>Nécessite un utilisateur correspondant disposant du même rôle sur le site cible et un rôle d'utilisateur de banque de données cible vSphere Replication supplémentaire sur le centre de données cible, le dossier de banque de données ou chaque banque de données cible.</p>	Banque de données.Parcourir la banque de données VRM distant.Afficher VR VRM distant.Afficher VRM Mappeur de banque de données VRM.Gérer Mappeur de banque de données VRM.Affichage Hôte.vSphere Replication.Gérer la réplication Machine virtuelle.vSphere Replication.Configurer la réplication Machine virtuelle.vSphere Replication.Gérer la réplication Machine virtuelle.vSphere Replication.Surveiller la réplication	Dossier racine de vCenter Server avec propagation sur les deux sites. Ou dossier racine de vCenter Server sans propagation sur les deux sites, machine virtuelle sans propagation sur le site source, banques de données source sans propagation sur le site source.

Tableau 1-2. Rôles de vSphere Replication (suite)

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
Administrateur VRM	Englobe tous les privilèges de vSphere Replication.	VRM distant.Gérer VR VRM distant.Afficher VR VRM distant.Gérer VRM VRM distant.Afficher VRM Mappeur de banque de données VRM.Gérer Mappeur de banque de données VRM.Affichage Diagnostics de VRM .Gérer Session VRM .Terminer Banque de données.Parcourir la banque de données Banque de données.Opérations de fichier de niveau bas Hôte.vSphere Replication.Gérer la réplication Ressource.Attribuer une machine virtuelle au pool de ressources Machine virtuelle.Configuration.Ajouter un disque existant Machine virtuelle.Configuration.Ajouter ou supprimer un périphérique Machine virtuelle.Interaction.Mettre sous tension Machine virtuelle.Interaction.Connexion de périphérique Machine virtuelle.Inventaire .Registre Machine virtuelle.vSphere Replication.Configurer la réplication Machine virtuelle.vSphere Replication.Gérer la réplication Machine virtuelle.vSphere Replication.Surveiller la réplication	Dossier racine de vCenter Server avec propagation sur les deux sites. Ou dossier racine de vCenter Server sans propagation sur les deux sites, machine virtuelle sans propagation sur le site source, banque de données cible, dossier de machine virtuelle cible avec propagation sur le site cible, hôte ou cluster cible avec propagation sur le site cible.
Diagnostics de VRM	Générer, récupérer et supprimer des bundles de journaux.	VRM distant.Afficher VR VRM distant.Afficher VRM Diagnostics de VRM .Gérer	Dossier racine de vCenter Server sur les deux sites.

Tableau 1-2. Rôles de vSphere Replication (suite)

Rôle	Actions autorisées par le rôle	Privilèges inclus dans le rôle	Objets de l'inventaire de vCenter Server auxquels le rôle peut accéder
Utilisateur de banque de données VRM cible	Configurer et reconfigurer des répliquions. Utilisé sur le site cible en combinaison avec le rôle d'utilisateur de répliquion de machine virtuelle VRM sur les deux sites.	Banque de données.Parcourir la banque de données Banque de données.Opérations de fichier de niveau bas	Objets de banque de données sur le site cible ou dossier de banque de données avec propagation sur le site cible ou centre de données cible avec propagation.
Utilisateur de récupération de machine virtuelle VRM	Récupérer les machines virtuelles.	Banque de données.Parcourir la banque de données Banque de données.Opérations de fichier de niveau bas Hôte.vSphere Replication.Gérer la répliquion Machine virtuelle.Configuration.Ajouter un disque existant Machine virtuelle.Configuration.Ajouter ou supprimer un périphérique Machine virtuelle.Interaction.Mettre sous tension Machine virtuelle.Interaction.Connexion de périphérique Machine virtuelle.Inventaire .Registre Ressource.Attribuer une machine virtuelle au pool de ressources	Dossier racine secondaire de vCenter Server avec propagation. Ou dossier racine secondaire de vCenter Server sans propagation, banque de données cible sans propagation, dossier de machine virtuelle cible avec propagation, hôte ou cluster cible avec propagation.

Réplication de machines virtuelles

2

Avant de créer des groupes de protection, vous devez configurer la réplication sur les machines virtuelles à protéger.

Vous pouvez répliquer des machines virtuelles en utilisant une réplication basée sur la baie, vSphere Replication ou les deux.

Ces informations concernent la réplication effectuée à l'aide de vSphere Replication. Pour configurer une réplication basée sur la baie sur des machines virtuelles, référez-vous à la documentation disponible auprès du fournisseur du gestionnaire de baies de stockage (SRA).

Ce chapitre contient les rubriques suivantes :

- [Impact de la valeur de l'objectif de point de récupération sur la planification de la réplication](#)
- [Réplication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques](#)
- [Utilisation de vSphere Replication avec le stockage Virtual SAN](#)
- [Configurer la réplication d'une machine virtuelle unique](#)
- [Configurer la réplication de nombreuses machines virtuelles](#)
- [Répliquer des machines virtuelles en utilisant des amorces de réplication](#)
- [Reconfigurer des réplifications](#)
- [Arrêter la réplication d'une machine virtuelle](#)

Impact de la valeur de l'objectif de point de récupération sur la planification de la réplication

La valeur de l'objectif de point de récupération (RPO) que vous avez définie lors de la configuration de la réplication affecte la planification de la réplication.

Un RPO de x minutes signifie que l'instance de réplication disponible la plus récente ne peut jamais refléter un état datant de plus de x minutes. Une instance de réplication reflète l'état d'une machine virtuelle au moment où la réplication commence.

Le RPO est réglé sur 15 minutes lors de la configuration de la réplication. Si la réplication commence à 12:00 et que cinq minutes sont nécessaires pour le transfert vers le site secondaire, l'instance sera disponible à 12:05, mais elle reflétera l'état de la machine virtuelle à 12:00. La réplication suivante commencera au plus tard à 12:10. Cette instance de réplication sera alors disponible à 12:15 lorsque la première instance de réplication qui a commencé à 12:00 aura expiré.

Si vous avez réglé le RPO sur 15 minutes et que le transfert de la réplication dure 7 minutes 30, vSphere Replication transfère une instance en permanence. Si la réplication dure plus de 7 minutes 30, des violations RPO périodiques se produiront. Par exemple, si la réplication commence à 12:00 et que le transfert d'une instance dure 10 minutes, la réplication se terminera à 12:10. Vous pourrez immédiatement commencer une nouvelle réplication, mais elle se terminera à 12:20. Pendant l'intervalle de temps entre 12:15 et 12:20, une violation RPO se produira car l'instance disponible la plus récente aura commencé à 12:00 et sera trop ancienne.

Le planificateur de réplication essaye de répondre à ces contraintes en chevauchant les réplications afin d'optimiser la consommation de bande passante, et il est possible qu'il commence les réplications de certaines machines virtuelles plus tôt que prévu.

Pour déterminer le temps de transfert de la réplication, le planificateur de réplication utilise la durée des quelques dernières instances pour estimer la durée de la suivante.

Replication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques

Vous pouvez récupérer les machines virtuelles à différents moments spécifiques (PIT), par exemple lors du dernier état cohérent connu.

Note Vous ne pouvez pas utiliser l'interface de Site Recovery Manager pour configurer une réplication qui utilise des snapshots à un moment précis (PIT). Pour activer les snapshots PIT, configurez la réplication d'une machine virtuelle à l'aide de Client Web vSphere. Reportez-vous à [Configurer la réplication d'une machine virtuelle unique](#) dans *Administration de vSphere Replication*.

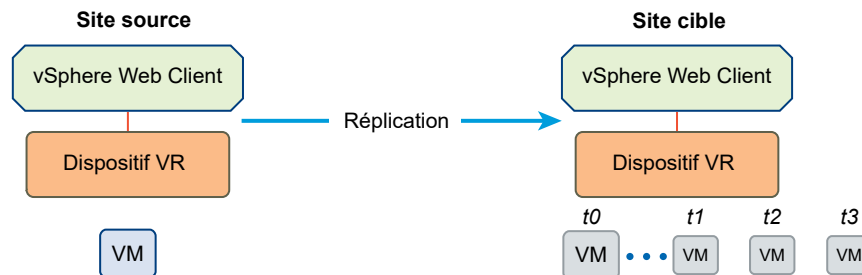
Lorsque vous configurez la réplication d'une machine virtuelle, vous pouvez activer des instances à plusieurs moments spécifiques (PIT) dans les paramètres de récupération de l'assistant de configuration de la réplication. vSphere Replication conserve un certain nombre d'instances de snapshots de machine virtuelle sur le site cible en fonction de la stratégie de rétention que vous avez spécifiée. vSphere Replication prend en charge un maximum de 24 instances de snapshots. Après avoir récupéré une machine virtuelle, vous pouvez la restaurer à un snapshot spécifique.

Au cours de la réplication, vSphere Replication réplique tous les aspects de la machine virtuelle vers le site cible, y compris les éventuels virus et applications endommagées. Si une machine virtuelle contient un virus ou une application endommagée et que vous avez configuré vSphere Replication pour qu'il conserve des snapshots à des moments spécifiques, vous pouvez récupérer la machine virtuelle et la restaurer à l'un de ses snapshots dans un état correct.

Vous pouvez également utiliser les instances à des moments spécifiques pour récupérer le dernier état correct connu d'une base de données.

Note vSphere Replication ne réplique pas les snapshots des machines virtuelles.

Figure 2-1. Récupération d'une machine virtuelle à différents moments spécifiques (PIT)



Au cours d'une récupération, Site Recovery Manager ne récupère que le snapshot du moment spécifique le plus récent. Pour récupérer des snapshots plus anciens, vous devez activer l'option **vrReplication > preserveMpitImagesAsSnapshots** sous **Paramètres avancés** dans l'interface de Site Recovery Manager. Reportez-vous à [Modifier les paramètres de vSphere Replication](#).

Pour récupérer une machine virtuelle à partir d'un snapshot à un moment spécifique plus ancien, vous devez restaurer manuellement la machine virtuelle à ce snapshot après la récupération. Reportez-vous à [Récupérer un snapshot d'une machine virtuelle à un moment spécifique](#).

Si vous récupérez un snapshot PIT d'une machine virtuelle pour laquelle vous avez configuré la personnalisation IP, Site Recovery Manager applique uniquement la personnalisation au snapshot PIT le plus récent. Si vous récupérez un ancien snapshot PIT d'une machine virtuelle avec la personnalisation IP, vous devez configurer manuellement les paramètres IP.

Utilisation de vSphere Replication avec le stockage Virtual SAN

Vous pouvez utiliser les banques de données VMware Virtual SAN en tant que banques de données sources et cibles lors de la configuration des répliquations. Suivez les instructions ci-dessous lorsque vous utilisez vSphere Replication avec le stockage Virtual SAN.

Note VMware Virtual SAN est une fonctionnalité entièrement prise en charge de vSphere 5.5u1.

- Vous pouvez utiliser Virtual SAN dans des environnements de production avec vSphere Replication 5.5.1 et vSphere 5.5u1.
- Virtual SAN est une fonctionnalité expérimentale dans vSphere 5.5. Vous pouvez effectuer des tests à l'aide de Virtual SAN dans vSphere Replication 5.5.0 et vSphere 5.5, mais cette fonctionnalité n'est pas prise en charge pour une utilisation dans des environnements de production. Pour obtenir des informations sur l'activation de Virtual SAN dans vSphere 5.5, reportez-vous aux notes de mise à jour de vSphere Replication 5.5.0.

vSphere Replication ne prend en charge ni la réplication ni la récupération des machines virtuelles dans les dossiers racines portant un nom convivial dans les banques de données Virtual SAN. Ces noms sont susceptibles de changer, ce qui génère des erreurs de réplication. Lors de la sélection des banques de données Virtual SAN, sélectionnez toujours des dossiers portant un nom UUID qui ne change pas.

Configuration des réplications

Lors de la configuration des réplications pour une machine virtuelle unique, vSphere Replication crée le dossier de destination de votre choix, obtient la référence UUID de ce dossier, puis utilise le nom UUID à la place du nom convivial. Le nom UUID est visible au moment où vSphere Replication affiche les dossiers cibles lors de la reconfiguration des réplications.

Lorsque vous configurez la réplication pour plusieurs machines virtuelles, créez un dossier racine dans la banque de données Virtual SAN, récupérez son nom UUID et utilisez le dossier identifié par cet UUID dans l'assistant de réplication.

Configurez vSphere Replication sur des lots incluant un nombre maximal de 30 machines virtuelles à la fois.

Configuration des réplications en utilisant des amorces de réplication

Lors de la copie des fichiers d'amorce de réplication dans la banque de données cible, vous pouvez utiliser Client Web vSphere pour créer un nouveau dossier racine dans une banque de données Virtual SAN ou placer les fichiers dans un dossier existant. Lorsque vous configurez des réplications qui utilisent des amorces de réplication, vous devez sélectionner le dossier à l'aide de son nom UUID. La sélection des noms de dossiers conviviaux n'est pas prise en charge.

Reconfiguration des réplications

Si vous souhaitez modifier le dossier de destination d'un disque ou les fichiers de configuration d'une machine virtuelle, vous devez effectuer les opérations suivantes :

- Sélectionner le nom UUID d'un dossier existant.
- Autoriser vSphere Replication à créer un dossier et à obtenir son nom UUID.

Limites de l'utilisation de vSphere Replication avec le stockage Virtual SAN

Pour des raisons de charge et de latence E/S, le stockage Virtual SAN est soumis à des limites en termes de nombre d'hôtes susceptibles d'intégrer un cluster Virtual SAN et de nombre de machines virtuelles pouvant être exécutées sur chaque hôte. Reportez-vous à la section Limites du *Guide de dimensionnement et de conception de VMware Virtual SAN*, disponible à la page suivante : <http://www.vmware.com/products/virtual-san/resources.html>.

L'utilisation de vSphere Replication augmente la charge sur le stockage. Chaque machine virtuelle génère régulièrement des opérations de lecture et d'écriture. La configuration de vSphere Replication sur ces machines virtuelles ajoute une opération de lecture aux opérations de lecture et d'écriture standard, ce qui augmente la latence E/S sur le stockage. Le nombre exact de machines virtuelles susceptibles d'être répliquées sur le stockage Virtual SAN à l'aide de vSphere Replication dépend de votre infrastructure. Si vous remarquez un ralentissement des temps de réponse lors de la configuration de vSphere Replication pour des machines virtuelles sur le stockage Virtual SAN, surveillez la latence E/S de l'infrastructure Virtual SAN. Essayez de réduire le nombre de machines virtuelles répliquées dans la banque de données Virtual SAN.

Conservation des snapshots à un moment donné lors de l'utilisation du stockage Virtual SAN

Le stockage Virtual SAN stocke les fichiers de disque de machine virtuelle sous forme d'ensemble d'objets et de composants. Chaque objet de disque présent sur le stockage Virtual SAN est associé à des objets miroirs et témoins. Dans la stratégie de stockage Virtual SAN par défaut, un objet de disque est associé à deux miroirs et à un témoin. Le nombre de composants miroirs dépend de la taille du disque de machine virtuelle et du nombre d'échecs à tolérer défini dans la stratégie du stockage Virtual SAN. Un objet miroir se divise en composants dont la taille maximale respective est de 256 Go.

- Si une machine virtuelle possède un disque de 256 Go et que vous utilisez la stratégie par défaut du stockage Virtual SAN, l'objet de disque sera associé à deux composants miroirs de 256 Go chacun et à un composant témoin, soit à un total de trois composants.
- Si une machine virtuelle possède un disque de 512 Go et que vous utilisez la stratégie par défaut du stockage Virtual SAN, l'objet de disque sera associé à quatre composants miroirs de 256 Go chacun et à un composant témoin, soit à un total de cinq composants.

Pour plus d'informations sur les objets, les composants, les miroirs, les témoins et les stratégies de stockage Virtual SAN, reportez-vous au *Guide de dimensionnement et de conception de VMware Virtual SAN*, disponible à la page suivante : <http://www.vmware.com/products/virtual-san/resources.html>.

Si vous utilisez plusieurs snapshots à un moment donné (snapshots PIT, point-in-time), vous devez prendre en compte les composants supplémentaires créés par chacun des snapshots sur le stockage Virtual SAN, en fonction du nombre de disques par machine virtuelle, de la taille de ces disques, du nombre de snapshots PIT à conserver et du nombre d'échecs à tolérer. Si vous conservez des snapshots PIT et que vous utilisez le stockage Virtual SAN, vous devez calculer le nombre de composants supplémentaires nécessaires pour chaque machine virtuelle :

Nombre de disques x nombre de snapshots PIT x nombre de composants miroirs et témoins

Les exemples d'application de cette formule démontrent que la conservation de snapshots PIT fait rapidement augmenter le nombre de composants dans le stockage Virtual SAN pour chaque machine virtuelle configurée pour vSphere Replication :

- Vous utilisez une machine virtuelle possédant deux disques de 256 Go, pour laquelle vous conservez dix snapshots à un moment donné, et vous configurez la stratégie par défaut du stockage Virtual SAN :
 - $2 \text{ (nombre de disques)} \times 10 \text{ (nombre de snapshots PIT)} \times 3 \text{ (2 composants miroirs + 1 témoin)} = 60 \text{ composants uniquement pour cette machine virtuelle.}$
- Vous utilisez une machine virtuelle possédant deux disques de 512 Go, pour laquelle vous conservez dix snapshots à un moment donné, et vous configurez la stratégie par défaut du stockage Virtual SAN :
 - $2 \text{ (nombre de disques)} \times 10 \text{ (nombre de snapshots PIT)} \times 5 \text{ (4 composants miroirs de 256 Go chacun + 1 témoin)} = 100 \text{ composants uniquement pour cette machine virtuelle.}$

Le nombre de snapshots PIT que vous conservez peut entraîner l'augmentation de la latence E/S sur le stockage Virtual SAN.

Configurer la réplication d'une machine virtuelle unique

vSphere Replication peut protéger les machines virtuelles individuelles et leurs disques virtuels en les répliquant dans un autre emplacement.

Lorsque vous configurez la réplication, vous définissez un objectif de point de récupération (RPO) pour déterminer la fréquence des répliquations. Par exemple, un objectif (RPO) d'une heure vise à ce qu'une machine virtuelle ne perde pas plus d'une heure de données lors de la récupération. Pour les RPO plus petits, moins de données sont perdues au cours d'une récupération, mais une plus grande quantité de bande passante réseau est consommée en conservant la réplique à jour.

Chaque fois qu'une machine virtuelle atteint sa cible RPO, vSphere Replication enregistre environ 3 800 octets de données dans la base de données des événements de vCenter Server. Si vous définissez un délai RPO court, vous risquez de générer un volume de données important dans la base de données. Afin d'éviter de créer de grands volumes de données dans la base de données des événements dans vCenter Server, limitez le nombre de jours pendant lesquels vCenter Server conserve les données des événements. Reportez-vous à Configurer la règle de rétention de base de donnée dans le *Guide de gestion de vCenter Server et des hôtes*. Vous pouvez également définir un délai RPO plus long.

Note Vous ne pouvez pas utiliser l'interface de Site Recovery Manager pour configurer une réplication qui utilise des snapshots à un moment précis (PIT). Pour activer les snapshots PIT, configurez la réplication d'une machine virtuelle à l'aide de Client Web vSphere. Reportez-vous à [Configurer la réplication d'une machine virtuelle unique](#) dans Administration de *vSphere Replication*.

Pour récupérer une machine virtuelle à partir d'un snapshot à un moment spécifique plus ancien, vous devez restaurer manuellement la machine virtuelle à ce snapshot après la récupération. Reportez-vous à [Récupérer un snapshot d'une machine virtuelle à un moment spécifique](#).

vSphere Replication assure la cohérence des défaillances entre tous les disques appartenant à une machine virtuelle. Si vous utilisez la mise au repos VSS, vous pouvez obtenir un niveau de cohérence plus élevé. Les types de mise au repos disponibles sont définis par le système d'exploitation de la machine virtuelle. Pour la prise en charge de la mise au repos de Microsoft VSS (Volume Shadow Copy Service) pour machines virtuelles Windows, reportez-vous à [Matrices de compatibilité pour vSphere Replication 5.5](#).

Vous pouvez utiliser vSphere Replication avec une banque de données Virtual SAN sur les sites sources et cibles. Cependant, vous devez utiliser Client Web vSphere pour configurer vSphere Replication lors d'une réplique sur le stockage Virtual SAN. Le client Site Recovery Manager ne vous permet pas de sélectionner le stockage Virtual SAN lorsque vous sélectionnez la banque de données cible.

Note VMware Virtual SAN est une fonctionnalité entièrement prise en charge de vSphere 5.5u1.

- Vous pouvez utiliser Virtual SAN dans des environnements de production avec vSphere Replication 5.5.1 et vSphere 5.5u1.
 - Virtual SAN est une fonctionnalité expérimentale dans vSphere 5.5. Vous pouvez effectuer des tests à l'aide de Virtual SAN dans vSphere Replication 5.5.0 et vSphere 5.5, mais cette fonctionnalité n'est pas prise en charge pour une utilisation dans des environnements de production. Pour obtenir des informations sur l'activation de Virtual SAN dans vSphere 5.5, reportez-vous aux notes de mise à jour de vSphere Replication 5.5.0.
-

Conditions préalables

Vérifiez que vous avez déployé et connecté les dispositifs vSphere Replication et les instances du Serveur Site Recovery Manager sur chaque site.

Procédure

- 1 Sur la page d'accueil de vSphere Client, cliquez sur **VM et modèles**.
- 2 Parcourez l'inventaire pour rechercher la seule machine virtuelle à répliquer en utilisant vSphere Replication.
- 3 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **vSphere Replication**.
- 4 Utilisez le curseur RPO ou entrez une valeur pour configurer la quantité maximale de données pouvant être perdues en cas de défaillance d'un site.

La plage de l'objectif de point de récupération (RPO) est comprise entre 15 minutes et 24 heures.
- 5 Sélectionnez une configuration de mise au repos au niveau du système d'exploitation client, si cela s'applique au système d'exploitation de la machine virtuelle source.

- 6 Si aucun emplacement de fichier cible n'est spécifié ou si vous souhaitez remplacer l'emplacement par défaut défini par les mappages des banques de données, cliquez sur **Parcourir** pour sélectionner un emplacement cible pour la machine virtuelle.

Option	Description
Placer une machine virtuelle directement dans une banque de données	Sélectionnez une banque de données et cliquez sur OK .
Placer une machine virtuelle dans un dossier dans une banque de données	Sélectionnez Spécifier le dossier de la banque de données , cliquez sur Parcourir pour rechercher le dossier, puis cliquez deux fois sur le dossier.

- 7 Sélectionnez une destination de réplication pour chaque périphérique média de la machine virtuelle.

Les pages suivantes sont créées dynamiquement en fonction des périphériques de support installés sur la machine virtuelle. Ils peuvent inclure plusieurs périphériques virtuels que vous pouvez configurer individuellement. Si le lecteur virtuel est répliqué, les paramètres configurables comprennent la destination de réplication du lecteur virtuel et les informations concernant la configuration du lecteur virtuel répliqué. Si le disque doit être répliqué, sélectionnez la destination de réplication du disque avant de continuer.

- 8 Acceptez l'attribution automatique d'un serveur vSphere Replication ou sélectionnez un serveur spécifique sur le site cible.
- 9 Consultez les paramètres et cliquez sur **Terminer** pour mettre en œuvre la réplication.
- vSphere Replication commence une synchronisation complète initiale des fichiers de machine virtuelle dans la banque de données désignée sur le site cible.
- 10 (Facultatif) Sélectionnez la vue vSphere Replication dans l'interface de Site Recovery Manager.
- 11 (Facultatif) Sélectionnez le site distant vSphere Replication et cliquez sur l'onglet **Machines virtuelles**.

Vous pouvez surveiller l'avancement de la synchronisation complète initiale des fichiers de machine virtuelle sur le site cible.

Configurer la réplication de nombreuses machines virtuelles

Vous pouvez configurer la réplication de plusieurs machines virtuelles à l'aide de l'assistant de configuration de répliquions multiples.

Lorsque vous configurez la réplication, vous définissez un objectif de point de récupération (RPO) pour déterminer la fréquence des répliquions. Par exemple, un objectif (RPO) d'une heure vise à ce qu'une machine virtuelle ne perde pas plus d'une heure de données lors de la récupération. Pour les RPO plus petits, moins de données sont perdues au cours d'une récupération, mais une plus grande quantité de bande passante réseau est consommée en conservant la réplique à jour.

Chaque fois qu'une machine virtuelle atteint sa cible RPO, vSphere Replication enregistre environ 3 800 octets de données dans la base de données des événements de vCenter Server. Si vous définissez un délai RPO court, vous risquez de générer un volume de données important dans la base de données. Afin d'éviter de créer de grands volumes de données dans la base de données des événements dans vCenter Server, limitez le nombre de jours pendant lesquels vCenter Server conserve les données des événements. Reportez-vous à *Configurer la règle de rétention de base de donnée* dans le *Guide de gestion de vCenter Server et des hôtes*. Vous pouvez également définir un délai RPO plus long.

Note Vous ne pouvez pas utiliser l'interface de Site Recovery Manager pour configurer des répliquions qui utilisent des snapshots à un moment précis (PIT). Pour activer les snapshots à un moment précis (PIT), configurez la répliquion de machines virtuelles à l'aide de Client Web vSphere. Consultez [Configurer la répliquion de nombreuses machines virtuelles](#) dans *vSphere Replication Administration*.

Pour récupérer une machine virtuelle à partir d'un snapshot à un moment spécifique plus ancien, vous devez restaurer manuellement la machine virtuelle à ce snapshot après la récupération. Reportez-vous à [Récupérer un snapshot d'une machine virtuelle à un moment spécifique](#).

vSphere Replication assure la cohérence des défaillances entre tous les disques appartenant à une machine virtuelle. Si vous utilisez la mise au repos VSS, vous pouvez obtenir un niveau de cohérence plus élevé. Les types de mise au repos disponibles sont définis par le système d'exploitation de la machine virtuelle. Pour la prise en charge de la mise au repos de Microsoft VSS (Volume Shadow Copy Service) pour machines virtuelles Windows, reportez-vous à [Matrices de compatibilité pour vSphere Replication 5.5](#).

Vous pouvez utiliser vSphere Replication avec une banque de données Virtual SAN sur les sites sources et cibles. Cependant, vous devez utiliser Client Web vSphere pour configurer vSphere Replication lors d'une répliquion sur le stockage Virtual SAN. Le client Site Recovery Manager ne vous permet pas de sélectionner le stockage Virtual SAN lorsque vous sélectionnez la banque de données cible.

Note VMware Virtual SAN est une fonctionnalité entièrement prise en charge de vSphere 5.5u1.

- Vous pouvez utiliser Virtual SAN dans des environnements de production avec vSphere Replication 5.5.1 et vSphere 5.5u1.
 - Virtual SAN est une fonctionnalité expérimentale dans vSphere 5.5. Vous pouvez effectuer des tests à l'aide de Virtual SAN dans vSphere Replication 5.5.0 et vSphere 5.5, mais cette fonctionnalité n'est pas prise en charge pour une utilisation dans des environnements de production. Pour obtenir des informations sur l'activation de Virtual SAN dans vSphere 5.5, reportez-vous aux notes de mise à jour de vSphere Replication 5.5.0.
-

La configuration de vSphere Replication simultanément sur un grand nombre de machines virtuelles lors de l'utilisation du stockage Virtual SAN peut ralentir considérablement la synchronisation complète initiale des fichiers de machine virtuelle. Les opérations de synchronisation complète initiale génèrent un trafic d'E/S intense et la configuration d'un trop grand nombre de répliquions en même temps peut surcharger le stockage Virtual SAN. Configurez vSphere Replication sur des lots incluant un nombre maximal de 30 machines virtuelles à la fois.

Conditions préalables

Pour répliquer une machine virtuelle en utilisant vSphere Replication, vous devez déployer le dispositif vSphere Replication sur les sites source et cible. Vous devez mettre sous tension les machines virtuelles pour commencer la répliquion.

Avant de répliquer plusieurs machines, configurez les mappages de banques de données dans l'interface utilisateur Site Recovery Manager. Vous configurez les mappages pour que les informations soient disponibles pour Site Recovery Manager concernant les destinations de banque de données cibles de la répliquion.

Procédure

- 1 Dans la page d'accueil Client Web vSphere, cliquez sur **VM et modèles**.
- 2 Sélectionnez un dossier ou un centre de données dans le volet de gauche et cliquez sur l'onglet **Machines virtuelles**.
- 3 Sélectionnez les machines virtuelles à répliquer en utilisant les touches Ctrl ou Maj.
- 4 Cliquez avec le bouton droit sur les machines virtuelles et sélectionnez **vSphere Replication**.
- 5 Utilisez le curseur RPO ou entrez une valeur pour configurer la quantité maximale de données pouvant être perdues en cas de défaillance d'un site.

La plage de l'objectif de point de récupération (RPO) est comprise entre 15 minutes et 24 heures.

- 6 Sélectionnez une configuration de mise au repos au niveau du système d'exploitation client, si cela s'applique au système d'exploitation de la machine virtuelle source.
- 7 (Facultatif) Activez ou désactivez l'option **Les copies initiales des fichiers .vmdk ont été placés dans la banque de données cible**.

Sélectionnez cette option si vous avez copié physiquement des fichiers VMDK vers le site cible à utiliser comme des amorces de répliquion. Site Recovery Manager utilise des mappages de banque de données et des informations des machines virtuelles sources pour rechercher et utiliser les copies initiales. Site Recovery Manager affiche la progression et l'état au fur et à mesure qu'il cherche les copies initiales. Vous pouvez arrêter le processus de recherche ou le relancer.

- 8 Acceptez l'attribution automatique d'un serveur vSphere Replication ou sélectionnez un serveur spécifique sur le site cible.

- 9 Consultez les paramètres et cliquez sur **Terminer** pour mettre en œuvre la réplication.
vSphere Replication commence une synchronisation complète initiale des fichiers de machine virtuelle dans la banque de données désignée sur le site cible.
- 10 (Facultatif) Sélectionnez la vue vSphere Replication dans l'interface de Site Recovery Manager.
- 11 (Facultatif) Sélectionnez le site distant vSphere Replication et cliquez sur l'onglet **Machines virtuelles**.
Vous pouvez surveiller l'avancement de la synchronisation complète initiale des fichiers de machine virtuelle sur le site cible.

Étape suivante

Si vous n'avez pas configuré les mappages de banques de données pour vSphere Replication avant de configurer la réplication, les machines virtuelles s'affichent dans l'onglet **vSphere Replication > Machines virtuelles** en rouge avec l'état *Les mappages de banques de données n'ont pas été configurés*. Configurez les mappages de banques de données et reconfigurez vSphere Replication sur les machines virtuelles.

Répliquer des machines virtuelles en utilisant des amorces de réplication

Vous pouvez rendre la réplication initiale des fichiers VDMK plus efficace en déplaçant physiquement les fichiers sur un périphérique de stockage. vSphere Replication utilise les fichiers déplacés physiquement comme amorces de réplication.

Vous pourrez être amené à utiliser les amorces de réplication s'il n'est pas pratique de copier les fichiers sur le réseau parce que les données sont trop volumineuses, la bande passante disponible trop petite, ou les deux.

Lors de la réplication de machines virtuelles, assurez-vous que celles-ci sont répliquées vers des sous-répertoires dans des banques de données. Les disques copiés fonctionnent si la méthode de transfert préserve les informations d'identité stockées dans le fichier VMDK.

Conditions préalables

- Vous avez déployé le dispositif vSphere Replication sur les deux sites.
- Vous avez couplé les instances du Serveur Site Recovery Manager sur chaque site et vous avez couplé les dispositifs vSphere Replication.
- Mettez la machine virtuelle hors tension avant de télécharger les fichiers VMDK à utiliser comme amorces pour la réplication. Replication begins when the virtual machine is powered on.

Procédure

- 1 Utilisez vSphere Client pour vous connecter à un vCenter Server pouvant gérer les machines virtuelles à déplacer physiquement.

- 2 Cliquez sur **Banques de données**.
- 3 Dans le volet gauche, naviguez jusqu'à la banque de données contenant les fichiers de la machine virtuelle, sélectionnez cette banque de données, puis, dans le volet droit, cliquez sur **Parcourir cette banque de données**.
- 4 Sélectionnez les dossiers pour toutes les machines virtuelles à déplacer physiquement, cliquez avec le bouton droit sur la sélection, puis cliquez sur **Télécharger**
- 5 Sélectionnez une destination sur laquelle copier les fichiers et cliquez sur **OK**.
- 6 Cliquez sur **Oui**.
- 7 Une fois que le téléchargement est terminé, transférez les fichiers vers un emplacement sur le site couplé pour les télécharger.
- 8 Sur la page d'accueil de vSphere Client du site couplé, cliquez sur **Banques de données**.
- 9 Dans le volet de gauche, naviguez jusqu'à la banque de données contenant les fichiers de la machine virtuelle, sélectionnez cette banque de données, puis, dans le volet de droite, cliquez sur **Parcourir cette banque de données**.
- 10 Sélectionnez le dossier qui contient les copies des machines virtuelles, cliquez avec le bouton droit sur la sélection, puis cliquez sur **Télécharger dossier**
- 11 Sélectionnez le dossier contenant les machines virtuelles, puis cliquez sur **OK**.
- 12 Sur le site protégé, cliquez avec le bouton droit sur la machine virtuelle à répliquer et sélectionnez **vSphere Replication**.
- 13 Définissez l'objectif de point de récupération et l'emplacement du fichier cible comme étant normaux et cliquez sur **Suivant**.
- 14 Cliquez sur **Parcourir** dans le panneau Emplacement du fichier de disque cible.
- 15 Sélectionnez la banque de données cible, cochez la case **Spécifier le dossier de la banque de données**, puis cliquez sur **Parcourir**.
- 16 Sélectionnez la banque de données cible et cliquez sur **Ouvrir**.
- 17 Sélectionnez le dossier de banque de données dans lequel figurent les fichiers d'amorce, modifiez le type de fichier par Tous les fichiers, sélectionnez le fichier VMDK à utiliser en tant qu'amorce de réplication, puis cliquez sur **OK**.
- 18 Cliquez sur Oui pour confirmer que vous souhaitez utiliser ce fichier en tant que copie initiale.
- 19 Suivez les invites pour sélectionner un serveur vSphere Replication et cliquez sur **Terminer** pour terminer la configuration.

Reconfigurer des répliquions

Vous pouvez reconfigurer la réplication pour activer ou désactiver un fichier de disque de machine virtuelle pour la réplication, modifier les options de réplication, par exemple l'objectif de point de récupération (RPO) ou la méthode de mise au repos. Vous pouvez également spécifier une autre

banque de données cible pour la configuration de réplication et les fichiers de disque, et transférer la machine virtuelle vers un autre serveur vSphere Replication.

Conditions préalables

Vous avez configuré vSphere Replication sur une ou plusieurs machines virtuelles.

Procédure

- 1 Sélectionnez la vue vSphere Replication de l'interface de Site Recovery Manager.
- 2 Sélectionnez un serveur vSphere Replication et cliquez sur l'onglet **Machines virtuelles**.
- 3 Sélectionnez une machine virtuelle ou utilisez les touches Ctrl ou Maj pour sélectionner plusieurs machines virtuelles, cliquez avec le bouton droit et sélectionnez **Configurer la réplication**.
- 4 (Facultatif) Utilisez le curseur RPO et entrez une valeur pour reconfigurer la quantité maximale de données pouvant être perdue en cas de panne de site.

La plage de l'objectif de point de récupération (RPO) est comprise entre 15 minutes et 24 heures.

- 5 (Facultatif) Changez la configuration de mise au repos du système d'exploitation invité, si cela s'applique au système d'exploitation invité de la machine virtuelle.
- 6 (Facultatif) Changez l'emplacement cible des fichiers de la machine virtuelle.

Option	Description
Reconfigurer la réplication d'une machine virtuelle spécifique	Cliquez sur Parcourir pour changer l'emplacement cible des fichiers de la machine virtuelle.
Reconfigurer la réplication de plusieurs machines virtuelles	Sélectionnez Les copies initiales des fichiers .vmdk ont été placées dans la banque de données cible si vous avez copié les amorces de réplication dans une nouvelle banque de données cible.

- 7 (Facultatif) Changez la destination de réplication pour chaque périphérique de support de la machine virtuelle.

Les pages suivantes sont créées dynamiquement en fonction des périphériques de support installés sur la machine virtuelle. Ils peuvent inclure plusieurs périphériques virtuels que vous pouvez configurer individuellement. Si le lecteur virtuel est répliqué, les paramètres configurables comprennent la destination de réplication du lecteur virtuel et les informations concernant la configuration du lecteur virtuel répliqué. Si le disque doit être répliqué, sélectionnez la destination de réplication du disque avant de continuer.

- 8 (Facultatif) Sélectionnez un autre serveur vSphere Replication pour gérer la réplication de cette machine virtuelle.
- 9 Consultez les paramètres et cliquez sur **Terminer** pour mettre en œuvre la réplication.

vSphere Replication commence une synchronisation complète initiale des fichiers de machine virtuelle dans la banque de données désignée sur le site cible.

Arrêter la réplication d'une machine virtuelle

Si vous n'avez pas besoin de répliquer une machine virtuelle, vous pouvez arrêter sa réplication.

L'arrêt de la réplication d'une machine virtuelle ne supprime pas celle-ci des groupes de protection dont elle est membre.

Conditions préalables

Vous avez configuré vSphere Replication sur une machine virtuelle que vous n'avez plus besoin de protéger.

Procédure

- 1 Sélectionnez la vue vSphere Replication dans l'interface de Site Recovery Manager.
- 2 Sélectionnez un serveur vSphere Replication et cliquez sur l'onglet **Machines virtuelles**.
- 3 Sélectionnez une machine virtuelle et cliquez sur **Supprimer la réplication**.
- 4 Cliquez sur **Oui** pour confirmer l'arrêt de la réplication de cette machine virtuelle.
- 5 Sélectionnez la vue Groupes de protection de l'interface de Site Recovery Manager.
- 6 Sélectionnez le groupe de protection dont la machine virtuelle est membre, puis cliquez sur l'onglet **Machines virtuelles**.
- 7 Sélectionnez la machine virtuelle dont vous avez arrêté la réplication et cliquez sur **Supprimer la protection**.
- 8 Cliquez sur **Oui** pour confirmer l'arrêt de la protection de cette machine virtuelle.

Résultats

La machine virtuelle n'est pas répliquée sur le site cible.

La machine virtuelle ne fait plus partie d'un groupe de protection.

Création de groupes de protection

3

Après avoir configuré une solution de réplication, vous pouvez créer des groupes de protection. Un groupe de protection est un ensemble de machines virtuelles et de modèles que vous protégez ensemble en utilisant Site Recovery Manager.

Vous pouvez inclure un ou plusieurs groupes de protection dans chaque plan de récupération. Un plan de récupération spécifie la manière dont les machines virtuelles sont récupérées par Site Recovery Manager dans les groupes de protection qu'il contient.

Vous devez configurer les machines virtuelles d'un groupe de protection de telle sorte qu' Site Recovery Manager puisse les ajouter à l'inventaire de vCenter Server au niveau du site de récupération.

Vous pouvez configurer les machines virtuelles et créer des groupes de protection différemment, selon que vous utilisez une réplication basée sur la baie ou vSphere Replication. En revanche, vous ne pouvez pas créer des groupes de protection combinant les machines virtuelles pour lesquelles vous avez configuré la réplication basée sur la baie, avec des machines virtuelles pour lesquelles vous avez configuré vSphere Replication. Il est cependant possible d'inclure les groupes de protection basés sur la baie et les groupes de protection de vSphere Replication dans le même plan de récupération.

- **À propos des groupes de protection basés sur la baie et des groupes de banques de données**

Lorsque vous créez un groupe de protection pour une réplication basée sur la baie, vous spécifiez des informations sur la baie et Site Recovery Manager calcule l'ensemble des machines virtuelles dans le groupe de banques de données. Les groupes de banque de données contiennent tous les fichiers des machines virtuelles protégées.

- **Créer des groupes de protection pour vSphere Replication**

Vous pouvez créer des groupes de protection contenant des machines virtuelles protégées par vSphere Replication.

