

Administration de Site Recovery Manager

Site Recovery Manager 8.2

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 © 2008-2019 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

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

Informations mises à jour 9

1 Rôles, privilèges et autorisations Site Recovery Manager 10

- Gestion des autorisations par Site Recovery Manager 11
- Site Recovery Manager et le rôle d'administrateur de vCenter Server 12
- Rôles de Site Recovery Manager et devSphere Replication 13
- Gestion des autorisations dans une configuration de site de récupération partagé 14
- Attribuer des rôles et des autorisations Site Recovery Manager 16
- Référence de rôles Site Recovery Manager 18

2 Réplication de machines virtuelles 29

- Utilisation de la réplication basée sur la baie avec Site Recovery Manager 29
 - Configurer la réplication basée sur la baie 30
- Utilisation de vSphere Replication avec Site Recovery Manager 38
 - Réplication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques 39
- Utilisation de la réplication basée sur la baie et de vSphere Replication avec Site Recovery Manager 40

3 Configuration des mappages 42

- Mappages d'inventaire pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication 43
- Mappages d'inventaire pour les groupes de protection de stratégie de stockage 44
 - Configurer des mappages réservés temporaires 46
 - Les utilisateurs obtiennent l'accès aux machines virtuelles après la configuration des mappages réservés temporaires 48
- Configurer les mappages d'inventaire 49
- À propos des mappages de stratégies de stockage 52
- Sélectionner des mappages de stratégies de stockage 52

4 À propos des machines virtuelles à espace réservé 54

- Ce qui arrive aux machines virtuelles à espace réservé pendant la récupération 55
- Sélectionner une banque de données à espace réservé 57

5 Création et gestion des groupes de protection 59

- À propos des groupes de protection de réplication basée sur la baie et des groupes de banques de données 60

Comment Site Recovery Manager calcule les groupes de banques de données	61
Groupes de protection vSphere Replication	63
À propos des groupes de protection de stratégie de stockage	64
Conditions préalables pour les groupes de protection de stratégie de stockage	66
Limitations des groupes de protection de stratégie de stockage	67
Groupes de protection de stratégie de stockage et machines virtuelles non protégées	70
Protection d'une machine virtuelle chiffrée	72
Présentation des états des groupes de protection	73
Présentation des états de protection des machines virtuelles	74
Création de groupes de protection	76
Créer des groupes de protection pour vSphere Replication	76
Créer des groupes de protection de stratégie de stockage	78
Créer des groupes de protection de réplication basée sur la baie	79
Organiser des groupes de protection en dossiers	80
Ajouter et supprimer des groupes de banques de données ou des machines virtuelles dans un groupe de protection	81
Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication	83
Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication	84
Modification des paramètres d'une machine virtuelle dans un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication	86
Suppression de la protection d'une machine virtuelle	87
Supprimer la protection d'une machine virtuelle	88

6 Création, test, et exécution de plans de récupération 90

Tester un plan de récupération	91
Tester les réseaux et les réseaux de centre de données	92
Exécution d'une migration planifiée ou d'une récupération d'urgence via un plan de récupération	93
Exécution d'une récupération à l'aide de la fonction de récupération forcée	94
Différences entre tester et exécuter un plan de récupération	96
Exécution d'une récupération test de machines virtuelles dans plusieurs hôtes sur le site de récupération	97
Créer, tester et exécuter un plan de récupération	98
Créer un plan de récupération	99
Organiser des plans de récupération en dossiers	100
Modifier un plan de récupération	100
Tester un plan de récupération	101
Nettoyage après l'essai d'un plan de récupération	102
Exécuter un plan de récupération	103
Récupérer un snapshot d'une machine virtuelle à un moment spécifique	104
Annuler un test ou une récupération	105

Désactiver la récupération d'une machine virtuelle dans un groupe de protection de stratégie de stockage 106

Désactiver la récupération d'un groupe de cohérence dans un groupe de protection de stratégie de stockage 106

Étapes pour exporter le plan de récupération 107

Afficher et exporter un rapport historique du plan de récupération 108

Supprimer un plan de récupération 109

Présentation des états des plans de récupération 109

7 Configuration d'un plan de récupération 114

Étapes d'un plan de récupération 114

Créer des étapes de récupération personnalisées 116

Types d'étapes de récupération personnalisée 117

Gestion des échecs des étapes de récupération personnalisée par Site Recovery Manager 118