- **Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection**

Si vous ajoutez des machines virtuelles à un groupe de protection, ou si les machines virtuelles perdent leur protection, vous pouvez configurer la protection de toutes les machines virtuelles non configurées en utilisant les mappages d'inventaire existants, en une étape.

À propos des groupes de protection basés sur la baie et des groupes de banques de données

Lorsque vous créez un groupe de protection pour une réplication basée sur la baie, vous spécifiez des informations sur la baie et Site Recovery Manager calcule l'ensemble des machines virtuelles dans le groupe de banques de données. Les groupes de banque de données contiennent tous les fichiers des machines virtuelles protégées.

Vous pouvez ajouter des machines virtuelles au groupe de protection en les créant dans l'une des banques de données appartenant aux groupes de banques de données que Site Recovery Manager associe au groupe de protection. Vous pouvez également ajouter des machines virtuelles au groupe de protection à l'aide de Storage vMotion pour déplacer leur stockage vers l'une des banques de données du groupe de banques de données. Vous pouvez supprimer un membre d'un groupe de protection en déplaçant les fichiers de la machine virtuelle vers une autre banque de données.

Si vous désactivez la protection sur une machine virtuelle, vous devez transférer les fichiers de cette machine virtuelle vers une banque de données non protégée. Si vous laissez les fichiers d'une machine virtuelle non protégée dans une banque de données protégée, la récupération échoue pour toutes les machines virtuelles contenues dans cette banque de données.

Pour configurer la réplication basée sur la baie, vous devez attribuer chaque machine virtuelle à un pool de ressources, un dossier et un réseau existant sur le site de récupération. Vous pouvez spécifier des options par défaut pour ces affectations en sélectionnant les mappages d'inventaire. Site Recovery Manager applique des mappages d'inventaire lors de la création du groupe de protection. Si vous ne spécifiez pas les mappages d'inventaires, vous devez les configurer manuellement pour chaque membre du groupe de protection. Site Recovery Manager ne protège pas les machines virtuelles non configurées ou mal configurées pour la réplication, même si elles se trouvent sur une banque de données protégée.

Si votre baie de stockage prend en charge les groupes de cohérence, Site Recovery Manager est compatible avec vSphere Storage DRS et vSphere Storage vMotion. Vous pouvez utiliser Storage DRS et Storage vMotion pour déplacer des fichiers de machines virtuelles au sein d'un groupe de cohérence protégé par Site Recovery Manager. Si votre baie de stockage ne prend pas en charge les groupes de cohérence, vous ne pouvez pas utiliser Storage DRS et Storage vMotion avec Site Recovery Manager.

- [Comment Site Recovery Manager calcule les groupes de banques de données](#)

Site Recovery Manager détermine la composition d'un groupe de banques de données selon l'ensemble de machines virtuelles possédant des fichiers sur les banques de données du groupe et les périphériques sur lesquels ces banques de données sont stockées.

- [Créer des groupes de protection basés sur la baie](#)

Vous pouvez créer des groupes de protection basés sur des baies pour activer la protection des machines virtuelles contenues dans des groupes de banques de données configurées par vos soins, afin d'utiliser la réplication basée sur des baies.

■ Modifier des groupes de protection basés sur la baie

Vous pouvez modifier le nom et la description d'un groupe de protection basé sur la baie et ajouter ou supprimer des groupes de banques de données qui font partis du groupe de protection.

Comment Site Recovery Manager calcule les groupes de banques de données

Site Recovery Manager détermine la composition d'un groupe de banques de données selon l'ensemble de machines virtuelles possédant des fichiers sur les banques de données du groupe et les périphériques sur lesquels ces banques de données sont stockées.

Lorsque vous utilisez la réplication basée sur la baie, chaque baie de stockage prend en charge un ensemble de banques de données répliquées. Sur les baies Réseau de zone de stockage (SAN) utilisant des protocoles de connexion tels que Fibre Channel et iSCSI, ces banques de données sont appelées LUN (unités de stockage logiques) comprenant une ou plusieurs banques de données physiques. Sur les baies du système de fichiers du réseau (NFS), les banques de données répliquées sont généralement appelées volumes. Dans chaque paire de périphériques de stockage répliqués, une banque de données est la source de réplication et l'autre est la cible. Les données écrites sur la banques de données source sont répliquées vers la banques de données cible, selon un plan contrôlé par le logiciel de réplication de la baie. Lorsque vous configurez Site Recovery Manager pour fonctionner avec un adaptateur de réplication de stockage (SRA), la source de réplication se trouve sur le site protégé et la cible de réplication sur le site de récupération.

Une banque de données stocke les fichiers des machines virtuelles. En masquant les détails concernant les périphériques de stockage physiques, les banques de données simplifient l'allocation d'une capacité de stockage et fournissent un modèle uniforme, afin de répondre aux besoins de stockage des machines virtuelles. Étant donné qu'une banque de données peut s'étendre sur plusieurs périphériques, Site Recovery Manager doit s'assurer que tous les périphériques sauvegardant la banque de données sont répliqués avant de pouvoir protéger les machines virtuelles utilisant cette même banque de données. Site Recovery Manager doit s'assurer que toutes les banques de données contenant les fichiers de la machine virtuelle protégée sont répliquées. Au cours d'une récupération ou d'un test, Site Recovery Manager doit traiter toutes les banques de données ensemble.

Pour y parvenir, Site Recovery Manager regroupe les banques de données en groupes de banques de données, afin qu'ils puissent contenir les machines virtuelles s'étendant sur plusieurs banques de données. Site Recovery Manager contrôle et vérifie régulièrement que les groupes de banques de données contiennent toutes les banques de données nécessaires à la protection des machines virtuelles concernées. Si nécessaire, Site Recovery Manager recalcule les groupes de banques de données. Cela peut par exemple se produire lorsque de nouveaux périphériques sont ajoutés à une machine virtuelle et que ceux-ci sont stockés sur une banque de données qui ne faisait pas partie du groupe de banques de données.

Un groupe de banques de données se compose du plus petit ensemble de banques de données requis pour s'assurer que, si un fichier d'une machine virtuelle est stocké sur une banque de données appartenant au groupe, tous les fichiers de cette machine virtuelle sont stockés sur les banques de données faisant partie du même groupe. Par exemple, si une machine virtuelle dispose de disques sur deux banques de données différentes, alors Site Recovery Manager combine ces deux banques de données pour former un groupe de banques de données. Site Recovery Manager combine également des périphériques dans des groupes de banques de données, en fonction de critères définis.

- Deux banques de données différentes contiennent des fichiers qui appartiennent à la même machine virtuelle.
- Les banques de données qui appartiennent à deux machines virtuelles partagent un périphérique RDM (Raw Disk Mapping) sur une baie SAN, comme dans le cas d'un cluster MSCS (Microsoft Cluster Server).
- Deux banques de données englobent des extensions correspondant à des partitions différentes sur le même périphérique.
- Une banque de données unique englobe deux extensions correspondant aux partitions de deux périphériques différents. Les deux extensions doivent se trouver dans un groupe de cohérence unique et le SRA doit rapporter, depuis la baie, des informations sur le groupe de cohérence à l'étape de découverte de périphérique. Dans le cas contraire, la création des groupes de protection basés sur cette banque de données est impossible, même si le SRA rapporte que les extensions qui constituent cette banque de données sont répliquées.
- Plusieurs banques de données appartiennent à un groupe de cohérence. Un groupe de cohérence est une collection de banques de données répliquées, dans lequel chaque état de l'ensemble de banques de données cible existait à un moment précis en tant qu'état de l'ensemble de banques de données source. Officieusement, les banques de données sont répliquées ensemble afin que, lorsque la récupération se produit avec ces banques de données, le logiciel accédant aux cibles ne voie pas les données dans un état qu'il n'est pas prêt à gérer.

Protection des machines virtuelles sur les banques de données VMFS qui englobent plusieurs LUN ou extensions

Tous les SRA ne rapportent pas d'informations sur le groupe de cohérence depuis la baie de stockage, car toutes les baies de stockage ne prennent pas en charge les groupes de cohérence. Si un SRA rapporte des informations sur le groupe de cohérence depuis la baie suivant une commande de découverte de banque de données, les LUN qui constituent une banque de données VMFS à plusieurs extensions doivent se trouver dans le même groupe de cohérence de la baie de stockage. Si la baie ne prend pas en charge les groupes de cohérence et que le SRA ne rapporte aucune information sur le groupe de cohérence, Site Recovery Manager ne peut pas protéger les machines virtuelles se trouvant sur la banque de données à plusieurs extensions.

Créer des groupes de protection basés sur la baie

Vous pouvez créer des groupes de protection basés sur des baies pour activer la protection des machines virtuelles contenues dans des groupes de banques de données configurées par vos soins, afin d'utiliser la réplication basée sur des baies.

Site Recovery Manager calcule les groupes de banque de données lorsque vous configurez une paire de baies ou lorsque vous actualisez la liste de périphériques.

Après la création d'un groupe de protection, Site Recovery Manager crée des machines virtuelles à espace réservé et applique les mappages d'inventaire à chaque machine virtuelle du groupe. Si Site Recovery Manager ne parvient pas à mapper une machine virtuelle à un dossier, un réseau et un pool de ressources sur le site de récupération, Site Recovery Manager définit l'état de la machine virtuelle comme étant Mappage manquant, sans lui créer d'espace réservé.

Vous pouvez organiser les groupes de protection dans les dossiers. Différentes vues dans l'interface Récupération affichent les noms des groupes de protection, mais elles n'affichent pas les noms de dossier. Si deux groupes de protection portent le même nom dans des dossiers différents, il peut être difficile de les différencier dans certaines vues de l'interface Récupération. Par conséquent, veillez à ce que chaque nom de groupe de protection soit unique dans tous les dossiers. Dans des environnements dans lesquels tous les utilisateurs n'ont pas de privilèges de vue pour tous les dossiers, pour être sûr de l'unicité des noms des groupes de protection, ne placez pas de groupes de protection dans des dossiers.

Lorsque vous créez des groupes de protection, patientez afin de vous assurer que les opérations se terminent comme prévu. Assurez-vous que Site Recovery Manager crée le groupe de protection et que la protection des machines virtuelles du groupe aboutisse.

Procédure

- 1 Cliquez sur **Groupes de protection** dans l'interface de Site Recovery Manager, puis sur **Créer un groupe de protection**.
- 2 Sur la page Sélectionner un site et un type de groupe de protection, sélectionnez le site à protéger puis **Réplication basée sur la baie**.
- 3 Sélectionnez une paire de baies, et cliquez sur **Suivant**.
- 4 Sélectionnez un groupe de banques de données dans la liste, puis cliquez sur **Suivant**.

Lorsque vous sélectionnez un groupe de banque de données, les machines virtuelles de ce groupe de banques de données apparaissent dans le volet Machines virtuelles des groupes de banques de données sélectionnés. Elles sont marquées de façon à être incluses dans le groupe de protection après la création de ce dernier.

- 5 Tapez un nom et une description facultative pour le groupe de protection, puis cliquez sur **Suivant**.

- 6 Cliquez sur **Terminer** pour créer le groupe de protection et commencer la protection des machines virtuelles spécifiées.

Vous pouvez surveiller l'avancement des tâches pour créer le groupe de protection et protéger les machines virtuelles dans le volet Tâches récentes de vSphere Client.

Étape suivante

Créez un plan de récupération pour y associer vos groupes de protection. Reportez-vous à la section [Créer un plan de récupération](#).

Modifier des groupes de protection basés sur la baie

Vous pouvez modifier le nom et la description d'un groupe de protection basé sur la baie et ajouter ou supprimer des groupes de banques de données qui font partis du groupe de protection.

Procédure

- 1 Cliquez sur **Groupes de protection**, puis cliquez avec le bouton droit de la souris sur un groupe de protection basé sur la baie et sélectionnez **Modifier le groupe de protection**.
- 2 Cliquez sur **Suivant**.
- 3 Ajoutez ou supprimez les groupes de banques de données dans le groupe de protection et cliquez sur **Suivant**.
- 4 Modifiez le nom ou la description du groupe de protection et cliquez sur **Suivant**.
- 5 Cliquez sur **Terminer**.

Créer des groupes de protection pour vSphere Replication

Vous pouvez créer des groupes de protection contenant des machines virtuelles protégées par vSphere Replication.

Vous pouvez organiser les groupes de protection dans les dossiers. Différentes vues dans l'interface Récupération affichent les noms des groupes de protection, mais elles n'affichent pas les noms de dossier. Si deux groupes de protection portent le même nom dans des dossiers différents, il peut être difficile de les différencier dans certaines vues de l'interface Récupération. Par conséquent, veillez à ce que chaque nom de groupe de protection soit unique dans tous les dossiers. Dans des environnements dans lesquels tous les utilisateurs n'ont pas de privilèges de vue pour tous les dossiers, pour être sûr de l'unicité des noms des groupes de protection, ne placez pas de groupes de protection dans des dossiers.

Lorsque vous créez un groupe de protection vSphere Replication, vous pouvez ajouter toutes les machines virtuelles configurées pour vSphere Replication au groupe de protection.

Conditions préalables

Utilisez vSphere Client pour configurer vSphere Replication pour les machines virtuelles. Reportez-vous à la section [Configurer la réplication d'une machine virtuelle unique](#) ou [Configurer la réplication de nombreuses machines virtuelles](#).

Procédure

- 1 Cliquez sur **Groupes de protection** dans l'interface de Site Recovery Manager, puis sur **Créer un groupe de protection**.
- 2 Sélectionnez le site qui sera le site protégé, puis **vSphere Replication** et cliquez sur **Suivant**.
- 3 Sélectionnez les machines virtuelles dans la liste, puis cliquez sur **Suivant**.
Seules les machines virtuelles configurées pour vSphere Replication et ne se trouvant pas encore dans un groupe de protection apparaissent dans la liste.
- 4 Tapez un nom et une description facultative pour le groupe de protection, puis cliquez sur **Suivant**.
- 5 Cliquez sur **Terminer** pour créer le groupe de protection.

Étape suivante

Créez un plan de récupération pour y associer vos groupes de protection. Reportez-vous à la section [Créer un plan de récupération](#).

Modifier des groupes de protection de vSphere Replication

Vous pouvez modifier un groupe de protection de vSphere Replication pour le renommer et pour ajouter des machines au groupe ou en supprimer.

Procédure

- 1 Cliquez sur **Groupes de protection** dans le panneau de gauche, puis cliquez avec le bouton droit sur un groupe de protection de vSphere Replication.
- 2 Sélectionnez **Modifier le groupe de protection** et cliquez sur **Suivant**.
Vous ne pouvez pas modifier le **Site protégé** ou les paramètres **Type de groupe de protection**.
- 3 Ajoutez des machines virtuelles au groupe de protection et cliquez sur **Suivant**.
- 4 Modifiez le nom ou la description du groupe de protection et cliquez sur **Suivant**.
- 5 Cliquez sur **Terminer**.
- 6 (Facultatif) Pour retirer une machine virtuelle d'un groupe de protection de vSphere Replication, cliquez sur l'onglet **Machines virtuelles**, sélectionnez une machine virtuelle et cliquez sur **Supprimer la protection**.

Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection

Si vous ajoutez des machines virtuelles à un groupe de protection, ou si les machines virtuelles perdent leur protection, vous pouvez configurer la protection de toutes les machines virtuelles non configurées en utilisant les mappages d'inventaire existants, en une étape.

Procédure

- 1 Cliquez sur **Groupes de protection** dans le volet gauche, sélectionnez un groupe de protection, puis cliquez sur l'onglet **Machines virtuelles**.
- 2 Cliquez sur **Tout configurer**.

Au moins une machine virtuelle du groupe de protection doit être dans l'état Non configurée pour que le bouton **Tout configurer** soit activé.

Création, test, et exécution de plans de récupération

4

Après avoir configuré Site Recovery Manager au niveau des sites protégés et de récupération, il est possible de créer, de tester et d'exécuter un plan de récupération.

Un plan de récupération est semblable à un runbook (compilation) automatique. Il contrôle chaque étape du processus de récupération, y compris l'ordre dans lequel les machines virtuelles sont mises hors tension ou activées par Site Recovery Manager et les adresses réseau utilisées par les machines virtuelles récupérées, etc. Les plans de récupération sont flexibles et personnalisables.

Un plan de récupération comprend un ou plusieurs groupes de protection. Vous pouvez inclure un groupe de protection dans plusieurs plans de récupération. Par exemple, vous pouvez créer un plan de récupération permettant de gérer une migration planifiée des services, du site protégé vers le site de récupération, et un autre permettant de gérer un événement non planifié, tel qu'une panne de courant ou une catastrophe naturelle. Ces plans de récupération différents vous permettent de déterminer le mode de récupération.

Le test d'un plan de récupération permet d'exécuter le plan sans affecter les services sur les sites protégés ou de récupération, mis à part la suspension des machines virtuelles non critiques sur le site de récupération si vous configurez le plan de récupération en conséquence. Vous pouvez effectuer des migrations planifiées du site protégé vers le site de récupération ou des récupérations d'urgence en exécutant un plan de récupération.

Vous ne pouvez exécuter qu'un seul plan de récupération à la fois pour récupérer un groupe de protection particulier. Si des plans de récupération multiples spécifiant le même groupe de protection sont testés ou exécutés en même temps, seul un plan de récupération pourra fonctionner sur le groupe de protection. Les autres plans de récupération en cours d'exécution spécifiant le même groupe de protection signalent des avertissements pour le groupe de protection et les machines virtuelles qu'il contient. Les avertissements expliquent que les machines virtuelles ont été récupérées, mais ne signalent pas d'autres groupes de protection couverts par les autres plans de récupération.

■ Tester un plan de récupération

Lorsque vous créez ou modifiez un plan de récupération, testez-le avant de l'utiliser pour une migration planifiée ou une récupération d'urgence.

- [Exécution d'une migration planifiée ou d'une récupération d'urgence via un plan de récupération](#)

Vous pouvez exécuter un plan de récupération de façon planifiée, afin de migrer les machines virtuelles du site protégé vers le site de récupération. Vous pouvez également exécuter un plan de récupération de façon non planifiée si le site protégé subit un événement imprévu susceptible d'entraîner une perte de données.

- [Différences entre tester et exécuter un plan de récupération](#)

Le test d'un plan de récupération n'a pas d'effets durables sur le site protégé ou le site de récupération, mais un plan de récupération a un impact important sur les deux sites.

- [Interaction de Site Recovery Manager avec DPM et DRS lors d'une récupération](#)

Les fonctionnalités DPM (Distributed Power Management) et DRS (Distributed Resource Scheduler) ne sont pas obligatoires, mais Site Recovery Manager prend en charge les deux services et leur activation offre certains avantages lors de l'utilisation de Site Recovery Manager.

- [Interaction entre Site Recovery Manager et Storage DRS ou Storage vMotion](#)

Vous pouvez utiliser Site Recovery Manager lorsque vous protégez des machines virtuelles sur des sites configurés pour Storage DRS ou Storage vMotion si vous suivez certaines directives.

- [Interaction entre Site Recovery Manager et vSphere High Availability](#)

Vous pouvez utiliser Site Recovery Manager pour protéger les machines virtuelles sur lesquelles HA (vSphere High Availability) est activé.

- [Protection de machines virtuelles MSCS \(Microsoft Cluster Server\) et tolérantes aux pannes](#)

Vous pouvez utiliser Site Recovery Manager pour protéger des machines virtuelles MSCS (Microsoft Cluster Server) et tolérantes aux pannes, mais cela comprend certaines restrictions.

- [Créer, tester et exécuter un plan de récupération](#)

Vous pouvez effectuer plusieurs groupes de tâches pour créer, tester et exécuter un plan de récupération.

- [Étapes pour exporter le plan de récupération](#)

Vous pouvez exporter les étapes d'un plan de récupération dans divers formats pour y faire référence ultérieurement, ou pour conserver une copie imprimée de vos plans.

- [Afficher et exporter l'historique du plan de récupération](#)

Vous pouvez afficher et exporter un rapport de chaque exécution d'un plan de récupération, d'un test de plan de récupération ou d'un nettoyage de test.

- [Annuler un test ou une récupération](#)

Vous pouvez annuler un test de plan de récupération à tout moment de son exécution. Vous pouvez annuler une migration planifiée ou de récupération d'urgence à certains moments de leur exécution.

■ Supprimer un plan de récupération

Vous pouvez supprimer un plan de récupération si vous n'en avez pas besoin.

Tester un plan de récupération

Lorsque vous créez ou modifiez un plan de récupération, testez-le avant de l'utiliser pour une migration planifiée ou une récupération d'urgence.

En testant un plan de récupération, veillez à ce que les machines virtuelles protégées par ce plan récupèrent correctement vers le site de récupération. Si vous ne testez pas vos plans de récupération, une réelle situation de récupération d'urgence pourrait ne pas récupérer toutes les machines virtuelles et causer la perte de données.

Le test d'un plan de récupération en étudie presque tous les aspects, même si Site Recovery Manager fait plusieurs concessions pour éviter d'interrompre les opérations en cours sur le site protégé et le site de récupération. Les plans de récupération qui interrompent les machines virtuelles locales le font pour les tests ainsi que pour les récupérations en cours. Avec cette exception, l'exécution d'une récupération test n'interrompt pas la réplication ou les activités en cours sur l'un de ces sites.

Si vous utilisez vSphere Replication, lorsque vous testez un plan de récupération, la machine virtuelle sur le site protégé peut encore se synchroniser avec les fichiers de disque de la réplication de la machine virtuelle sur le site de récupération. Le serveur vSphere Replication crée des journaux de répétition sur les fichiers du disque de la machine virtuelle du site de récupération, afin que la synchronisation puisse continuer normalement. Lorsque vous effectuez un nettoyage après avoir réalisé un test, le serveur vSphere Replication supprime les journaux de répétition des disques sur le site de récupération.

À cet effet, vous pouvez exécuter des récupérations tests aussi souvent que nécessaire. Vous pouvez annuler un test de plan de récupération à tout moment.

L'autorisation de tester un plan de récupération n'inclut pas l'autorisation d'exécuter un plan de récupération. L'autorisation d'exécuter un plan de récupération n'inclut pas l'autorisation de tester un plan de récupération. Vous devez assigner chaque autorisation séparément. Reportez-vous à la section [Attribuer des rôles et des autorisations Site Recovery Manager](#).

Réseaux de test et réseaux de centre de données

Lorsque vous testez un plan de récupération, Site Recovery Manager peut créer un réseau de test qu'il utilisera pour connecter les machines virtuelles récupérées. La création d'un réseau de test permet d'effectuer le test sans risque d'interrompre les machines virtuelles dans l'environnement de production.

Le réseau de test est géré par son propre commutateur virtuel et, dans la plupart des cas, les machines virtuelles récupérées peuvent l'utiliser sans devoir changer de propriétés réseau, telles que l'adresse IP, la passerelle, etc. Vous pouvez utiliser ce réseau de test en sélectionnant **Auto** pendant la configuration des paramètres réseau lorsque vous préparez l'exécution d'un test.

Un réseau de centre de données est un réseau prenant généralement en charge les machines virtuelles existantes sur le site de récupération. Pour l'utiliser, les machines virtuelles récupérées doivent se conformer à ses règles de disponibilité d'adresse réseau. Ces machines virtuelles doivent utiliser une adresse réseau qui peut être desservie et distribuée par le commutateur réseau ; de plus, elles doivent être configurées de façon à utiliser la passerelle et l'hôte DNS adéquats, etc. Les machines virtuelles récupérées utilisant DHCP peuvent se connecter à ce réseau sans aucune autre personnalisation. Les autres machines virtuelles nécessitent des étapes de personnalisation d'IP et de plan de récupération supplémentaire pour appliquer la personnalisation.

Vous devez récupérer les machines virtuelles devant interagir entre elles sur le même réseau de test. Si, par exemple, un serveur Web accède à des informations sur une base de données, les machines virtuelles du serveur Web et de la base de données doivent être récupérées ensemble sur le même réseau.

Exécution d'une migration planifiée ou d'une récupération d'urgence via un plan de récupération

Vous pouvez exécuter un plan de récupération de façon planifiée, afin de migrer les machines virtuelles du site protégé vers le site de récupération. Vous pouvez également exécuter un plan de récupération de façon non planifiée si le site protégé subit un événement imprévu susceptible d'entraîner une perte de données.

Pendant une migration planifiée, Site Recovery Manager synchronise les machines virtuelles sur le site de récupération avec celles du site protégé, puis arrête la réplication. Site Recovery Manager tente de répliquer toutes les machines virtuelles et d'arrêter normalement les machines protégées. Si des erreurs surviennent pendant une migration planifiée, le plan s'arrête pour que vous puissiez corriger les erreurs et exécuter le plan de nouveau. Vous pouvez procéder à la reprotection des machines virtuelles après la récupération.

Pendant les récupérations d'urgence, Site Recovery Manager restaure les machines virtuelles sur le site de récupération à leur état le plus récent, selon l'objectif de point de récupération (RPO). Lorsque vous exécutez un plan de récupération pour procéder à une récupération d'urgence, Site Recovery Manager tente d'arrêter les machines virtuelles sur le site protégé. Si Site Recovery Manager ne peut arrêter les machines virtuelles, Site Recovery Manager va tout de même démarrer les copies sur le site de récupération, et il peut s'avérer impossible de procéder à une reprotection automatique.

Si Site Recovery Manager détecte qu'une banque de données d'un site protégé est en état Tous chemins hors service (APD) et que, par conséquent, elle empêche une machine virtuelle de s'éteindre, le Site Recovery Manager attend pendant une certaine période avant d'essayer à nouveau d'arrêter la machine virtuelle en question. L'état APD est généralement transitoire. Ainsi, en attendant qu'une banque de données à l'état APD revienne en ligne, Site Recovery Manager peut arrêter normalement les machines virtuelles protégées de cette banque de données.

Site Recovery Manager utilise le signal de pulsation de VMware Tools pour déterminer si une machine virtuelle est en cours d'exécution sur le site de récupération. De cette manière, Site Recovery Manager peut s'assurer que toutes les machines virtuelles fonctionnent sur le site de récupération. Pour cette raison, installez VMware Tools sur les machines virtuelles protégées. Si vous ne souhaitez pas ou ne pouvez pas installer VMware Tools sur les machines virtuelles protégées, vous devez configurer Site Recovery Manager de manière à ne pas attendre le démarrage de VMware Tools sur les machines virtuelles récupérées et à ignorer l'étape de mise à l'arrêt du système d'exploitation invité. Reportez-vous à la section [Modifier les paramètres de récupération](#).

Une fois que Site Recovery Manager a achevé la dernière réplication, Site Recovery Manager apporte des modifications sur les deux sites nécessitant beaucoup de temps et d'efforts pour être inversés. En raison de ce temps et de ces efforts, vous devez assigner séparément le privilège de tester un plan de récupération et celui d'en exécuter un.

Exécution d'une récupération à l'aide de la fonction de récupération forcée

Si le site protégé est hors ligne et Site Recovery Manager ne peut exécuter ses tâches habituelles, vous pouvez exécuter une récupération à l'aide de l'option de récupération forcée. La récupération forcée démarre les machines virtuelles sur le site de récupération sans effectuer d'opérations sur le site protégé.

La récupération forcée sera utilisée dans les cas où les baies de stockage échouent au niveau du site protégé et où, en conséquence, les machines virtuelles protégées sont ingérables et ne peuvent être arrêtées, mises hors tension ou désenregistrées. Dans ce type de cas, l'état du système ne peut pas être changé durant une longue période. Pour résoudre cette situation, vous pouvez forcer la récupération. Forcer la récupération ne termine pas le processus de mise hors tension des machines virtuelles sur le site protégé. En résultat, un scénario de split-brain se produit, mais la récupération peut se terminer plus rapidement.

Attention Utilisez uniquement la récupération forcée lorsque l'objectif de temps de récupération (RTO) est sérieusement affecté par un manque de connectivité au site de protection.

Exécuter une récupération forcée avec une réplication basée sur la baie peut influencer sur la mise en miroir entre la baie de stockage protégée et la baie de stockage de récupération. Après l'exécution d'une récupération forcée, vous devez vérifier que la mise en miroir entre la baie protégée et la baie de récupération est correctement configurée avant de pouvoir effectuer des opérations de réplication supplémentaires. Si la mise en miroir n'est pas correctement configurée, vous devez la réparer en utilisant le logiciel de la baie de stockage.

Lorsque la récupération forcée est activée, tout changement en cours sur le site de protection n'est pas répliqué sur le site de récupération avant que la séquence ne commence. La réplication des changements se produit en accord avec la période d'objectif de point de récupération (RPO) de la baie de stockage. Si une nouvelle machine virtuelle ou un nouveau modèle est ajouté sur le site de protection et que la récupération est initiée avant que la période de RPO du stockage ne

soit terminée, la nouvelle machine virtuelle ou le nouveau modèle n'apparaît pas sur la banque de données répliquée et est perdu. Pour éviter de perdre la nouvelle machine virtuelle ou le nouveau modèle, attendez la fin de la période de RPO avant d'exécuter le plan de récupération avec une récupération forcée.

Une fois la récupération forcée terminée et après vérification de la mise en miroir des baies de stockage, vous pouvez résoudre le problème qui a nécessité la récupération forcée. Une fois le problème sous-jacent résolu, exécutez de nouveau une migration planifiée sur le plan de récupération, résolvez tout problème qui surviendrait, et relancez le plan jusqu'à ce qu'il se termine avec succès. Une fois encore, l'exécution du plan de récupération n'affecte pas les machines virtuelles récupérées au niveau du site de récupération.

Différences entre tester et exécuter un plan de récupération

Le test d'un plan de récupération n'a pas d'effets durables sur le site protégé ou le site de récupération, mais un plan de récupération a un impact important sur les deux sites.

Des privilèges différents sont nécessaires lors du test et de l'exécution d'un plan de récupération.

Tableau 4-1. Différences entre test et exécution d'un plan de récupération

Point de divergence	Tester un plan de récupération	Exécuter un plan de récupération
Privilèges requis	Nécessite Site Recovery Manager.Plans de récupération.Test une autorisation.	Nécessite Site Recovery Manager.Plans de récupération.Récupération .
Effet sur les machines virtuelles du site protégé	Aucun	Site Recovery Manager arrête les machines virtuelles en inversant l'ordre de priorité.
Effet sur les machines virtuelles du site de récupération	Site Recovery Manager suspend les machines virtuelles locales lorsque le plan de récupération l'exige. Site Recovery Manager redémarre les machines virtuelles suspendues après avoir nettoyé les résultats du test.	Site Recovery Manager suspend les machines virtuelles locales lorsque le plan de récupération l'exige.
Effet sur la réplication	Site Recovery Manager crée des snapshots temporaires de stockage répliqué au niveau du site de récupération. En ce qui concerne la réplication basée sur des baies, Site Recovery Manager analyse les baies pour les détecter.	Au cours d'une migration planifiée, Site Recovery Manager synchronise les banques de données répliquées, arrête la réplication, puis rend inscriptibles les périphériques cibles du site de récupération. Durant une récupération d'urgence, Site Recovery Manager entreprend les mêmes étapes. Toutefois, Site Recovery Manager ignore les erreurs en cas d'échec.

Tableau 4-1. Différences entre test et exécution d'un plan de récupération (suite)

Point de divergence	Tester un plan de récupération	Exécuter un plan de récupération
Réseau	Si vous affectez explicitement les réseaux test, Site Recovery Manager connecte les machines virtuelles récupérées à un réseau test. Si l'affectation de réseau de machine virtuelle est Auto , Site Recovery Manager affecte les machines virtuelles à des réseaux temporaires qui ne sont connectés à aucun réseau physique.	Site Recovery Manager connecte les machines virtuelles récupérées à un réseau de centre de données.
Interruption d'un plan de récupération	Vous pouvez annuler un test à tout moment.	Vous pouvez annuler la récupération dans certains cas.

Interaction de Site Recovery Manager avec DPM et DRS lors d'une récupération

Les fonctionnalités DPM (Distributed Power Management) et DRS (Distributed Resource Scheduler) ne sont pas obligatoires, mais Site Recovery Manager prend en charge les deux services et leur activation offre certains avantages lors de l'utilisation de Site Recovery Manager.

DPM (Gestion de l'alimentation distribuée) est une fonction VMware qui gère la consommation d'énergie par les hôtes ESX. DRS est un outil VMware chargé de la gestion de l'attribution de machines virtuelles aux hôtes ESX.

Site Recovery Manager désactive temporairement DPM pour le cluster et vérifie que tous les hôtes qui s'y trouvent sont mis sous tension avant le début de la récupération. À la fin de la récupération ou du test, Site Recovery Manager réactive DPM pour le cluster. Les hôtes du cluster sont maintenus en état de fonctionnement, de sorte que DPM puisse les mettre hors tension au besoin. Site Recovery Manager enregistre les machines virtuelles sur les hôtes disponibles ESX de manière circulaire, afin de distribuer la charge potentielle aussi uniformément que possible. Site Recovery Manager utilise toujours l'emplacement DRS pour répartir intelligemment la charge entre les hôtes et ce, avant de mettre sous tension les machines récupérées sur le site de récupération, même si DRS est désactivé sur le cluster. Si DRS est activé et fonctionne complètement en mode automatique, il peut déplacer les autres machines virtuelles pour mieux équilibrer la charge dans le cluster pendant que Site Recovery Manager met sous tension les machines virtuelles récupérées. DRS continue d'équilibrer toutes les machines virtuelles dans le cluster une fois que Site Recovery Manager a mis sous tension les machines virtuelles récupérées.

Interaction entre Site Recovery Manager et Storage DRS ou Storage vMotion

Vous pouvez utiliser Site Recovery Manager lorsque vous protégez des machines virtuelles sur des sites configurés pour Storage DRS ou Storage vMotion si vous suivez certaines directives.

Le comportement de Storage DRS ou de Storage vMotion est différent selon que vous utilisez Site Recovery Manager avec une réplication basée sur la baie ou avec vSphere Replication.

Utilisation de Site Recovery Manager avec la réplication basée sur la baie pour des sites avec Storage DRS ou Storage vMotion

Vous devez suivre les directives si vous utilisez la réplication basée sur la baie afin de protéger les machines virtuelles sur des sites qui utilisent Storage DRS ou Storage vMotion.

- Si votre baie de stockage prend en charge les groupes de cohérence, Site Recovery Manager est compatible avec vSphere Storage DRS et vSphere Storage vMotion. Vous pouvez utiliser Storage DRS et Storage vMotion pour déplacer des fichiers de machines virtuelles au sein d'un groupe de cohérence protégé par Site Recovery Manager. Si votre baie de stockage ne prend pas en charge les groupes de cohérence, vous ne pouvez pas utiliser Storage DRS et Storage vMotion avec Site Recovery Manager.
- Si vous activez Storage DRS sur le site de protection, un cluster de banques de données doit contenir un et un seul groupe de cohérence. N'incluez aucune banque de données qui n'appartient pas au groupe de cohérence du cluster. Le placement de plusieurs groupes de cohérence dans le même cluster risque d'entraîner la perte de machines virtuelles lors d'une récupération. Cette directive s'applique également au site de récupération si Storage DRS est activé sur le site de récupération.
- N'utilisez pas Storage DRS ni Storage vMotion pour déplacer régulièrement des machines virtuelles. N'acceptez pas les recommandations pour déplacer régulièrement des machines virtuelles manuellement. Vous pouvez déplacer occasionnellement des machines virtuelles, mais un mouvement excessif des machines virtuelles peut générer des problèmes. Déplacer des machines virtuelles nécessite que la baie réplique des machines virtuelles sur le réseau, ce qui demande du temps et consomme de la bande passante. Lorsque Storage DRS ou Storage vMotion déplace des machines virtuelles, vous pouvez rencontrer des problèmes pendant une récupération :
 - Si Storage DRS ou Storage vMotion déplace une machine virtuelle vers un groupe de cohérence différent au sein du même groupe de protection, un court délai s'écoule entre la propagation par Site Recovery Manager du nouvel emplacement de la machine virtuelle vers le site de récupération et la réplication par la baie des modifications vers le site de récupération. De plus, un autre délai est nécessaire afin que les baies puissent répliquer les groupes de cohérence source et cible dans un état cohérent sur le site de récupération. Lors de la propagation par la baie de toutes les modifications sur le site de récupération, la reprise après sinistre de cette machine virtuelle risque d'échouer.
 - Si Storage DRS ou Storage vMotion déplace une machine virtuelle vers un groupe de protection différent, Site Recovery Manager génère une erreur de protection pour cette machine virtuelle. Vous devez annuler la configuration de la protection de la machine

virtuelle dans l'ancien groupe de protection et configurer la protection de la machine virtuelle dans le nouveau groupe de protection. Tant que la protection n'est pas configurée pour le nouveau groupe de protection, la migration planifiée ou la reprise après sinistre de cette machine virtuelle échoue.

- L'ajout d'un disque à une machine virtuelle protégée génère les mêmes problèmes que le déplacement d'une machine virtuelle entière. Site Recovery Manager ne vous empêche pas de le faire, mais si une machine virtuelle contient un disque non répliqué et que vous n'excluez pas le disque de la protection, la mise sous tension de la machine virtuelle échoue après le déplacement.
- Déplacer un disque protégé vers un groupe de cohérence différent génère les mêmes problèmes que le déplacement d'une machine virtuelle entière. Ces problèmes se produisent si vous déplacez un disque vers un groupe de cohérence différent au sein du même groupe de protection ou si vous le déplacez dans un groupe de protection différent. Site Recovery Manager ne vous empêche pas de le faire, mais si un disque a été déplacé vers un groupe de cohérence différent, la mise sous tension de la machine virtuelle échoue après le déplacement.

Utilisation de Site Recovery Manager avec vSphere Replication sur les sites disposant de Storage DRS ou de Storage vMotion

Vous devez suivre les directives si vous utilisez vSphere Replication pour protéger les machines virtuelles sur des sites qui utilisent Storage DRS ou Storage vMotion.

- vSphere Replication est compatible avec vSphere Storage vMotion et vSphere Storage DRS sur le site protégé. Vous pouvez utiliser Storage vMotion et Storage DRS pour déplacer les fichiers de disque d'une machine virtuelle protégée par vSphere Replication sans affecter la réplication.
- vSphere Replication est compatible avec Storage vMotion et enregistre l'état d'un disque ou d'une machine virtuelle lorsque le répertoire de base d'un disque ou d'une machine virtuelle est déplacé. La réplication du disque ou de la machine virtuelle se poursuit normalement après le déplacement.
- Une synchronisation complète entraîne le déclenchement de Storage vMotion par Storage DRS uniquement si vous configurez une valeur élevée de Storage DRS ou si un grand nombre de machines virtuelles effectuent une synchronisation complète en même temps. Le seuil de latence E/S par défaut de Storage DRS est de 15 ms. Par défaut, Storage DRS effectue des opérations d'équilibrage de charge toutes les 8 heures. Storage DRS attend également d'avoir recueilli suffisamment de statistiques sur la charge E/S pour générer des recommandations de Storage vMotion. Par conséquent, une synchronisation complète n'affecte les recommandations de Storage DRS que si cette synchronisation dure longtemps et si, pendant ce temps, suite aux E/S supplémentaires générées par la synchronisation complète, la latence dépasse le seuil de latence E/S.

Interaction entre Site Recovery Manager et vSphere High Availability

Vous pouvez utiliser Site Recovery Manager pour protéger les machines virtuelles sur lesquelles HA (vSphere High Availability) est activé.

HA protège les machines virtuelles des défaillances de l'hôte ESXi en redémarrant les machines virtuelles des hôtes défaillants sur de nouveaux hôtes du même site. Site Recovery Manager protège les machines virtuelles contre les défaillances intégrales d'un site en redémarrant les machines virtuelles sur le site de récupération. La différence principale entre HA et Site Recovery Manager réside dans le fait que HA opère sur des machines virtuelles individuelles et redémarre automatiquement les machines virtuelles. Site Recovery Manager opère au niveau du plan de récupération et nécessite qu'un utilisateur lance la récupération manuelle.

Pour transférer les paramètres HA à une machine virtuelle sur le site de récupération, vous devez configurer les paramètres HA sur une machine virtuelle à espace réservé avant d'effectuer la récupération. Vous pouvez le faire n'importe quand une fois que la protection de la machine virtuelle est configurée.

Vous pouvez répliquer les machines virtuelles HA à l'aide d'une réplication basée sur des baies ou de vSphere Replication. Si HA redémarre une machine virtuelle protégée sur un autre hôte du site protégé, vSphere Replication effectuera une synchronisation complète après le redémarrage de la machine virtuelle.

Site Recovery Manager ne nécessite pas HA comme condition préalable pour protéger les machines virtuelles. De même, HA n'a pas besoin de Site Recovery Manager.

Protection de machines virtuelles MSCS (Microsoft Cluster Server) et tolérantes aux pannes

Vous pouvez utiliser Site Recovery Manager pour protéger des machines virtuelles MSCS (Microsoft Cluster Server) et tolérantes aux pannes, mais cela comprend certaines restrictions.

Avant d'utiliser Site Recovery Manager pour protéger des machines virtuelles MSCS et tolérantes aux pannes, il peut être nécessaire de modifier votre environnement.

Limitations générales de la protection de machines virtuelles MSCS et tolérantes aux pannes

La protection de machines virtuelles MSCS et tolérantes aux pannes fait l'objet des limitations suivantes.

- Vous ne pouvez protéger les machines virtuelles MSCS qu'avec une réplication basée sur la baie. La protection de machines virtuelles MSCS avec vSphere Replication n'est pas prise en charge.
- La reprotection de machines virtuelles MSCS ou tolérantes aux pannes nécessite VMware High Availability (HA) et VMware Distributed Resource Scheduler (DRS). Lorsque vous transférez

des machines virtuelles MSCS ou tolérantes aux pannes entre leurs sites principaux et secondaires au cours de la reprotection, vous devez activer HA et DRS, et définir les règles d'affinité et d'anti-affinité de manière appropriée. Reportez-vous à la section [Conditions requises de DRS pour la protection de machines virtuelles MSCS](#).

- vSphere ne prend pas en charge vSphere vMotion pour les machines virtuelles MSCS.

Conditions requises des hôtes ESXi pour la protection de machines virtuelles MSCS

Pour protéger des machines virtuelles MSCS ou tolérantes aux pannes, les ordinateurs hôtes ESXi sur lesquels les machines virtuelles s'exécutent doivent répondre à certains critères.

- Vous devez exécuter une machine virtuelle tolérante aux pannes et son fantôme sur deux instances distinctes d'ESXi Server.
- Vous pouvez exécuter un cluster de machines virtuelles MSCS dans les configurations suivantes.

Cluster dans un boîtier

Les machines virtuelles MSCS du cluster s'exécutent sur un seul ESXi Server. Vous pouvez disposer d'un maximum de cinq nœuds MSCS sur un ESXi Server.

Cluster sur boîtiers

Vous pouvez répartir le cluster MSCS sur un maximum de cinq instances d'ESXi Server. Vous ne pouvez protéger qu'un seul nœud de machine virtuelle d'un cluster MSCS sur une instance d'ESXi Server. Plusieurs machines virtuelles du nœud MSCS peuvent être exécutées sur un hôte ESXi, pour autant qu'elles ne fassent pas partie du même cluster MSCS. Cette configuration requiert un stockage partagé sur un Fibre Channel SAN pour le disque quorum.

Conditions requises de DRS pour la protection de machines virtuelles MSCS

Pour utiliser DRS sur des sites contenant des machines virtuelles MSCS, vous devez configurer les règles DRS de sorte à permettre à Site Recovery Manager de protéger les machines virtuelles. En suivant les directives, vous pouvez protéger les machines virtuelles MSCS sur des sites qui exécutent DRS si les machines virtuelles à espace réservé se trouvent dans un déploiement MSCS CAB (cluster-across-boxes) ou un déploiement MSCS CIB (cluster-in-a-box).

- Dans la mesure où vSphere ne prend pas en charge vSphere vMotion pour les machines virtuelles MSCS, vous devez définir la règle DRS `VM/hôte` de telle sorte que DRS n'exécute pas vMotion sur les nœuds MSCS. Définissez la règle `VM/hôte` pour les machines virtuelles sur le site protégé et pour les machines virtuelles fantômes sur le site de récupération.
- Définissez les règles DRS sur les machines virtuelles du site protégé avant de configurer MSCS dans les systèmes d'exploitation invités. Définissez les règles DRS immédiatement après le déploiement, la configuration ou la mise sous tension des machines virtuelles.

- Sur le site de récupération, définissez les règles DRS sur les machines virtuelles immédiatement après la création d'un groupe de protection de nœuds MSCS, dès que les machines virtuelles à espace réservé se retrouvent sur le site de récupération.
- Les règles DRS que vous définissez sur le site protégé ne sont pas transférées sur le site de récupération après une récupération. Pour cette raison, vous devez définir les règles DRS sur les machines virtuelles à espace réservé sur le site de récupération.
- N'exécutez pas un test de récupération ou une récupération réelle avant d'avoir défini les règles DRS sur le site de récupération.

Si vous ne suivez pas les directives sur le site protégé ou le site de récupération, vSphere vMotion risque de déplacer des machines virtuelles MSCS vers une configuration non prise en charge par Site Recovery Manager.

- Dans un déploiement CIB (cluster-in-a-box) sur le site protégé ou le site de récupération, vSphere vMotion peut transférer les machines virtuelles MSCS vers d'autres hôtes ESXi.
- Dans un déploiement CIB (cluster-in-a-box) sur le site protégé ou de récupération, vSphere vMotion peut transférer une partie ou l'ensemble des machines virtuelles MSCS vers un hôte ESXi spécifique.

Créer, tester et exécuter un plan de récupération

Vous pouvez effectuer plusieurs groupes de tâches pour créer, tester et exécuter un plan de récupération.

Procédure

1 Créer un plan de récupération

Vous pouvez créer un plan de récupération pour établir la manière dont les machines seront récupérées par Site Recovery Manager.

2 Modifier un plan de récupération

Vous pouvez modifier un plan de récupération, afin de changer les propriétés que vous avez spécifiées lors de sa création. Vous pouvez modifier les plans de récupération à partir du site protégé ou du site de récupération.

3 Suspendre les machines virtuelles lors de l'exécution d'un plan de récupération

Site Recovery Manager peut suspendre des machines virtuelles sur le site de récupération au cours d'un test de récupération ou d'une récupération réelle.

4 Tester un plan de récupération

Lorsque vous testez un plan de récupération, Site Recovery Manager exécute le plan de récupération sur un réseau de test et un snapshot temporaire des données répliquées au niveau du site de récupération. Site Recovery Manager n'interrompt aucune opération au niveau du site protégé.

5 Nettoyage après l'essai d'un plan de récupération

Après avoir testé un plan de récupération, vous pouvez restaurer ce dernier à l'état Prêt en exécutant une opération de nettoyage.

6 Exécuter un plan de récupération

Lorsque vous exécutez un plan de récupération, Site Recovery Manager migre toutes les machines virtuelles de ce plan vers le site de récupération. Site Recovery Manager tente ensuite d'arrêter les machines virtuelles correspondantes sur le site protégé.

7 Récupérer un snapshot d'une machine virtuelle à un moment spécifique

Avec vSphere Replication, vous pouvez conserver des snapshots d'une machine virtuelle à un moment spécifique. Vous pouvez configurer Site Recovery Manager afin de récupérer un certain nombre de snapshots d'une machine virtuelle à un moment spécifique (PIT) lorsque vous exécutez un plan de récupération.

Créer un plan de récupération

Vous pouvez créer un plan de récupération pour établir la manière dont les machines seront récupérées par Site Recovery Manager.

Pendant les tests, isolez les machines virtuelles récupérées par Site Recovery Manager. Lorsque Site Recovery Manager met en ligne des machines dupliquées et qu'elles commencent à interagir avec des machines virtuelles non protégées de votre réseau de production, des erreurs peuvent se produire.

Procédure

- 1 Cliquez sur **Plans de récupération**, cliquez sur l'onglet **Résumé** puis sur **Créer un plan de récupération**.
- 2 Sélectionnez le site de récupération.
- 3 Sélectionnez un ou plusieurs groupes de protection pour le plan à récupérer et cliquez sur **Suivant**.
- 4 Sélectionnez un réseau de site de récupération auquel les machines virtuelles récupérées se connectent durant les tests du plan de récupération et cliquez sur **Suivant**.

Vous pouvez isoler des restaurations de machines virtuelles Site Recovery Manager pendant les récupérations de tests en sélectionnant **Auto**, qui est un réseau isolé, ou en sélectionnant un réseau que vous avez créé manuellement mais qui n'est pas connecté aux autres réseaux.
- 5 Entrez un nom pour le plan dans la zone de texte **Nom du plan de récupération**, ajoutez une description facultative et cliquez sur **Suivant**.
- 6 Consultez les informations récapitulatives et cliquez sur **Terminer** pour créer le plan de récupération.

Vous pouvez suivre la création du plan dans la vue Tâches récentes.

Modifier un plan de récupération

Vous pouvez modifier un plan de récupération, afin de changer les propriétés que vous avez spécifiées lors de sa création. Vous pouvez modifier les plans de récupération à partir du site protégé ou du site de récupération.

Procédure

- 1 Cliquez sur **Plans de récupération**, puis cliquez avec le bouton droit de la souris sur un plan de récupération et sélectionnez **Modifier le plan de récupération**.
- 2 Cliquez sur **Suivant**.
Vous ne pouvez pas modifier le site de récupération.
- 3 Sélectionnez un ou plusieurs groupes de protection pour le plan à récupérer et cliquez sur **Suivant**.
- 4 Sélectionnez un réseau de site de récupération auquel les machines virtuelles récupérées se connectent pendant les tests du plan de récupération, puis cliquez sur **Suivant**.
- 5 Modifiez le nom du plan dans la zone de texte **Nom du plan de récupération** et ajoutez une description facultative.
- 6 Cliquez sur **Suivant**.
- 7 Consultez les informations récapitulatives et cliquez sur **Terminer** pour appliquer les modifications spécifiées au plan de récupération.

Vous pouvez suivre la mise à jour du plan dans la vue Tâches récentes.

Suspendre les machines virtuelles lors de l'exécution d'un plan de récupération

Site Recovery Manager peut suspendre des machines virtuelles sur le site de récupération au cours d'un test de récupération ou d'une récupération réelle.

La suspension de machines virtuelles sur le site de récupération est utile dans les environnements de centre de données actifs-actifs et lorsque les charges de travail non critiques sont exécutées sur les sites de récupération. En suspendant des machines virtuelles qui hébergent des charges de travail non critiques sur le site de récupération, Site Recovery Manager libère de la capacité pour les machines virtuelles récupérées.

Vous pouvez uniquement ajouter des machines virtuelles pour suspendre au niveau du site de récupération. Pour suspendre des machines virtuelles au niveau des sites protégé et de récupération, vous devez exécuter une récupération puis inverser la protection en exécutant une opération de reprotection avant de pouvoir ajouter des machines virtuelles à suspendre sur le site protégé d'origine. Si vous configurez des machines virtuelles à suspendre au niveau des deux sites, le plan démarre des machines virtuelles sur un site et les suspend sur l'autre avec chaque récupération que vous exécutez.

Procédure

- 1 Sur le site de récupération, cliquez sur **Plans de récupération** dans le volet de gauche et sélectionnez le plan de récupération à modifier.
- 2 Cliquez sur l'onglet **Étapes de récupération** et cliquez sur **Ajouter une VM non critique**.
- 3 Développez la liste hiérarchique pour sélectionner les machines virtuelles sur le site de récupération à suspendre pendant la récupération.
- 4 Cliquez sur **OK**.

Résultats

Site Recovery Manager suspend les machines virtuelles sur le site de récupération lorsque le plan de récupération s'exécute.

Tester un plan de récupération

Lorsque vous testez un plan de récupération, Site Recovery Manager exécute le plan de récupération sur un réseau de test et un snapshot temporaire des données répliquées au niveau du site de récupération. Site Recovery Manager n'interrompt aucune opération au niveau du site protégé.

Le test d'un plan de récupération exécute toutes les étapes du plan, à l'exception de la mise hors tension des machines virtuelles au niveau du site protégé et du forçage des périphériques au niveau du site de récupération pour s'attribuer le contrôle des données répliquées. Si le plan nécessite la suspension des machines virtuelles locales au niveau du site de récupération, Site Recovery Manager suspend ces machines virtuelles durant le test. L'exécution d'un test de plan de récupération n'apporte aucune modification à l'environnement de production de l'un des deux sites.

Le test d'un plan de récupération crée un snapshot sur le site de récupération de tous les fichiers de disque des machines virtuelles incluses dans le plan de récupération. La création des snapshots augmente la latence E/S du stockage. Si vous remarquez un ralentissement des temps de réponse lors du test de plans de récupération et si vous utilisez le stockage VMware Virtual SAN, surveillez la latence d'E/S à l'aide de l'outil de surveillance intégré à l'interface de Virtual SAN.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager.
- 2 Sélectionnez le plan de récupération à tester, puis cliquez sur **Test**.
- 3 (Facultatif) Sélectionnez **Répliquer les changements récents vers le site de récupération**.
La sélection de cette option permet de s'assurer que le site de récupération possède la copie la plus récente des machines virtuelles protégées, mais la synchronisation peut demander plus de temps.
- 4 Cliquez sur **Suivant**.
- 5 Passez en revue les informations du test et cliquez sur **Démarrer**.

- 6 Cliquez sur l'onglet **Étapes de récupération** pour surveiller l'avancement du test et répondre aux messages.

L'onglet **Étapes de récupération** affiche la progression des étapes individuelles. L'onglet **Résumé** indique la progression du plan dans son ensemble.

Note Site Recovery Manager initie les étapes de récupération dans l'ordre prescrit, avec une exception. Il n'attend pas que l'étape Préparation du stockage ne se finisse pour tous les groupes de protection avant de passer aux étapes suivantes.

Étape suivante

Exécutez une opération de nettoyage une fois le test du plan de récupération terminé, afin de restaurer le plan de récupération à son état d'origine (antérieur au test).

Nettoyage après l'essai d'un plan de récupération

Après avoir testé un plan de récupération, vous pouvez restaurer ce dernier à l'état Prêt en exécutant une opération de nettoyage.

Site Recovery Manager effectue plusieurs opérations de nettoyage après un test.

- Met hors tension les machines virtuelles récupérées.
- Remplace les machines virtuelles récupérées par des espaces réservés, préservant ainsi les informations relatives à l'identité et à la configuration.
- Nettoie les snapshots de stockage répliqués utilisés au cours du test par les machines virtuelles récupérées.

Conditions préalables

Vérifiez que vous avez testé un plan de récupération.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager, sélectionnez le plan de récupération que vous avez testé, puis cliquez sur **Nettoyer**.
- 2 Passez en revue les informations de nettoyage et cliquez sur **Suivant**.
- 3 Cliquez sur **Démarrer**.
- 4 Une fois le nettoyage terminé, si des erreurs sont signalées, exécutez à nouveau le nettoyage en sélectionnant l'option **Forcer le nettoyage**.

L'option **Forcer le nettoyage** force la suppression des machines virtuelles, en ignorant les erreurs, et ramène le plan à l'état Prêt. Si nécessaire, exécutez le nettoyage plusieurs fois avec l'option **Forcer le nettoyage** jusqu'à ce qu'il aboutisse.

Exécuter un plan de récupération

Lorsque vous exécutez un plan de récupération, Site Recovery Manager migre toutes les machines virtuelles de ce plan vers le site de récupération. Site Recovery Manager tente ensuite d'arrêter les machines virtuelles correspondantes sur le site protégé.

Attention Un plan de récupération fait des modifications importantes dans la configuration des sites protégé et de récupération et arrête la réplication. N'exécutez pas un plan de récupération que vous n'avez pas testé. Dans le cas de la réplication basée sur la baie, les machines virtuelles et les services récupérés peuvent devoir être pris en charge sur le site de récupération pendant un certain temps. Inverser ces modifications pourrait coûter du temps et des efforts considérables et provoquer un temps d'arrêt prolongé du service.

Conditions préalables

Pour utiliser la récupération forcée, vous devez préalablement activer cette fonction. La récupération forcée s'active en activant le paramètre **recovery.forceRecovery** comme décrit dans [Modifier les paramètres de récupération](#).

Procédure

- 1 Cliquez sur **Plans de récupération** dans le volet de gauche, sélectionnez le plan de récupération à exécuter, et cliquez sur **Récupération**.
- 2 Vérifiez les informations indiquées dans l'invite de confirmation et sélectionnez **Je comprends que ce processus modifiera de façon permanente les machines virtuelles ainsi que l'infrastructure des centres de données protégés et de récupération**.
- 3 Sélectionnez le type de récupération à exécuter.

Option	Description
Migration planifiée	Récupère des machines virtuelles vers le site de récupération lorsque les deux sites sont en cours de fonctionnement. Si une erreur se produit sur le site protégé lors d'une migration planifiée, l'opération de migration planifiée échoue.
Récupération d'urgence	Récupère les machines virtuelles vers le site de récupération si le site protégé rencontre un problème. Si des erreurs se produisent sur le site protégé lors d'une reprise après sinistre, la reprise après sinistre continue et n'échoue pas.

- 4 (Facultatif) Sélectionnez la case à cocher **Récupération forcée - opérations de site de récupération uniquement**.

Cette option est disponible si vous avez sélectionné **Récupération d'urgence** et activé la fonction de récupération forcée.

- 5 Cliquez sur **Suivant**.
- 6 Passez en revue les informations de récupération et cliquez sur **Démarrer**.

7 Cliquez sur l'onglet **Étapes de récupération**.

L'onglet **Étapes de récupération** affiche la progression des étapes individuelles. La zone Tâches récentes indique la progression de l'intégralité du plan.

Récupérer un snapshot d'une machine virtuelle à un moment spécifique

Avec vSphere Replication, vous pouvez conserver des snapshots d'une machine virtuelle à un moment spécifique. Vous pouvez configurer Site Recovery Manager afin de récupérer un certain nombre de snapshots d'une machine virtuelle à un moment spécifique (PIT) lorsque vous exécutez un plan de récupération.

Vous configurez la rétention de snapshots PIT lors de la configuration de vSphere Replication sur une machine virtuelle. Pour plus d'informations sur les snapshots PIT, reportez-vous à [Réplication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques](#).

Note Vous ne pouvez pas utiliser l'interface de Site Recovery Manager pour configurer une réplication qui utilise des snapshots à un moment précis (PIT). Pour activer les snapshots PIT, configurez la réplication d'une machine virtuelle à l'aide de Client Web vSphere. Reportez-vous à [Configurer la réplication d'une machine virtuelle unique](#) dans Administration de *vSphere Replication*.

Au cours d'une récupération, Site Recovery Manager ne récupère que le snapshot du moment spécifique le plus récent. Pour récupérer des snapshots plus anciens, vous devez activer l'option **vrReplication > preserveMpitImagesAsSnapshots** sous **Paramètres avancés** dans l'interface de Site Recovery Manager. Reportez-vous à [Modifier les paramètres de vSphere Replication](#).

Si vous récupérez un snapshot PIT d'une machine virtuelle pour laquelle vous avez configuré la personnalisation IP, Site Recovery Manager applique uniquement la personnalisation au snapshot PIT le plus récent. Si vous récupérez un ancien snapshot PIT d'une machine virtuelle avec la personnalisation IP, vous devez configurer manuellement les paramètres IP.

La récupération à un moment spécifique n'est pas disponible avec la réplication basée sur la baie.

Procédure

- 1 Configurez Site Recovery Manager afin de conserver d'anciens snapshots PIT en paramétrant l'option **vrReplication > preserveMpitImagesAsSnapshots**.
- 2 Utilisez Client Web vSphere pour configurer la réplication d'une machine virtuelle en sélectionnant l'option permettant de conserver un certain nombre de snapshots PIT.
- 3 Dans l'interface de Site Recovery Manager, ajoutez la machine virtuelle à un groupe de protection vSphere Replication.
- 4 Incluez le groupe de protection vSphere Replication à un plan de récupération.

5 Exécutez le plan de récupération.

Lorsque le plan de récupération est terminé, la machine virtuelle est récupérée sur le site de récupération, avec le nombre de snapshots PIT que vous avez configuré.

6 Dans la vue **VM et modèles**, cliquez avec le bouton droit de la souris sur la machine virtuelle récupérée puis sélectionnez **Snapshot > Gestionnaire de snapshot**.

7 Sélectionnez l'un des snapshots PIT de cette machine virtuelle et cliquez sur **Aller à**.

La machine virtuelle récupérée revient au snapshot PIT que vous avez sélectionné.

8 (Facultatif) Si vous avez configuré la machine virtuelle pour une personnalisation IP, et si vous avez sélectionné un snapshot PIT plus ancien que le plus récent, configurez manuellement les paramètres IP sur la machine virtuelle récupérée.

Étapes pour exporter le plan de récupération

Vous pouvez exporter les étapes d'un plan de récupération dans divers formats pour y faire référence ultérieurement, ou pour conserver une copie imprimée de vos plans.

Vous ne pouvez pas exporter les étapes d'un plan de récupération au cours d'un test de récupération ou d'une récupération réelle.

Conditions préalables

Vérifiez que vous disposez d'un plan de récupération.

Procédure

1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager, sélectionnez un plan de récupération, puis cliquez sur l'onglet **Étapes de récupération**.

2 Cliquez sur **Exporter les étapes**.

Vous pouvez enregistrer les étapes du plan de récupération sous la forme d'un document MS Word, Excel, HTML, CSV ou XML.

Afficher et exporter l'historique du plan de récupération

Vous pouvez afficher et exporter un rapport de chaque exécution d'un plan de récupération, d'un test de plan de récupération ou d'un nettoyage de test.

L'historique d'un plan de récupération fournit des informations sur chaque exécution, test ou nettoyage du plan de récupération. L'historique contient des informations sur le résultat et les heures de début et de fin du plan complet, et de chaque étape qu'il comporte. Vous ne pouvez pas exporter l'historique du plan de récupération pendant le déroulement d'un test de récupération, d'une récupération réelle ou d'un nettoyage de test.

Conditions préalables

Vous avez exécuté ou testé un plan de récupération, ou vous avez procédé à un nettoyage après un test.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager, sélectionnez un plan de récupération, puis cliquez sur l'onglet **Historique**.
- 2 (Facultatif) Cliquez sur **Affichage** pour une opération d'exécution, de test ou de nettoyage d'un plan de récupération.

L'historique s'ouvre dans un navigateur.

- 3 (Facultatif) Cliquez sur **Exporter** pour une opération d'exécution, de test ou de nettoyage d'un plan de récupération.

Vous pouvez enregistrer l'historique du plan de récupération sous la forme d'un document MS Word, Excel, HTML, CSV ou XML.

Annuler un test ou une récupération

Vous pouvez annuler un test de plan de récupération à tout moment de son exécution. Vous pouvez annuler une migration planifiée ou de récupération d'urgence à certains moments de leur exécution.

Lorsque vous annulez un test ou une récupération, Site Recovery Manager ne démarre aucune étape et utilise certaines règles pour arrêter les étapes en cours.

- Les étapes ne pouvant être arrêtées, telles que la mise sous tension ou l'attente d'un signal de pulsation, continuent jusqu'à ce qu'elles soient achevées avant que l'annulation ne soit effectuée.
- Si vous annulez, les étapes ajoutant ou supprimant des périphériques de stockage le sont par le nettoyage.

La durée d'annulation d'un test ou d'une récupération dépend du type et du nombre d'étapes actuellement en cours.

Procédure

- ◆ Pour annuler un test ou une récupération, cliquez sur **Annuler** dans la barre d'outils Plan de récupération.

Supprimer un plan de récupération

Vous pouvez supprimer un plan de récupération si vous n'en avez pas besoin.

La suppression d'un plan de récupération n'efface pas l'historique de ce plan, auquel vous pouvez toujours accéder via l'onglet **Tous les plans de récupération > Tout l'historique**.

Procédure

- 1 Cliquez sur **Plans de récupération** et sélectionnez le plan de récupération à supprimer.
- 2 (Facultatif) Cliquez sur l'onglet **Historique**, puis sur **Exporter la liste** pour télécharger l'historique de ce plan.
- 3 Cliquez avec le bouton droit de la souris sur le plan de récupération à supprimer, puis sélectionnez **Supprimer le plan de récupération**.

Reprotection des machines virtuelles après une récupération

5

Après une récupération, le site de récupération devient le nouveau site protégé, mais il n'est pas encore protégé. Si le site protégé d'origine est toujours opérationnel, vous pouvez inverser la direction de protection afin d'utiliser le site protégé d'origine comme nouveau site de récupération et protéger le nouveau site protégé.

Le rétablissement manuel de la protection dans le sens opposé en recréant tous les groupes de protection et plans de récupération prend beaucoup de temps et constitue une source d'erreurs. Site Recovery Manager offre une fonction de reprotection, qui consiste en une inversion automatisée du sens de protection.

Après que Site Recovery Manager a effectué une récupération, les machines virtuelles protégées démarrent sur le site de récupération. Dans la mesure où le site précédemment protégé peut être hors ligne, ces machines virtuelles ne sont pas protégées. En exécutant une reprotection lorsque le site protégé revient en ligne, vous pouvez inverser le sens de réplication, afin de protéger les machines virtuelles récupérées sur le site de récupération qui sont de retour sur le site protégé d'origine.

La reprotection utilise les informations relatives à la protection établies par vos soins avant une récupération pour inverser le sens de protection. Vous pouvez uniquement exécuter le processus de reprotection après une récupération. Si la récupération se termine avec des erreurs, vous devez supprimer toutes les erreurs et effectuer à nouveau la récupération, en répétant ce processus jusqu'à ce qu'il n'y ait plus d'erreurs.

Vous pouvez effectuer des tests après une opération de reprotection, afin de confirmer que les nouvelles configurations du site protégé et du site de récupération sont valides.

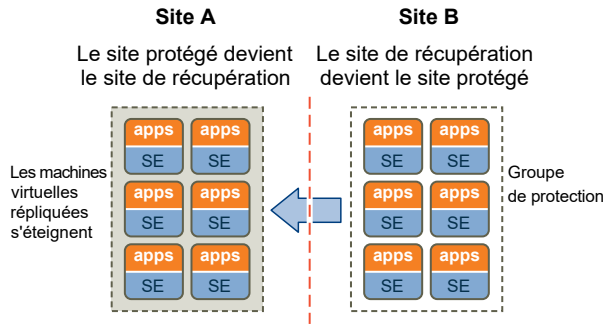
Vous pouvez exécuter la reprotection sur des groupes de protection qui contiennent des machines virtuelles étant configurées pour la réplication basée sur la baie et pour vSphere Replication.

Exemple : Exécution d'une opération de reprotection

Le site A est le site protégé et le site B est le site de récupération. Si le site A passe au statut hors ligne, Site Recovery Manager récupère les machines virtuelles protégées sur le site B. Après la récupération, les machines virtuelles protégées du site A démarrent sans protection sur le site B.

Lorsque le site A revient en ligne, vous pouvez exécuter une opération de reprotection, afin de protéger les machines virtuelles récupérées sur le site B. Le site B devient alors le site protégé et le site A le site de récupération. Site Recovery Manager inverse le sens de réplication du site B vers le site A.

Figure 5-1. Processus de reprotection Site Recovery Manager



Le sens de la réplication est inversé après une migration planifiée

- **Exécution d'une opération de reprotection par Site Recovery Manager**

Le processus de reprotection comprend deux étapes. Site Recovery Manager inverse la direction de protection, puis force une synchronisation du stockage du nouveau site protégé vers le nouveau site de récupération.

- **Conditions préalables à l'exécution d'une opération de reprotection**

Vous ne pouvez effectuer une opération de reprotection que si certaines conditions préalables sont remplies.

- **Reprotéger les machines virtuelles**

La reprotection entraîne la reconfiguration des groupes de protection et des plans de récupération Site Recovery Manager de sorte qu'ils fonctionnent dans le sens inverse. Grâce à la reprotection, vous pouvez restaurer des machines virtuelles sur leur site initial après une récupération.

- **États de reprotection**

Le processus de reprotection passe par plusieurs états que vous pouvez visualiser dans le plan de récupération du plug-in Site Recovery Manager de vSphere Client.

Exécution d'une opération de reprotection par Site Recovery Manager

Le processus de reprotection comprend deux étapes. Site Recovery Manager inverse la direction de protection, puis force une synchronisation du stockage du nouveau site protégé vers le nouveau site de récupération.

Lorsque vous initiez le processus de reprotection, Site Recovery Manager ordonne aux baies de stockage sous-jacentes ou à vSphere Replication d'inverser la direction de réplication. Après l'inversion de la réplication, Site Recovery Manager crée les machines virtuelles à espace réservé sur le nouveau site de récupération (qui était le site protégé initial, avant la reprotection).

Lors de la création des machines virtuelles à espace réservé sur le nouveau site protégé, Site Recovery Manager utilise l'emplacement de la machine virtuelle protégée initiale pour déterminer l'emplacement où créer la machine virtuelle à espace réservé. Site Recovery Manager utilise l'identité de la machine virtuelle protégée initiale pour créer la machine virtuelle à espace réservé ainsi que toute autre machine virtuelle récupérée ultérieurement. Si les machines virtuelles protégées initiales ne sont plus disponibles, Site Recovery Manager utilise les mappages d'inventaire du site de récupération initial vers le site protégé initial, afin de déterminer les pools de ressources et les dossiers des machines virtuelles à espace réservé. Vous devez configurer les mappages d'inventaire sur les deux sites avant d'effectuer la reprotection, sous peine d'échec de l'opération.

Lors de la reprotection à l'aide de la réplication basée sur des baies, Site Recovery Manager place les fichiers des machines virtuelles à espace réservé dans la banque de données à espace réservé du site protégé initial et non dans la banque de données qui contenait les machines virtuelles protégées initiales.

Forcer la synchronisation des données, à partir du nouveau site de protection vers le nouveau site de récupération, contribue à garantir que le site de récupération dispose d'une copie actuelle des machines virtuelles protégées en cours d'exécution sur le site de protection. Cela permet également de garantir qu'une récupération est possible dès que la reprotection est terminée.

Lors de la reprotection à l'aide de vSphere Replication, Site Recovery Manager utilise les fichiers VMDK originaux comme copies initiales pendant la synchronisation. La synchronisation complète, qui apparaît dans les étapes de la récupération, effectue surtout des totaux de contrôles. Seule une petite partie des données est transférée via le réseau.

Conditions préalables à l'exécution d'une opération de reprotection

Vous ne pouvez effectuer une opération de reprotection que si certaines conditions préalables sont remplies.

Vous pouvez exécuter la reprotection sur des groupes de protection qui contiennent des machines virtuelles étant configurées pour la réplication basée sur la baie et pour vSphere Replication.

Avant de pouvoir effectuer une opération de reprotection, vous devez remplir ces conditions préalables.

- 1 Exécutez une migration planifiée et veillez à ce que toutes les étapes du plan de récupération s'achèvent avec succès. Si des erreurs surviennent pendant la récupération, résolvez les

problèmes qui en sont à l'origine et exécutez à nouveau la récupération. Lorsque vous réexécutez une récupération, les opérations qui ont abouti précédemment sont ignorées. Par exemple, les machines virtuelles récupérées avec succès ne le sont pas de nouveau et continuent de fonctionner sans interruption.

- 2 Le site protégé d'origine doit être disponible. Les instances vCenter Server, les serveurs ESXi, les instances du Serveur Site Recovery Manager et les bases de données correspondantes doivent tous être récupérables.
- 3 Si vous effectuez une opération de récupération d'urgence, vous devez aussi effectuer une migration planifiée lorsque les deux sites fonctionnent encore. Si des erreurs se produisent pendant la tentative de migration planifiée, vous devez résoudre les erreurs et réexécuter la migration planifiée jusqu'à ce qu'elle réussisse.

L'opération de reprotection n'est pas disponible dans certaines circonstances.

- Il est impossible de terminer des plans de récupération sans erreurs. Pour que la reprotection soit disponible, toutes les étapes du plan de récupération doivent se terminer avec succès.
- Le site d'origine ne peut être restauré si, par exemple, il est détruit physiquement. Pour annuler le couplage entre le site protégé et le site de récupération et le recréer, les deux sites doivent être disponibles. Si vous ne pouvez pas restaurer le site protégé d'origine, vous devez réinstaller Site Recovery Manager sur les sites protégé et de récupération.

Reprotéger les machines virtuelles

La reprotection entraîne la reconfiguration des groupes de protection et des plans de récupération Site Recovery Manager de sorte qu'ils fonctionnent dans le sens inverse. Grâce à la reprotection, vous pouvez restaurer des machines virtuelles sur leur site initial après une récupération.

Conditions préalables

Reportez-vous à [Conditions préalables à l'exécution d'une opération de reprotection](#).

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager, sélectionnez un plan de récupération, puis cliquez sur **Reprotéger**.
- 2 Cochez la case pour confirmer que vous comprenez que l'opération de reprotection est irréversible.
- 3 Passez en revue les informations de reprotection et cliquez sur **Suivant**.
- 4 Cliquez sur l'onglet **Étapes de récupération** pour surveiller l'avancement de l'opération de reprotection.

Certaines étapes ne s'appliquent pas à toutes les machines virtuelles. Par exemple, les machines virtuelles que vous avez configurées pour une répllication basée sur la baie

s'affichent dans la section **Configurer le stockage en direction inverse > Groupe de protection > Configurer la réplication VR**, même si cette étape n'effectue aucune action sur ces machines. Ces machines virtuelles sont libellées comme Non applicables pendant l'exécution de cette étape.

- 5 Lorsque l'opération de reprotection se termine, sélectionnez le plan de récupération, cliquez sur **Historique**, puis sur **Afficher** pour l'opération de reprotection.

Le rapport d'historique de l'opération de reprotection s'ouvre dans un navigateur. Le plan de récupération peut renvoyer l'état Prêt même si des erreurs se sont produites lors de l'opération de reprotection. Vérifiez le rapport d'historique de l'opération de reprotection pour vous assurer qu'aucune erreur ne s'est produite. Des erreurs se sont produites lors de la reprotection ; essayez de corriger les erreurs et exécutez une récupération test pour vous assurer que les erreurs ont été corrigées. Si vous ne corrigez pas les erreurs qui se sont produites lors de la reprotection, puis que vous tentez d'exécuter une migration planifiée ou une reprise après sinistre sans les avoir corrigées, il est possible que la récupération de certaines machines virtuelles échoue.

Résultats

Site Recovery Manager inverse le site de récupération et les sites protégés. Site Recovery Manager crée des copies réservées des machines virtuelles du nouveau site protégé, au niveau du nouveau site de récupération.

États de reprotection

Le processus de reprotection passe par plusieurs états que vous pouvez visualiser dans le plan de récupération du plug-in Site Recovery Manager de vSphere Client.

Si la reprotection échoue, ou ne réussit qu'en partie, vous pouvez prendre des mesures correctives et achever la reprotection.

Tableau 5-1. États de reprotection

État	Description	Mesure corrective
Reprotection en cours	Site Recovery Manager exécute la reprotection.	Aucun
Reprotection partielle	Survient lorsque plusieurs plans de récupération partagent les mêmes groupes de protection et que la reprotection réussit pour certains groupes de certains plans, mais pas pour d'autres.	Exécutez une nouvelle reprotection des plans reprotégés en partie.

Tableau 5-1. États de reprotection (suite)

État	Description	Mesure corrective
Reprotection incomplète	Apparaît à cause d'échecs lors de la reprotection. Cet état peut, par exemple, survenir en raison d'un échec de synchronisation du stockage ou d'un échec de création de machines virtuelles à espace réservé.	<ul style="list-style-type: none"> ■ Si un échec de synchronisation du stockage fait échouer une opération de reprotection, assurez-vous que les sites sont connectés, examinez la progression de la reprotection dans vSphere Client, puis redémarrez la tâche de reprotection. Si la reprotection ne peut toujours pas être menée à son terme, exécutez-la à nouveau à l'aide de l'option Forcer le nettoyage. ■ Si la création de machines virtuelles à espace réservé par Site Recovery Manager échoue, il est toujours possible de procéder à des récupérations. Examinez les étapes de reprotection dans vSphere Client, corrigez tous les problèmes en cours et redémarrez la tâche de reprotection.
Reprotection interrompue	Survient lorsque l'un des serveurs Site Recovery Manager s'arrête de façon inattendue au cours du processus de reprotection.	Assurez-vous que les deux serveurs Site Recovery Manager sont en cours d'exécution, puis redémarrez la tâche de reprotection.

Restauration de la configuration du site de pré-récupération par l'exécution d'un retour arrière

6

Pour rétablir la configuration d'origine des sites protégé et de récupération après une récupération, vous pouvez exécuter une séquence de procédures facultatives appelée « retour arrière ».

Après une migration planifiée ou une récupération d'urgence, l'ancien site de récupération devient le site protégé. Immédiatement après la récupération, le nouveau site protégé ne dispose pas de site de récupération où exécuter une récupération. Si vous exécutez une reprotection, le nouveau site protégé est protégé par le site de protection d'origine, ce qui inverse le sens initial de protection. Pour obtenir des informations sur la reprotection, reportez-vous à [Chapitre 5 Reprotection des machines virtuelles après une récupération](#).

Pour rétablir la configuration du site protégé et du site de récupération à la configuration initiale (avant la récupération), effectuez un retour arrière.

Pour procéder à un retour arrière, exécutez une séquence d'opérations de reprotection et de migration planifiée.

- 1 Effectuer une reprotection. Le site de récupération devient le site protégé. Le site précédemment protégé devient le site de récupération.
- 2 Effectuez une migration planifiée afin d'éteindre les machines virtuelles du site protégé et démarrez les machines virtuelles du site de récupération. Pour éviter les ruptures de disponibilité des machines virtuelles, il peut être judicieux d'effectuer un test afin de procéder à la migration planifiée. Ainsi, si le test détecte des erreurs, vous pourrez corriger celles-ci avant d'effectuer la migration planifiée.
- 3 Effectuez une deuxième reprotection, afin de restaurer les configurations d'origine du site protégé et du site de récupération, telles qu'elles étaient avant la récupération.

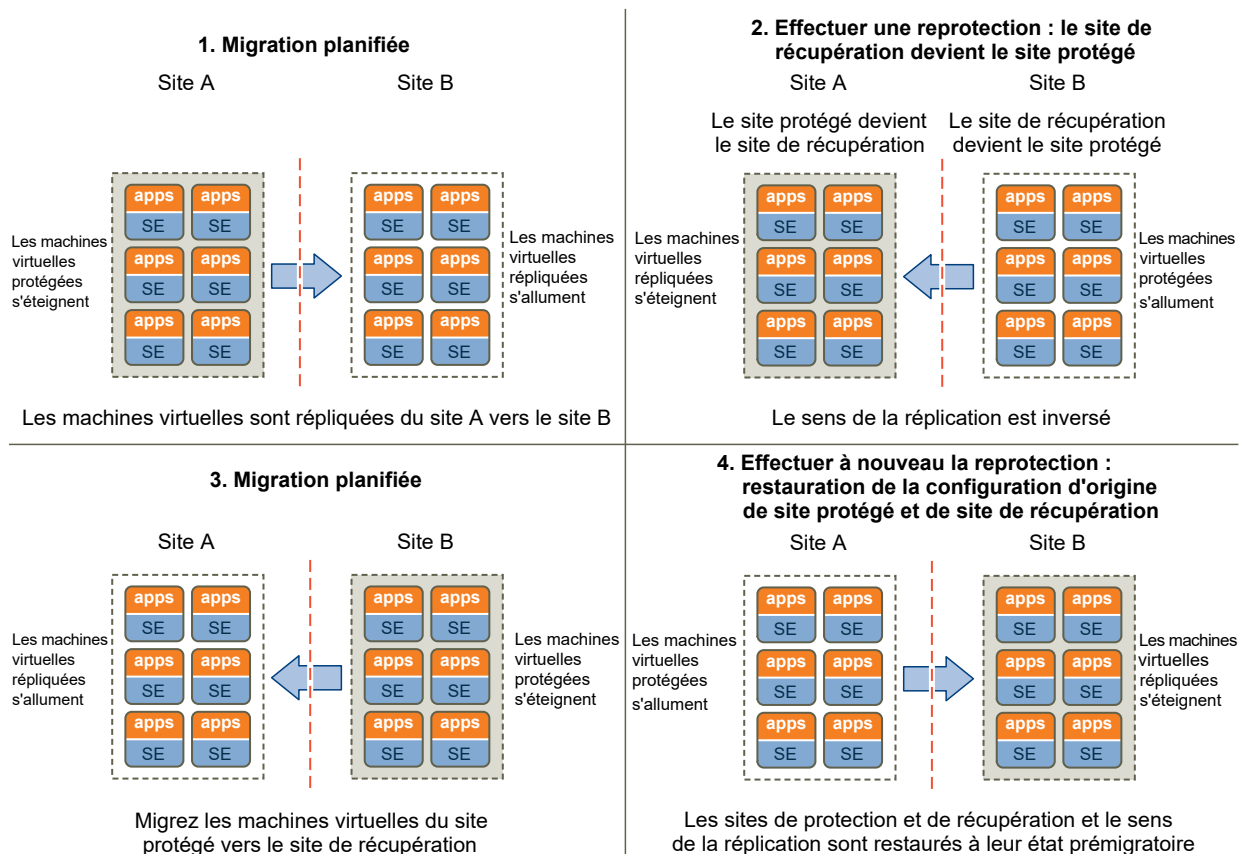
Vous pouvez configurer et exécuter un retour arrière lorsque vous êtes prêt à rétablir les services pour le site protégé d'origine, après l'avoir ramené en ligne après un incident.