Instructions pour l'écriture des étapes de commande 119

Variables d'environnement pour les étapes de commande 120

Créer des étapes de commande ou des invites de messages de niveau supérieur 123

Créer des invites de messages ou des étapes de commande pour des machines virtuelles individuelles 124

Suspendre les machines virtuelles lors de l'exécution d'un plan de récupération 125

Spécifier la priorité de récupération d'une machine virtuelle 126

Configuration des dépendances de machines virtuelles 127

Activer vSphere vMotion pour la migration planifiée 128

Configurer les options de démarrage et d'arrêt de machine virtuelle 129

Limitations de la protection et de la récupération des machines virtuelles 131

8 Personnalisation des propriétés IP des machines virtuelles 134

Personnalisation manuelle des propriétés IP pour une machine virtuelle individuelle 135

Appliquer des règles de personnalisation IP à une machine virtuelle 137

Personnalisation des propriétés IP pour plusieurs machines virtuelles 138

Personnalisation des propriétés IP pour plusieurs machines virtuelles à l'aide de l'outil DR IP Customizer 138

Personnaliser les propriétés IP pour plusieurs machines virtuelles en définissant des règles de personnalisation 160

9 Reprotection des machines virtuelles après une récupération 162

Reprotection par Site Recovery Manager des machines virtuelles avec la réplication basée sur la baie 164

Comment Site Recovery Manager reprotège les machines virtuelles avec vSphere Replication 165

Reprotection de machines virtuelles par Site Recovery Manager avec une protection de stratégie de stockage 165

Conditions préalables à l'exécution d'une opération de reprotection 166

- Reprotéger les machines virtuelles 167
- Présentation des états de reprotection 168

10 Restauration de la configuration du site de prérécupération par l'exécution d'un retour arrière 170

- Effectuer un retour arrière 172

11 Interoperabilité de Site Recovery Manager avec d'autres logiciels 175

- Site Recovery Manager et vCenter Server 176
- Utilisation de Site Recovery Manager avec le stockage VMware vSAN et vSphere Replication 177
- Interaction de Site Recovery Manager avec DPM et DRS lors d'une récupération 177
- Interaction entre Site Recovery Manager et Storage DRS ou Storage vMotion 178
 - Utilisation de Site Recovery Manager avec la réplication basée sur la baie pour des sites avec Storage DRS ou Storage vMotion 178
 - Utilisation de Site Recovery Manager avec vSphere Replication sur les sites disposant de Storage DRS ou de Storage vMotion 180
- Interaction entre Site Recovery Manager et vSphere High Availability 181
- Interaction de Site Recovery Manager avec le stockage étiré 181
- Utilisation de Site Recovery Manager avec NSX Data Center for vSphere 183
- Site Recovery Manager et vSphere PowerCLI 184
- Site Recovery Manager et chiffrement des machines virtuelles 184
- Site Recovery Manager et vRealize Orchestrator 185
- Protection de machines virtuelles MSCS (Microsoft Cluster Server) et tolérantes aux pannes 186
- Utilisation de Site Recovery Manager avec les banques de données SIOC 188
- Utilisation de Site Recovery Manager avec des clusters de contrôle d'admission 189
- Site Recovery Manager et machines virtuelles associées aux périphériques de disque RDM 190
- Site Recovery Manager et contrôleurs de domaine Active Directory 190

12 Configuration avancée de Site Recovery Manager 191

- Reconfigurer les paramètres de Site Recovery Manager 191
 - Modifier les paramètres des connexions 191
 - Modifier le paramètre de collecte du rapport d'historique de Site Recovery Manager 192
 - Modifier les paramètres du site local 193
 - Modifier les paramètres de journalisation 194
 - Modifier les paramètres de récupération 197
 - Modifier les paramètres du gestionnaire distant 203
 - Modifier les paramètres du site distant 204
 - Modifier les paramètres de réplication 205
 - Modifier le paramètre SSO 206
 - Modifier les paramètres de stockage 207
 - Modifier les paramètres de stratégie de stockage de la réplication basée sur la baie 208
 - Modifier les paramètres du fournisseur de stockage 209