Exemple : Exécution d'une opération de retour arrière

Le site A est le site protégé et B est le site de récupération. Une récupération est effectuée, faisant migrer les machines virtuelles du site A vers le site B. Pour restaurer le site A en tant que site protégé, vous effectuez un retour arrière.

- Effectuer une reprotection. Le site B, précédemment site de récupération, devient le site protégé. Site Recovery Manager utilise les informations de protection afin d'établir la protection du site B. Le site A devient le site de récupération.
- Effectuez une migration planifiée pour récupérer les machines virtuelles du site B sur le site A.
- Effectuez une deuxième reprotection. Le site A devient le site protégé et le site B le site de récupération.

Figure 6-1. Processus de retour arrière Site Recovery Manager



Ce chapitre contient les rubriques suivantes :

- [Effectuer un retour arrière](#)

Effectuer un retour arrière

Après que Site Recovery Manager a procédé à une récupération, vous pouvez effectuer un retour arrière, afin de restaurer la configuration d'origine des sites protégé et de récupération.

Pour faciliter la compréhension, le site protégé d'origine d'avant la récupération est appelé site A. Le site de récupération d'origine est appelé site B. Après une récupération du site A vers le site B, les machines virtuelles récupérées fonctionnent sans protection sur le site B sans.

Conditions préalables

Vérifiez que les conditions suivantes sont réunies.

- Vous avez procédé à une récupération, dans le cadre d'une migration planifiée ou d'une récupération d'urgence.
- Le site protégé d'origine, site A, fonctionne.
- Si vous avez procédé à une récupération d'urgence, vous devez effectuer une récupération de migration planifiée lorsque les hôtes et banques de données du site protégé, le site A, fonctionnent encore.
- Vous n'avez effectué aucune reprotection depuis la récupération.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager, sélectionnez un plan de récupération, puis cliquez sur **Reprotéger**.

- 2 Cochez la case pour confirmer que vous comprenez que l'opération de reprotection est irréversible.

- 3 Passez en revue les informations de reprotection et cliquez sur **Suivant**.

- 4 Surveillez l'opération de reprotection de l'onglet **Étapes de récupération** jusqu'à la fin.

- 5 (Facultatif) Si nécessaire, exécutez à nouveau la reprotection jusqu'à ce qu'elle s'achève sans erreurs.

À la fin de l'opération de reprotection, Site Recovery Manager aura inversé la réplication, de sorte que le site de récupération d'origine, le site B, soit dorénavant le site protégé.

- 6 (Facultatif) Cliquez sur **Test** puis suivez les invites pour tester le plan de récupération.

Le test du plan de récupération vérifie que ce plan fonctionne après l'opération de reprotection.

- 7 Cliquez sur **Récupération** pour exécuter le plan de récupération en tant que migration planifiée.

- 8 Vérifiez les informations indiquées dans l'invite de confirmation et sélectionnez **Je comprends que ce processus modifiera de façon permanente les machines virtuelles ainsi que l'infrastructure des centres de données protégés et de récupération**.

- 9 Sélectionnez **Migration planifiée**, cliquez sur **Suivant**, puis sur **Démarrer**.

- 10 Surveillez l'opération de migration planifiée de l'onglet **Étapes de récupération** jusqu'à la fin.

La migration planifiée éteint les machines virtuelles du nouveau site protégé, le site B, puis démarre les machines virtuelles du nouveau site de récupération, le site A. Au besoin, exécutez à nouveau la migration planifiée jusqu'à ce qu'elle s'achève sans erreurs.

À la fin de la migration planifiée, les machines virtuelles fonctionnent sur le site protégé d'origine, le site A, mais elles ne sont pas protégées. Les machines virtuelles du site de récupération d'origine, le site B, sont mises hors tension.

- 11 Cliquez sur **Reprotection** et suivez les instructions de l'assistant afin d'effectuer une seconde opération de reprotection.

Le fait d'effectuer une seconde reprotection rétablit la protection dans sa direction d'origine (avant la récupération).

Résultats

Vous avez restauré les sites protégé et de récupération à leur configuration d'origine, précédant la récupération. Le site A est le site protégé et le site B, le site de récupération.

Configuration d'un plan de récupération

7

Vous pouvez configurer un plan de récupération pour exécuter des commandes sur Serveur Site Recovery Manager ou sur une machine virtuelle, afficher des messages nécessitant une réponse lorsque le plan s'exécute, suspendre des machines virtuelles non essentielles lors de la récupération, configurer des dépendances entre les machines virtuelles, personnaliser les paramètres réseau des machines virtuelles et modifier la priorité de récupération des machines virtuelles protégées.

Un simple plan de récupération, spécifiant uniquement un réseau de test auquel les machines virtuelles récupérées se connectent et des valeurs de délai d'expiration en attendant la mise sous tension et la personnalisation des machines virtuelles, peut être un moyen efficace de tester une configuration Site Recovery Manager. La plupart des plans de récupération nécessitent une configuration adaptée pour une utilisation en production. Par exemple, un plan de récupération destiné à la gestion d'une urgence sur le site protégé peut être différent d'un plan de récupération assurant la migration planifiée des services d'un site à l'autre.

Note Un plan de récupération reflète toujours l'état actuel des groupes de protection qu'il récupère. Si un membre d'un groupe de protection affiche un statut autre que OK, vous devez résoudre les problèmes avant de pouvoir modifier le plan de récupération.

■ Étapes d'un plan de récupération

Un plan de récupération exécute une série d'étapes devant être effectuées dans un ordre spécifique. Vous ne pouvez pas modifier l'ordre ou l'objectif de ces étapes, mais vous pouvez insérer vos propres étapes affichant des messages et exécutant des commandes.

■ Spécifier la priorité de récupération d'une machine virtuelle

Site Recovery Manager définit par défaut toutes les machines virtuelles d'un nouveau plan de récupération sur le niveau 3 de priorité de récupération. Vous pouvez cependant augmenter ou réduire le niveau de priorité de récupération d'une machine virtuelle.

■ Créer des étapes de récupération personnalisées

Vous pouvez créer des étapes de récupération personnalisées qui exécutent des commandes ou présentent des messages à l'utilisateur lors d'une récupération.

■ Personnaliser la récupération d'une machine virtuelle individuelle

Vous pouvez configurer une machine virtuelle dans un plan de récupération, afin qu'elle utilise une spécification de personnalisation donnée ou exécute des étapes de message ou de commande lorsqu'elle est récupérée.

Étapes d'un plan de récupération

Un plan de récupération exécute une série d'étapes devant être effectuées dans un ordre spécifique. Vous ne pouvez pas modifier l'ordre ou l'objectif de ces étapes, mais vous pouvez insérer vos propres étapes affichant des messages et exécutant des commandes.

Site Recovery Manager exécute les diverses étapes de ce plan de différentes manières.

- Certaines étapes sont exécutées durant toutes les récupérations.
- D'autres ne sont exécutées que lors des récupérations test.
- Certaines étapes sont toujours ignorées pendant les récupérations test.

L'assimilation de ces étapes de récupération, leur ordre et le contexte dans lequel elles sont exécutées est un facteur important de la personnalisation de vos plans de récupération.

Ordre de Récupération

Lorsque vous exécutez un plan de récupération, il commence par désactiver les machines virtuelles sur le site protégé. Site Recovery Manager désactive les machines virtuelles en fonction de la priorité que vous avez définie ; ainsi, les machines à priorité élevée sont les dernières à être mises hors tension. Site Recovery Manager omet cette étape lorsque vous testez un plan de récupération.

Site Recovery Manager met sous tension des groupes de machines virtuelles du site de récupération suivant l'ordre de priorité que vous avez défini. Avant qu'un groupe de priorité ne démarre, toutes les machines virtuelles du groupe à priorité plus élevée suivant doivent avoir été récupérées, ou leur récupération doit avoir échoué. S'il existe des dépendances entre des machines virtuelles du même groupe de priorité, Site Recovery Manager met d'abord sous tension les machines virtuelles dont dépendent d'autres machines virtuelles. Si Site Recovery Manager peut satisfaire les dépendances de la machine virtuelle, Site Recovery Manager va tenter de mettre sous tension en parallèle autant de machines virtuelles que peut en prendre en charge vCenter Server.

Délais d'expiration et pauses du plan de récupération

Plusieurs types d'expiration peuvent se produire durant l'exécution des étapes du plan de récupération. Ces délais d'expiration provoquent une interruption du plan pendant un intervalle spécifié, afin qu'il y ait suffisamment de temps pour que l'étape s'achève.

Les étapes de message forcent la mise en pause du plan jusqu'à ce que l'utilisateur reconnaisse ce message. Avant d'ajouter une étape de message à un plan de récupération, assurez-vous qu'elle est nécessaire. Avant de tester ou d'exécuter un plan de récupération contenant des étapes de message, assurez-vous qu'un utilisateur peut surveiller l'avancement du plan et répondre aux messages, si nécessaire.

Spécifier la priorité de récupération d'une machine virtuelle

Site Recovery Manager définit par défaut toutes les machines virtuelles d'un nouveau plan de récupération sur le niveau 3 de priorité de récupération. Vous pouvez cependant augmenter ou réduire le niveau de priorité de récupération d'une machine virtuelle.

Si vous changez la priorité d'une machine virtuelle, Site Recovery Manager applique la nouvelle priorité à tous les plans de récupération concernant la machine virtuelle en question.

Site Recovery Manager démarre les machines virtuelles du site de récupération suivant l'ordre de priorité que vous avez défini. Site Recovery Manager démarre d'abord les machines virtuelles de priorité 1, puis les machines virtuelles de priorité 2, et ainsi de suite. Site Recovery Manager utilise le signal de pulsation de VMware Tools pour déterminer si une machine virtuelle est en cours d'exécution sur le site de récupération. De cette manière, Site Recovery Manager peut s'assurer que toutes les machines virtuelles d'une priorité donnée sont en cours d'exécution avant de démarrer les machines virtuelles de la priorité suivante. C'est pourquoi vous devez installer VMware Tools sur des machines virtuelles protégées.

Procédure

- 1 Cliquez sur **Plans de récupération** dans le volet gauche, sélectionnez un plan de récupération, puis cliquez sur l'onglet **Machines virtuelles** ou sur l'onglet **Étapes de récupération**.
- 2 Cliquez avec le bouton droit de la souris sur une machine virtuelle et sélectionnez **Priorité**.
- 3 Sélectionnez une nouvelle priorité pour la machine virtuelle.
1 représente la priorité la plus élevée et 5 la plus faible.
- 4 Cliquez sur **Oui** pour confirmer le changement de priorité.

Créer des étapes de récupération personnalisées

Vous pouvez créer des étapes de récupération personnalisées qui exécutent des commandes ou présentent des messages à l'utilisateur lors d'une récupération.

Site Recovery Manager peut exécuter des étapes personnalisées sur le Serveur Site Recovery Manager ou dans une machine virtuelle faisant partie du plan de récupération.

Pendant la reprotection, Site Recovery Manager conserve toutes les étapes de récupération personnalisées dans le plan de récupération. Si vous effectuez une récupération ou un test après une reprotection, les étapes de récupération personnalisées sont exécutées sur le nouveau site de récupération, qui était le site protégé d'origine.

Après la reprotection, vous pouvez d'ordinaire utiliser les étapes de récupération personnalisée qui affichent directement des messages sans modifications. Il pourra toutefois être nécessaire de modifier certaines étapes de récupération personnalisées après une reprotection, si ces étapes exécutent des commandes contenant des informations spécifiques au site, telles que les configurations du réseau.

- **Types d'étapes de récupération personnalisée**

Vous pouvez créer divers types d'étapes de récupération personnalisée pour inclusion dans vos plans de récupération.

- **Gestion des échecs des étapes de récupération personnalisée par Site Recovery Manager**

Site Recovery Manager gère les échecs des étapes de récupération personnalisée différemment selon le type d'étape de récupération.

- **Créer des étapes de commande de niveau supérieur**

Vous pouvez ajouter des commandes de niveau supérieur à n'importe quel endroit du plan de récupération.

- **Créer des étapes d'invite de message de niveau supérieur**

Vous pouvez ajouter des invites de messages de niveau supérieur à n'importe quel endroit du plan de récupération.

- **Créer des étapes de commande pour les machines virtuelles individuelles**

Vous pouvez configurer des étapes de récupération personnalisée afin d'exécuter les tâches d'une machine virtuelle avant et après leur activation par Site Recovery Manager.

- **Créer des étapes d'invites de message pour les machines virtuelles individuelles**

Vous pouvez configurer les étapes de récupération personnalisée pour inviter les utilisateurs à exécuter les tâches affectées à une machine virtuelle avant et après que la machine virtuelle ne s'active.

- **Instructions pour l'écriture des étapes de commande**

Tous les fichiers de commandes ou les commandes associés aux étapes de récupération personnalisée que vous ajoutez à un plan de récupération doivent répondre à certaines exigences.

- **Variables d'environnement pour les étapes de commande**

Site Recovery Manager propose des variables d'environnement utilisables dans les commandes des étapes de récupération personnalisée.

Types d'étapes de récupération personnalisée

Vous pouvez créer divers types d'étapes de récupération personnalisée pour inclusion dans vos plans de récupération.

Les étapes de récupération personnalisée sont des étapes de récupération de commandes ou d'invites de message.

Étapes de récupération de commande

Les étapes de récupération de commande comportent des commandes de niveau supérieur ou des commandes par machine virtuelle.

Commandes de niveau supérieur

Exécuter sur le Serveur Site Recovery Manager. Vous pouvez par exemple utiliser ces commandes pour activer des périphériques physiques ou rediriger le trafic réseau.

Commandes par machine virtuelle

Site Recovery Manager associe les commandes par machine virtuelle aux machines virtuelles nouvellement récupérées au cours du processus de récupération. Vous pouvez utiliser ces commandes pour réaliser ces tâches de configuration après avoir mis sous tension une machine virtuelle. Vous pouvez exécuter ces commandes avant ou après la mise sous tension d'une machine virtuelle. Les commandes que vous configurez pour s'exécuter après la mise sous tension de la machine virtuelle peuvent s'exécuter sur le Serveur Site Recovery Manager ou la machine virtuelle nouvellement récupérée. Les commandes s'exécutant sur la machine virtuelle nouvellement récupérée s'exécutent dans le contexte du compte utilisateur que VMware Tools utilise sur la machine virtuelle récupérée. Selon la fonction de la commande que vous écrivez, vous devrez éventuellement changer le compte d'utilisateur que VMware Tools utilise sur la machine virtuelle récupérée.

Étapes de récupération des messages d'invite

Présenter un message dans l'interface utilisateur de Site Recovery Manager au cours de la récupération. Vous pouvez utiliser ce message pour interrompre la récupération et fournir des informations à l'utilisateur exécutant le plan de récupération. Le message peut par exemple inviter les utilisateurs à effectuer un processus de récupération manuel ou à vérifier des étapes. La seule action que les utilisateurs peuvent accomplir en réponse directe à une invite est de cliquer sur **OK**, ce qui rejette le message et permet à la récupération de continuer.

Gestion des échecs des étapes de récupération personnalisée par Site Recovery Manager

Site Recovery Manager gère les échecs des étapes de récupération personnalisée différemment selon le type d'étape de récupération.

Site Recovery Manager tente d'effectuer toutes les étapes de récupération personnalisée, mais certaines étapes de récupération peuvent échouer.

Étapes de récupération de commande

Par défaut, Site Recovery Manager attend pendant 5 minutes que les étapes de récupération de commande s'achèvent. Vous pouvez configurer le délai d'attente pour chaque commande. Si une commande se termine pendant cette période d'attente, l'étape de récupération suivante du plan de récupération est exécutée. La gestion par Site Recovery Manager des échecs des commandes personnalisées dépend du type de commande.

Type de Commande	Description
Commandes de niveau supérieur	Lorsqu'une étape de récupération échoue, Site Recovery Manager journalise l'échec et affiche un avertissement dans l'onglet Étapes de récupération . Les étapes de récupération personnalisée suivantes continuent d'être exécutées.
Commandes par machine virtuelle	Exécuter le mode de traitement par lots avant ou après l'activation d'une machine virtuelle. Si une commande échoue, les commandes par machine virtuelle restant dans le lot ne sont pas exécutées. Par exemple, si vous ajoutez cinq commandes avant la mise sous tension et cinq commandes à exécuter après l'activation, et que la troisième commande du lot avant la mise sous tension échoue, les deux autres commandes devant être exécutées avant la mise sous tension ne sont pas exécutées. Site Recovery Manager ne met pas sous tension la machine virtuelle et ne peut donc exécuter aucune commande de post-mise sous tension.

Étapes de récupération des messages d'invite

Les étapes de récupération personnalisée émettant une invite de message ne peuvent pas échouer. Le plan de récupération est suspendu jusqu'à ce que l'utilisateur ignore l'invite.

Créer des étapes de commande de niveau supérieur

Vous pouvez ajouter des commandes de niveau supérieur à n'importe quel endroit du plan de récupération.

Conditions préalables

Vous disposez d'un plan de récupération auquel ajouter des étapes personnalisées.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager et sélectionnez un plan de récupération.
- 2 Cliquez sur l'onglet **Étapes de récupération**.
- 3 Cliquez avec le bouton droit sur une étape avant ou après laquelle ajouter une étape personnalisée, puis sélectionnez **Ajouter une étape**.
- 4 Sélectionnez **Commande sur le serveur SRM**.
- 5 Dans la zone de texte **Nom**, tapez un nom à affecter à l'étape.
- 6 Dans la zone de texte **Contenu**, tapez les commandes de manière à ce que les étapes s'exécutent.
- 7 (Facultatif) Modifiez le paramètre **Expiration**.
- 8 Sélectionnez le moment où vous souhaitez insérer la nouvelle étape dans la suite d'étapes.
 - **Avant l'étape sélectionnée**
 - **Après l'étape sélectionnée**
- 9 Cliquez sur **OK** pour ajouter l'étape dans le plan de récupération.

Créer des étapes d'invite de message de niveau supérieur

Vous pouvez ajouter des invites de messages de niveau supérieur à n'importe quel endroit du plan de récupération.

Conditions préalables

Vous disposez d'un plan de récupération auquel ajouter des étapes personnalisées.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager et sélectionnez un plan de récupération.
- 2 Cliquez sur l'onglet **Étapes de récupération**.
- 3 Cliquez avec le bouton droit sur une étape avant ou après laquelle ajouter une étape personnalisée, puis sélectionnez **Ajouter une étape**.
- 4 Sélectionnez **Invite**.
- 5 Dans la zone de texte **Nom**, tapez un nom à affecter à l'étape.
- 6 Dans la zone de texte **Contenu**, tapez le message d'invite.
- 7 Sélectionnez le moment où vous souhaitez insérer la nouvelle étape dans la suite d'étapes.
 - **Avant l'étape sélectionnée**
 - **Après l'étape sélectionnée**
- 8 Cliquez sur **OK** pour ajouter l'étape dans le plan de récupération.

Créer des étapes de commande pour les machines virtuelles individuelles

Vous pouvez configurer des étapes de récupération personnalisée afin d'exécuter les tâches d'une machine virtuelle avant et après leur activation par Site Recovery Manager.

Site Recovery Manager associe les étapes de commande avec une machine virtuelle protégée ou récupérée de la même manière que les informations de personnalisation. Si différents plans de récupération contiennent la même machine virtuelle, les commandes et les invites sont les mêmes.

Conditions préalables

Vous disposez d'un plan de récupération auquel ajouter des étapes personnalisées.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager et sélectionnez un plan de récupération.
- 2 Cliquez sur l'onglet **Machines virtuelles**.
- 3 Cliquez avec le bouton droit de la souris sur une machine virtuelle puis cliquez sur **Configurer**.

- 4 Sélectionnez **Étapes de pré-mise sous tension** ou **Étapes de post-mise sous tension** dans le volet gauche, puis cliquez sur **Ajouter**.
- 5 Sélectionnez **Commande sur le serveur SRM** ou **Commande sur la VM récupérée**.
- 6 Dans la zone de texte **Nom**, tapez un nom à affecter à l'étape.
- 7 Dans la zone de texte **Contenu**, tapez les commandes de manière à ce que les étapes s'exécutent.
- 8 (Facultatif) Modifiez le paramètre **Expiration**.
- 9 Cliquez sur **OK** pour ajouter l'étape dans le plan de récupération.
- 10 Cliquez sur **OK** pour reconfigurer la machine virtuelle afin qu'elle exécute la commande avant ou après activation.

Créer des étapes d'invites de message pour les machines virtuelles individuelles

Vous pouvez configurer les étapes de récupération personnalisée pour inviter les utilisateurs à exécuter les tâches affectées à une machine virtuelle avant et après que la machine virtuelle ne s'active.

Site Recovery Manager associe les étapes d'invite de message à une machine virtuelle protégée de la même manière que les informations de personnalisation. Si différents plans de récupération contiennent la même machine virtuelle, les commandes et les invites sont les mêmes.

Conditions préalables

Vous disposez d'un plan de récupération auquel ajouter des étapes personnalisées.

Procédure

- 1 Cliquez sur **Plans de récupération** dans l'interface de Site Recovery Manager et sélectionnez un plan de récupération.
- 2 Cliquez sur l'onglet **Machines virtuelles**.
- 3 Cliquez avec le bouton droit de la souris sur une machine virtuelle puis cliquez sur **Configurer**.
- 4 Sélectionnez **Étapes de pré-mise sous tension** ou **Étapes de post-mise sous tension** dans le volet gauche, puis cliquez sur **Ajouter**.
- 5 Sélectionnez **Invite**.
- 6 Dans la zone de texte **Nom**, tapez un nom à affecter à l'étape.
- 7 Dans la zone de texte **Contenu**, tapez le message d'invite.
- 8 Cliquez sur **OK** pour ajouter l'étape dans le plan de récupération.
- 9 Cliquez sur **OK** pour reconfigurer la machine virtuelle afin qu'elle invite l'utilisateur avec un message avant ou après activation.

Instructions pour l'écriture des étapes de commande

Tous les fichiers de commandes ou les commandes associés aux étapes de récupération personnalisée que vous ajoutez à un plan de récupération doivent répondre à certaines exigences.

Lorsque vous créez une étape de commande à ajouter à un plan de récupération, assurez-vous qu'elle prend en compte l'environnement dans lequel elle doit être exécutée. Les erreurs qui se produisent lors d'une étape de commande affectent l'intégrité d'un plan de récupération. Testez la commande sur le site de récupération du Serveur Site Recovery Manager avant de l'ajouter au plan.

- Vous devez démarrer le shell de commande Windows en utilisant son chemin complet sur l'hôte local. Par exemple, pour exécuter un script situé dans `c:\alarmscript.bat`, utilisez la ligne de commande suivante :

```
c:\windows\system32\cmd.exe /c c:\alarmscript.bat
```

- Vous devez installer les fichiers de commandes et les commandes sur le Serveur Site Recovery Manager, au niveau du site de récupération.
- Les fichiers de commandes et les commandes doivent s'exécuter dans un délai de 300 secondes. Autrement, le plan de récupération s'achève avec une erreur. Pour modifier cette limite, voir [Modifier les paramètres de récupération](#).
- Les fichiers de commandes et commandes qui produisent des résultats contenant des caractères disposant de valeurs ASCII supérieures à 127 doivent utiliser l'encodage UTF-8. Site Recovery Manager enregistre uniquement le dernier bloc de 4 Ko des sorties script dans des fichiers de journalisation et dans l'historique de récupération. Les scripts produisant plus de sorties doivent rediriger les sorties vers un fichier plutôt que de les envoyer vers la sortie standard devant être répertoriée dans un journal.

Variables d'environnement pour les étapes de commande

Site Recovery Manager propose des variables d'environnement utilisables dans les commandes des étapes de récupération personnalisée.

Les étapes de commande s'exécutent avec l'identité du compte LocalSystem sur l'hôte du Serveur Site Recovery Manager du site de récupération. Lorsqu'une étape de commande s'exécute, Site Recovery Manager met à sa disposition les variables d'environnement.

Tableau 7-1. Variables d'environnement disponibles pour toutes les étapes de commande

Nom	Valeur	Exemple
<i>VMware_RecoveryName</i>	Nom du plan de récupération en cours d'exécution.	Plan A
<i>VMware_RecoveryMode</i>	Mode de récupération.	Test ou récupération

Tableau 7-1. Variables d'environnement disponibles pour toutes les étapes de commande (suite)

Nom	Valeur	Exemple
<i>VMware_VC_Host</i>	Nom de l'hôte vCenter Server sur le site de récupération.	vc_hostname.example.com
<i>VMware_VC_Port</i>	Port réseau utilisé pour contacter vCenter Server.	443

Site Recovery Manager met à disposition des variables d'environnement supplémentaires pour les étapes de commande par machine virtuelle qui s'exécutent sur le Serveur Site Recovery Manager ou sur la machine virtuelle récupérée.

Tableau 7-2. Variables d'environnement disponibles pour les étapes de commande par machine virtuelle

Nom	Valeur	Exemple
<i>VMware_VM_Uuid</i>	UUID utilisé par vCenter pour identifier de façon unique cette machine virtuelle.	4212145a-eeae-a02c-e525-ebba70b0d4f3
<i>VMware_VM_Name</i>	Nom de cette machine virtuelle, comme définie sur le site protégé.	Ma nouvelle machine virtuelle
<i>VMware_VM_Ref</i>	ID de l'objet géré de la machine virtuelle.	vm-1199
<i>VMware_VM_Guest</i> Nom	Nom du SE client, tel que défini par VIM API.	otherGuest
<i>VMware_VM_GuestIP</i>	Adresse IP de la machine virtuelle, si connue.	192.168.0.103
<i>VMware_VM_Path</i>	Chemin vers le VMDK de cette machine virtuelle.	[datastore-123] jquser-vm2/jquser-vm2.vmdk

Personnaliser la récupération d'une machine virtuelle individuelle

Vous pouvez configurer une machine virtuelle dans un plan de récupération, afin qu'elle utilise une spécification de personnalisation donnée ou exécute des étapes de message ou de commande lorsqu'elle est récupérée.

Les étapes de message ou de commande ajoutées aux étapes de récupération pour une machine virtuelle fonctionnent de la même façon que les étapes de message ou de commande ajoutées à un plan de récupération. Reportez-vous à [Instructions pour l'écriture des étapes de commande](#).

Procédure

- 1 Connectez vSphere Client à l'instance de vCenter Server, sur le site de récupération.
- 2 Dans l'interface Site Recovery Manager, cliquez sur **Plans de récupération** dans le volet gauche, puis sur le plan à personnaliser.
- 3 Cliquez sur l'onglet **Étapes de récupération** ou sur l'onglet **Machines virtuelles**.

4 Faites un clic droit sur une machine virtuelle de la liste, puis cliquez sur **Configurer**.

5 Cliquez sur **Paramètres IP**.

Vous pouvez également entrer une description de la spécification que vous appliquez. Seules les propriétés IP issues de la spécification sélectionnée sont appliquées. Si vous avez utilisé la commande `dr-ip-customizer.exe` pour personnaliser les machines virtuelles dans le plan de récupération, il n'est pas nécessaire de spécifier cette personnalisation ici.

6 Sélectionnez l'entrée concernée pour ajouter une étape de message ou de commande s'exécutant avant l'activation de la machine.

7 Sélectionnez l'entrée concernée pour ajouter une étape de message ou de commande qui s'exécute après l'activation de la machine.

Résultats

Les personnalisations que vous spécifiez sont associées à la machine virtuelle protégée. Par conséquent, les paramètres sont partagés entre tous les plans de récupération qui s'appliquent à cette machine virtuelle.

Note Si vous supprimez la protection d'une machine virtuelle, toutes les personnalisations de récupération sont perdues.

Personnalisation des propriétés IP des machines virtuelles



Il est possible de personnaliser les paramètres IP des machines virtuelles des sites protégé et de récupération. La personnalisation des propriétés IP d'une machine virtuelle remplace les paramètres IP par défaut lorsque la machine virtuelle récupérée démarre au niveau du site de destination.

Lorsque les propriétés IP d'une machine virtuelle se sont pas personnalisées, Site Recovery Manager utilise les paramètres IP pour le site de récupération durant une récupération ou un test de passage du site de protection vers le site de récupération. Site Recovery Manager utilise les paramètres IP pour le site de protection après la reprotection, durant la récupération ou un test de passage du site de récupération d'origine vers le site de protection d'origine.

Site Recovery Manager prend en charge différents types de personnalisation d'IP.

- Utilisez les adresses IPv4 et IPv6.
- Configurez différentes personnalisations de l'IP pour chaque site.
- Utilisez DHCP et les adresses statiques IPv4 ou IPv6.
- Personnalisez les adresses pour les machines virtuelles Windows et Linux.
- Personnalisez plusieurs cartes réseau pour chaque machine virtuelle.

Reportez-vous à la [Matrice de compatibilité de vCenter Site Recovery Manager 5.5](#) pour consulter la liste des systèmes d'exploitation invités pour lesquels Site Recovery Manager prend en charge la personnalisation IP.

Vous pouvez associer les paramètres de personnalisation à des machines virtuelles protégées. Par conséquent, si la même machine virtuelle protégée fait partie de plusieurs plans de récupération, tous les plans de récupération utilisent une copie unique des paramètres de personnalisation. Vous pouvez configurer la personnalisation IP dans le cadre du processus de configuration des propriétés de récupération d'une virtuelle machine. Si vous ne personnalisez pas une carte réseau sur un site, ladite carte utilise les paramètres IP de l'autre site.

Vous pouvez appliquer des personnalisations IP à des machines virtuelles individuelles ou multiples.

Lorsque vous configurez une personnalisation IP sur des machines virtuelles, Site Recovery Manager ajoute les étapes de récupération à ces machines virtuelles.

Démarrage du SE client

Le processus de démarrage Client se produit en parallèle pour toutes les machines virtuelles pour lesquelles la personnalisation IP est configurée.

Personnaliser l'IP

Site Recovery Manager pousse les personnalisations IP vers la machine virtuelle.

Arrêt du SE client

Site Recovery Manager arrête la machine virtuelle et la redémarre afin de s'assurer que les changements prennent effet et que les services du système d'exploitation client les appliquent lors du redémarrage de la machine virtuelle.

Au terme du processus de personnalisation IP, les machines virtuelles s'activent en fonction des groupes de priorité et des dépendances que vous avez définis. L'activation se produit juste avant le processus d'Attente de VMTools pour chaque machine virtuelle.

Note Pour personnaliser les propriétés IP d'une machine virtuelle, vous devez installer VMware Tools ou les packages spécifiques du système d'exploitation VMware (OSP) sur la machine virtuelle. Reportez-vous à <http://www.vmware.com/download/packages.html>.

- **Personnaliser les propriétés IP pour une machine virtuelle individuelle**

Vous pouvez personnaliser les paramètres IP pour des machines virtuelles individuelles pour le site protégé et le site de récupération.

- **Signaler les mappages d'adresses IP pour les plans de récupération**

Le rapporteur de mappages d'adresse IP génère un document XML décrivant les propriétés IP des machines virtuelles protégées et de leurs espaces réservés, regroupées par site et par plan de récupération. Ces informations peuvent vous aider à comprendre les exigences de réseau d'un plan de récupération.

- **Personnalisation des propriétés IP pour plusieurs machines virtuelles**

La configuration manuelle des paramètres IP de nombreuses machines virtuelles sur un site de récupération peut être chronophage et provoquer des erreurs de configuration. Afin de faciliter le processus de configuration de plusieurs machines virtuelles, Site Recovery Manager est équipé de l'outil DR IP Customizer.

Personnaliser les propriétés IP pour une machine virtuelle individuelle

Vous pouvez personnaliser les paramètres IP pour des machines virtuelles individuelles pour le site protégé et le site de récupération.

Procédure

- 1 Cliquez sur **Plans de récupération**, puis cliquez sur le plan que vous souhaitez personnaliser.
- 2 Cliquez sur l'onglet **Machines virtuelles**, puis cliquez avec le bouton droit de la souris sur une machine virtuelle et sélectionnez **Configurer**.

- 3 Sélectionnez la NIC dont vous allez modifier les paramètres IP.
- 4 Pour personnaliser les paramètres, activez l'option **Personnaliser les paramètres IP au cours de la récupération**.
- 5 Cliquez sur **Configurer la protection** ou **Configurer la récupération**, en fonction de l'ensemble de paramètres IP que vous souhaitez configurer.
- 6 Cliquez sur l'onglet **Général** pour configurer les paramètres.
 - a Choisissez le type d'adressage à utiliser.
Les choix possibles comprennent DHCP, IPv4 statique ou IPv6 statique.
 - b Pour les adresses statiques, entrez une adresse IP, les informations concernant le sous-réseau et les adresses de serveur de passerelle.

Si la machine virtuelle est activée et dispose de VMware Tools installé, vous pouvez également cliquer sur **Mise à jour** pour importer les paramètres actuels configurés sur la machine virtuelle.
- 7 Cliquez sur l'onglet **DNS** pour configurer les paramètres DNS.
 - a Choisissez comment trouver les serveurs DNS.

Vous pouvez utiliser DHCP pour trouver des serveurs DNS. Vous pouvez également spécifier des serveurs DNS principaux et alternatifs.
 - b Entrez un suffixe DNS puis cliquez sur **Ajouter**, ou sélectionnez un suffixe DNS existant puis cliquez sur **Supprimer**, **Monter** ou **Descendre**.
- 8 Cliquez sur l'onglet **WINS** pour entrer les adresses WINS primaires et secondaires.

L'onglet **WINS** est disponible uniquement lors de la configuration des adresses DHCP ou IPv4 pour les machines virtuelles Windows.
- 9 Répétez les [Étape 5](#) à [Étape 8](#) pour configurer les paramètres de récupération ou de protection, si nécessaire.

Par exemple, si vous avez configuré des paramètres IP pour le site protégé, vous souhaitez peut-être configurer les paramètres pour le site de récupération.
- 10 Répétez le processus de configuration pour les autres NIC, si nécessaire, en commençant par choisir une autre NIC, tel que décrit dans [Étape 3](#).

Signaler les mappages d'adresses IP pour les plans de récupération

Le rapporteur de mappages d'adresse IP génère un document XML décrivant les propriétés IP des machines virtuelles protégées et de leurs espaces réservés, regroupées par site et par plan de récupération. Ces informations peuvent vous aider à comprendre les exigences de réseau d'un plan de récupération.

Étant donné que le rapporteur de mappages d'adresse IP doit se connecter aux deux sites, vous pouvez exécuter la commande sur le site de votre choix. Vous êtes invité(e) à fournir les informations d'identification de la connexion vCenter pour chaque site lors de l'exécution de la commande.

Procédure

- 1 Ouvrez un shell de commande sur l'hôte du Serveur Site Recovery Manager sur le site protégé ou le site de récupération.
- 2 Accédez au répertoire `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
- 3 Exécutez la commande `dr-ip-reporter.exe`, tel que décrit dans cet exemple.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
```

Pour limiter la liste de réseaux à ceux uniquement requis par un plan de récupération spécifique, incluez l'option `-plan` sur la ligne de commande, tel que décrit dans l'exemple ci-dessous.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out path_to_report_file.xml
--vc vcenter_server_address
--plan recovery_plan_name
```

Note La commande vous demande normalement de vérifier les empreintes présentées par les certificats sur chaque site. Vous pouvez supprimer la demande de vérification en incluant l'option `-I`.

Personnalisation des propriétés IP pour plusieurs machines virtuelles

La configuration manuelle des paramètres IP de nombreuses machines virtuelles sur un site de récupération peut être chronophage et provoquer des erreurs de configuration. Afin de faciliter le processus de configuration de plusieurs machines virtuelles, Site Recovery Manager est équipé de l'outil DR IP Customizer.

Utilisez l'outil DR IP Customizer pour appliquer des paramètres de réseau personnalisés aux machines virtuelles lorsqu'elles démarrent sur le site de récupération. Fournissez les paramètres personnalisés à l'outil DR IP Customizer via un fichier CSV (comma-separated value).

Au lieu de créer manuellement un fichier CSV, vous pouvez utiliser l'outil DR IP Customizer pour exporter un fichier CSV contenant les informations sur les configurations de réseau des machines virtuelles protégées. Si vous personnalisez les valeurs du fichier, celui-ci peut servir de modèle de fichier CSV à appliquer sur le site de récupération.

- 1 Exécutez l'outil DR IP Customizer pour générer un fichier CSV contenant les informations de réseau pour les machines virtuelles protégées.
- 2 Modifiez le fichier CSV généré en utilisant les informations de réseau pertinentes pour le site de récupération.
- 3 Réexécutez DR IP Customizer pour appliquer le fichier CSV contenant les configurations de réseau modifiées à appliquer lors du démarrage des machines virtuelles sur le site de récupération.

Vous pouvez utiliser l'outil DR IP Customizer sur le site protégé ou le site de récupération. Les ID de machines virtuelles protégées sont différents pour chaque site. De ce fait, quel que soit le site choisi pour exécuter l'outil DR IP Customizer et générer le fichier CSV, vous devez utiliser le même site lorsque vous exécutez à nouveau DR IP Customizer pour appliquer les paramètres.

Personnalisez les paramètres IP des sites protégés et de récupération afin que Site Recovery Manager utilise les configurations correctes pendant les opérations de reprotction.

Reportez-vous à la [Matrice de compatibilité de vCenter Site Recovery Manager 5.5](#) pour consulter la liste des systèmes d'exploitation invités pour lesquels Site Recovery Manager prend en charge la personnalisation IP.

■ [Syntaxe de l'outil DR IP Customizer](#)

L'outil DR IP Customizer comprend des options permettant de rassembler des informations de réseau sur les machines virtuelles protégées par Site Recovery Manager. Vous pouvez également utiliser les options pour personnaliser les machines virtuelles lorsqu'elles démarrent sur le site de récupération.

■ [Structure du fichier CSV de DR IP Customizer](#)

Le fichier CSV (comma-separated-value) de DR IP Customizer consiste en une ligne d'en-tête, qui donne la signification de chaque colonne du fichier, et d'une ou plusieurs lignes supplémentaires pour chaque machine virtuelle à espace réservé dans un plan de récupération.

■ [Modification du fichier CSV de DR IP Customizer](#)

Modifiez le fichier CSV (comma-separated-file) de DR IP Customizer afin d'appliquer des paramètres de réseau personnalisés aux machines virtuelles lorsqu'elles démarrent sur le site de récupération.

■ [Exécutez DR IP Customizer pour personnaliser les propriétés IP de plusieurs machines virtuelles](#)

Vous pouvez utiliser l'outil DR IP Customizer pour personnaliser les propriétés IP de plusieurs machines virtuelles protégées par Site Recovery Manager.

Syntaxe de l'outil DR IP Customizer

L'outil DR IP Customizer comprend des options permettant de rassembler des informations de réseau sur les machines virtuelles protégées par Site Recovery Manager. Vous pouvez également utiliser les options pour personnaliser les machines virtuelles lorsqu'elles démarrent sur le site de récupération.

Vous trouverez le fichier `dr-ip-customizer.exe` sous `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` sur la machine hôte du Serveur Site Recovery Manager. Lorsque vous exécutez `dr-ip-customizer.exe`, spécifiez différentes options selon que vous générez ou appliquez un fichier CSV (comma-separated-value).

```
dr-ip-customizer.exe
--cfg XML de configuration du serveur SRM
--cmd apply/drop/generate
[--csv Nom du fichier CSV existant]
[--out Nom du nouveau fichier CSV à générer]
[--vc Adresse de vCenter Server]
[--ignore-thumbprint]
[--extra-dns-columns]
[--verbose]
```

Vous pouvez utiliser l'outil DR IP Customizer sur le site protégé ou le site de récupération. Les ID de machines virtuelles protégées sont différents pour chaque site. De ce fait, quel que soit le site choisi pour exécuter l'outil DR IP Customizer et générer le fichier CSV, vous devez utiliser le même site lorsque vous exécutez à nouveau DR IP Customizer pour appliquer les paramètres.

Certaines options de l'outil DR IP Customizer sont obligatoires et d'autres sont facultatives.

Tableau 8-1. Options de DR IP Customizer

Option	Description	Obligatoire
<code>-h [--help]</code>	Affiche des informations d'utilisation sur <code>dr-ip-customizer.exe</code> .	Non
<code>--cfg arg</code>	Chemin d'accès du fichier de configuration XML du Serveur Site Recovery Manager, le fichier <code>vmware-dr.xml</code> .	Oui

Tableau 8-1. Options de DR IP Customizer (suite)

Option	Description	Obligatoire
<code>--cmd arg</code>	<p>Spécifiez différentes commandes pour exécuter DR IP Customizer dans différents modes.</p> <ul style="list-style-type: none"> ■ La commande <code>Appliquer</code> applique les paramètres de personnalisation du réseau aux plans de récupération sur les instances du Serveur Site Recovery Manager à partir d'un fichier CSV existant. ■ La commande <code>generate</code> génère un fichier CSV de base pour toutes les machines virtuelles protégées par Site Recovery Manager pour une instance de vCenter Server. ■ La commande <code>drop</code> supprime les paramètres de récupération des machines virtuelles spécifiées par le fichier CSV d'entrée. <p>Utilisez toujours la même instance de vCenter Server que celle utilisée pour générer le fichier CSV pour les commandes <code>apply</code> et <code>drop</code>.</p>	Oui
<code>--csv arg</code>	Chemin d'accès au fichier CSV à utiliser comme entrée.	Oui, lors de l'exécution des commandes <code>apply</code> et <code>drop</code> .
<code>-o [--out] arg</code>	Nom du nouveau fichier de sortie CSV créé par la commande <code>generate</code> . Si vous saisissez le nom d'un fichier CSV existant, la commande <code>generate</code> écrase son contenu actuel.	Oui, lorsque vous exécutez la commande <code>generate</code> .
<code>--vc arg</code>	Nom d'hôte de vCenter Server. Les ID des machines virtuelles protégées sont différents sur chaque site. Utilisez la même instance de vCenter Server lorsque vous générez le fichier CSV et lorsque vous l'appliquez.	Oui
<code>-i [--ignore-thumbprint]</code>	Ignorer l'invite de confirmation de l'empreinte vCenter Server.	Non
<code>-e [--extra-dns-columns]</code>	Obsolète.	Non
<code>-v [--verbose]</code>	Permettre une sortie détaillée. Vous pouvez inclure une option <code>--verbose</code> sur toute ligne de commande <code>dr-ip-customizer.exe</code> pour journaliser d'autres messages de diagnostic.	Non

Structure du fichier CSV de DR IP Customizer

Le fichier CSV (comma-separated-value) de DR IP Customizer consiste en une ligne d'en-tête, qui donne la signification de chaque colonne du fichier, et d'une ou plusieurs lignes supplémentaires pour chaque machine virtuelle à espace réservé dans un plan de récupération.

La configuration des paramètres IP des deux sites est facultative. Vous pouvez fournir des paramètres pour le site protégé, pour le site de récupération ou pour les deux. Vous pouvez configurer chaque site pour qu'ils utilisent un ensemble distinct d'adaptateurs réseau de manière complètement différente.

Certains champs du fichier CSV doivent être complétés pour chaque ligne. D'autres champs peuvent rester vides si aucun paramètre personnalisé n'est requis.

Tableau 8-2. Colonne du fichier CSV de DR IP Customizer

Colonne	Description	Règles de personnalisation
ID de la VM	Identifiant unique utilisé par DR IP Customizer pour collecter des informations de plusieurs lignes et les appliquer à une seule machine virtuelle. Cet ID est interne à DR IP Customizer et est différent de celui de la machine virtuelle utilisé par vCenter Server.	Non personnalisable. Ne peut pas être vide.
Nom de VM	Nom de la machine virtuelle, lisible par un œil humain, tel qu'il apparaît dans l'inventaire vCenter Server.	Non personnalisable. Ne peut pas être vide.
vCenter Server	Adresse d'une instance de vCenter Server sur le site protégé ou le site de récupération. Configurez les paramètres IP d'une machine virtuelle sur chaque site dans la colonne vCenter Server.	Non personnalisable. Ne peut pas être vide. Cette colonne peut contenir les deux instances de vCenter Server. Chaque instance de vCenter Server doit avoir sa propre ligne. Vous pouvez configurer un ensemble de paramètres IP à utiliser sur un site et un autre ensemble pour l'autre site. Vous pouvez également fournir des paramètres IP à utiliser sur les deux sites pour des opérations de reProtection.

Tableau 8-2. Colonnes du fichier CSV de DR IP Customizer (suite)

Colonne	Description	Règles de personnalisation
ID de l'adaptateur	ID de l'adaptateur à personnaliser. L'ID d'adaptateur 0 définit les paramètres généraux de tous les adaptateurs d'une machine virtuelle. Définir des valeurs sur l'ID d'adaptateur 1, 2, 3, etc. configure les paramètres pour des NIC spécifiques d'une machine virtuelle.	<p>Personnalisable. Ne peut pas être vide.</p> <p>Les seuls champs que vous pouvez modifier pour une ligne où l'ID d'adaptateur est 0 sont Serveur(s) DNS et Suffixe(s) DNS. Ces valeurs, si elles sont spécifiées, sont héritées par tous les autres adaptateurs utilisés par cet ID de VM.</p> <p>Vous pouvez inclure plusieurs serveurs DNS sur plusieurs lignes du fichier CSV. Si, par exemple, vous avez besoin de deux hôtes DNS globaux, vous incluez deux lignes pour l'ID d'adaptateur 0.</p> <ul style="list-style-type: none"> ■ Une ligne contenant toutes les informations de la machine virtuelle et un hôte DNS. ■ Une ligne contenant uniquement le second hôte DNS. <p>Pour ajouter un autre serveur DNS à un adaptateur spécifique, ajoutez ce serveur DNS à la ligne Adaptateur appropriée. Par exemple, ajoutez le serveur DNS à l'ID d'adaptateur 1.</p>
le domaine DNS ;	Domaine DNS pour cet adaptateur.	<p>Personnalisable. Peut être vide.</p> <p>Si vous saisissez une valeur, elle doit être au format exemple.société.com.</p>
Net BIOS	Choisissez d'activer ou non le NetBIOS sur cet adaptateur.	<p>Personnalisable. Peut être vide.</p> <p>Cette colonne, si elle n'est pas vide, doit contenir l'une des chaînes suivantes :</p> <p>disableNetBIOS, enableNetBIOS OU enableNetBIOSViaDhcp.</p>
WINS primaire	DR IP Customizer confirme que les paramètres WINS sont appliqués seulement sur les machines virtuelles Windows, mais ne valide pas les paramètres NetBIOS.	Personnalisable. Peut être vide.
WINS secondaire	DR IP Customizer confirme que les paramètres WINS sont appliqués seulement sur les machines virtuelles Windows, mais ne valide pas les paramètres NetBIOS.	Personnalisable. Peut être vide.

Tableau 8-2. Colonnes du fichier CSV de DR IP Customizer (suite)

Colonne	Description	Règles de personnalisation
Adresse IP	Adresse IPv4 pour cette machine virtuelle.	<p>Personnalisable. Ne peut pas être vide.</p> <p>Les machines virtuelles peuvent disposer de plusieurs adaptateurs réseau virtuels. Vous pouvez configurer chaque adaptateur réseau virtuel avec une adresse IPv4 ou IPv6 statique. Si, par exemple, vous définissez une adresse IPv4 statique, vous devez définir l'adresse IPv6 sur DHCP.</p>
Masque de sous-réseau	Masque de sous-réseau pour cette machine virtuelle.	Personnalisable. Peut être vide.
Passerelle(s)	Passerelle(s) IPv4 pour cette machine virtuelle.	Personnalisable. Peut être vide.
Adresse IPv6	Adresse IPv6 pour cette machine virtuelle.	<p>Personnalisable. Peut être vide si vous n'utilisez pas IPv6.</p> <p>Les machines virtuelles peuvent disposer de plusieurs adaptateurs réseau virtuels. Vous pouvez configurer chaque adaptateur réseau virtuel avec une adresse IPv4 ou IPv6 statique. Si, par exemple, vous définissez une adresse IPv6 statique, vous devez définir l'adresse IPv4 sur DHCP.</p> <p>Si vous exécutez le Serveur Site Recovery Manager sur Windows Server 2003 et personnalisez les adresses IPv6 d'une machine virtuelle, vous devez activer IPv6 sur les instances du Serveur Site Recovery Manager. Site Recovery Manager effectue la validation des adresses IP pendant la personnalisation, ce qui requiert l'activation d'IPv6 sur le Serveur Site Recovery Manager si vous personnalisez les adresses IPv6. Le protocole IPv6 est activé par défaut sur les versions les plus récentes de Windows Server.</p>
Longueur préfixe sous-réseau IPv6	Longueur de préfixe du sous-réseau IPv6 à utiliser.	Personnalisable. Peut être vide.
Passerelle(s) IPv6	Passerelle(s) IPv4 pour cet adaptateur.	Personnalisable. Peut être vide.

Tableau 8-2. Colonnes du fichier CSV de DR IP Customizer (suite)

Colonne	Description	Règles de personnalisation
Serveur(s) DNS	Adresse du ou des serveurs DNS.	<p>Personnalisable. Peut être vide.</p> <p>Si vous entrez ce paramètre dans une ligne ID d'adaptateur 0, il est considéré comme paramètre général. Sur les machines virtuelles Windows, ce paramètre s'applique à tous les adaptateurs si vous le définissez dans les lignes de l'ID d'adaptateur autres que l'ID d'adaptateur 0.</p> <p>Sur les machines virtuelles Linux, il s'agit toujours d'un paramètre général pour tous les adaptateurs.</p> <p>Cette colonne peut contenir un ou plusieurs serveurs DNS IPv4 ou IPv6 pour chaque NIC.</p>
Suffixe(s) DNS	Suffixe(s) des serveurs DNS.	<p>Personnalisable. Peut être vide.</p> <p>Il s'agit de paramètres généraux pour tous les adaptateurs des machines virtuelles Windows et Linux.</p>

Modification du fichier CSV de DR IP Customizer

Modifiez le fichier CSV (comma-separated-file) de DR IP Customizer afin d'appliquer des paramètres de réseau personnalisés aux machines virtuelles lorsqu'elles démarrent sur le site de récupération.

La représentation des configurations réseau de machines virtuelles dans un fichier CSV est un défi, en ce sens que les configurations de la machine virtuelle incluent des informations hiérarchiques. Par exemple, une seule machine virtuelle pourrait contenir plusieurs adaptateurs et chaque adaptateur pourrait avoir plusieurs listes d'éléments tels que les passerelles. Le format CSV ne constitue pas un système pour les représentations hiérarchiques. Par conséquent, chaque ligne du fichier CSV généré par DR IP Customizer pourrait fournir tout ou partie des informations pertinentes pour une machine virtuelle spécifique.

Pour une machine virtuelle ayant une simple configuration réseau, toutes les informations peuvent être contenues dans une seule ligne. Dans le cas d'une machine virtuelle plus complexe, plusieurs lignes peuvent être requises. Les machines virtuelles équipées de plusieurs cartes réseaux ou passerelles requièrent plusieurs lignes. Chaque ligne du fichier CSV inclut des informations d'identification décrivant la machine virtuelle et l'adaptateur auxquels les informations s'appliquent. Les informations sont regroupées pour être appliquées à la machine virtuelle appropriée.

Suivez ces recommandations lorsque vous modifiez le fichier CSV de DR IP Customizer.

- Vous pouvez omettre les valeurs si un paramètre n'est pas obligatoire.
- Utilisez un nombre minimum de lignes pour chaque adaptateur.

- N'utilisez pas de virgule dans les champs.
- Spécifiez les paramètres de l'ID d'adaptateur en fonction de vos besoins. DR IP Customizer applique les paramètres que vous spécifiez pour l'ID d'adaptateur 0 à toutes les NIC. Pour appliquer les paramètres à des NIC individuelles, spécifiez les valeurs dans les champs ID d'adaptateur 1, 2, etc. *n*.
- Pour spécifier plus d'une valeur pour une colonne, créez une ligne supplémentaire pour cet adaptateur et indiquez la valeur dans cette ligne de la colonne. Pour assurer l'association de la ligne supplémentaire avec la machine virtuelle cible, copiez les valeurs des colonnes ID de la VM, Nom de la VM, vCenter Server et ID d'adaptateur.
- Pour spécifier plusieurs adresses IP pour un adaptateur réseau ou pour spécifier plusieurs adresses de serveur DNS, ajoutez une nouvelle ligne par adresse. Copiez les valeurs ID de la VM, Nom de la VM et ID d'adaptateur sur chaque ligne.

Exemples de fichiers CSV de DR IP Customizer

Vous obtenez le fichier CSV contenant les informations de réseau pour les machines virtuelles protégées sur vCenter Server en exécutant `dr-ip-customizer.exe` avec la commande `--cmd generate`. Modifiez le fichier CSV pour personnaliser les paramètres IP des machines virtuelles protégées.

Exemple : Fichier CSV de DR IP Customizer généré

Pour une configuration simple avec seulement deux machines virtuelles protégées, le fichier CSV généré peut contenir uniquement l'ID et le nom de la machine virtuelle, les noms des instances de vCenter Server sur les deux sites et un seul adaptateur.

```
VM ID,VM Name,vCenter Server,Adapter ID,DNS Domain,Net BIOS,
Primary WINS,Secondary WINS,IP Address,Subnet Mask,Gateway(s),
IPv6 Address,IPv6 Subnet Prefix length,IPv6 Gateway(s),
DNS Server(s),DNS Suffix(es)
protected-vm-10301,vm-3-win,vcenter-server-site-B,0,,,,,,,,,
protected-vm-10301,vm-3-win,vcenter-server-site-A,0,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-A,0,,,,,,,,,
```

Ce fichier CSV généré affiche deux machines virtuelles, `vm-3-win` et `vm-1-linux`. Les machines virtuelles se trouvent sur le site protégé et sur le site de récupération, `vcenter-server-site-B` et `vcenter-server-site-A`. DR IP Customizer génère une entrée pour chaque machine virtuelle et chaque site avec l'ID d'adaptateur 0. Vous pouvez ajouter des lignes supplémentaires pour personnaliser chaque NIC une fois que vous connaissez le nombre de NIC se trouvant sur chaque machine virtuelle.

Exemple : Configuration d'adresses IPv4 statiques

Vous pouvez modifier le fichier CSV généré afin d'assigner deux adaptateurs réseau ayant des adresses IPv4 statiques à l'une des machines virtuelles, `vm-3-win`, sur le site protégé et sur le site de récupération.

Pour plus de lisibilité, l'exemple de fichier CSV dans le tableau suivant omet les colonnes vides. Les colonnes Domaine DNS, NetBIOS, Adresse IPv6, Longueur de préfixe du sous-réseau IPv6 et Passerelle(s) IPv6 sont toutes omises.

Tableau 8-3. Configuration des adresses IPv4 statiques dans un fichier CSV modifié

ID de la VM	Nom de VM	vCenter Server	ID de l'adaptateur	WINS primaires	WINS secondaires	Adresse IP	Masque de sous-réseau	Passerelle(s)	Serveur(s) DNS	Suffixe(s) DNS
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

Les informations de ce fichier CSV appliquent différents paramètres IPv4 statiques à vm-3-win sur le site protégé et le site de récupération.

- Sur le site vcenter-server-site-B :
 - Configure les suffixes DNS example.com et eng.example.com de toutes les NIC de cette machine virtuelle.

- Ajoute une NIC, l'ID d'adaptateur 1 avec les serveurs WINS primaire et secondaire 2.2.3.4 et 2.2.3.5, une adresse IPv4 statique 192.168.1.21 et un serveur DNS 1.1.1.1.
- Ajoute une NIC, l'ID d'adaptateur 2 avec les serveurs WINS primaire et secondaire 2.2.3.4 et 2.2.3.5, une adresse IPv4 statique 192.168.1.22 et un serveur DNS 1.1.1.2.
- Sur le site vcenter-server-site-A :
 - Configure les suffixes DNS example.com et eng.example.com de toutes les NIC de cette machine virtuelle.
 - Configure les serveurs DNS 1.1.0.1 et 1.1.0.2 de toutes les NIC de cette machine virtuelle.
 - Ajoute une NIC, l'ID d'adaptateur 1 avec une adresse IPv4 statique 192.168.0.21.
 - Ajoute une NIC, l'ID d'adaptateur 2 avec les serveurs WINS primaire et secondaire 1.2.3.4 et 1.2.3.5 et une adresse IPv4 statique 192.168.0.22.

Exemple : Configuration des adresses IPv4 DHCP et statiques

Vous pouvez modifier le fichier CSV généré afin d'assigner plusieurs NIC à l'une des machines virtuelles, vm-3-win, qui utilise une combinaison d'adresses IPv4 DHCP et statiques. Les paramètres peuvent être différents sur le site protégé et le site de récupération.

Pour plus de lisibilité, l'exemple de fichier CSV dans le tableau suivant omet les colonnes vides. Les colonnes Domaine DNS, NetBIOS, Adresse IPv6, Longueur de préfixe du sous-réseau IPv6 et Passerelle(s) IPv6 sont toutes omises.

Tableau 8-4. Configuration des adresses IPv4 DHCP et statiques sur un fichier CSV modifié

ID de la VM	Nom de VM	vCenter Server	ID de l'adaptateur	WINS primaires	WINS secondaires	Adresse IP	Masque de sous-réseau	Passerelle(s)	Serveur(s) DNS	Suffixe(s) DNS
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com

Tableau 8-4. Configuration des adresses IPv4 DHCP et statiques sur un fichier CSV modifié (suite)

ID de la VM	Nom de VM	vCenter Server	ID de l'adaptateur	WINS primaires	WINS secondaires	Adresse IP	Masque de sous-réseau	Passerelle(s)	Serveur(s) DNS	Suffixe(s) DNS
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp				
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

Les informations de ce fichier CSV appliquent différents paramètres IPv4 statiques et dynamiques à vm-3-win sur le site protégé et le site de récupération.

- Sur le site vcenter-server-site-B :
 - Configure les suffixes DNS example.com et eng.example.com de toutes les NIC de cette machine virtuelle.
 - Ajoute une NIC, l'ID d'adaptateur 1 avec les serveurs WINS primaire et secondaire 2.2.3.4 et 2.2.3.5 utilisant DHCP pour obtenir une adresse IP et configure le serveur DNS statique 1.1.1.1.
 - Ajoute une NIC, l'ID d'adaptateur 2 avec les serveurs WINS primaire et secondaire 2.2.3.4 et 2.2.3.5 ayant une adresse IPv4 statique 192.168.1.22 et un serveur DNS 1.1.1.2.
- Sur le site vcenter-server-site-A :
 - Configure les suffixes DNS sur example.com et eng.example.com de toutes les NIC de cette machine virtuelle.
 - Configure les serveurs DNS 1.1.0.1 et 1.1.0.2 de toutes les NIC de cette machine virtuelle.
 - Ajoute une NIC, l'ID d'adaptateur 1 utilisant DHCP pour obtenir une adresse IPv4 et les informations sur le serveur DNS globalement attribuées.
 - Ajoute une NIC, l'ID d'adaptateur 2 avec les serveurs WINS primaire et secondaire 1.2.3.4 et 1.2.3.5 et une adresse IPv4 statique 192.168.0.22.

Exemple : Configuration des adresses IPv4 et IPv6 DHCP et statiques

Vous pouvez modifier le fichier CSV généré pour attribuer plusieurs NIC à vm-3-win, l'une des machines virtuelles. Les NIC peuvent utiliser une combinaison d'adresses IPv4 et IPv6 DHCP et statiques. Les paramètres peuvent être différents sur le site protégé et le site de récupération.

Pour plus de lisibilité, l'exemple de fichier CSV dans le tableau suivant omet les colonnes vides. Les colonnes Domaine DNS et NetBIOS sont omises.

Tableau 8-5. Configuration des adresses IPv4 et IPv6 DHCP statiques sur un fichier CSV modifié

ID de la VM	Nom de VM	vCenter Server	ID de l'adaptateur	WIN S primaire	WIN S secondaire	Adresse IP	Masque de sous-réseau	Passerelle(s)	Adresse IPv6	Longueur de préfixe de sous-réseau IPv6	Passerelle(s) IPv6	Serveur(s) DNS	Suffixe(s) DNS
protecte-d-vm-1-0301	vm-3-win	vcen-ter-server-site-B	0										exemple.com
protecte-d-vm-1-0301	vm-3-win	vcen-ter-server-site-B	0										eng.example.com
protecte-d-vm-1-0301		vcen-ter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.0	192.168.1.1	dhcp			1.1.1.1	
protecte-d-vm-1-0301		vcen-ter-server-site-B	2	2.2.3.4	2.2.3.5	dhcp			::ffff:192.168.1.22	32	::ffff:192.168.1.1	1.1.1.2	
protecte-d-vm-1-0301	vm-3-win	vcen-ter-server-site-A	0										exemple.com
protecte-d-vm-1-0301	vm-3-win	vcen-ter-server-site-A	0										eng.example.com

Tableau 8-5. Configuration des adresses IPv4 et IPv6 DHCP statiques sur un fichier CSV modifié (suite)

ID de la VM	Nom de VM	vCenter Server	ID de l'adaptateur	WINS primaires	WINS secondaires	Adresse IP	Masque de sous-réseau	Passerelle(s)	Adresse IPv6	Longueur de préfixe de sous-réseau IPv6	Passerelle(s) IPv6	Serveur(s) DNS	Suffixe(s) DNS
protecte-d-vm-1-0301		vcen-ter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	
protecte-d-vm-1-0301		vcen-ter-server-site-A	1									::ffff:192.168.0.251	
protecte-d-vm-1-0301		vcen-ter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.0	192.168.0.1				1.1.1.1	

Les informations de ce fichier CSV appliquent différents paramètres IP à vm-3-win sur le site protégé et le site de récupération.

- Sur le site vcenter-server-site-B :
 - Configure les suffixes DNS example.com et eng.example.com de toutes les NIC de cette machine virtuelle.
 - Ajoute une NIC, l'ID d'adaptateur 1 avec les serveurs WINS primaire et secondaire 2.2.3.4 et 2.2.3.5 qui définit une adresse IPv4 statique 192.168.1.21, utilise DHCP pour obtenir une adresse IPv6 et utilise le serveur DNS 1.1.1.1.
 - Ajoute une NIC, l'ID d'adaptateur 2 avec les serveurs WINS primaire et secondaire 2.2.3.4 et 2.2.3.5 utilisant DHCP pour obtenir une adresse IPv4, définit une adresse IPv6 statique ::ffff:192.168.1.22 et utilise le serveur DNS 1.1.1.2.
- Sur le site vcenter-server-site-A :
 - Configure les suffixes DNS sur example.com et eng.example.com de toutes les NIC de cette machine virtuelle.
 - Ajoute une NIC, l'ID d'adaptateur 1 utilisant DHCP pour obtenir une adresse IPv4 et définit une adresse IPv6 statique ::ffff:192.168.1.22. L'ID d'adaptateur 1 utilise les serveurs DNS IPv6 statiques ::ffff:192.168.0.250 et ::ffff:192.168.0.251.

- Ajoute une NIC, l'ID d'adaptateur 2 avec les serveurs WINS primaire et secondaire 1.2.3.4 et 1.2.3.5, une adresse IPv4 statique 192.168.0.22 et un serveur DNS 1.1.1.1. En laissant la colonne IPv6 vide, l'ID d'adaptateur 2 utilise DHCP pour les adresses IPv6.

Exécutez DR IP Customizer pour personnaliser les propriétés IP de plusieurs machines virtuelles

Vous pouvez utiliser l'outil DR IP Customizer pour personnaliser les propriétés IP de plusieurs machines virtuelles protégées par Site Recovery Manager.

Conditions préalables

Utilisez l'outil DR IP Customizer sur un ordinateur ayant accès aux instances de vCenter Server de votre environnement.

Procédure

- 1 Ouvrez un shell de commande sur l'hôte du Serveur Site Recovery Manager .
- 2 Modifiez le répertoire en `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
- 3 Exécutez la commande `dr-ip-customizer.exe` afin de générer un fichier CSV (comma-separated-value) contenant des informations sur les machines virtuelles protégées.

```
dr-ip-customizer.exe --cfg ..\config\vmware-dr.xml --cmd generate --out
"C:\MassIPCustCSVs\MassIPCust-generate-output.csv" --vc vc04.eng.example.com
```

Cet exemple indique `dr-ip-customizer.exe` sur le fichier `vmware-dr.xml` du Serveur Site Recovery Manager et génère le fichier `MassIPCust-generate-output.csv` pour l'instance de vCenter Server, `vc04.eng.example.com`.

- 4 (Facultatif) Vérifiez l'empreinte de vCenter Server et saisissez **y** pour confirmer que vous faites confiance à cette instance de vCenter Server.

Si vous avez spécifié l'option `--ignore-thumbprint`, vous n'êtes pas invité à vérifier l'empreinte.

- 5 Saisissez les informations d'identification pour vous connecter à l'instance de vCenter Server.

Vous pouvez être invité à confirmer une nouvelle fois que vous faites confiance à cette instance de vCenter Server.

- 6 Modifiez le fichier CSV généré pour personnaliser les propriétés IP des machines virtuelles du plan de récupération.

Vous pouvez utiliser une application de feuille de calcul pour modifier le fichier CSV. Enregistrez le fichier CSV modifié sous un nouveau nom.

- 7 Exécutez `dr-ip-customizer.exe` pour appliquer les propriétés IP personnalisées du fichier CSV modifié.

Vous pouvez utiliser l'outil DR IP Customizer sur le site protégé ou le site de récupération. Les ID de machines virtuelles protégées sont différents pour chaque site. De ce fait, quel que soit le site choisi pour exécuter l'outil DR IP Customizer et générer le fichier CSV, vous devez utiliser le même site lorsque vous exécutez à nouveau DR IP Customizer pour appliquer les paramètres.

```
dr-ip-customizer.exe --cfg ..\config\vmware-dr.xml --cmd apply --csv  
"C:\MassIPCustCSVs\MassIPCust-ipv6.csv" --vc vc04.eng.example.com
```

Cet exemple indique `dr-ip-customizer.exe` sur le fichier `vmware-dr.xml` du Serveur Site Recovery Manager et applique les personnalisations du fichier `MassIPCustCSVs\MassIPCust-ipv6.csv` à l'instance de vCenter Server, `vc04.eng.example.com`.

Résultats

Les personnalisations spécifiées sont appliquées à toutes les machines virtuelles nommées dans le fichier CSV au cours d'une récupération. Il n'est pas nécessaire de configurer manuellement les paramètres IP pour ces machines lors de la modification des propriétés de leur plan de récupération.

Configuration avancée Site Recovery Manager

9

La configuration Site Recovery Manager par défaut active quelques scénarios de récupération simples. Les utilisateurs avancés peuvent personnaliser Site Recovery Manager, de façon à ce qu'il prenne en charge une gamme plus étendue d'exigences de récupération de site.

Ce chapitre contient les rubriques suivantes :

- Configurer la protection d'une machine virtuelle ou d'un modèle
- Configurer les mappages de ressources pour une machine virtuelle
- Spécifier une banque de données non répliquée pour les fichiers d'échange
- Récupération de machines virtuelles dans plusieurs hôtes sur le site de récupération
- Redimensionner les fichiers disque de la machine virtuelle pendant la réplication en utilisant des amorces de réplication
- Redimensionner les fichiers disque de la machine virtuelle pendant la réplication sans utiliser des amorces de réplication
- Reconfigurer les paramètres de Site Recovery Manager

Configurer la protection d'une machine virtuelle ou d'un modèle

Vous pouvez modifier les propriétés de protection de n'importe quelle machine virtuelle ou n'importe quel modèle se trouvant dans un groupe de protection. Vous pouvez changer les mappages de ressources, les périphériques de stockage connectés et leurs banques de données, ainsi que les autres propriétés qui contrôlent la configuration avec laquelle Site Recovery Manager récupère la machine virtuelle.

Vous devez configurer la protection des machines virtuelles qui ont comme statut Non configurée ou Mappage manquant.

Si vous utilisez la réplication basée sur la baie, la modification des propriétés d'une machine virtuelle pour ajouter ou modifier les périphériques de stockage (tels que les disques durs ou les lecteurs de DVD), peut affecter la protection de la machine si le périphérique que vous ajoutez est stocké dans une banque de données qui n'est pas répliquée ou qui est protégée par un groupe de protection différent.

- Si le nouveau périphérique est créé dans une banque de données répliquée ne faisant pas partie d'un groupe de protection, la banque de données est ajoutée au groupe de banques de données protégées de la machine virtuelle et la protection de la machine n'est pas affectée.
- Si le nouveau périphérique est créé dans une banque de données répliquée protégée par un groupe de protection différent, la protection de la machine virtuelle est invalidée.
- Si le nouveau périphérique est créé dans une banque de données non répliquée, la protection de la machine virtuelle est invalidée.
- Si vous utilisez Storage vMotion pour transférer une machine virtuelle vers une banque de données non répliquée ou une banque de données répliquée dans une baie que Site Recovery Manager ne gère pas (par l'intermédiaire d'un SRA), la protection de la machine virtuelle est invalidée. Vous pouvez utiliser Storage vMotion pour transférer une machine virtuelle vers une banque de données faisant partie d'un autre groupe de protection.

Procédure

- 1 Cliquez sur **Groupes de protection** dans l'interface de Site Recovery Manager et sélectionnez le groupe de protection dans lequel figure la machine virtuelle à configurer.
- 2 Dans l'onglet **Machines virtuelles**, cliquez avec le bouton droit de la souris sur une machine virtuelle et sélectionnez **Configurer la protection**.
- 3 Dans la fenêtre **Propriétés de machine virtuelle**, consultez et configurez les propriétés selon vos besoins.
 - a Cliquez sur **Dossier** pour spécifier un dossier de destination de remplacement.
 - b Cliquez sur **Pool de récupération** pour spécifier un pool de ressources de remplacement dans lequel mettre la machine virtuelle récupérée.
 - c Si vous configurez la protection d'un modèle, cliquez sur **Hôte de récupération** pour spécifier un hôte de remplacement dans lequel récupérer la machine virtuelle.
Cette étape s'applique uniquement aux modèles.
 - d Cliquez sur **Réseau** pour spécifier un réseau de récupération de remplacement dans lequel restaurer la machine virtuelle.
- 4 Cliquez sur **OK** pour appliquer la nouvelle configuration à la machine virtuelle sélectionnée.

Configurer les mappages de ressources pour une machine virtuelle

Si vous n'avez pas spécifié les mappages d'inventaire pour votre site, vous devez configurer les mappages de ressources pour chaque machine virtuelle. Vous pouvez configurer les mappages de ressources uniquement si les mappages d'inventaire au niveau du site n'ont pas été établis.

Si les mappages d'inventaire ont été établis pour un site, vous ne pouvez pas les remplacer en configurant la protection de machines virtuelles individuelles. Si vous devez remplacer les mappages d'inventaire pour quelques membres d'un groupe de protection, utilisez vSphere Client pour vous connecter au site de récupération et modifier les paramètres des espaces réservés ou pour les déplacer vers un autre dossier ou un autre pool de ressources.

Procédure

- 1 Cliquez sur **Groupes de protection** et accédez au groupe de protection qui comprend la machine virtuelle que vous souhaitez configurer.
- 2 Sur la page Machines virtuelles, faites un clic droit sur une machine virtuelle et cliquez sur **Configurer la protection**.

Si vous avez établi les mappages d'inventaire, ceux-ci sont appliqués.

- 3 Configurer les mappages au besoin.

Pour la plupart des machines virtuelles, vous pouvez modifier le dossier et de calculer les mappages de ressources. Pour plus d'informations, voir [Configurer la protection d'une machine virtuelle ou d'un modèle](#).

Spécifier une banque de données non répliquée pour les fichiers d'échange

Chaque machine virtuelle requiert un fichier d'échange. Par défaut, vCenter Server crée des fichiers d'échange dans la même banque de données que les autres fichiers de la machine virtuelle. Pour empêcher Site Recovery Manager de répliquer les fichiers d'échange, vous pouvez configurer les machines virtuelles de façon à pouvoir créer ces fichiers dans une banque de données non répliquée.

Attention Dans des circonstances normales, vous devez conserver les fichiers d'échange dans la même banque de données que les autres fichiers de la machine virtuelle. Toutefois, vous pouvez vouloir empêcher la réplication de ces fichiers d'échange, afin d'éviter une consommation excessive de la bande passante du réseau. De même, certains fournisseurs de stockage recommandent de ne pas répliquer les fichiers d'échange. N'empêchez la réplication des fichiers d'échange que si cela est absolument nécessaire.

Si vous utilisez une banque de données non répliquée pour les fichiers d'échange, vous devez créer une banque de données non répliquée pour tous les clusters protégés, à la fois sur le site protégé et sur le site de récupération. La banque de données non répliquée doit être visible pour tous les hôtes du cluster. Dans le cas contraire, vMotion ne pourra pas fonctionner.

Procédure

- 1 Dans vSphere Client, cliquez avec le bouton droit de la souris sur un cluster ESXi, puis cliquez sur **Modifier les paramètres**.
- 2 Dans la page des paramètres du cluster, cliquez sur **Emplacement du fichier d'échange**, sélectionnez **Stocker le fichier d'échange dans la banque de données spécifiée par l'hôte**, puis cliquez sur **OK**.
- 3 Sélectionnez une banque de données non répliquée pour chaque hôte du cluster.
 - a Sélectionnez un hôte et cliquez sur l'onglet **Configuration**.
 - b Dans le panneau Logiciel, cliquez sur **Emplacement des fichiers d'échange des machines virtuelles**, puis cliquez sur **Modifier** dans la partie supérieure droite du panneau principal.
 - c Dans la page de l'emplacement du fichier d'échange de la machine virtuelle, sélectionnez une banque de données non répliquée, puis cliquez sur **OK**.
- 4 Pour des hôtes autonomes ne faisant pas partie d'un cluster, sélectionnez l'hôte concerné et cliquez sur l'onglet **Configuration**.
- 5 Dans le panneau Logiciel, cliquez sur **Emplacement des fichiers d'échange des machines virtuelles**, puis cliquez sur **Modifier** dans la partie supérieure droite du panneau principal.
- 6 Sélectionnez **Enregistrer le fichier d'échange dans la banque de données de fichiers d'échange sélectionnée ci-dessous**, sélectionnez la banque de données, puis cliquez sur **OK**.
- 7 Mettez hors tension puis sous tension toutes les machines virtuelles du cluster.
 La réinitialisation du système d'exploitation invité n'est pas suffisante. Le changement d'emplacement de fichier d'échange prend effet après la mise hors tension puis sous tension des machines virtuelles.
- 8 Parcourez la banque de données que vous avez sélectionnée pour les fichiers d'échange et vérifiez que des fichiers VSWP sont présents pour les machines virtuelles dans le cluster.

Récupération de machines virtuelles dans plusieurs hôtes sur le site de récupération

Vous pouvez créer des plans de récupération qui récupèrent des machines virtuelles dans plusieurs hôtes du site de récupération, contenus dans un réseau de test en quarantaine.

Site Recovery Manager permet aux vSwitches d'être basés sur DVS et d'étendre les hôtes. Si vous acceptez le réseau de test par défaut configuré sur **Auto**, les machines virtuelles récupérées sur l'ensemble des hôtes sont placées dans leur propre réseau de test. Chaque commutateur de test est isolé entre les hôtes. Ainsi, les machines virtuelles d'un même plan sont isolées à la fin de la

récupération. Pour permettre aux machines virtuelles de communiquer, établissez et sélectionnez des commutateurs DVS ou des VLAN. Avec un VLAN isolé connectant l'ensemble des hôtes les uns aux autres, et non à un réseau de production, vous pouvez tester une récupération de manière plus réaliste. Pour parvenir à une connectivité entre les hôtes de récupération, tout en les isolant du réseau de production, suivez les recommandations suivantes :

- Créez des commutateurs DVS qui sont connectés à un VLAN isolé et privé. Un tel VLAN permet aux hôtes et aux machines virtuelles d'être connectés, tout en étant isolés des machines virtuelles de production. Utilisez une convention de dénomination qui désigne clairement que le DVS existe aux fins de test, puis sélectionnez ce DVS dans la colonne de réseau test de l'éditeur du plan de récupération.
- Créez des VLAN de test sur un réseau physique, en ne fournissant aucune route de retour vers le site protégé. Tronquez les VLAN test vers les clusters vSphere du site de récupération et créez des commutateurs virtuels pour les identifiants des VLAN test. Utilisez une convention de dénomination claire pour identifier ces commutateurs comme étant destinés aux tests. Sélectionnez ces commutateurs à partir de la colonne de réseau de récupération test dans l'éditeur de plan de récupération.

Redimensionner les fichiers disque de la machine virtuelle pendant la réplication en utilisant des amorces de réplication

vSphere Replication vous empêche de redimensionner le fichier disque de la machine virtuelle pendant la réplication. Si vous avez utilisé des amorces de réplication pour le disque cible, vous pouvez redimensionner le disque manuellement.

Procédure

- 1 Annulez la configuration de la réplication sur la machine virtuelle.
- 2 Redimensionnez le disque sur le site source.
- 3 Redimensionnez le disque cible restant au terme de l'annulation de la configuration.
- 4 Reconfigurez la réplication sur la machine virtuelle.

Redimensionner les fichiers disque de la machine virtuelle pendant la réplication sans utiliser des amorces de réplication

vSphere Replication vous empêche de redimensionner le fichier disque de la machine virtuelle pendant la réplication. Si vous n'avez pas utilisé les amorces de réplication lors de la configuration du disque cible, vSphere Replication supprime le disque cible lorsque vous arrêtez la réplication.

Pour redimensionner un disque de machine virtuelle si vous n'avez pas initialement utilisé les amorces de réplication, vous devez effectuer un test de récupération, cloner la machine virtuelle récupérée et reconfigurer le disque manuellement en utilisant les amorces de réplication.

Procédure

- 1 Effectuer un test de récupération de la machine virtuelle.
- 2 Clonez la machine virtuelle récupérée sur la même banque de données que celle où la réplication a lieu après avoir configuré la réplication.
- 3 Annulez le test de récupération.
- 4 Annulez la configuration de la réplication.
- 5 Redimensionnez le disque sur le site source.
- 6 Redimensionnez le disque de la machine virtuelle clonée sur le site cible.
- 7 Annulez l'enregistrement de la machine virtuelle clonée sur le site cible, mais ne supprimez pas les disques.
- 8 Activez la réplication en utilisant les disques de la machine virtuelle clonée comme amorces.

Reconfigurer les paramètres de Site Recovery Manager

L'utilisation des **Paramètres avancés** vous permet d'afficher ou de modifier de nombreux paramètres personnalisés pour le service Site Recovery Manager. Les paramètres avancés permettent à un utilisateur disposant des privilèges adéquats de modifier plusieurs valeurs par défaut affectant le fonctionnement de diverses fonctionnalités de Site Recovery Manager.

Important Lors d'une mise à niveau, Site Recovery Manager ne conserve pas les paramètres avancés que vous avez configurés dans l'installation précédente. Ce fonctionnement est propre à la conception. En raison de modifications dans les valeurs par défaut ou d'améliorations des performances, il est possible que les paramètres avancés que vous définissez dans une version précédente de Site Recovery Manager ne soient pas requis ou compatibles avec la nouvelle version. De même, si vous désinstallez puis réinstallez la même version de Site Recovery Manager en réutilisant la base de données de l'installation précédente, les paramètres avancés ne sont pas conservés.