	Modifier les paramètres de vSphere Replication	213
	Modifier les paramètres de télémétrie	214
	Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager	215
	Paramètres pour grands environnements Site Recovery Manager	217
13	Évènements et alarmes Site Recovery Manager	220
	Contrôle des connexions entre sites par Site Recovery Manager	220
	Créer des alarmes Site Recovery Manager	221
	Référence d'événements Site Recovery Manager	222
14	Collecte des fichiers journaux de Site Recovery Manager	236
	Collecter les fichiers journaux de Site Recovery Manager à l'aide de l'interface de Site Recovery Manager	236
	Collectez manuellement les fichiers journaux de Site Recovery Manager	237
	Modifier la taille et le nombre des fichiers journaux de Site Recovery Manager Server	238
	Configurer les vidages de mémoire de Site Recovery Manager	240
15	Dépannage de Site Recovery Manager	243
	La mise sous tension simultanée de nombreuses machines virtuelles sur le site de récupération peut entraîner des erreurs	243
	L'ajout de machines virtuelles à un groupe de protection échoue avec une erreur de périphériques non résolue	244
	La configuration de la protection échoue avec une erreur de création d'un espace réservé	245
	Échec de la suppression rapide et de la recréation d'espaces réservés	246
	La migration planifiée échoue car l'hôte est dans un état incorrect	246
	La migration planifiée échoue en raison d'une synchronisation infructueuse du groupe de protection de stratégie de stockage	247
	Échec de la récupération avec erreur de délai d'expiration pendant la personnalisation du réseau de certaines machines virtuelles	247
	La récupération échoue avec une erreur de non-disponibilité d'hôte et de banque de données	248
	Échec de la reprotection avec une erreur de délai d'attente de vSphere Replication	249
	Le plan de récupération arrive à expiration lors de l'attente de VMware Tools	249
	Échec de synchronisation des groupes de protection vSphere Replication	250
	La réanalyse des banques de données échoue car les périphériques de stockage ne sont pas prêts	251
	La récupération s'interrompt à 36 % lors d'une migration planifiée	252
	Échec de la récupération avec une erreur concernant une absence de réplication	252
	Échec de la récupération en raison d'autorisations d'utilisateur limitées	253
	Échec de la récupération en raison d'une combinaison de VMware Tools et ESXi non prise en charge	254

À propos de l'administration de VMware Site Recovery Manager

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

Ce guide *Administration de Site Recovery Manager 8.2* est mis à jour à chaque nouvelle version du produit ou lorsque cela s'avère nécessaire.

Ce tableau fournit l'historique de mise à jour du guide *Administration de Site Recovery Manager 8.2*.

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.
14 août 2019	<ul style="list-style-type: none">■ Ajout de la nouvelle section Site Recovery Manager et chiffrement des machines virtuelles.■ Mise à jour des informations de la section Syntaxe de l'outil DR IP Customizer.■ Mise à jour des informations de la section Exécutez DR IP Customizer pour personnaliser les propriétés IP de plusieurs machines virtuelles.
9 mai 2019	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 de vCenter Server](#)

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

- [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.

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

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

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

Au cours de l'installation de Site Recovery Manager, les utilisateurs dotés du rôle d'administrateur de vCenter Server se voient accordés le rôle d'administrateur sur Site Recovery Manager. Actuellement, seuls les administrateurs de vCenter Server peuvent se connecter à Site Recovery Manager, excepté 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. Site Recovery Manager effectue les opérations à l'aide des informations d'identification d'administrateur fournies lors de la connexion aux sites protégés et de récupération.

Site Recovery Manager maintient une base de données d'autorisations pour les objets Site Recovery Manager internes qui utilisent un modèle semblable à celui utilisé 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 récupération** sur la banque de données cible au lieu de vérifier plusieurs autorisations de niveau inférieur, 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 la section *vSphere ReplicationAdministration*.

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

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

Si vous attribuez le rôle d'administrateur de vCenter Server à des utilisateurs ou à des groupes d'utilisateurs après avoir installé Site Recovery Manager, vous devez attribuer manuellement les rôles Site Recovery Manager à ces utilisateurs sur les objets Site Recovery Manager.