Modifier les paramètres du site local

Site Recovery Manager surveille la consommation des ressources sur l'hôte du Serveur Site Recovery Manager et émet un signal d'alarme si le seuil d'une ressource est atteint. Vous pouvez modifier les seuils et la façon dont Site Recovery Manager émet des signaux d'alarme.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.

- 2 Cliquez sur **localSiteStatus**.
- 3 Modifiez les paramètres selon vos besoins.

Option	Action
Modifiez l'intervalle selon lequel Site Recovery Manager contrôle l'utilisation du CPU, l'espace disque et la mémoire libre sur le site local	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.checkInterval .
Modifiez le nom du site local	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.displayName .
Modifiez le délai pendant lequel Site Recovery Manager attend entre l'émission de signaux d'alarme concernant l'utilisation du CPU, l'espace disque et la mémoire libre sur le site local	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.eventFrequency .
Modifiez le pourcentage d'utilisation du CPU qui provoque l'émission d'un événement d'utilisation élevé du CPU par Site Recovery Manager	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.maxCpuUsage .
Modifiez le pourcentage d'espace disque disponible qui amène Site Recovery Manager à déclencher un événement d'espace disque insuffisant.	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.minDiskSpace .
Modifiez la quantité de mémoire libre provoquant l'émission d'un événement de mémoire insuffisante par Site Recovery Manager	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.minMemory .

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier les paramètres de journalisation

Vous pouvez modifier les niveaux de journalisation fournis par Site Recovery Manager pour les composants du Serveur Site Recovery Manager.

Le Serveur Site Recovery Manager effectue une rotation des journaux. Lorsque vous redémarrez le Serveur Site Recovery Manager ou qu'un fichier journal devient trop volumineux, le Serveur Site Recovery Manager crée un fichier journal et écrit tous les messages suivants dans ce nouveau fichier. Lorsque le Serveur Site Recovery Manager crée des fichiers journaux, il compresse les anciens fichiers journaux pour économiser de l'espace.

Vous pouvez réduire les niveaux de journalisation de certains composants du Serveur Site Recovery Manager, car les fichiers journaux deviennent trop volumineux trop rapidement. Vous pouvez augmenter les niveaux de journalisation de certains composants pour permettre de diagnostiquer les problèmes. La liste des niveaux de journalisation disponibles est la même pour tous les composants du Serveur Site Recovery Manager.

aucun

Désactive la journalisation.

silencieux

Enregistre les entrées de journal minimales.

panique

Enregistre uniquement les entrées de journal de panique. Les messages de panique se déclenchent en cas de panne complète.

erreur

Enregistre les entrées de journal de panique et d'erreur. Les messages d'erreur se déclenchent lorsque des problèmes se produisent, qu'ils soient ou non susceptibles d'entraîner une panne.

avertissement

Enregistre les entrées de journal de panique, d'erreur et d'avertissement. Les messages d'avertissement se déclenchent en cas de comportement indésirable, mais qui peut faire partie du déroulement attendu du fonctionnement.

info

Enregistre les entrées de journal de panique, d'erreur, d'avertissement et d'informations. Les messages d'informations fournissent des informations sur le déroulement normal du fonctionnement.

verbose

Enregistre les entrées de journal de panique, d'erreur, d'avertissement, d'informations et de détails. Les messages détaillés fournissent des informations plus détaillées que les messages d'informations.

trivia

Enregistre les entrées de journal de panique, d'erreur, d'avertissement, d'informations, de détails et trivia. Les messages trivia fournissent toutes les informations disponibles. Ce niveau de journalisation est utile pour le débogage, mais il peut générer une telle quantité de données que cela risque d'affecter les performances.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **logManager**.
- 3 Modifiez le paramètre de journalisation.

Par défaut, tous les composants enregistrent des journaux de niveau détaillé, sauf indication contraire dans la description du niveau de journalisation.

Option	Description
Définir un niveau de journalisation pour tous les composants qui n'ont pas d'entrée dans logManager	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Default .
Définir un niveau de journalisation pour un module API externe	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.ExternalAPI .
Définir un niveau de journalisation pour vSphere Replication	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.HbrProvider .
Définir un niveau de journalisation pour l'outil IP Customizer	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.IPCustomizer .
Définir un niveau de journalisation pour le mappage d'inventaire	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.InventoryMapper .
Définir un niveau de journalisation pour les problèmes de licence	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Licensing .
Définir un niveau de journalisation pour les problèmes de persistance	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Persistence .
Définir un niveau de journalisation pour les opérations de récupération	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Recovery . Par défaut, la journalisation de la récupération est définie sur trivia .
Définir un niveau de journalisation pour les opérations de configuration de récupération	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.RecoveryConfig .
Définir un niveau de journalisation pour les opérations de réplication basée sur la baie	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Replication .
Définir un niveau de journalisation pour les problèmes d'autorisation entre le Serveur Site Recovery Manager et vCenter Server	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.ServerAuthorization .
Définir un niveau de journalisation pour la gestion des sessions	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.SessionManager .
Définir un niveau de journalisation pour l'adaptateur de services Web SOAP	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.SoapAdapter . En raison des niveaux de trafic générés par l'adaptateur SOAP, la sélection du niveau de journalisation trivia peut affecter les performances. Par défaut, la journalisation de l'adaptateur SOAP est définie sur info .

Option	Description
Définir un niveau de journalisation pour les problèmes de stockage	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Storage .
Définir un niveau de journalisation pour les messages provenant du fournisseur de stockage basé sur la baie	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.StorageProvider .

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Les nouveaux niveaux de journalisation s'appliquent dès que vous cliquez sur **OK**. Il est inutile de redémarrer le service Site Recovery Manager. Si vous redémarrez le Serveur Site Recovery Manager, la journalisation reste définie au niveau que vous avez choisi.

Modifier les paramètres de récupération

Vous pouvez ajuster les valeurs par défaut des délais d'expiration qui se produisent lorsque vous testez ou exécutez un plan de récupération. Vous pouvez régler les valeurs par défaut si les tâches échouent à se terminer en raison de l'expiration des délais.

Plusieurs types de délais d'expiration peuvent se produire lorsque les étapes du plan de récupération sont exécutées. Ces délais d'expiration provoquent une interruption du plan pendant un intervalle spécifié afin qu'il y ait suffisamment de temps pour que l'étape s'achève.

Site Recovery Manager applique des paramètres avancés à une machine virtuelle lorsque vous configurez la protection sur cette machine virtuelle :

- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`
- `recovery.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

Si vous modifiez ces paramètres avancés après la configuration de la protection d'une machine virtuelle, les nouveaux paramètres ne s'appliquent pas à cette machine virtuelle. Les modifications apportées à ces paramètres avancés s'appliquent uniquement aux machines virtuelles que vous protégez après la modification. Cette particularité est intentionnelle, car si Site Recovery Manager appliquait des paramètres avancés modifiés à des machines virtuelles disposant déjà d'une protection configurée, cela entraînerait des modifications non souhaitées dans la protection de ces machines virtuelles.

Pour appliquer aux machines virtuelles précédemment protégées les modifications que vous apportez à ces paramètres avancés, vous devez reconfigurer ces machines virtuelles individuellement. Par exemple, si vous reconfigurez le paramètre `defaultPriority`, vous pouvez manuellement reconfigurer la priorité d'une machine virtuelle précédemment protégée pour la

faire correspondre au nouveau paramètre `defaultPriority`. Vous pouvez également appliquer tous les nouveaux paramètres avancés en supprimant la protection d'une machine virtuelle en retirant celle-ci du groupe de protection, puis en la rajoutant à ce groupe. Le fait d'ajouter de nouveau la machine virtuelle au groupe de protection permet d'appliquer les paramètres avancés plus récents à la machine virtuelle.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **recovery**.
- 3 Modifiez les paramètres du site de récupération.

Option	Action
Modifiez l'expiration de la personnalisation d'IP	Tapez une nouvelle valeur dans la zone de texte recovery.customizationTimeout .
Modifiez la priorité par défaut pour la récupération d'une machine virtuelle	Entrez une nouvelle valeur dans la zone de texte recovery.defaultPriority .
Activez ou désactivez la récupération forcée	Cochez ou décochez la case recovery.forceRecovery . La récupération forcée doit uniquement être activée si une absence de connectivité au site protégé affecte sérieusement RTO.
Modifiez le délai d'expiration pour la mise sous tension des hôtes dans un cluster	Entrez une nouvelle valeur dans la zone de texte recovery.hostPowerOnTimeout .
Modifiez le délai d'expiration pour la mise hors tension du système d'exploitation client	Entrez une nouvelle valeur dans la zone de texte recovery.powerOffTimeout . La nouvelle valeur de dépassement de délai s'applique aux tâches de mise hors tension des machines virtuelles du site de récupération.
Modifiez le délai après la mise sous tension d'une machine virtuelle avant le lancement des tâches dépendantes	Entrez une nouvelle valeur dans la zone de texte recovery.powerOnDelay . La nouvelle valeur s'applique aux tâches de mise sous tension des machines virtuelles du site de récupération.
Modifiez le délai d'expiration à attendre pour VMware Tools lors de la mise sous tension des machines virtuelles	Entrez une nouvelle valeur dans la zone de texte recovery.powerOnTimeout . La nouvelle valeur de mise sous tension s'applique aux tâches de mise sous tension des machines virtuelles du site de récupération. Si VMware Tools n'est pas installé sur les machines virtuelles protégées, définissez cette valeur sur 0.
Activez ou désactivez l'évitement de l'arrêt du système d'exploitation client	Cochez ou décochez la case recovery.skipGuestShutdown . Si VMware Tools n'est pas installé sur les machines virtuelles protégées et que le délai d'attente de l'arrêt client n'est pas défini sur 0, vous devez sélectionner cette option. Si vous ne sélectionnez pas cette option et que VMware Tools n'est pas installé, le processus de récupération ne peut pas se poursuivre après l'étape Arrêt des VM sur le site de récupération.

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier les paramètres du site distant

Vous pouvez modifier les valeurs par défaut utilisées par le Serveur Site Recovery Manager sur le site protégé pour déterminer si le Serveur Site Recovery Manager du site distant est disponible.

Site Recovery Manager contrôle la connexion entre le site protégé et le site de récupération et émet des signaux d'alarme si la connexion est interrompue. Vous pouvez modifier les critères qui provoquent l'émission d'un événement de connexion par Site Recovery Manager et modifier la façon dont Site Recovery Manager émet des signaux d'alarme.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **remoteSiteStatus**.
- 3 Modifier les paramètres.

Option	Action
Modifiez le nombre de tentatives de contrôle de statut du site distant (commandes Ping) avant de déclarer la défaillance du contrôle	Entrez une nouvelle valeur dans la zone de texte remoteSiteStatus.pingFailedDelay .
Modifiez le nombre d'échecs des commandes Ping avant d'émettre un événement de type arrêt du site	Entrez une nouvelle valeur dans la zone de texte remoteSiteStatus.panicDelay .
Modifiez l'intervalle selon lequel Site Recovery Manager contrôle si le Serveur Site Recovery Manager du site distant est disponible	Entrez une nouvelle valeur dans la zone de texte remoteSiteStatus.pingInterval .

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier le délai d'expiration pour la création de machines virtuelles à espace réservé

Vous pouvez régler les paramètres de réplique pour modifier le temps d'attente de Site Recovery Manager lors de la création d'espaces réservés de machines virtuelles.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **replication**.
- 3 Modifiez le paramètre **replication.placeholderVmCreationTimeout** pour modifier le nombre de secondes d'attente lors de la création d'une machine virtuelle à espace réservé.
- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier les paramètres de stockage

Vous pouvez ajuster les paramètres de votre baie de stockage, afin de modifier la façon dont Site Recovery Manager et vCenter Server communiquent avec l'adaptateur de réplication de stockage (SRA).

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **storage**.
- 3 Modifiez les paramètres de stockage.

Option	Action
Modifiez le délai d'expiration de la mise à jour du SRA	Entrez une nouvelle valeur dans la zone de texte storage.commandTimeout .
Modifiez le nombre maximum d'opérations simultanées du SRA	Entrez une nouvelle valeur dans la zone de texte storage.maxConcurrentCommandCnt .
Modifiez le délai minimum en secondes entre les calculs de groupe de banques de données	Entrez une nouvelle valeur dans la zone de texte storage.minDsGroupComputationInterval .
Modifiez l'intervalle entre les mises à jour de statut pour les opérations de synchronisation des données en cours	Entrez une nouvelle valeur dans la zone de texte storage.querySyncStatusPollingInterval .
Modifiez l'intervalle entre les contrôles de détection de baie de stockage	Entrez une nouvelle valeur dans la zone de texte storage.storagePingInterval .
Modifiez le délai maximal autorisé pour que les opérations de synchronisation des données s'effectuent	Entrez une nouvelle valeur dans la zone de texte storage.syncTimeout .

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier les paramètres du fournisseur de stockage

Dans le cas de la réplication basée sur la baie, le fournisseur de SAN est l'interface entre Site Recovery Manager et votre adaptateur de réplication de stockage (SRA). Avec certains SRA, vous devez modifier les valeurs par défaut du fournisseur SAN. Vous pouvez modifier les valeurs de dépassement de délai définies par défaut et d'autres comportements du fournisseur de SAN de Site Recovery Manager.

Vous pouvez modifier les paramètres de resignature, de détermination des noms de banques de données, du nombre d'analyses d'hôtes et d'expiration de délais. Pour plus d'informations sur ces valeurs, consultez la documentation SRA de votre fournisseur de baies.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **storageProvider**.
- 3 Modifiez les paramètres du fournisseur de SAN.

Option	Action
Faites essayer à Site Recovery Manager de détacher et rattacher les LUN avec des volumes dupliqués	Cochez la case storageProvider.autoDetachLUNsWithDuplicateVolume .
Définissez l'indicateur IWM.EnableResignature sur les hôtes ESXi pendant le test et la récupération	Dans la zone de texte storageProvider.autoResignatureMode , entrez 0 pour désactiver, 1 to activer, ou 2 pour ignorer l'indicateur. La valeur par défaut est 0. Si vous définissez cet indicateur sur 1, Site Recovery Manager résigne tous les volumes de snapshots VMFS connus, notamment tous ceux qui ne sont pas gérés par Site Recovery Manager. Si vous laissez l'indicateur à la valeur 0, Site Recovery Manager résigne uniquement les volumes de snapshots VMFS qu'il gère.
Dès qu'une récupération est réussie, forcez la suppression du préfixe snap-xx appliqué aux noms de banques de données récupérées	Cochez la case storageProvider.fixRecoveredDatastoreNames .
Retarder les analyses d'hôtes au cours des tests et de la récupération	<p>Les SRA peuvent envoyer des réponses à Site Recovery Manager avant qu'un périphérique de stockage promu sur le site de récupération ne soit disponible pour les hôtes ESXi. Lorsque Site Recovery Manager reçoit une réponse d'un SRA, il réanalyse les périphériques de stockage. Si les périphériques de stockage ne sont pas encore totalement disponibles, ESXi Server ne les détecte pas et Site Recovery Manager ne trouve pas les périphériques répliqués lorsqu'il effectue la réanalyse. Les banques de données ne sont pas créées et les machines virtuelles récupérées sont introuvables.</p> <p>Pour retarder le démarrage de la réanalyse des périphériques de stockage jusqu'à ce que ceux-ci soient disponibles sur les hôtes ESXi, tapez une nouvelle valeur dans la zone de texte storageProvider.hostRescanDelaySec. Ne modifiez cette valeur que si vous rencontrez des problèmes avec des banques de données indisponibles.</p>
Répétez des analyses d'hôtes pendant le test et la récupération	<p>Entrez une nouvelle valeur dans la zone de texte storageProvider.hostRescanRepeatCnt. Certaines baies de stockage nécessitent plusieurs réanalyses, par exemple, pour découvrir les snapshots des LUN basculées.</p> <p>dans les versions précédentes, vous avez peut-être utilisé le paramètre storageProvider.hostRescanRepeatCnt pour introduire un délai dans les récupérations. Utilisez plutôt le paramètre storageProvider.hostRescanDelaySec.</p>
Modifiez l'intervalle pendant lequel Site Recovery Manager attend que chaque nouvelle analyse HBA soit terminée	Entrez une nouvelle valeur dans la zone de texte storageProvider.hostRescanTimeoutSec .

Option	Action
Définissez le nombre de fois où Site Recovery Manager tente de procéder à la resignature d'un volume VMFS	Entrez une nouvelle valeur dans la zone de texte storageProvider.resignatureFailureRetryCount .
Définir un délai d'expiration pour la resignature d'un volume VMFS	Tapez une nouvelle valeur dans la zone de texte storageProvider.resignatureTimeoutSec . Si vous modifiez le paramètre storageProvider.hostRescanTimeoutSec , augmentez le paramètre storageProvider.resignatureTimeoutSec en définissant la même valeur de délai d'expiration que vous avez utilisée pour storageProvider.hostRescanTimeoutSec .
Rechercher des fichiers VMX dans des banques de données récupérées pour identifier les machines virtuelles que Storage vMotion a déplacé au cours d'un test ou d'une récupération	L'option est sélectionnée par défaut. Décochez la case storageProvider.storageVmotionVmxSearch pour désactiver cette option.
Identifiez les chemins de fichiers VMX que Site Recovery Manager ne doit pas considérer comme des candidats potentiels de fichiers VMX après Storage vMotion	Certaines baies créent des chemins de fichiers VMX que l'algorithme de recherche storageProvider.storageVmotionVmxSearch doit ignorer. Entrez une liste de chaînes séparées par une virgule dans le champ storageProvider.storageVmotionVmxFilePathsToSkip afin d'identifier les chemins de fichiers VMX à ignorer après Storage vMotion. Site Recovery Manager ne considère pas les chemins de fichiers contenant une ou plusieurs de ces chaînes comme des candidats potentiels de fichiers VMX après Storage vMotion.
Changez l'intervalle pendant lequel Site Recovery Manager attend la disponibilité des banques de données récupérées	Tapez une nouvelle valeur dans la zone de texte storageProvider.waitForAccessibleDatastoreTimeoutSec . Changez cette valeur si vous subissez des expirations de délai d'attente se produisant lorsque Site Recovery Manager vérifie des banques de données qui ne sont pas encore disponibles. Ce paramètre est disponible dans Site Recovery Manager 5.5.1 et versions ultérieures.
Changez l'intervalle pendant lequel Site Recovery Manager attend des banques de données récupérées à ajouter à vCenter Server	Tapez une nouvelle valeur dans la zone de texte storageProvider.waitForRecoveredDatastoreTimeoutSec . Changez cette valeur si vous subissez des expirations de délai d'attente se produisant lorsque Site Recovery Manager vérifie des banques de données pas encore détectées par vCenter Server. Ce paramètre est disponible dans Site Recovery Manager 5.5.1 et versions ultérieures.
Changez l'intervalle pendant lequel Site Recovery Manager attend le montage de volumes VMFS	Tapez une nouvelle valeur dans la zone de texte storageProvider.waitForVmfsVolumesMountedStateTimeoutSec . Changez cette valeur si vous subissez des expirations de délai d'attente se produisant lorsque Site Recovery Manager vérifie des volumes VMFS dont le montage est trop long. Ce paramètre est disponible dans Site Recovery Manager 5.5.1 et versions ultérieures.

4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier les paramètres de vSphere Replication

Vous pouvez régler les paramètres globaux pour modifier le mode d'interaction de Site Recovery Manager avec vSphere Replication.

Procédure

- 1 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 2 Cliquez sur **vrReplication**.
- 3 Modifier les paramètres de vSphere Replication.

Option	Description
Autoriser Site Recovery Manager à récupérer des machines virtuelles gérées par d'autres solutions. La valeur par défaut est false.	vSphere Replication autorise différentes solutions à gérer la réplication de machines virtuelles. Par défaut, Site Recovery Manager récupère uniquement les machines virtuelles qu'il gère. Pour autoriser Site Recovery Manager à récupérer des machines virtuelles gérées par d'autres solutions, cochez la case allowOtherSolutionTagInRecovery .
Conserver les anciens snapshots à un moments précis (PIT) au cours de la récupération	Si vous configurez vSphere Replication pour prendre des snapshot PIT des machines virtuelles protégées, Site Recovery Manager récupérera uniquement les snapshots les plus récents lorsque vous effectuerez une récupération. Pour récupérer les anciens snapshots PIT au cours d'une récupération, cochez la case preserveMpitImagesAsSnapshots .
Modifier le délai d'expiration pour l'inversion de la réplication au cours des opérations de reprotection	Tapez une nouvelle valeur dans la zone de texte reverseReplicationTimeout . La valeur saisie doit être égale à la moitié du délai d'expiration que vous voulez définir. La valeur par défaut est 7 200 et correspond à un délai d'expiration de synchronisation de 14 400 secondes. Modifiez cette valeur si vous rencontrez des problèmes de délai d'expiration lorsque vSphere Replication inverse la réplication au cours des opérations de reprotection.
Modifier le délai d'expiration pour les opérations de synchronisation de vSphere Replication	Tapez une nouvelle valeur dans la zone de texte synchronizationTimeout . Modifiez cette valeur si vous rencontrez des problèmes de délai d'expiration lorsque vSphere Replication synchronise les machines virtuelles sur le site de récupération.
Modifier le paramètre RPO par défaut pour les répliques	Entrez une nouvelle valeur dans la zone de texte vrReplication.timeDefault . La valeur par défaut est 240 minutes (4 heures). Cette valeur est sélectionnée lors de la configuration des répliques, mais vous pouvez spécifier une autre valeur de RPO dans l'Assistant Configurer la réplication lorsque vous configurez une réplication pour une machine virtuelle individuelle ou un groupe de machines virtuelles.

- 4 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager

Si vous utilisez Site Recovery Manager pour tester ou récupérer un grand nombre de machines virtuelles, vous devrez peut-être modifier les paramètres Site Recovery Manager par défaut pour obtenir les meilleurs temps de récupération possibles pour votre environnement ou pour éviter des expirations de délai d'attente.

Dans de grands environnements, Site Recovery Manager peut simultanément mettre sous tension ou hors tension un grand nombre de machines virtuelles. Une telle action simultanée est susceptible de créer une charge lourde sur l'infrastructure virtuelle, ce qui pourrait provoquer des délais d'expiration. Vous pouvez modifier certains paramètres Site Recovery Manager pour éviter les expirations de délai d'attente en limitant le nombre de mises sous et hors tension effectuées simultanément par Site Recovery Manager ou en allongeant les délais d'attente.

Les limites que vous définissez pour les opérations de mise sous et hors tension dépendent du nombre d'opérations simultanées que peut supporter votre infrastructure.

Vous pouvez modifier certaines options dans les **Paramètres avancés** de vSphere Client ou dans le plug-in client Site Recovery Manager. Pour modifier d'autres paramètres, éditez le fichier de configuration `vmware-dr.xml` fichier de configuration sur le Serveur Site Recovery Manager. Modifiez toujours les paramètres à l'aide des menus du client lorsqu'une option existe. Si vous modifiez les paramètres, vous devez apporter les mêmes modifications sur les instances du Serveur Site Recovery Manager et vCenter Server, sur le site protégé et le site de récupération.

Pour une description des paramètres modifiables, référez-vous à [Paramètres pour grands environnements Site Recovery Manager](#).

Procédure

- 1 Cliquez avec le bouton droit sur un cluster de l'inventaire vCenter Server et sélectionnez **Modifier les paramètres > vSphere DRS > Options avancées**.
- 2 Réglez le paramètre `srmMaxBootShutdownOps`.

Option	Description
Zone de texte Option	Tapez <code>srmMaxBootShutdownOps</code> .
Zone de texte Valeur	Tapez le nombre maximal d'opérations d'arrêt et de démarrage, par exemple 32. Si vous définissez la valeur sur 32, le prochain invité commence à démarrer ou à s'arrêter dès que le premier lot de 32 est terminé, à savoir les machines virtuelles de 1 à 32 démarrent simultanément, puis la machine virtuelle 33 démarre une fois qu'une des machines du premier lot a terminé, la machine virtuelle 34 démarre quand la deuxième machine virtuelle du premier lot a terminé, etc.

- 3 Cliquez sur **OK** pour enregistrer vos modifications.
- 4 Connectez-vous à l'hôte du Serveur Site Recovery Manager.
- 5 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.

Le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config`.

- 6 Modifiez les paramètres `defaultMaxBootAndShutdownOpsPerCluster` et `defaultMaxBootAndShutdownOpsPerHost` dans le fichier `vmware-dr.xml` :

```
<config>
```

```

...
<defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
<defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>

```

Si ces éléments n'existent pas encore dans le fichier `vmware-dr.xml`, vous pouvez les ajouter n'importe où dans la section `<config>`. Si vous définissez la valeur de `<defaultMaxBootAndShutdownOpsPerCluster>` sur 24, le prochain invité commence à démarrer ou à s'arrêter dès que le premier lot de 24 est terminé, à savoir les machines virtuelles de 1 à 24 démarrent simultanément, puis la machine virtuelle 25 démarre une fois qu'une des machines du premier lot a terminé, la machine virtuelle 26 démarre quand la deuxième machine virtuelle du premier lot a terminé, etc.

- 7 Redémarrez Serveur Site Recovery Manager pour appliquer les nouveaux paramètres.
- 8 Cliquez sur **Sites** dans l'interface de Site Recovery Manager, cliquez avec le bouton droit sur le site dont vous voulez modifier les paramètres, puis sélectionnez **Paramètres avancés**.
- 9 Sélectionnez **vrReplication** et augmentez le paramètre `synchronizationTimeout`.
La valeur par défaut est 7 200 et correspond à un délai d'expiration de synchronisation de 14 400 secondes.
- 10 Sélectionnez **stockage** et augmentez le paramètre `commandTimeout`.
Par exemple, augmentez la valeur `commandTimeout` à 3600 secondes.
- 11 Cliquez sur **OK** pour enregistrer vos modifications.

Paramètres pour grands environnements Site Recovery Manager

Pour protéger un grand nombre de machines virtuelles, vous pouvez modifier les paramètres Site Recovery Manager par défaut afin d'obtenir les meilleurs temps de récupération possibles pour votre environnement ou d'éviter des délais d'expiration.

Vous pouvez modifier certaines options dans les **Paramètres avancés** de vSphere Client ou dans le plug-in client Site Recovery Manager. Pour modifier d'autres paramètres, éditez le fichier de configuration `vmware-dr.xml` fichier de configuration sur le Serveur Site Recovery Manager. Modifiez toujours les paramètres à l'aide des menus du client lorsqu'une option existe. Si vous modifiez les paramètres, vous devez apporter les mêmes modifications sur les instances du Serveur Site Recovery Manager et vCenter Server, sur le site protégé et le site de récupération.

Pour modifier les paramètres, voir [Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager](#).

Tableau 9-1. Paramètres de modification du nombre d'opérations simultanées de mise sous et hors tension

Option	Description
srmMaxBootShutdownOps	Spécifie le nombre maximum de mises sous tension simultanées pour un cluster donné. Les arrêts clients et non forcés sont limités en fonction de cette valeur. Les arrêts clients surviennent au cours des arrêts du site principal (basculement planifié) et des workflows de personnalisation d'IP. Modifiez cette option par cluster dans vSphere Client en cliquant avec le bouton droit sur un cluster et en sélectionnant Modifier les paramètres > vSphere DRS > Options avancées . Ce paramètre remplace la valeur defaultMaxBootAndShutdownOpsPerCluster que vous pouvez définir dans le fichier <code>vmware-dr.xml</code> . Vous pouvez définir une valeur globale defaultMaxBootAndShutdownOpsPerCluster dans le fichier <code>vmware-dr.xml</code> , puis définir des valeurs srmMaxBootShutdownOps différentes pour chaque cluster individuel de vSphere Client. Par défaut, la limitation est désactivée.
defaultMaxBootAndShutdownOpsPerCluster	Spécifie le nombre maximum de mises sous tension simultanées pour tous les clusters protégés par Site Recovery Manager. Les arrêts clients et non forcés sont limités en fonction de cette valeur. Les arrêts clients surviennent au cours des arrêts du site principal (basculement planifié) et des workflows de personnalisation d'IP. Vous pouvez modifier ce paramètre dans le fichier <code>vmware-dr.xml</code> . La valeur srmMaxBootShutdownOps que vous pouvez définir dans vSphere Client remplace la valeur defaultMaxBootAndShutdownOpsPerCluster . Vous pouvez définir une valeur globale defaultMaxBootAndShutdownOpsPerCluster dans le fichier <code>vmware-dr.xml</code> , puis définir des valeurs srmMaxBootShutdownOps différentes pour chaque cluster individuel de vSphere Client. Par défaut, la limitation est désactivée.
defaultMaxBootAndShutdownOpsPerHost	Spécifie le nombre maximum de mises sous tension simultanées sur tout hôte autonome. Vous pouvez définir cette option dans le fichier <code>vmware-dr.xml</code> uniquement. Par défaut, la limitation est désactivée.

Tableau 9-2. Paramètres de modification des périodes d'expiration

Option	Description
<code>synchronizationTimeout</code>	Site Recovery Manager impose un délai d'expiration afin d'effectuer une synchronisation en ligne ou hors ligne des machines virtuelles répliquées par vSphere Replication lors d'un test ou d'un basculement. Si la synchronisation ne s'achève pas dans le délai d'expiration défini, du fait, par exemple, de la lenteur du réseau ou de la grande taille de la machine virtuelle, Site Recovery Manager signale un échec pendant le test ou le basculement. Modifiez cette option dans Paramètres avancés > vrReplication du plug-in client de Site Recovery Manager. La valeur par défaut est 7 200 et correspond à un délai d'expiration de synchronisation de 14 400 secondes.
<code>commandTimeout</code>	Le délai d'expiration pour l'exécution des commandes SRA est lié à ABR workflows. Dans certains cas, comme pour les LUN de surface et les snapshots, le temps de réponse de certaines baies est plus long que celui de la valeur par défaut. Modifiez cette option dans Paramètres avancés > stockage du plug-in client de Site Recovery Manager. La valeur par défaut est de 5 minutes.

Dépannage de Site Recovery Manager

10

En cas de difficultés lors de la création des groupes de protection et des plans de récupération, pendant la récupération ou la personnalisation client, vous pouvez résoudre le problème.

Lors de la recherche de l'origine d'un problème, vérifiez également la base de connaissances VMware à l'adresse <http://kb.vmware.com/>.

Limitations de la protection et de la récupération des machines virtuelles

La protection et la récupération des machines virtuelles par Site Recovery Manager sont soumises à des limitations.

Protection et récupération des machines virtuelles suspendues

Lorsque vous suspendez une machine virtuelle, vSphere crée et enregistre l'état de sa mémoire. Lorsque la machine virtuelle reprend, vSphere restaure l'état enregistré de la mémoire pour permettre à la machine virtuelle de continuer sans interrompre les applications et les systèmes d'exploitation clients qu'elle exécute.

Protection et récupération des machines virtuelles avec des snapshots

La réplication basée sur la baie prend en charge la protection et la récupération des machines virtuelles avec des snapshots, mais avec des limitations.

Vous pouvez définir un emplacement personnalisé pour stocker les fichiers delta de snapshot en définissant le paramètre `workingDir` dans les fichiers VMX. Site Recovery Manager ne permet pas d'utiliser le paramètre `workingDir`.

Les limitations s'appliquent également si vous utilisez des versions d'ESX ou ESXi Server antérieures à la version 4.1.

- Si la machine virtuelle dispose de plusieurs fichiers de disque VMDK, tous les fichiers de disque doivent se trouver dans le même dossier que le fichier VMX.

- Si une machine virtuelle est attachée à un périphérique de disque RDM (Raw Disk Mapping), vous devez stocker le fichier de mappage dans le même dossier que le fichier VMX. Les snapshots RDM sont disponibles uniquement si vous créez le mappage RDM en utilisant le mode de compatibilité virtuelle.

Si vous utilisez ESX ou ESXi Server 4.1 ou une version ultérieure, ces limitations ne s'appliquent pas.

vSphere Replication prend en charge la protection des machines virtuelles avec snapshots, mais vous ne pouvez récupérer que le dernier snapshot. vSphere Replication efface les données des snapshots de la machine virtuelle récupérée, ce qui signifie que les snapshots ne sont plus disponibles après la récupération.

Protection et récupération des machines virtuelles avec des snapshots d'état de mémoire

Lorsque vous protégez des machines virtuelles avec des snapshots d'état de mémoire, les hôtes ESXi des sites de protection et de récupération doivent disposer de CPU compatibles, comme indiqué dans les articles de la base de connaissances VMware [Conditions de compatibilité de CPU VMotion pour les processeurs Intel](#) et [Conditions de compatibilité de CPU VMotion pour les processeurs AMD](#). Les hôtes doivent également avoir les mêmes fonctions BIOS activées. Si les configurations BIOS des serveurs ne correspondent pas, elles affichent un message d'erreur de compatibilité, même si elles sont identiques. Les deux fonctions devant, le plus souvent, être contrôlées sont : la Protection mémoire des microprocesseurs (NX / XD) et la Technologie de virtualisation (VT / AMD-V).

Protection et récupération des machines virtuelles qui sont des clones liés

vSphere Replication ne prend pas en charge la protection et la récupération des machines virtuelles qui sont des clones liés.

La réplication basée sur la baie prend en charge la protection et la récupération des machines virtuelles qui sont des clones liés si tous les noeuds de l'arborescence de snapshot sont répliqués.

Protection et récupération des machines virtuelles avec réservations, règles d'affinité ou limites

Lorsque Site Recovery Manager récupère une machine virtuelle vers le site de récupération, il ne conserve pas les réservations, règles d'affinité ou limites auxquelles était soumise cette machine virtuelle. Site Recovery Manager ne conserve pas les réservations, règles d'affinité ou limites sur le site de récupération, car celui-ci peut avoir des exigences de ressources différentes de celles du site protégé.

Vous pouvez définir des réservations, règles d'affinité ou limites des machines virtuelles récupérées en configurant les réservations et les limites sur les pools de ressources du site de récupération et en paramétrant en conséquence le mappage de ces pools. Sinon, vous pouvez définir manuellement les réservations, règles d'affinité ou limites des machines virtuelles à espace réservé sur le site de récupération.

Protection et récupération des machines attachées aux périphériques de disques RDM

La protection et la récupération des machines virtuelles attachées à un périphérique de disque de mappage de disque brut (RDM) dépendent de divers supports, selon que vous utilisiez une réplication basée sur des baies ou vSphere Replication.

- La réplication basée sur des baies prend en charge les périphériques RDM en mode physique et en mode virtuel.
- vSphere Replication prend en charge des périphériques RDM en mode virtuel uniquement, pour les périphériques source et cible.

Migration planifiée des machines virtuelles sur des banques de données utilisant SIOC

Vous ne pouvez utiliser Site Recovery Manager pour effectuer une migration planifiée des machines virtuelles sur des banques de données ayant le contrôle d'E/S de stockage (SIOC) activée. Les banques de données activées par SIOC ne peuvent être démontées et, par conséquent, ne peuvent faire partie d'une migration planifiée. Vous devez désactiver SIOC de toutes les banques de données d'un plan de récupération avant d'effectuer une migration planifiée.

Récupération d'urgence et reprotection des machines virtuelles sur des banques de données utilisant SIOC

Si vous effectuez une récupération lorsque la commande SIOC est activée, cette récupération s'achèvera avec des erreurs. Après la récupération, vous devez désactiver manuellement SIOC sur le site protégé et exécuter de nouveau une récupération de la migration planifiée. Vous ne pouvez exécuter la fonction de reprotection qu'après avoir exécuté avec succès une migration planifiée.

Protection et récupération des machines virtuelles avec des composants sur plusieurs baies

La réplication basée sur les baies de Site Recovery Manager dépend du concept d'une paire de baies. Site Recovery Manager définit des groupes de banques de données, récupérées sous forme d'unités. Par conséquent, des limitations s'appliquent au mode de stockage des composants des machines virtuelles que vous protégez à l'aide d'une réplication basée sur des baies.

- Site Recovery Manager ne prend pas en charge le stockage des composants des machines virtuelles s'étendant sur plusieurs baies du site protégé qui effectue la réplication vers une seule baie du site de récupération.

- Site Recovery Manager ne prend pas en charge le stockage des composants des machines virtuelles s'étendant sur plusieurs baies du site protégé qui effectue la réplication vers plusieurs baies du site de récupération, si ces composants couvrent les deux baies.

Si vous répliquez les composants de la machine virtuelle depuis plusieurs baies vers une seule baie, ou vers une série de baies du site de récupération, les configurations VMX de l'UUID des banques de données du site protégé ne correspondront pas à celles du site de récupération.

L'emplacement du fichier VMX d'une machine virtuelle détermine la paire de baies à laquelle appartient une machine virtuelle. Une machine virtuelle ne peut appartenir à deux paires de baies ; ainsi, si elle dispose de plus d'un disque et si l'un de ces disques se trouve dans une baie ne faisant pas partie de la paire de baies à laquelle appartient la machine, Site Recovery Manager ne peut assurer la protection de la machine virtuelle entière. Site Recovery Manager considère alors comme périphérique non répliqué le disque ne faisant pas partie de la même paire de baies que la machine virtuelle.

En conséquence, stockez tous les disques virtuels, fichiers d'échange, périphériques RDM et le répertoire de travail de la machine virtuelle sur des LUN de la même baie, de sorte que Site Recovery Manager puisse protéger tous les composants de la machine virtuelle.

Protection et récupération des contrôleurs de domaine Active Directory

N'utilisez pas Site Recovery Manager pour protéger les contrôleurs de domaine Active Directory. Active Directory offre sa propre technologie de réplication et son propre mode de restauration. Utilisez la technologie de réplication Active Directory et celles relatives au mode de restauration pour gérer les situations de récupération d'urgence.

Utilisation de Site Recovery Manager avec des clusters de contrôle d'admission

Vous pouvez utiliser le contrôle d'admission sur un cluster pour réserver des ressources sur le site de récupération. Cependant, l'utilisation du contrôle d'admission peut compromettre la récupération d'urgence en empêchant Site Recovery Manager de mettre sous tension des machines virtuelles lors de l'exécution d'un plan de récupération. Le contrôle d'admission peut empêcher la mise sous tension de machines virtuelles si cette opération enfreint les contraintes pertinentes du contrôle d'admission.

Vous pouvez ajouter une étape de commande à un plan de récupération pour exécuter un script PowerCLI qui désactive le contrôle d'admission pendant la récupération. Pour plus d'informations sur la création d'étapes de commande, reportez-vous à [Créer des étapes de récupération personnalisées](#).

- 1 Créez une étape de commande antérieure à la mise sous tension dans le plan de récupération qui exécute un script PowerCLI pour désactiver le contrôle d'admission.

```
Get-Cluster cluster_name | Set-Cluster -HAA AdmissionControlEnabled:$false
```

- 2 Créez une étape de commande postérieure à la mise sous tension dans le plan de récupération pour réactiver le contrôle d'admission après la mise sous tension de la machine virtuelle.

```
Get-Cluster cluster_name | Set-Cluster -HAAmissionControlEnabled:$true
```

Si vous désactivez le contrôle d'admission pendant la récupération, vous devez manuellement le réactiver après l'exécution d'un nettoyage à la suite d'un test de récupération. La désactivation du contrôle d'admission peut compromettre la capacité de la fonction High Availability à redémarrer des machines virtuelles sur le site de récupération. Ne désactivez pas le contrôle d'admission pendant des périodes prolongées.

Limitations de vSphere Replication

vSphere Replication est soumis à certaines limitations lors de la réplication de machines virtuelles.

Réplication de grands volumes

vSphere Replication peut répliquer des machines virtuelles d'une capacité supérieure à 2 To avec les limitations suivantes :

- Si vous transférez une machine virtuelle disposant de disques répliqués de plus de 2 032 Go vers une machine sur une version plus ancienne, vSphere Replication ne peut ni répliquer ni mettre sous tension la machine virtuelle.
- La synchronisation complète de disques très volumineux peut prendre plusieurs jours.
- vSphere Replication doit suivre les blocs modifiés et consomme davantage de mémoire sur les disques volumineux.
- vSphere Replication suit les blocs plus volumineux sur des disques supérieurs à 2 To. Les performances de réplication sur un disque d'une capacité supérieure à 2 To peuvent être différentes sur un disque supérieur à 2 To pour la même charge de travail, en fonction de la part du disque qui transite par le réseau pour un ensemble particulier de blocs modifiés.
- La réplication peut utiliser plus ou moins de bande passante selon la charge de travail et le mode de modification des blocs sur le disque pendant l'intervalle RPO.

Prise en charge de disque partagé

vSphere Replication ne peut pas répliquer des machines virtuelles qui partagent des fichiers vmdk dans cette version.

Évènements et alarmes Site Recovery Manager

Site Recovery Manager prend en charge l'enregistrement d'évènements. Chaque évènement inclut une alarme correspondante que Site Recovery Manager peut déclencher lorsque l'évènement se produit. Ceci permet de surveiller la santé de votre système et de résoudre les problèmes potentiels avant qu'ils n'affectent la protection fournie par Site Recovery Manager.

Contrôle des connexions entre sites par Site Recovery Manager

Site Recovery Manager contrôle la connexion entre les sites protégés et de récupération. De même, il enregistre les événements lorsque le site distant cesse de répondre.

Lorsque Site Recovery Manager établit la connexion entre deux instances couplées du Serveur Site Recovery Manager, le Serveur Site Recovery Manager ayant initié la connexion envoie un `RemoteSiteUpEvent`.

Si Site Recovery Manager détecte qu'une connexion surveillée a été interrompue, il commence des vérifications périodiques de connexion en envoyant une requête `ping` au site distant. Site Recovery Manager surveille les vérifications de connexion et enregistre les événements dans le journal.

- Site Recovery Manager envoie des pings à intervalles réguliers. Vous pouvez configurer cet intervalle en paramétrant la valeur `remoteSiteStatus.pingInterval`. La valeur par défaut est de cinq minutes.
- Le moniteur de connexion saute un nombre de pings qui ont échoués. Vous pouvez configurer ce nombre en paramétrant la valeur `remoteSiteStatus.pingFailedDelay`.
- Lorsque le nombre de pings ignorés ayant échoué excède la valeur du paramètre `remoteSiteStatus.pingFailedDelay`, Site Recovery Manager envoie un événement `RemoteSitePingFailedEvent`.
- Lorsque le nombre de pings ignorés ayant échoué excède la limite supérieure, Site Recovery Manager envoie un événement `RemoteSiteDownEvent` pour chaque échec de test ping, puis cesse d'envoyer des événements `RemoteSitePingFailedEvent`. Vous pouvez configurer ce nombre maximal d'échecs de test ping en paramétrant le `remoteSiteStatus.panicDelay`.
- Site Recovery Manager continue d'envoyer des événements `RemoteSiteDownEvent` jusqu'à ce que la connexion soit rétablie.

Configurer les alarmes Site Recovery Manager

Site Recovery Manager ajoute des alarmes à celles que vCenter Server prend en charge. Vous pouvez configurer les alarmes Site Recovery Manager pour envoyer une notification par e-mail, envoyer une interruption SNMP ou exécuter un script sur l'hôte vCenter Server.

L'onglet **Alarmes** de l'interface Site Recovery Manager répertorie toutes les alarmes Site Recovery Manager. Vous pouvez modifier les paramètres de chaque alarme pour spécifier l'action à entreprendre par Site Recovery Manager lorsqu'un événement déclenche l'alarme. Par défaut, aucune des alarmes Site Recovery Manager ne s'active tant que vous ne l'avez pas configurée.

Conditions préalables

Pour que les alarmes envoient des notifications par e-mail, vous devez configurer les paramètres de **Messagerie** dans le menu **Paramètres de vCenter Server**.

Procédure

- 1 Dans le panneau de gauche, cliquez sur **Sites** et sélectionnez un site.
- 2 Cliquez sur l'onglet **Alarmes** pour afficher la liste des alarmes Site Recovery Manager.
- 3 Effectuez un clic droit sur une alerte et cliquez sur **Modifier les paramètres**.
- 4 Cliquez sur l'onglet **Actions**.
- 5 Cliquez sur **Ajouter** pour ajouter une action à accomplir lorsque cette alarme est déclenchée.
- 6 Sélectionnez une action dans la liste déroulante.

Option	Description
Envoyer un e-mail	L'action par défaut. Saisissez une adresse e-mail dans la zone de texte Valeur .
Envoyer une interruption SNMP	Site Recovery Manager envoie une interruption SNMP si un événement déclenche l'alarme.
Exécuter le script	Entrez le chemin vers le script à exécuter dans la zone de texte Valeur .

- 7 Cliquez sur l'onglet **Général**.
- 8 Sélectionnez la case à cocher **Activer cette alarme** pour activer l'action pour cette alarme.

Référence d'événements Site Recovery Manager

Site Recovery Manager surveille les différents types d'événements.

Événements de statut du site

Les événements d'état du site fournissent des informations sur la connexion entre le site protégé et le site de récupération, ainsi que sur leurs états respectifs.

Tableau 10-1. Événements de statut du site

Clé de l'événement	Description de l'événement	Cause
UnknownStatusEvent	Statut inconnu	L'état de Serveur Site Recovery Manager n'est pas disponible
RemoteSiteDownEvent	Site distant interrompu	Serveur Site Recovery Manager a perdu sa connexion avec l'instance distante de Serveur Site Recovery Manager.
RemoteSitePingFailedEvent	Échec du ping du site distant	Échecs au niveau du site distant ou problèmes de connectivité réseau.
RemoteSiteCreatedEvent	Site distant créé	Site distant créé.

Tableau 10-1. Événements de statut du site (suite)

Clé de l'événement	Description de l'événement	Cause
RemoteSiteUpEvent	Site distant prêt	Serveur Site Recovery Manager rétablit sa connexion avec l'instance distante de Serveur Site Recovery Manager.
RemoteSiteDeletedEvent	Site distant supprimé	Le site distant a été supprimé.

Événements de groupe de protection

Les événements de groupe de protection fournissent des informations sur les actions et l'état des groupes de protection.

Ces événements ont trois catégories :

- Événements d'information de réplication de groupe de protection
- Événements d'avertissement de réplication de groupe de protection
- Événements d'erreur de réplication de groupe de protection

Tableau 10-2. Événements d'information de réplication de groupe de protection

Clé de l'événement	Description de l'événement	Cause
ProtectionGroup > CreatedEvent	Groupe de protection créé.	Posté sur les deux serveurs vCenter dans l'achèvement de la phase de validation de la création d'un groupe de protection.
ProtectionGroup > RemovedEvent	Groupe de protection supprimé.	Posté sur les deux serveurs vCenter dans l'achèvement de la phase de validation de la suppression d'un groupe de protection.
ProtectionGroup > ReconfiguredEvent	Groupe de protection reconfiguré.	Posté sur les deux serveurs vCenter dans l'achèvement de la phase de validation de la reconfiguration d'un groupe de protection.
ProtectedVmCreatedEvent	Une machine virtuelle dans un groupe est configurée pour être protégée.	Posté sur les deux serveurs vCenter dans l'achèvement de la phase de validation de la protection d'une machine virtuelle.
ProtectedVmRemovedEvent	Une machine virtuelle dans un groupe n'est plus configurée pour être protégée.	Posté sur les deux serveurs vCenter dans l'achèvement de la phase de validation de la non-protection d'une machine virtuelle.
ProtectedVmReconfiguredProtectionSettingsEvent	Paramètres de protection reconfigurés pour machine virtuelle.	Posté sur les deux serveurs vCenter dans l'achèvement de la phase de validation de la reconfiguration des paramètres de protection de machine virtuelle.

Tableau 10-2. Événements d'information de réplication de groupe de protection (suite)

Clé de l'événement	Description de l'événement	Cause
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	Paramètres d'emplacement de récupération reconfigurés pour machine virtuelle.	Posté sur le site protégé vCenter Server uniquement lors de l'achèvement réussi de la reconfiguration des paramètres d'emplacement de récupération pour une machine virtuelle protégée.
PlaceholderVmCreatedEvent	La machine virtuelle à espace réservé a été créée dans l'inventaire VMware vCenter Server.	Posté sur le site de récupération vCenter Server seulement lorsque nous créons la machine virtuelle à espace réservé comme résultat d'une protection ou d'une réparation.
PlaceholderVmCreatedFromOldProductionVmEvent	La machine virtuelle à espace réservé a été créée dans l'inventaire VMware vCenter Server avec l'identité de l'ancienne machine virtuelle protégée.	Posté sur le site de récupération vCenter Server uniquement lorsque nous créons la machine virtuelle à espace réservé comme résultat de l'échange de l'ancienne machine virtuelle protégée pendant ou après la reprotction.

Tableau 10-3. Événements d'avertissement de réplication de groupe de protection

Clé de l'événement	Description de l'événement	Cause
VmNotFullyProtectedEvent	Machine virtuelle dans un groupe : un ou plusieurs dispositifs doivent être configurés pour la protection.	Posté sur le site protégé vCenter Server uniquement lors de la gestion de périphériques en cours de mise à jour des paramètres d'emplacement de récupération avec un ensemble unresolvedDevices non vide. Cela peut être déclenché par les modifications apportées à la machine virtuelle protégée ou pendant la reprotction d'une machine virtuelle.
PlaceholderVmUnexpectedlyDeletedEvent	Machine virtuelle dans un groupe : La machine virtuelle à espace réservé a été supprimée dans l'inventaire VMware vCenter Server.	Posté sur le site de récupération vCenter Server seulement lorsque nous détectons que la machine virtuelle à espace réservé a été supprimée ou retirée de l'inventaire vCenter de manière imprévue.

Tableau 10-4. Événements d'erreur de réplication de groupe de protection

Clé de l'événement	Description de l'événement	Cause
ProductionVmDeletedEvent	Machine virtuelle dans un groupe : La machine virtuelle protégée a été supprimée de l'inventaire vCenter Server de la machine virtuelle.	Posté lorsque nous détectons que la machine virtuelle protégée de la machine virtuelle protégée a été supprimée ou retirée de l'inventaire vCenter.
ProductionVmInvalidEvent	Machine virtuelle dans un groupe : Impossible de résoudre les emplacements de fichier de la machine virtuelle protégée pour réplication.	Posté à chaque fois que nous gérons les modifications d'emplacement de périphérique ou de récupération, mais remarquons que le fournisseur ne peut pas trouver les fichiers de la machine virtuelle protégée pour les répliquer.

Événements de récupération

Les événements de récupération fournissent des informations sur les actions et l'état des processus de récupération Site Recovery Manager.

Tableau 10-5. Événements de récupération

Événement	Description	Cause
RecoveryVmBegin	Le plan de récupération a commencé à récupérer la machine virtuelle spécifiée.	Signalé lorsque la machine virtuelle de récupération a été créée avec succès. Si des erreurs se produisent avant que l'ID de machine virtuelle ne soit connu, l'événement n'est pas déclenché.
RecoveryVmEnd	Le plan de récupération a terminé la récupération de la machine virtuelle.	Signalé à la fin du dernier script de post-mise sous tension ou après la survenue d'une erreur qui stoppe la récupération pour la machine virtuelle.
PlanCreated	Le plan de récupération <i>hostname</i> a été créé.	Signalé lorsqu'un plan est créé. Il est envoyé à chaque instance de vCenter Server sur laquelle le plan est hébergé.
PlanDestroy	Le plan de récupération a été détruit.	Signalé lorsqu'un plan a été supprimé du site. Notez que sur le site où le plan a été requis pour suppression, il peut y avoir un délai d'attente significatif pendant qu'il attend que le plan soit supprimé sur l'autre site. Il sera envoyé à chaque instance vCenter Server où le plan est hébergé.
PlanEdit	Le plan de récupération a été modifié.	Signalé lorsqu'un plan existant est modifié.

Tableau 10-5. Événements de récupération (suite)

Événement	Description	Cause
PlanExecTestBegin	Le plan de récupération a commencé un test.	Signalé sur un site de récupération lorsqu'un test de récupération est lancé.
PlanExecTestEnd	Le plan de récupération a terminé un test.	Signalé sur un site de récupération lorsqu'un test de récupération est terminé.
PlanExecCleanupBegin	Le plan de récupération a commencé un nettoyage test.	Signalé sur un site de récupération lorsqu'un nettoyage test est lancé.
PlanExecCleanupEnd	Le plan de récupération a terminé un nettoyage test.	Signalé sur le site de récupération lorsqu'un nettoyage test est terminé.
PlanExecBegin	Le plan de récupération a commencé une récupération.	Signalé sur un site de récupération lorsqu'une récupération est lancée.
PlanExecEnd	Le plan de récupération a terminé une récupération.	Signalé sur un site de récupération lorsqu'une récupération est terminée.
PlanExecReprotectBegin	Le plan de récupération a commencé une opération de reprotection.	Signalé sur le site de récupération lorsqu'une reprotection est lancée.
PlanExecReprotectEnd	Le plan de récupération a terminé une opération de reprotection.	Signalé sur le site de récupération lorsqu'une reprotection est terminée.
PlanPromptDisplay	Le plan de récupération affiche une invite et attend la saisie de l'utilisateur.	Signalé sur le site de récupération lorsqu'une étape d'invite a lieu. La clé est un identifiant unique pour l'invite.
PlanPromptResponse	Le plan de récupération a reçu une réponse à son invite.	Signalé sur le site de récupération lorsqu'une étape d'invite est fermée.
PlanServerCommandBegin	Le plan de récupération a démarré pour exécuter une commande sur la machine Serveur Site Recovery Manager.	Signalé sur le site de récupération lorsque Site Recovery Manager a commencé à exécuter une commande de légende sur la machine Serveur Site Recovery Manager.
PlanServerCommandEnd	Le plan de récupération a terminé l'exécution d'une commande sur la machine Serveur Site Recovery Manager.	Signalé sur le site de récupération lorsque Site Recovery Manager a terminé l'exécution d'une commande de légende sur la machine Serveur Site Recovery Manager.
PlanVmCommandBegin	Le Plan de récupération a commencé l'exécution d'une commande sur une machine virtuelle récupérée.	Signalé sur le site de récupération lorsque Site Recovery Manager a commencé à exécuter une commande de légende sur une machine virtuelle récupérée.
PlanVmCommandEnd	Le Plan de récupération a terminé l'exécution d'une commande sur une machine virtuelle récupérée.	Signalé sur le site de récupération lorsque Site Recovery Manager a terminé l'exécution d'une commande de légende sur une machine virtuelle récupérée.

Événements fournisseur de stockage et stockage

Les événements fournisseur de stockage et stockage présentent des informations sur les actions et les états concernant le stockage ou les fournisseurs de stockage.

Tableau 10-6. Événements de SRA

Événement	Description	Cause
<code>StorageAdaptLoadEvent</code>	A chargé le SRA spécifié.	Site Recovery Manager a détecté un nouvel adaptateur SRA durant le démarrage ou durant le rechargement des adaptateurs SRA lancé par l'utilisateur.
<code>StorageAdaptReloadFailEvent</code>	Échec de chargement du SRA depuis le chemin spécifié.	Site Recovery Manager n'a pas pu recharger l'adaptateur SRA connu précédemment durant le démarrage ou le rechargement des adaptateurs SRA lancé par l'utilisateur.
<code>StorageAdaptChangeEvent</code>	A chargé une nouvelle version du SRA spécifié.	Site Recovery Manager a détecté que l'adaptateur SRA connu précédemment a été mis à niveau.

Tableau 10-7. Événements du gestionnaire de baies

Événement	Description	Cause
<code>SAManagerAddedEvent</code>	A créé le gestionnaire de baies spécifié en utilisant le SRA spécifié.	L'utilisateur a ajouté un gestionnaire de baies.
<code>SAManagerRemovedEvent</code>	A supprimé le gestionnaire de baies spécifié.	L'utilisateur a supprimé un gestionnaire de baies.
<code>SAManagerReconfigEvent</code>	A reconfiguré le gestionnaire de baies spécifié.	L'utilisateur a modifié les propriétés du gestionnaire de baies.
<code>SAManagerPingOkEvent</code>	Envoi réussi d'un ping au gestionnaire de baies spécifié.	Serveur Site Recovery Manager a correctement envoyé un test Ping au gestionnaire de baies.
<code>SAManagerPingFailEvent</code>	Échec d'envoi d'un ping au gestionnaire de baies spécifié.	Une erreur s'est produite lors de l'envoi d'un ping au gestionnaire de baies.

Tableau 10-8. Événements de paire de baies

Événement	Description	Cause
<code>SAPairDiscoveredEvent</code>	A identifié une paire de baies répliquée avec le gestionnaire de baies.	L'utilisateur a créé un gestionnaire de baies qui a identifié des paires de baies répliquées.
<code>SAPairEnabledEvent</code>	A activé une paire de baies répliquées avec le gestionnaire de baies.	L'utilisateur a activé une paire de baies.
<code>SAPairDisabledEvent</code>	A désactivé une paire de baies répliquées avec le gestionnaire de baies.	L'utilisateur a désactivé une paire de baies.

Tableau 10-8. Événements de paire de baies (suite)

Événement	Description	Cause
SAPairPingOkEvent	Envoi réussi d'un ping à une paire de baies répliquées.	Serveur Site Recovery Manager a correctement envoyé un test Ping à la paire de baies.
SAPairPingFailEvent	Échec d'envoi d'un ping à la paire de baies répliquées.	Une erreur s'est produite lors de l'envoi d'un ping à une paire de baies.

Tableau 10-9. Événements de banque de données

Événement	Description	Cause
StorageDsDiscoveredEvent	A identifié une banque de données répliquée.	Serveur Site Recovery Manager a identifié une banque de données répliquée.
StorageDsLostEvent	La banque de données spécifiée n'est plus répliquée.	L'utilisateur a désactivé la réplication des périphériques de stockage assurant la sauvegarde de la banque de données.
StorageRdmDiscoveredEvent	A identifié des RDM répliqués joints à la machine virtuelle spécifiée.	Serveur Site Recovery Manager a identifié un mappage RDM répliqué. Cet élément est déclenché lorsque vous ajoutez un disque RDM à une machine virtuelle protégée.
StorageRdmLostEvent	Le RDM joint à la machine virtuelle spécifiée n'est plus répliqué.	L'utilisateur a désactivé la réplication du LUN assurant la sauvegarde du RDM.

Tableau 10-10. Événements de protection

Événement	Description	Cause
SPDsProtEvent	Banque de données protégée dans le groupe de protection spécifié.	L'utilisateur a inclus la banque de données dans un groupe de protection nouveau ou existant.
SPDsUnprotEvent	Banque de données spécifiée non protégée.	L'utilisateur a supprimé la banque de donnée du groupe de protection ou supprimé le groupe de protection qui contenait cette banque de données. Cet élément est déclenché lorsque vous déprotégez une banque de données en la retirant d'un groupe de protection ou en supprimant ce groupe de protection.
SPVmDiscoveredEvent	A identifié une machine virtuelle répliquée.	L'utilisateur a créé une machine virtuelle sur une banque de données répliquée.
SPVmLostEvent	La machine virtuelle spécifiée n'est plus répliquée.	L'utilisateur a migré la machine virtuelle hors de la banque de données répliquée.

Tableau 10-10. Événements de protection (suite)

Événement	Description	Cause
SPDsProtMissingEvent	La banque de données répliquée doit être incluse dans le groupe de protection spécifié mais est incluse dans un autre groupe de protection.	Ceci est augmenté si vous disposez d'une banque de données devant être fusionnée et qui n'est pas encore protégée. Lors de l'événement de conflit, la banque de données est déjà protégée.
SPDsProtConflictEvent	La banque de données répliquée doit être incluse dans le groupe de protection spécifié.	Ceci est augmenté si vous disposez d'une banque de données devant être fusionnée et qui n'est pas encore protégée. Lors de l'événement de conflit, la banque de données est déjà protégée.
SPDsReplicationLostEvent	La banque de données incluse dans un groupe de protection spécifié n'est plus répliquée.	L'utilisateur a désactivé la réplication pour les périphériques de sauvegarde de la banque de données.
SPGroupProtRestoredEvent	La protection a été restaurée pour le groupe de protection spécifié.	Les problèmes précédents (non vides) d'un groupe de protection sont effacés.
SPVmdsProtMissingEvent	La banque de données utilisée par la machine virtuelle doit être incluse dans le groupe de protection spécifié.	Si vous ajoutez une banque de données à une machine virtuelle qui est déjà protégée par un groupe de protection et que cette banque de données ne fait pas partie du groupe de protection en question, vous devez l'y ajouter.
SPVmdsProtConflictEvent	La banque de données utilisée par la machine virtuelle spécifiée doit être ajoutée au groupe de protection spécifié, mais est actuellement utilisée par un autre groupe de protection.	Si vous ajoutez une banque de données à une machine virtuelle qui est déjà protégée par un groupe de protection et que cette banque de données ne fait pas partie du groupe de protection en question, vous devez l'y ajouter.
SPVmdsReplicationLostEvent	La banque de données utilisée par la machine virtuelle spécifiée et incluse dans le groupe de protection spécifié n'est plus répliquée.	Voir la description.
SPVmProtRestoredEvent	La protection pour la machine virtuelle spécifiée dans le groupe de protection spécifié a été restaurée.	Les problèmes précédents (non vides) d'une machine virtuelle protégée sont effacés. L'événement ne sera pas envoyé lorsque des problèmes concernant la machine virtuelle non protégée sont effacés.

Tableau 10-10. Événements de protection (suite)

Événement	Description	Cause
SPCgSpansProtGroupsEvent	Le groupe de cohérence spécifié couvre les groupes de protection spécifiés.	Cet élément est déclenché lorsque vous protégez deux banques de données par des groupes de protection distincts, mais les fusionnez plus tard dans un seul groupe de cohérence de la baie.
SPCgDsMissingProtEvent	La banque de données provenant du groupe de cohérence spécifié doit être incluse dans le groupe de protection spécifié.	Voir la description.
SPDsSpansConsistGroupsEvent	La banque de données couvre des périphériques provenant de différents groupes de cohérence.	Cet élément est déclenché lorsque vous placez une banque de données au-dessus de plusieurs LUN, sans que ces LUN n'appartiennent pour autant au même groupe de cohérence.
SPNfsDsUrlConflictEvent	Les banques de données NFS montées à partir d'un volume spécifié ont des URL différentes montées depuis l'hôte distant. Le chemin distant présente l'URL spécifiée, alors que la banque de données montée depuis l'autre hôte présente l'URL spécifiée.	Le même volume NFS est monté en utilisant les différentes adresses IP du même serveur NFS dans deux différentes banques de données.

Événements de licence

Les événements de licence fournissent des informations sur les modifications des statuts de licence Site Recovery Manager.

Tableau 10-11. Événements de licence

Type	Description	Contenu
LicenseExpiringEvent	La licence Site Recovery Manager sur le site spécifié expire dans le délai (en jours) indiqué.	Toutes les 24 heures, le nombre de jours restant pour les licences qui ne sont pas des licences d'évaluation et arrivant à expiration est vérifié. Cet événement est posté avec les résultats.
EvaluationLicenseExpiringEvent	La licence d'évaluation Site Recovery Manager sur le site spécifié expire dans le délai (en jours) indiqué.	Toutes les 24 heures, le nombre de jours restant pour les licences d'évaluation est vérifié. Cet événement est posté avec les résultats.
LicenseExpiredEvent	La licence Site Recovery Manager de la licence de site spécifiée a expiré.	Toutes les 30 minutes, cet événement sera posté pour les licences expirées (licences qui ne sont pas des licences d'évaluation).

Tableau 10-11. Événements de licence (suite)

Type	Description	Contenu
EvaluationLicenseExpiredEvent	La licence d'évaluation Site Recovery Manager de la licence de site spécifiée a expiré.	Toutes les 30 minutes, cet événement sera posté pour les licences d'évaluation.
UnlicensedFeatureEvent	La licence Site Recovery Manager sur le site spécifié est surattribuée par le nombre spécifié de licences.	Toutes les 24 heures et en fonction de la protection ou de la non-protection d'une machine virtuelle, cet événement sera posté si le nombre total de licences dépasse la capacité de la licence.
LicenseUsageChangedEvent	La licence Site Recovery Manager sur le site spécifié utilise le nombre indiqué sur le nombre total de licences.	Toutes les 24 heures et en fonction de la protection ou de la non-protection d'une machine virtuelle, cet événement sera posté si le nombre total de licences ne dépasse pas la capacité de la licence.

Événements d'autorisations

Les événements d'autorisations fournissent des informations sur les modifications apportées aux autorisations Site Recovery Manager.

Tableau 10-12. Événements d'autorisations

Type	Description	Contenu
PermissionsAddedEvent	Autorisation créée pour l'entité dans Site Recovery Manager.	Une autorisation pour l'entité a été créée à l'aide du rôle spécifié. L'indicateur <code>IsPropagate</code> indique si l'autorisation est propagée dans la hiérarchie de l'entité.
PermissionsDeletedEvent	Règle d'autorisation supprimée pour l'entité dans Site Recovery Manager.	L'autorisation pour l'entité a été supprimée.
PermissionsUpdatedEvent	Autorisation modifiée pour l'entité dans Site Recovery Manager.	L'autorisation pour l'entité indiquée a été modifiée.

Interruptions SNMP

Site Recovery Manager envoie des interruptions SNMP aux cibles de communauté définies dans vCenter Server. Vous pouvez les configurer avec Client Web vSphere. Lorsque vous entrez localhost ou 127.0.0.1 comme hôte cible pour les interruptions SNMP, Site Recovery Manager utilise l'adresse IP ou le nom d'hôte de vSphere Server conformément à la configuration du programme d'installation de Site Recovery Manager.

Les interruptions SNMP pour Site Recovery Manager 5.x sont rétrocompatibles avec Site Recovery Manager 4.0 et versions ultérieures.

Tableau 10-13. Interruptions SNMP

Événement	Description	Cause
RecoveryPlanExecuteTestBeginTrap	Cette interruption est envoyée lorsqu'un plan de récupération démarre un test.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution.
RecoveryPlanExecuteTestEndTrap	Cette interruption est envoyée lorsqu'un plan de récupération termine un test.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, statut du résultat.
RecoveryPlanExecuteCleanupBeginTrap	Cette interruption est envoyée lorsqu'un plan de récupération démarre un nettoyage test.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution.
RecoveryPlanExecuteCleanupEndTrap	Cette interruption est envoyée lorsqu'un plan de récupération termine un nettoyage test.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, statut du résultat.
RecoveryPlanExecuteBeginTrap	Cette interruption est envoyée lorsqu'un plan de récupération démarre une récupération.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution.
RecoveryPlanExecuteEndTrap	Cette interruption est envoyée lorsqu'un plan de récupération termine une récupération.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, statut du résultat.
RecoveryPlanExecuteReprotectBeginTrap	Cette interruption est envoyée lorsque Site Recovery Manager démarre le workflow de reprotection pour un plan de récupération.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution.
RecoveryPlanExecuteReprotectEndTrap	Cette interruption est envoyée lorsque Site Recovery Manager a terminé le workflow de reprotection pour un plan de récupération.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, statut du résultat.
RecoveryVmBeginTrap	Cette interruption est envoyée lorsqu'un plan de récupération démarre la récupération d'une machine virtuelle.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la machine virtuelle, UUID de la machine virtuelle.
RecoveryVmEndTrap	Cette interruption est envoyée lorsqu'un plan de récupération a terminé la récupération d'une machine virtuelle.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la machine virtuelle, UUID de la machine virtuelle, statut du résultat.
RecoveryPlanServerCommandBeginTrap	Cette interruption est envoyée lorsqu'un plan de récupération démarre l'exécution d'un appel de commande sur une machine Serveur Site Recovery Manager.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la commande.

Tableau 10-13. Interruptions SNMP (suite)

Événement	Description	Cause
RecoveryPlanServerCommandEndTrap	Cette interruption est envoyée lorsqu'un plan de récupération a terminé l'exécution d'un appel de commande sur une machine Serveur Site Recovery Manager.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la commande, statut du résultat.
RecoveryPlanVmCommandBeginTrap	Cette interruption est envoyée lorsqu'un plan de récupération démarre l'exécution d'un appel de commande sur une machine virtuelle récupérée.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la commande, nom de la machine virtuelle, UUID de la machine virtuelle.
RecoveryPlanVmCommandEndTrap	Cette interruption est envoyée lorsqu'un plan de récupération a terminé l'exécution d'un appel de commande sur une machine virtuelle récupérée.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la commande, nom de la machine virtuelle, UUID de la machine virtuelle, statut du résultat.
RecoveryPlanPromptDisplayTrap	Cette interruption est envoyée lorsqu'un plan de récupération nécessite des informations de l'utilisateur pour continuer.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, chaîne d'invite.
RecoveryPlanPromptResponseTrap	Cette interruption est envoyée lorsqu'un plan de récupération ne nécessite plus d'informations de l'utilisateur pour continuer.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération et état d'exécution.

Événements et alarmes de vSphere Replication

vSphere Replication prend en charge l'enregistrement d'événements. Vous pouvez définir des alarmes en cas de déclenchement d'un événement lorsque celui-ci se produit. Cette fonction permet de surveiller l'intégrité du système et de résoudre les problèmes potentiels, garantissant ainsi la fiabilité de la réplication de machines virtuelles.

Configurer des alarmes vSphere Replication

Vous pouvez définir et modifier des alarmes pour vous alerter lorsqu'un événement vSphere Replication spécifique se produit.

Vous pouvez créer une alarme qui se déclenche quand un événement spécifique se produit, par exemple après avoir configuré une machine virtuelle pour la réplication. Reportez-vous à *Afficher et éditer les paramètres d'alarme dans vSphere Web Client* dans la documentation de Client Web vSphere.

Liste des événements de vSphere Replication

vSphere Replication surveille les réplications et l'infrastructure de réplication sous-jacente, et génère différents types d'événements.

Tableau 10-14. Événements de vSphere Replication

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie	Événement cible
vSphere Replication configurée	La machine virtuelle est configurée pour vSphere Replication	com.vmware.vcHms.replicationConfiguredEvent	Infos	Machine virtuelle
vSphere Replication non configurée	La configuration d'une machine virtuelle pour vSphere Replication a été annulée	com.vmware.vcHms.replicationUnconfiguredEvent	Infos	Machine virtuelle
Hôte configuré pour vSphere Replication	L'hôte est configuré pour vSphere Replication	com.vmware.vcHms.hostConfiguredForHbrEvent	Infos	Système hôte
Configuration de l'hôte annulée pour vSphere Replication	La configuration de l'hôte ayant l'ID d'objet <Host Moid> a été annulée pour vSphere Replication	com.vmware.vcHms.hostUnconfiguredForHbrEvent	Infos	Dossier
La machine virtuelle n'est pas configurée pour vSphere Replication	La machine virtuelle rencontre des problèmes avec vSphere Replication et doit être reconfigurée	com.vmware.vcHms.vmMissingReplicationConfigurationEvent	Erreur	Machine virtuelle
VM nettoyée à partir de vSphere Replication	La machine virtuelle a été nettoyée de la configuration de vSphere Replication	com.vmware.vcHms.vmReplicationConfigurationRemovedEvent	Infos	Machine virtuelle
RPO violé	L'objectif de point de récupération (RPO) de vSphere Replication pour la machine virtuelle n'est pas respecté de <x> minutes	com.vmware.vcHms.rpoViolatedEvent	Erreur	Machine virtuelle
RPO restauré	L'objectif de point de récupération (RPO) de vSphere Replication pour la machine virtuelle est maintenant respecté	com.vmware.vcHms.rpoRestoredEvent	Infos	Machine virtuelle
Le site vSphere Replication distant est déconnecté	La connexion au site vSphere Replication distant <siteName> est arrêtée	com.vmware.vcHms.remoteSiteDownEvent	Erreur	Dossier

Tableau 10-14. Événements de vSphere Replication (suite)

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie	Événement cible
Le site vSphere Replication distant est connecté	La connexion au site vSphere Replication distant <siteName> est établie	com.vmware.vcHms.remoteSiteUpEvent	Infos	Dossier
Serveur VR déconnecté	Le serveur vSphere Replication <VR Server> est déconnecté	com.vmware.vcHms.hbrDisconnectedEvent	Infos	Dossier
Serveur VR reconnecté	Le serveur vSphere Replication <VR Server> est reconnecté	com.vmware.vcHms.hbrReconnectedEvent	Infos	Dossier
Nettoyage de vSphere Replication non valide	La machine virtuelle <VM name> a été retirée de vCenter Server et son état vSphere Replication a été nettoyé	com.vmware.vcHms.replicationCleanedUpEvent	Infos	Dossier
Machine virtuelle récupérée à partir d'une réplique	La machine virtuelle <VM Name> a été récupérée à partir de l'image de vSphere Replication	com.vmware.vcHms.vmRecoveredEvent	Infos	Machine virtuelle
vSphere Replication ne peut pas accéder à la banque de données	La banque de données n'est pas accessible au serveur vSphere Replication	com.vmware.vcHms.datastoreInaccessibleEvent	Erreur	Banque de données
vSphere Replication a géré l'ajout de disques sur une machine virtuelle	vSphere Replication a détecté et traité l'ajout d'un disque à la machine virtuelle <VM name>. Les disques ajoutés sont <Disk name>	com.vmware.vcHms.handledVmDiskAddEvent	Infos	Machine virtuelle
vSphere Replication a traité le retrait d'un disque sur une machine virtuelle	vSphere Replication a détecté et traité l'ajout d'un disque à la machine virtuelle <VM name>. Les disques ajoutés sont <Disk name>	com.vmware.vcHms.handledVmDiskRemoveEvent	Infos	Machine virtuelle

Tableau 10-14. Événements de vSphere Replication (suite)

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie	Événement cible
Impossible de résoudre la règle de stockage	Impossible de résoudre une stratégie de stockage spécifique pour l'ID de profil de stockage <profile ID> fourni et la banque de données ayant l'ID d'objet géré <Moid>	com.vmware.vcHms.failedResolvingStoragePolicyEvent	Erreur	Banque de données
vSphere Replication suspendu	vSphere Replication a été suspendu suite à un changement de configuration, tel que l'ajout d'un disque ou la restauration d'un snapshot dans lequel les états des disques sont différents	hbr.primary.SystemPausedReplication	Erreur	Machine virtuelle
Configuration vSphere Replication non valide	Configuration vSphere Replication non valide	hbr.primary.InvalidVmReplicationConfigurationEvent	Erreur	Machine virtuelle
La synchronisation a démarré	La synchronisation a démarré	hbr.primary.DeltaStartedEvent	Infos	Machine virtuelle
La synchronisation cohérente d'application est terminée	La synchronisation cohérente d'application est terminée	hbr.primary.AppQuiescedDeltaCompletedEvent	Infos	Machine virtuelle
La synchronisation cohérente de système de fichiers est terminée	La synchronisation cohérente de système de fichiers est terminée	hbr.primary.FSQuiescedDeltaCompletedEvent	Avertissement	Machine virtuelle
La synchronisation cohérente de défaillance non mise au repos est terminée	La synchronisation cohérente de défaillance non mise au repos est terminée. La mise au repos a échoué ou la machine virtuelle est hors tension.	hbr.primary.UnquiescedDeltaCompletedEvent	Avertissement	Machine virtuelle
La synchronisation cohérente de défaillance est terminée	La synchronisation cohérente de défaillance est terminée	hbr.primary.DeltaCompletedEvent	Infos	Machine virtuelle

Tableau 10-14. Événements de vSphere Replication (suite)

Nom de l'événement	Description de l'événement	Type d'événement	Catégorie	Événement cible
La synchronisation n'a pas réussi à démarrer	La synchronisation n'a pas réussi à démarrer	hbr.primary.FailedToStartDeltaEvent	Erreur	Machine virtuelle
Synchronisation complète démarrée	Synchronisation complète démarrée	hbr.primary.SyncStartedEvent	Infos	Machine virtuelle
Synchronisation complète terminée	Synchronisation complète terminée	hbr.primary.SyncCompletedEvent	Infos	Machine virtuelle
La synchronisation complète n'a pas réussi à démarrer	La synchronisation complète n'a pas réussi à démarrer	hbr.primary.FailedToStartSyncEvent	Erreur	Machine virtuelle
La synchronisation a échoué	La synchronisation a échoué	hbr.primary.DeltaAbortedEvent	Avertissement	Machine virtuelle
Aucune connexion au serveur VR	Aucune connexion au serveur vSphere Replication	hbr.primary.NoConnectionToHbrServerEvent	Avertissement	Machine virtuelle
Connexion au serveur VR restaurée	La connexion au serveur VR a été restaurée	hbr.primary.ConnectionRestoredToHbrServerEvent	Infos	Machine virtuelle
Configuration vSphere Replication modifiée	La configuration de vSphere Replication a été modifiée	hbr.primary.VmReplicationConfigurationChangedEvent	Infos	Machine virtuelle

Recueillir les fichiers de journalisation Site Recovery Manager

Site Recovery Manager crée plusieurs fichiers de journalisation contenant des informations susceptibles d'aider le support VMware à diagnostiquer des problèmes. Vous pouvez utiliser le collecteur de journaux Site Recovery Manager pour simplifier la collecte des fichiers de journalisation.

Le Serveur Site Recovery Manager et le client utilisent des fichiers de journalisation différents. Les fichiers de journalisation du Serveur Site Recovery Manager contiennent des informations concernant la configuration du serveur, ainsi que des messages en rapport avec les opérations du serveur. Les fichiers de journalisation de client Site Recovery Manager contiennent des informations concernant la configuration du client, ainsi que des messages en rapport avec les opérations du plug-in client. Le fichier de journalisation Site Recovery Manager recueille ou récupère les fichiers et les compresse dans un fichier zippé qui est placé à l'emplacement de votre choix.

Site Recovery Manager prévoit également la collecte des fichiers de journalisation de la vSphere Replication comme partie intégrante de l'ensemble des journaux Site Recovery Manager. Les fichiers de journalisation issus des instances de vCenter Server et des instances serveur ESXi qui font partie de votre système Site Recovery Manager peuvent également contenir des informations utiles au diagnostic des problèmes concernant Site Recovery Manager.

- [Recueillir les fichiers journaux de Site Recovery Manager en utilisant l'interface de Site Recovery Manager](#)

Vous pouvez télécharger les journaux de Site Recovery Manager, le dispositif vSphere Replication et les serveurs vSphere Replication dans un emplacement spécifié par l'utilisateur.

- [Recueillir manuellement les fichiers journaux Site Recovery Manager](#)

Vous pouvez télécharger les fichiers journaux du Serveur Site Recovery Manager dans un ensemble de journaux généré manuellement. Ceci s'avère utile lorsqu'il vous est impossible d'accéder à vSphere Client.

Recueillir les fichiers journaux de Site Recovery Manager en utilisant l'interface de Site Recovery Manager

Vous pouvez télécharger les journaux de Site Recovery Manager, le dispositif vSphere Replication et les serveurs vSphere Replication dans un emplacement spécifié par l'utilisateur.

Utilisez ces informations pour comprendre et résoudre les problèmes. Pour de meilleurs résultats, recueillez les journaux à partir de chaque site.

Procédure

- 1 Cliquez sur **Sites** et sélectionnez un site.
- 2 Cliquez sur l'onglet **Résumé**, puis sur **Exporter les journaux système**.
- 3 Dans la zone de texte **Emplacement de téléchargement**, entrez un chemin ou cliquez sur **Parcourir** pour rechercher un emplacement.
- 4 (Facultatif) Décochez la case **Inclure les journaux système VR** pour désactiver le téléchargement des données des journaux de vSphere Replication.

Les journaux système de vSphere Replication sont téléchargés par défaut. Ces journaux contiennent des informations sur le serveur de gestion de vSphere Replication, le serveur vSphere Replication et les événements de réplication.

- 5 Cliquez sur **OK** pour télécharger les journaux.

Résultats

La fenêtre **Téléchargement des bundles de journaux système** fournit des informations sur les bundles de journaux.

- Une liste de chaque système hôte, le statut de téléchargement de leur bundle de journaux, ainsi que d'autres détails.

- La fonction Détails du téléchargement fournit des informations sur le nom de fichier du bundle de journaux, ainsi que sur sa destination.

Ce processus ne recueille pas les journaux client. Vous devez recueillir les journaux client séparément.

Recueillir manuellement les fichiers journaux Site Recovery Manager

Vous pouvez télécharger les fichiers journaux du Serveur Site Recovery Manager dans un ensemble de journaux généré manuellement. Ceci s'avère utile lorsqu'il vous est impossible d'accéder à vSphere Client.

L'ensemble de journaux que ces procédures génèrent est identique aux journaux que vous générez à l'aide de vSphere Client.