Vous pouvez attribuer des rôles Site Recovery Manager à des utilisateurs ou à des groupes d'utilisateurs qui ne disposent pas du rôle d'administrateur de 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 de 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 des autorisations sur Site Recovery Manager pour les utiliser avec un site de récupération partagé. L'administrateur de vCenter Server sur le site de récupération partagé doit gérer les autorisations pour que chaque client dispose de privilèges suffisants pour configurer et utiliser Site Recovery Manager, mais en veillant également à ce qu'aucun utilisateur n'ait accès aux ressources appartenant à un autre utilisateur.

Dans le contexte d'un site de récupération partagé, un utilisateur est le propriétaire d'une paire d'instances de Site Recovery Manager Server. Les utilisateurs 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 utilisateur. Aucun compte d'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 Site Recovery Manager Server, 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 Site Recovery Manager Server.

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 utilisateurs

Lorsque vous configurez le partage des ressources d'utilisateur sur le site de récupération partagé, suivez les instructions ci-dessous :

- Tous les utilisateurs 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 utilisateur l'autorisation de renommer, de déplacer ou de supprimer le centre de données ou l'hôte.
- N'accordez pas à un utilisateur l'autorisation de créer des machines virtuelles en dehors des dossiers et des pools de ressources qui lui sont dédiés.
- N'autorisez pas un utilisateur 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 utilisateurs

Lorsque vous configurez des autorisations pour l'isolement de ressources d'utilisateur sur le site de récupération partagé, suivez les instructions ci-dessous :

- Attribuez à chaque utilisateur un dossier de machine virtuelle distinct dans l'inventaire vCenter Server.
 - Définissez des autorisations sur ce dossier de manière à empêcher tout autre utilisateur d'y placer ses machines virtuelles. Par exemple, définissez le rôle Administrateur et activez l'option de propagation d'un utilisateur sur ce dossier. Cette configuration permet d'empêcher les erreurs de noms dupliqués susceptibles de se produire si plusieurs utilisateurs protègent des machines virtuelles portant des noms identiques.
 - Placez dans ce dossier toutes les machines virtuelles à espace réservé de l'utilisateur, afin qu'elles puissent hériter de ses autorisations.
 - N'attribuez pas à d'autres utilisateurs des autorisations d'accès à ce dossier.
- Attribuez des pools de ressources, des banques de données et des réseaux dédiés à chaque utilisateur, et configurez les autorisations de la même manière que pour des dossiers.

Attention Un déploiement dans lequel vous isolez les ressources d'utilisateurs suppose toujours une confiance entre les sites vSphere. Même si vous pouvez isoler les ressources des utilisateurs, vous ne pouvez pas isoler les utilisateurs eux-mêmes. Ce déploiement ne convient pas si vous devez maintenir tous les utilisateurs entièrement séparés.

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

Attribuer des rôles et des autorisations Site Recovery Manager

Au cours de l'installation de Site Recovery Manager, les utilisateurs dotés du rôle d'administrateur de vCenter Server se voient accordés le rôle d'administrateur sur Site Recovery Manager. Actuellement, seuls les administrateurs de vCenter Server peuvent se connecter à Site Recovery Manager, excepté s'ils octroient explicitement un droit d'accès à d'autres utilisateurs.

Afin d'autoriser d'autres utilisateurs à accéder à Site Recovery Manager, les administrateurs vCenter Server doivent leur accorder des autorisations dans l'interface utilisateur Site Recovery Manager. Lorsque vous attribuez des autorisations au niveau du site, les attributions s'appliquent à chaque site. Vous devez ajouter les autorisations correspondantes sur les deux sites.

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

Site Recovery Manager ajoute aux rôles et aux autorisations vCenter Server des autorisations supplémentaires qui permettent d'exercer un contrôle précis sur des tâches et des opérations spécifiques de Site Recovery Manager. Pour plus d'informations sur les autorisations de chaque rôle Site Recovery Manager, reportez-vous à [Référence de rôles Site Recovery Manager](#).

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

3 Dans le volet de gauche, cliquez sur **Autorisations**, sélectionnez un site et cliquez sur **Ajouter**.

- a Dans le menu déroulant **Domaine**, sélectionnez le domaine qui contient l'utilisateur ou le groupe.
- b Recherchez un utilisateur ou un groupe spécifique dans la liste **Utilisateur/groupe** et sélectionnez-le.