Procédure

- ◆ Initiez la collecte de fichiers journaux du Serveur Site Recovery Manager à partir du menu **Démarrer** :
 - Ouvrez une session sur l'hôte du Serveur Site Recovery Manager.
 - Sélectionnez **Démarrer > Programmes > VMware > VMware Site Recovery Manager > Générer un bundle de journaux vCenter Site Recovery Manager**.
- ◆ Initiez la collecte des fichiers de journalisation du Serveur Site Recovery Manager à partir de la ligne de commande Windows :
 - Démarrez un shell de commande Windows sur l'hôte de Serveur Site Recovery Manager.
 - Modifiez le répertoire en `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
 - Exécutez la commande suivante.

```
cscript srm-support.wsf
```

Résultats

Les fichiers de journalisation individuels sont recueillis dans un fichier nommé `srm-support-MM-JJ-AAAA-HH-MM.zip`, où `MM-JJ-AAAA-HH-MM` indique le mois, le jour, l'année, l'heure et la minute auxquels les fichiers de journalisation ont été créés.

Modifier la taille et le nombre des fichiers journaux de Serveur Site Recovery Manager

Vous pouvez modifier la taille, le nombre et l'emplacement des fichiers journaux de Serveur Site Recovery Manager.

Vous pouvez modifier les paramètres de journalisation de Site Recovery Manager dans le fichier de configuration `vmware-dr.xml` sur Serveur Site Recovery Manager.

Procédure

- 1 Connectez-vous à l'hôte du Serveur Site Recovery Manager.

- 2 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.

Le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config`.

- 3 Trouvez la section `<log>` dans le fichier `vmware-dr.xml`.
- 4 Définissez la taille maximale (en octets) des journaux à conserver.

Vous pouvez définir la taille maximale du journal en ajoutant une section `<maxFileSize>` à la section `<log>`. La valeur par défaut est 5242880 octets.

```
<log>

    <maxFileSize>5242880</maxFileSize>

</log>
```

- 5 Définissez le nombre maximal de fichiers journaux à conserver.

Vous définissez le nombre maximal de journaux en ajoutant une section `<maxFileNum>` à la section `<log>`. Le nombre par défaut de fichiers journaux est 10.

```
<log>

    <maxFileNum>50</maxFileNum>

</log>
```

- 6 Modifiez l'emplacement de stockage des journaux sur Serveur Site Recovery Manager.

Vous pouvez changer l'emplacement du journal en modifiant la section `<directory>` dans la section `<log>`.

```
<log>

    <directory>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\Logs</directory>

</log>
```

7 Modifier le préfixe par défaut pour les fichiers journaux.

Vous pouvez changer le préfixe par défaut en modifiant la section `<name>` dans la section `<log>`.

```
<log>

  <name>vmware-dr</name>

</log>
```

8 Modifier le niveau de journalisation.

Vous pouvez changer le niveau de journalisation en modifiant la section `<level>` dans la section `<log>`. Les niveaux de journalisation possibles sont erreur, avertissement, info, futile et prolix.

```
<log>

  <level>verbose</level>

</log>
```

9 Modifiez l'emplacement de stockage des vidages mémoire sur Serveur Site Recovery Manager.

Vous pouvez changer l'emplacement du vidage de mémoire en modifiant la section `<coreDump>` dans la section `<log>`.

```
<log>

  <coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\DumpFiles</coreDump>

</log>
```

10 (Facultatif) Définissez le niveau de journalisation pour les composants spécifiques du Serveur Site Recovery Manager.

Vous pouvez définir des niveaux de journalisation spécifiques pour les composants SoapAdapter, SanConfigManager, Recovery, Folders, Libs et HttpConnectionPool en modifiant les sections `<level>` appropriées. Les niveaux de journalisation possibles sont erreur, avertissement, info, futile et prolix.

```
<level id="Recovery">
  <logName>Recovery</logName>
  <logLevel>trivia</logLevel>
</level>
```

- 11 (Facultatif) Définissez le niveau de journalisation pour les adaptateurs de réplication de stockage.

La définition du niveau de journalisation de Site Recovery Manager ne définit pas le niveau de journalisation des SRA. Vous pouvez modifier le niveau de journalisation SRA en ajoutant une section `<level id="SraCommand">` à `vmware-dr.xml`, afin de définir le niveau de journalisation SRA. Les niveaux de journalisation possibles sont erreur, avertissement, info, futile et prolix.

```
<level id="SraCommand">
  <logName>SraCommand</logName>
  <logLevel>trivia</logLevel>
</level>
```

- 12 Redémarrez le service Serveur Site Recovery Manager pour appliquer les modifications.

Accéder aux journaux de vSphere Replication

Vous pouvez utiliser les journaux vSphere Replication pour surveiller et dépanner le système. Un technicien du support VMware peut demander ces journaux lors d'un appel d'assistance technique.

Pour accéder aux journaux vSphere Replication et les télécharger, vous devez accéder à l'interface de gestion du dispositif virtuel (VAMI) de vSphere Replication. vSphere Replication effectue une rotation de ses journaux lorsque les fichiers journaux atteignent 50 Mo et conserve tout au plus 12 fichiers journaux compressés.

Pour copier manuellement les fichiers journaux, voir [Accéder manuellement aux journaux vSphere Replication](#).

Conditions préalables

- Vérifiez que le dispositif vSphere Replication est hors tension.

Procédure

- 1 Connectez-vous au VAMI du dispositif vSphere Replication dans un navigateur Web.

L'URL de l'interface VAMI est `https://vr-appliance-address:5480`.

Vous pouvez également accéder à l'interface VAMI en cliquant sur **Configurer le dispositif VR** dans l'onglet **Résumé** de la vue vSphere Replication de l'interface de Site Recovery Manager.

- 2 Cliquez sur l'onglet **VRM** et sur **Support**.
- 3 Cliquez sur **Générer** pour générer un package .zip des journaux vSphere Replication en cours.

Un lien d'accès au package contenant les journaux de réplication et système s'affiche. Les fichiers journaux du dispositif vSphere Replication et de tous les serveurs vSphere Replication supplémentaires connectés sont inclus dans le même module.

- 4 Cliquez sur le lien pour télécharger le package.

- 5 (Facultatif) Cliquez sur **Supprimer** à côté des packages existants pour supprimer les packages individuellement.

Accéder manuellement aux journaux vSphere Replication

Vous pouvez copier et utiliser les journaux vSphere Replication pour surveiller et dépanner le système. Un technicien du support VMware peut demander ces journaux lors d'un appel d'assistance technique.

Utilisez SCP ou Win SCP pour copier les dossiers et les fichiers des journaux du dispositif vSphere Replication et de tous les serveurs vSphere Replication supplémentaires.

- /opt/vmware/hms/logs/
- /opt/vmware/var/log/lighttpd/
- /var/log/vmware/
- /var/log/boot.msg

Résoudre les problèmes de fonctionnement de Site Recovery Manager

Si vous rencontrez des problèmes lors de la création des groupes de protection et des plans de récupération, pendant le basculement, la récupération ou la personnalisation client, vous pouvez résoudre ce problème.

Site Recovery Manager double le nombre de barres obliques inverses contenues dans la ligne de commande pendant l'exécution des légendes

Lorsqu'une barre oblique inverse fait partie d'une ligne de commande de légende, Site Recovery Manager double toutes les barres obliques inverses.

Problème

L'interprète du système de ligne de commande traite les doubles barres obliques inverses comme barres obliques inverses simples uniquement dans les chemins de fichiers. Si la commande de légende requiert une barre oblique inverse dans un paramètre autre qu'un chemin de fichier et que ladite commande ne convertit pas les doubles barres obliques inverses en une barre oblique inverse simple, la commande de légende concernée peut échouer avec une erreur.

Par exemple, vous pouvez ajouter une étape de légende au workflow et entrer le texte suivant comme commande :

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \d\e\f \\g\h c:\myscript.log
```

Il résulte de l'étape de légende que Site Recovery Manager exécutera la commande ci-après :

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \d\e\f \\\g\\\h c:\
myscript.log
```

Si `myscript.cmd` ne change pas la double barre oblique inverse en barre oblique inverse simple et que les paramètres `\d\e\f` et `\\g\\h` sont sensibles au nombre de barres obliques inverses, la commande `myscript.cmd` peut échouer.

Solution

- 1 Créez un fichier de commandes supplémentaire pour la ligne de commande, afin d'y stocker les commandes et tous les paramètres requis. L'étape de légende exécute ce fichier de commandes supplémentaire sans argument. Pour cet exemple, la solution est la suivante :
 - a Dans un éditeur de texte comme le Bloc-notes, créez un fichier `c:\SRM_callout.cmd` ayant le contenu suivant : `C:\myscript.cmd a/b/c \d\e\f \\\g\\\h c:\myscript.log`
 - b Dans une étape de légende du plan de récupération, entrez la commande pour exécuter : `c:\Windows\system32\cmd.exe /C c:\SRM_callout.cmd`
- 2 Ajoutez un code au fichier de script d'origine qui remplace les doubles barres obliques inverses en barre oblique inverse simple.
 - a Ajoutez un code similaire à l'échantillon suivant, au début du fichier de script `c:\myscript.cmd`.

```
@echo off
set arg2=%2
set arg3=%3
set fixed_arg2=%arg2:\=\%
set fixed_arg3=%arg3:\=\%
```

Si vous utilisez la commande `shift` dans un script, tous les paramètres sensibles aux barres obliques inverses seront gérés de cette manière.

- b Si vous n'utilisez pas de commande `shift` dans un script, effectuez les modifications suivantes :

Remplacez `%2` par `%fixed_arg2%`.

Remplacez `%3` par `%fixed_arg3%`.
- c Ne changez pas la commande de l'étape de légende.

La mise sous tension simultanée de nombreuses machines virtuelles sur le site de récupération peut entraîner des erreurs

Lorsque de nombreuses machines virtuelles effectuent des opérations de démarrage en même temps, des erreurs peuvent survenir au cours de la récupération basée sur des baies et celle de vSphere Replication.

Problème

Lorsque vous mettez simultanément sous tension un grand nombre de machines virtuelles du site de récupération, il peut arriver que vous rencontriez ces erreurs dans les rapports de l'historique de récupération :

- La commande 'écho « Début de la personnalisation d'IP sous Windows ... » >
> % VMware_GuestOp_OutputFile%.
- Impossible de terminer la personnalisation, probablement du fait d'une erreur d'exécution de script ou de paramètres de script non valides.
- Une erreur est survenue lors du téléchargement des fichiers sur la VM cliente.
- Dépassement du délai d'attente de VMware Tools au bout de 600 secondes.

Cause

Par défaut, Site Recovery Manager ne limite pas le nombre d'opérations de mise sous tension que l'on peut effectuer simultanément. Si vous détectez des erreurs pendant la mise sous tension des machines virtuelles sur le site de récupération, vous pouvez modifier le fichier `vmware-dr.xml` afin de fixer la limite du nombre de machines virtuelles que l'on peut mettre sous tension simultanément.

Si vous détectez ces erreurs, limitez le nombre d'opérations de mise sous tension permis sur le site de récupération en fonction de la capacité de votre environnement pour un hôte autonome ou un cluster.

Solution

- 1 Sur le serveur de récupération, accédez à `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config`.
- 2 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.
- 3 Mettez à jour les valeurs `defaultMaxBootAndShutdownOpsPerCluster` et `defaultMaxBootAndShutdownOpsPerHost` afin de limiter le nombre d'opérations de mise sous tension sur le site de récupération.

L'exemple suivant montre comment fixer le nombre maximal d'opérations de mise sous tension à 32 par cluster et 4 par hôte autonome.

```
<config>
  <defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
  <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
</config>
```

- 4 Redémarrez le service Site Recovery Manager Server.

Le paramètre `LVM.enableResignature=1` est conservé après un basculement test Site Recovery Manager

Site Recovery Manager ne prend pas en charge les environnements ESXi dans lesquels l'indicateur `LVM.enableResignature` est fixé à 0.

Problème

Pendant un basculement test ou un basculement réel, Site Recovery Manager définit `LVM.enableResignature` sur 1 si l'indicateur n'est pas encore fixé. Site Recovery Manager définit l'indicateur pour resigner les volumes de snapshot et monte ces derniers sur les hôtes ESXi pour la récupération. Une fois l'opération terminée, l'indicateur reste défini sur la valeur 1.

Cause

Site Recovery Manager ne vérifie pas la méthode de présentation des volumes snapshots aux hôtes ESXi. Site Recovery Manager ne prend pas en charge la définition de l'indicateur `LVM.enableResignature` sur 0. Si vous fixez l'indicateur de 1 à 0, la machine virtuelle peut connaître une panne à chaque basculement test ou lors de basculements réels.

Le paramétrage de l'indicateur `LVM.enableResignature` sur des hôtes ESXi est une opération au niveau de l'hôte. Lorsque cet indicateur est défini sur 1, pendant l'analyse ou le prochain redémarrage de l'hôte, tous les LUN de snapshot visibles pour l'hôte ESXi et susceptibles d'être resignés, le sont.

Si des volumes de snapshot non-liés à Site Recovery Manager sont montés de force sur les hôtes ESXi du site de récupération, alors ces LUN seront resignés comme faisant partie d'une réanalyse de l'hôte pendant un processus de basculement test ou de basculement réel. Par conséquent, toutes les machines virtuelles de ces volumes deviennent inaccessibles.

Solution

Pour empêcher ces pannes, veillez à ce qu'aucun LUN de snapshot non-lié à Site Recovery Manager, et monté de force, ne soit visible pour les hôtes ESXi du site de récupération.

L'ajout de machines virtuelles à un groupe de protection échoue avec une erreur de périphériques non résolue

L'ajout de machines virtuelles à un groupe de protection échoue avec une erreur lorsque les mappages d'inventaire appropriés n'ont pas été configurés.

Problème

Lorsque vous ajoutez une machine virtuelle à un groupe de protection, l'erreur suivante s'affiche : Impossible de protéger la VM '*virtual machine name*' en raison de périphériques non résolus.

Cause

Vous n'avez pas configuré les mappages d'inventaire pour mapper les périphériques de la machine virtuelle sur le site protégé vers les périphériques correspondants au niveau du site de récupération.

Solution

Configurez les mappages d'inventaire comme décrit dans *Installation et configuration de Site Recovery Manager*.

La configuration de la protection échoue avec une erreur de création d'un espace réservé

Lorsque que vous configurez la protection sur plusieurs machines virtuelles, la configuration échoue avec une erreur de création d'un espace réservé.

Problème

La configuration de la protection simultanée sur un grand nombre de machines virtuelles échoue avec une erreur de délai d'attente de création d'un espace réservé ou une erreur de dénomination de création d'un espace réservé :

- Erreur de création de la VM à espace réservé : Opération expirée : 300 secondes
- Erreur de création de la VM à espace réservé : Le nom '*placeholder_name*' existe déjà

Ce problème se produit lorsque vous configurez la protection de différentes manières :

- Vous créez un groupe de protection qui contient une ou plusieurs banques de données contenant un grand nombre de machines virtuelles.
- Vous utilisez l'option **Groupes de protection > Machines virtuelles > Tout restaurer** dans l'interface de Site Recovery Manager sur un grand nombre de machines virtuelles.
- Vous utilisez l'API de Site Recovery Manager pour protéger manuellement un grand nombre de machines virtuelles.

Cause

L'infrastructure du site de récupération est incapable de traiter le volume de créations simultanées de machines virtuelles à espace réservé.

Solution

Augmentez la valeur du paramètre `replication.placeholderVmCreationTimeout` qui par défaut est de 300 secondes. Reportez-vous à la section [Modifier le délai d'expiration pour la création de machines virtuelles à espace réservé](#).

Vous n'avez pas besoin de redémarrer le Serveur Site Recovery Manager après la modification de ce paramètre. Site Recovery Manager appliquera le paramètre la prochaine fois que vous configurez la protection sur une machine virtuelle.

La migration planifiée échoue car l'hôte est dans un état incorrect

Si vous placez l'hôte ESXi sur le site de récupération en mode de maintenance pendant une migration planifiée, la migration échoue.

Problème

La migration planifiée échoue avec l'erreur `Erreur - L'opération n'est pas autorisée dans l'état actuel de l'hôte`.

Cause

Site Recovery Manager ne peut pas mettre sous tension des machines virtuelles sur le site de récupération lorsque l'hôte ESXi sur le site de récupération est en mode de maintenance.

Solution

Quittez le mode de maintenance sur l'hôte ESXi dans le site de récupération et relancez la migration planifiée.

Échec de la récupération avec erreur de délai d'expiration pendant la personnalisation du réseau de certaines machines virtuelles

Pendant une récupération, certaines machines virtuelles ne peuvent être récupérées et une erreur de délai d'expiration se produit pendant la personnalisation du réseau.

Problème

Pendant un basculement, certaines machines virtuelles ne peuvent être récupérées dans le délai d'expiration par défaut de 120 secondes.

Cause

Ce problème peut être dû à l'une des raisons suivantes.

- Le package VMware Tools n'est pas installé sur la machine virtuelle faisant l'objet d'une récupération.
- La banque de données du site de récupération est pleine.

Solution

- 1 Vérifiez que VMware Tools est installé sur la machine virtuelle faisant l'objet d'une récupération.

2 Vérifiez la capacité disponible de la banque de données du site de récupération.

Si la banque de données est pleine ou l'est presque, le fait d'étendre le délai d'expiration de la personnalisation client peut résoudre ce problème.

a Dans vSphere Client, sélectionnez l'hôte, puis **Configuration > Paramètres avancés**.

b Mettez à jour le paramètre Délai d'expiration sur 1200 secondes.

3 Exécutez une nouvelle récupération.

La récupération échoue avec une erreur de non-disponibilité d'hôte et de banque de données

La récupération ou le test de récupération échoue avec une erreur d'indisponibilité du matériel de l'hôte ou des banques de données si vous exécutez la récupération ou le test peu de temps après avoir apporté des modifications à l'inventaire de vCenter Server.

Problème

La récupération ou le test de récupération échoue avec l'erreur `Aucun hôte avec la version matérielle '7' et banque de données 'ds_id' sous tension et hors mode de maintenance n'est disponible....`

Cause

Serveur Site Recovery Manager conserve un cache de l'état de l'inventaire de l'hôte. Parfois, lorsque de récentes modifications sont apportées à l'inventaire (par exemple, si un hôte devient inaccessible, est déconnecté ou perd sa connexion avec certaines banques de données), la mise à jour du cache du Serveur Site Recovery Manager peut nécessiter jusqu'à 15 minutes. Si le Serveur Site Recovery Manager a dans son cache le mauvais état d'inventaire de l'hôte, une récupération ou un test de récupération peut échouer.

Solution

Patientez 15 minutes avant d'exécuter une récupération si vous modifiez l'inventaire de l'hôte. Si l'erreur persiste, patientez 15 minutes avant de relancer la récupération.

Échec de la reprotection avec une erreur de délai d'attente de vSphere Replication

Lorsque vous exécutez une reprotection sur un plan de récupération qui contient des groupes de protection de vSphere Replication, l'opération expire avec une erreur.

Problème

Les opérations de reprotection sur des plans de récupération qui contiennent des groupes de protection de vSphere Replication échouent avec l'erreur `Opération expirée : 7 200 secondes Échec lors de la synchronisation VR pour le groupe VRM <Non disponible>. Opération expirée : 7 200 secondes.`

Cause

Lorsque vous exécutez la reprotection, Site Recovery Manager effectue une synchronisation en ligne du groupe de protection de vSphere Replication, ce qui peut faire expirer l'opération. La valeur par défaut du délai d'expiration est 2 heures et correspond à un délai d'expiration de synchronisation de 4 heures.

Solution

Augmentez la valeur de délai d'attente `synchronizationTimeout` dans Paramètres avancés. Reportez-vous à [Modifier les paramètres de vSphere Replication](#).

Le plan de récupération arrive à expiration lors de l'attente de VMware Tools

L'exécution d'un plan de récupération échoue avec une erreur de délai d'expiration pendant l'attente du démarrage de VMware Tools.

Problème

Les opérations de récupération échouent après l'étape Arrêt des VM ou l'étape Attente de VMware Tools du plan de récupération.

Cause

Site Recovery Manager utilise le signal de pulsation de VMware Tools pour déterminer à quel moment des machines virtuelles récupérées s'exécutent sur le site de récupération. Les opérations de récupération nécessitent l'installation de VMware Tools sur les machines virtuelles protégées. La récupération échoue si vous n'avez pas installé VMware Tools sur les machines virtuelles protégées, ou si vous n'avez pas configuré le démarrage de Site Recovery Manager sans attendre le démarrage de VMware Tools.

Solution

Installez VMware Tools sur les machines virtuelles protégées. Si vous ne souhaitez pas ou ne pouvez pas installer VMware Tools sur les machines virtuelles protégées, vous devez configurer Site Recovery Manager de manière à ne pas attendre le démarrage de VMware Tools sur les machines virtuelles récupérées et à ignorer l'étape de mise à l'arrêt du système d'exploitation invité. Reportez-vous à la section [Modifier les paramètres de récupération](#).

Échec de la reprotection après le redémarrage de vCenter Server

Après le redémarrage de vCenter Server, lorsque vous utilisez vSphere Replication, les opérations de reprotection échouent parfois.

Problème

Après le redémarrage de vCenter Server, lorsque vous utilisez vSphere Replication, les opérations de reprotection échouent avec l'erreur

```
Erreur - Impossible d'inverser la répllication pour la machine virtuelle
'virtual_machine'. La session n'est pas authentifiée.
```

Cause

Après le redémarrage de vCenter Server, ce dernier ne parvient pas à actualiser certaines sessions que Site Recovery Manager utilise pour communiquer avec vSphere Replication, ce qui entraîne l'échec de la reprotection.

Solution

Redémarrez les services Site Recovery Manager sur les deux sites.

La réanalyse des banques de données échoue car les périphériques de stockage ne sont pas prêts

Lorsque vous lancez un test de récupération ou une récupération réelle, des adaptateurs de répllication de stockage (SRA) envoient des réponses à Site Recovery Manager avant qu'un périphérique de stockage promu sur le site de récupération ne soit disponible pour les hôtes ESXi. Site Recovery Manager réanalyse les périphériques de stockage et la réanalyse échoue.

Problème

Si les périphériques de stockage ne sont pas encore totalement disponibles, ESXi Server ne les détecte pas et Site Recovery Manager ne trouve pas les périphériques répliqués lorsqu'il effectue la réanalyse. Cela risque d'entraîner plusieurs problèmes.

- Les banques de données ne sont pas créées et les machines virtuelles récupérées sont introuvables.
- Les hôtes ESXi ne répondent plus au signal de pulsation de vCenter Server et se déconnectent de vCenter Server. Si cela se produit, vCenter Server envoie une erreur à Site Recovery Manager et le test de récupération ou la récupération réelle échoue.
- L'hôte ESXi est disponible, mais la réanalyse et la resignature de disques excèdent les délais d'attente de Site Recovery Manager ou de vCenter Server, entraînant une erreur Site Recovery Manager.

Cause

Les périphériques de stockage ne sont pas prêts lorsque Site Recovery Manager démarre la réanalyse.

Solution

Pour retarder le lancement des analyses de stockage jusqu'à ce que les périphériques de stockages soient disponibles sur les hôtes ESXi, augmentez le paramètre `storageProvider.hostRescanDelaySec` à une valeur comprise entre 20 et 180 secondes. Reportez-vous à la section [Modifier les paramètres du fournisseur de stockage](#).

Note Dans Site Recovery Manager 5.1 et les versions précédentes, vous avez peut-être utilisé le paramètre `storageProvider.hostRescanRepeatCnt` pour introduire un délai dans les récupérations. Utilisez plutôt le paramètre `storageProvider.hostRescanDelaySec`.

Problèmes d'évolutivité lors de la réplication de nombreuses machines virtuelles avec un RPO court vers une banque de données VMFS partagée sur ESXi Server 5.0

Les performances peuvent être lentes si vous répliquez un grand nombre de machines virtuelles avec un objectif de point de récupération (RPO) court vers une seule banque de données VMFS (« virtual machine file store ») à laquelle de nombreux hôtes peuvent accéder sur le site de récupération.

Problème

Ce problème se produit lors de l'exécution d'ESXi Server 5.0 sur le site de récupération. Il peut se traduire par des cibles RPO manquées.

Le nombre de machines virtuelles qui peut être répliqué vers une banque de données VMFS unique et partagée augmente lorsque les cibles RPO sont plus longues.

Suivez les directives lors du calcul du nombre de machines virtuelles que vous devez répliquer vers un seul volume VMFS sur le site de récupération.

- Si toutes vos machines virtuelles ont un RPO de 15 minutes, les performances s'en trouvent affectées lors de la réplication de 50 à 100 machines virtuelles vers une même banque de données VMFS.
- Si toutes vos machines virtuelles ont un RPO de 30 minutes, les performances s'en trouvent affectées lors de la réplication de 100 à 200 machines virtuelles vers une même banque de données VMFS.

Si l'un de vos groupes de protection contient des cibles RPO hétérogènes, calculez la moyenne harmonique des cibles RPO lors du calcul du nombre de machines virtuelles que vous pouvez répliquer vers un seul volume VMFS. Par exemple, si vous avez 100 machines avec un RPO de 20 minutes et 50 machines virtuelles avec un RPO de 600 minutes, procédez comme suit pour calculer la moyenne harmonique du RPO :

$$150 / (100 / 20 + 50 / 600) = \sim 30$$

Dans cet exemple, la configuration est similaire à une installation de 150 machines virtuelles, chacune ayant un RPO d'environ 30 minutes. Dans ce cas, les performances s'en trouvent affectées si ces 150 machines virtuelles sont répliquées vers un seul volume VMFS.

Cause

Ce problème affecte uniquement les banques de données VMFS partagées par de nombreux hôtes. Il ne se produit pas sur les banques de données locales à un hôte ou sur d'autres types de banques de données comme NFS. Ce problème affecte uniquement les installations exécutant ESXi Server 5.0.

Le nombre de serveurs vSphere Replication n'est pas pertinent. Ces limites s'appliquent au nombre de machines virtuelles que vous pouvez répliquer vers une même banque de données VMFS.

Solution

- 1 Mettez à niveau ESXi Server vers la version 5.1 ou une version ultérieure sur le site de récupération.
- 2 Si vous ne pouvez pas mettre à niveau ESXi Server vers la version 5.1 ou une version ultérieure, redistribuez les machines virtuelles répliquées ou ajustez leur objectif de point de récupération (RPO).
 - Réduisez le nombre de machines virtuelles avec un RPO court qui sont répliquées vers un même volume VMFS, par exemple en utilisant un grand nombre de banques de données de taille inférieure.
 - Augmentez le RPO des machines virtuelles répliquées vers un même volume VMFS pour créer une moyenne harmonique du RPO plus longue.

La mise au repos au niveau de l'application devient une mise au repos au niveau du système de fichiers lors d'un déplacement vMotion vers un hôte ancien

vSphere Replication peut créer une réplique mise au repos au niveau de l'application pour les machines virtuelles dotées des systèmes d'exploitation clients Windows Server 2008 et Windows 8 fonctionnant sur un hôte ESXi 5.1 ou un hôte plus récent.

Problème

L'hôte ESXi 5.1 ou un hôte plus récent se trouve dans un cluster avec des hôtes de versions antérieures, et vous utilisez vMotion pour déplacer la machine virtuelle répliquée vers un hôte ancien. vSphere Replication crée alors une réplique mise au repos au niveau du système de fichiers.

Cause

Le mélange d'hôtes ESXi 5.1 (ou plus récent) et d'hôtes anciens dans le cluster crée une réplique mise au repos du système de fichiers pendant le déplacement vMotion vers un ancien hôte. Le processus doit au lieu de cela créer une réplique mise au repos au niveau de l'application.

Solution

Assurez-vous que tous les hôtes dans le cluster exécutent ESXi 5.1 ou une version plus récente avant d'utiliser vMotion pour déplacer une machine virtuelle dotée de Windows Server 2008 et Windows 8 avec mise au repos au niveau de l'application.

Reconfigurer la réplication sur des machines virtuelles sans mappage de banque de données

Si vous n'avez pas configuré les mappages de banque de données avant de configurer vSphere Replication sur plusieurs machines virtuelles, la configuration de la réplication échouera.

Problème

Sur l'onglet **Machines virtuelles** d'un site vSphere Replication, les machines virtuelles s'affichent en rouge avec le statut `Aucun mappage de banque de données n'a été configuré`.

Cause

Vous n'avez pas configuré les mappages de banque de données avant de configurer la réplication sur plusieurs machines virtuelles. Vous devez reconfigurer individuellement la réplication des machines virtuelles.

Solution

- 1 Sélectionnez la vue vSphere Replication dans l'interface Site Recovery Manager.
- 2 Sélectionnez le site vSphere Replication distant et cliquez sur l'onglet **Machines virtuelles**.
- 3 Cliquez avec le bouton droit sur une machine virtuelle affichant le statut `Aucun mappage de banque de données configuré` et sélectionnez **Configurer la réplication**.

La valeur RPO et toute méthode de mise au repos choisie pendant les tentatives de configuration de plusieurs machines virtuelles sont déjà définies.

- 4 Cliquez sur **Parcourir** pour sélectionner la banque de données cible du fichier VMX, puis sur **Suivant**.
- 5 Cliquez sur **Parcourir** pour sélectionner la banque de données cible du fichier VMDK, puis sur **Suivant**.
- 6 Sélectionnez un serveur vSphere Replication du site cible et cliquez sur **Suivant**.
- 7 Cliquez sur **Terminer**.

Une fois la reconfiguration achevée, la machine virtuelle est synchronisée avec le site cible.

- 8 Répétez [Étape 3](#) ces étapes [Étape 7](#) pour toutes les machines virtuelles ayant pour statut `Aucun mappage de banque de données configuré`.

La configuration de la réplication échoue avec des machines virtuelles comportant deux disques sur des banques de données différentes

Si vous essayez de configurer vSphere Replication sur une machine virtuelle qui comporte deux disques se trouvant dans des banques de données différentes, la configuration échoue.

Problème

La configuration de la réplication échoue avec le message d'erreur `Plusieurs disques sources, avec des clés de périphérique device_keys, pointent vers la même banque de données de destination et le même chemin d'accès de fichier.`

Le groupe de répliquions reste à l'état d'erreur.

Cause

Ce problème se produit car vSphere Replication ne génère pas un chemin d'accès à la banque de données ou un nom de fichier uniques pour le disque virtuel de destination.

Solution

Si vous sélectionnez des banques de données différentes pour les fichiers VMDK sur le site protégé, vous devez également sélectionner des banques de données différentes pour les fichiers VMDK cibles sur le site secondaire.

Vous pouvez également créer un chemin d'accès unique à la banque de données en plaçant les fichiers VMDK dans des dossiers distincts sur une seule banque de données cible sur le site secondaire.

vSphere Replication - Violation de RPO

Vous pouvez faire face à des violations de RPO, même si vSphere Replication est correctement exécuté sur le site de récupération.

Problème

Lorsque vous répliquez des machines virtuelles, vous pouvez faire face à des violations de RPO.

Cause

Les violations de RPO peuvent être dues à l'une des raisons suivantes :

- Problèmes de connectivité réseau entre les hôtes source et les serveurs vSphere Replication sur le site cible.
- Modifier l'adresse IP entraîne un changement d'adresse IP pour le serveur vSphere Replication.
- Le serveur vSphere Replication ne peut pas accéder à la banque de données cible.
- Bande passante lente entre les hôtes source et les serveurs vSphere Replication.

Solution

- ◆ Recherchez le `vmkernel.log` sur l'hôte source pour trouver l'adresse IP du serveur vSphere Replication afin de voir tout problème de connectivité réseau.
- ◆ Vérifiez que l'adresse IP du serveur vSphere Replication est identique. Si elle est différente, reconfigurez toutes les répliquions afin que les hôtes source utilisent la nouvelle adresse IP.
- ◆ Vérifiez `/var/log/vmware/*hbrsrv*` sur le dispositif vSphere Replication du site cible pour trouver les problèmes de serveur accédant à la banque de données cible.
- ◆ Pour calculer la configuration requise pour la bande passante, consultez l'article de la base de connaissances 2037268 <http://kb.vmware.com/kb/2037268>.

vSphere Replication ne démarre pas après le déplacement de l'hôte

Si vous déplacez ESXi Server sur lequel est exécuté le dispositif vSphere Replication dans l'inventaire d'une autre instance de vCenter Server, les opérations de vSphere Replication ne sont pas disponibles. Les opérations de vSphere Replication ne sont pas non plus disponibles en cas de réinstallation de vCenter Server.

Problème

Si l'instance d'ESXi Server sur lequel est exécuté vSphere Replication est déconnecté de vCenter Server et connecté à une autre instance de vCenter Server, vous ne pouvez pas accéder aux fonctions de vSphere Replication. Si vous essayez de redémarrer vSphere Replication, le service ne redémarre pas.

Cause

L'environnement OVF du dispositif vSphere Replication est stocké dans la base de données vCenter Server. Lorsque l'hôte ESXi est supprimé de l'inventaire vCenter Server, l'environnement OVF du dispositif vSphere Replication est perdu. Cette action désactive les mécanismes utilisés par le dispositif vSphere Replication pour s'authentifier auprès de vCenter Server.

Solution

- 1 (Facultatif) Si possible, redéployez le dispositif vSphere Replication, configurez toutes les répliquions et réutilisez les fichiers `.vmdk` existants en tant que copies initiales.
 - a Mettez les anciens dispositifs vSphere Replication hors tension.
 - b Supprimez tous les fichiers `hbr*` temporaires des dossiers de la banque de données cible.
 - c Déployez de nouveaux dispositifs vSphere Replication et connectez les sites.
 - d Configurez toutes les répliquions en réutilisant les répliquions des fichiers `.vmdk` existants en tant que copies initiales.

- 2 (Facultatif) Si vous ne pouvez pas redéployer le dispositif vSphere Replication, utilisez l'interface VAMI pour connecter vSphere Replication à l'instance d'origine du système vCenter Server.
 - a Reconnectez l'hôte ESXi à vCenter Server.
 - b Connectez-vous à l'interface VAMI du serveur de vSphere Replication à l'adresse `https://vr-server-address:5480`.
 - c Sélectionnez l'onglet **Configuration**.
 - d Entrez **nom d'utilisateur:mot de passe@adresse_vcenter_server** dans **Adresse de vCenter Server**, où nom d'utilisateur et mot de passe sont les informations d'identification de l'administrateur de vCenter Server.
 - e Entrez l'id correct d'objet géré de VM du dispositif dans **valeur d'objet géré de VM du dispositif**. Utilisez le MOB de vCenter Server afin d'obtenir l'ID du dispositif.
 - f Cliquez sur **Enregistrer et redémarrer le service**.

Si vous utilisez la solution de l'interface VAMI, vous devez répéter la procédure chaque fois que vous modifiez le certificat de vSphere Replication.

Une défaillance inattendue de vSphere Replication a donné lieu à une erreur générique

vSphere Replication inclut un message d'erreur générique dans les journaux en cas de défaillances inattendues.

Problème

Certaines défaillances inattendues de vSphere Replication donnent le message d'erreur *Erreur générique du serveur VRM*. Pour obtenir des informations sur la résolution des problèmes, consultez la documentation.

En plus de l'erreur générique, le message fournit des informations plus détaillées sur le problème, comme dans les exemples suivants.

- Erreur générique du serveur VRM. Pour obtenir des informations sur la résolution des problèmes, consultez la documentation. L'exception détaillée est la suivante :
`'org.apache.http.conn.HttpHostConnectException: Connexion à https://vCenter_Server_address refusée'`. Cette erreur concerne les problèmes de connexion à vCenter Server.
- Erreur - Échec de synchronisation VR pour le groupe VRM *nom de machine virtuelle*. Abandon de la surveillance de synchronisation. Vérifiez la connectivité du trafic de réplication entre l'hôte source et le serveur VR cible. La synchronisation reprendra automatiquement une fois les problèmes de connectivité résolus.. Ce problème concerne une erreur de l'opération de synchronisation.

- Erreur - Impossible d'inverser la répllication de la machine virtuelle '*nom de machine virtuelle*'. Erreur générique du serveur VRM.
Pour obtenir des informations sur la résolution des problèmes, consultez la documentation. L'exception détaillée est la suivante :
'org.hibernate.exception.LockAcquisitionException: Transaction (Process ID 57) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Rerun the transaction. Ce problème concerne un blocage dans Microsoft SQL Server.

Cause

vSphere Replication envoie ce message lorsqu'il rencontre des erreurs de configuration ou d'infrastructure. Par exemple, des problèmes de réseaux, de connexion à la base de données ou de surcharge d'un hôte.

Solution

Vérifiez le message `Exception` détaillée pour obtenir plus d'informations sur le problème. En fonction des détails du messages, vous pouvez réessayer l'opération qui a échoué, redémarrer vSphere Replication ou corriger l'infrastructure.

La génération de bundles de support interrompt la récupération de vSphere Replication

Si vous générez un bundle de journaux vSphere Replication et en même temps tentez d'exécuter une récupération, la récupération risque d'échouer.

Problème

Dans des environnements très chargés, la génération de bundles de journaux peut causer des problèmes de connexion de vSphere Replication pendant les opérations de récupération. La récupération échoue avec l'erreur

```
Erreur générique du serveur VRM. Veuillez rechercher dans la documentation des
    informations sur la résolution des problèmes. L'exception détaillée est la suivante :
'Échec de l'objet de verrouillage
    de l'écriture :
    object_ID'.
```

Cause

Le serveur vSphere Replication est bloqué lors de la génération du bundle de journaux. Cette situation se produit si le stockage de la machine virtuelle vSphere Replication est surchargé.

Solution

Exécutez une nouvelle récupération. Si la récupération échoue toujours, réévaluez les exigences de bande passante de stockage du cluster sur lequel vSphere Replication s'exécute, ainsi que la bande passante du réseau si le stockage est NAS.

La synchronisation complète initiale des fichiers de machine virtuelle vers le stockage VMware Virtual SAN s'exécute lentement

L'utilisation du stockage VMware Virtual SAN et la configuration de vSphere Replication sur plusieurs machines virtuelles risquent de ralentir considérablement la synchronisation complète initiale.

Problème

La configuration de vSphere Replication simultanément sur un grand nombre de machines virtuelles lors de l'utilisation de vSphere Replication avec le stockage Virtual SAN ralentit considérablement la synchronisation complète initiale des fichiers de machine virtuelle.

Cause

Les opérations résultant de la synchronisation complète initiale génèrent un important trafic d'E/S. La configuration d'un trop grand nombre de répliqués simultanés risque de saturer le stockage Virtual SAN.

Solution

Configurez vSphere Replication sous forme de lots incluant un nombre maximal de 30 machines virtuelles à la fois.

La vitesse d'exécution des opérations de vSphere Replication est inversement proportionnelle au nombre de répliqués

Plus le nombre de machines virtuelles à répliquer augmente, plus la vitesse d'exécution des opérations de vSphere Replication risque de diminuer.

Problème

Les temps de réponse des opérations de vSphere Replication peuvent augmenter proportionnellement au nombre de machines virtuelles à répliquer. Les opérations de récupération peuvent expirer ou échouer pour certaines machines virtuelles, et des violations RPO risquent de se produire.

Cause

Chaque machine virtuelle d'une banque de données génère régulièrement des opérations de lecture et d'écriture. La configuration de vSphere Replication sur ces machines virtuelles ajoute une opération de lecture aux opérations de lecture et d'écriture standard, ce qui augmente la charge d'E/S sur le stockage. Les performances de vSphere Replication dépendent de la charge d'E/S des machines virtuelles à répliquer et des capacités du matériel de stockage. Si la charge résultant des machines virtuelles et des opérations d'E/S supplémentaires générées par vSphere Replication dépasse les capacités de votre matériel de stockage, les temps de réponses risquent d'augmenter.

Solution

Lorsque vous exécutez vSphere Replication, si les temps de réponse sont supérieurs à 30 ms, réduisez le nombre de machines virtuelles à répliquer vers la banque de données. Une autre solution consiste à augmenter la capacité de votre matériel de stockage. Si vous suspectez un problème au niveau de la charge d'E/S du stockage et que vous utilisez le stockage VMware Virtual SAN, contrôlez la latence E/S à l'aide de l'outil de surveillance intégré à l'interface de Virtual SAN.