Par défaut, vCenter Single Sign-On renvoie un maximum de 5 000 lignes, distribuées en deux moitiés. Une moitié pour l'utilisateur et l'autre moitié pour les groupes et les utilisateurs de la solution. Vous pouvez modifier ce paramètre dans les paramètres avancés de vCenter Server.

- c Dans le menu déroulant **Rôle**, sélectionnez un rôle à attribuer à l'utilisateur ou au groupe d'utilisateurs.

Le menu déroulant **Rôle** inclut l'ensemble des rôles mis à disposition 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 d'administration et de configuration de Site Recovery Manager.	Attribuer le rôle Administrateur de SRM .
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 SRM .
Autoriser un utilisateur ou un groupe d'utilisateurs à effectuer des récupérations et à tester des récupérations.	Attribuer le rôle Administrateur de récupération SRM .
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 SRM .
Autoriser un utilisateur ou un groupe d'utilisateurs à tester des plans de récupération.	Attribuer le rôle Administrateur de tests de récupération SRM .

4 Sélectionnez **Propager aux enfants** pour appliquer le rôle sélectionné à tous les objets enfants des objets d'inventaire que ce rôle peut affecter.

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.

- 5 Cliquez sur **Ajouter** pour attribuer le rôle et ses privilèges associés à l'utilisateur ou au groupe d'utilisateurs.
- 6 Répétez de [Étape 3](#) à [Étape 5](#) pour attribuer des rôles et des privilèges aux utilisateurs ou aux 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. L'utilisateur ou le groupe d'utilisateurs en question 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 des 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 SRM** à un groupe.
- 3 Attribuez le rôle **Administrateur de récupération SRM** à l'autre groupe.
- 4 Ajoutez l'utilisateur aux deux groupes d'utilisateurs.

En étant membre de groupes qui disposent des rôles **Administrateur de plans de récupération SRM** et **Administrateur de récupération SRM**, 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 Site Recovery Manager Server, 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. ■ Exécuter des plans de récupération. ■ Effectuer des opérations de reprotéger. ■ Configurer la protection sur les machines virtuelles. ■ Modifier les groupes de protection. ■ Supprimer des groupes de protection. 	<p>Site Recovery Manager.Paramètres avancés.Modifier Site Recovery Manager.Gestionnaire de baies.Configurer Site Recovery Manager.Diagnostics.Exporter Site Recovery Manager.Interne.Accès interne Site Recovery Manager.Préférences d'inventaire.Modifier Site Recovery Manager.Banques de données réservée.Configurer Site Recovery Manager.Groupe de protection.Attribuer au plan Site Recovery Manager.Groupe de protection.Créer Site Recovery Manager.Groupe de protection.Modifier Site Recovery Manager.Groupe de protection.Supprimer Site Recovery Manager.Groupe de protection.Supprimer du plan Site Recovery Manager.Historique de récupération.Supprimer l'historique Site Recovery Manager.Historique de récupération.Afficher les plans supprimés Site Recovery Manager.Plan de récupération.Configurer les commandes Site Recovery Manager.Plan de récupération.Créer Site Recovery Manager.Plan de récupération.Modifier Site Recovery Manager.Plan de récupération.Récupération Site Recovery Manager.Plan de récupération.Supprimer Site Recovery Manager.Plan de récupération.Reprotéger Site Recovery Manager.Plan de récupération.Test Site Recovery Manager.Site distant.Modifier Banque de données.Réplication.Protéger Banque de données.Réplication.Annuler la protection.Arrêter Ressource.Utilisation de la récupération Machine virtuelle. Protection SRM.Protéger Machine virtuelle. Protection SRM.Arrêter</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

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
	<ul style="list-style-type: none"> Afficher les objets de stratégie de stockage. <p>L'utilisateur administrateur de Site Recovery Manager ne peut pas modifier les autorisations héritées. Pour limiter l'accès d'un utilisateur spécifique ou pour accorder l'accès à un utilisateur, l'administrateur Site Recovery Manager doit ajouter un nouveau rôle.</p>	Site Recovery Manager.Stockage basé sur le profil.Vue du stockage basée sur le profil	<ul style="list-style-type: none"> Gestionnaires des baies
Administrateur de groupes de protection Site Recovery Manager	<p>Le rôle de l'administrateur de groupes de protection Site Recovery Manager permet aux utilisateurs de gérer des groupes de protection.</p> <ul style="list-style-type: none"> Créer 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. 	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.Annuler la protection.Arrêter Ressource.Utilisation de la récupération Machine virtuelle. Protection SRM.Protéger Machine virtuelle. Protection SRM.Arrêter	<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
	<ul style="list-style-type: none"> ■ Supprimer la protection des machines virtuelles. <p>Les utilisateurs disposant de ce rôle ne peuvent ni effectuer ou tester des récupérations, ni créer ou modifier des plans de récupération.</p>		

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 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</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.Test</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
	machines virtuelles, ni créer ou supprimer des 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
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,</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.Test</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 ■ Réseau x

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
	ni effectuer des opérations de récupération ou de reprotection.		

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 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 de protection ou des plans de récupération, ni effectuer des opérations de récupération ou de reprotction.</p>	<p>Site Recovery Manager.Plan de récupération.Modifier Site Recovery Manager.Plan de récupération.Test</p>	<ul style="list-style-type: none"> ■ Plans de récupération
Utilisateur distant de Site Recovery Manager	<p>Le rôle d'utilisateur distant de Site Recovery Manager accorde aux utilisateurs l'ensemble minimal de privilèges requis pour des opérations Site Recovery Manager entre sites.</p>	<p>Banque de données.Parcourir la banque de données Banque de données.Opérations de fichier de niveau bas Banque de données.Mettre à jour des fichiers de machine virtuelle Banque de données.Mettre à jour des métadonnées de machine virtuelle Hôte.vSphere Replication.Gérer la réplication Machine virtuelle .Gestion des snapshots.Supprimer un snapshot Machine virtuelle .vSphere Replication.Configurer la réplication</p>	<ul style="list-style-type: none"> ■ Machines virtuelles ■ Banques de données

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
		Machine virtuelle.vSphere Replication.Gérer la réplication Machine virtuelle.vSphere Replication.Surveiller la réplication	

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.

Ce chapitre contient les rubriques suivantes :

- [Utilisation de la réplication basée sur la baie avec Site Recovery Manager](#)
- [Utilisation de vSphere Replication avec Site Recovery Manager](#)
- [Utilisation de la réplication basée sur la baie et de vSphere Replication avec Site Recovery Manager](#)

Utilisation de la réplication basée sur la baie avec Site Recovery Manager

Lorsque vous utilisez la réplication basée sur la baie, une ou plusieurs baies de stockage du site protégé répliquent les données vers des baies homologues sur le site de récupération. Avec les adaptateurs de réplication de stockage (SRA), vous pouvez intégrer Site Recovery Manager à de nombreuses baies.

Pour utiliser la réplication basée sur la baie avec Site Recovery Manager, commencez par configurer la réplication avant de configurer Site Recovery Manager afin de l'utiliser.

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.

Vous pouvez protéger des machines virtuelles contenant des disques qui utilisent le stockage VMware vSphere Flash Read Cache. Étant donné que Flash Read Cache n'est pas nécessairement configuré sur l'hôte sur lequel la récupération d'une machine virtuelle s'effectue, Site Recovery Manager désactive Flash Read Cache sur les disques lorsqu'il démarre les machines virtuelles sur le site de récupération. Site Recovery Manager définit la réservation sur zéro. Avant d'effectuer une récupération sur une machine virtuelle configurée pour utiliser vSphere Flash Read Cache,

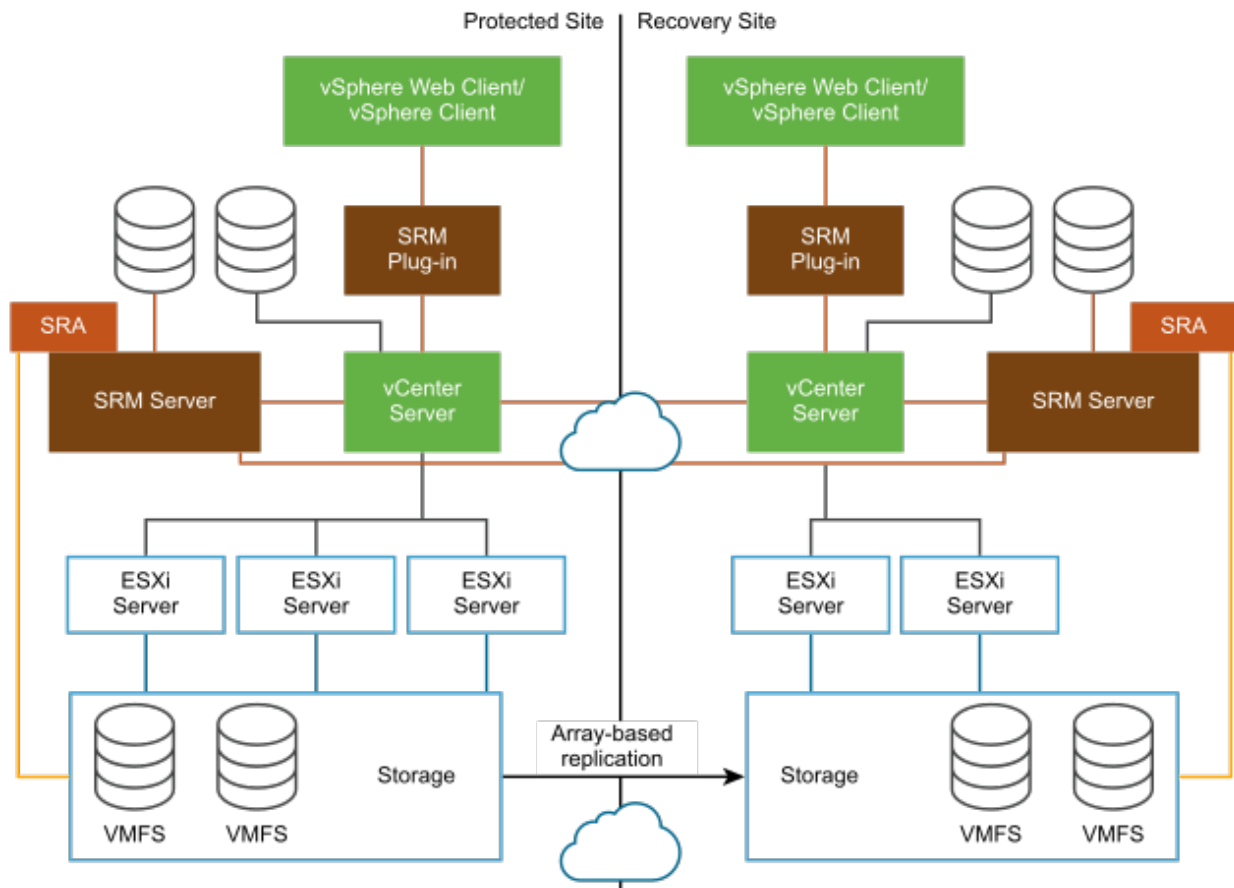
prenez note de la réservation de cache de la machine virtuelle à partir de vSphere Web Client. Après la récupération, vous pouvez migrer la machine virtuelle vers un hôte sur lequel le stockage Flash Read Cache est configuré et restaurer manuellement le paramètre initial de Flash Read Cache sur la machine virtuelle.

Si vous protégez les machines virtuelles à l'aide de groupes de protection de stratégie de stockage, vous devez répliquer ces machines virtuelles à l'aide d'une réplication basée sur la baie.

Adaptateurs de réplication de stockage

Les adaptateurs de réplication de stockage (SRA) ne sont pas intégrés à une version de Site Recovery Manager. Votre fournisseur de baies les développe et les prend en charge. Vous devez installer un SRA spécifique dans chaque baie que vous utilisez avec Site Recovery Manager sur l'hôte du serveur Site Recovery Manager Server. Site Recovery Manager prend en charge l'utilisation de plusieurs SRA.

Figure 2-1. Architecture Site Recovery Manager avec réplication basée sur la baie



Configurer la réplication basée sur la baie

Pour protéger des machines virtuelles que vous répliquez à l'aide d'une réplication basée sur la baie, notamment des machines virtuelles que vous protégez à l'aide de groupes de protection de

stratégie de stockage, vous devez configurer des adaptateurs de réplication de stockage (SRA, storage replication adapters) sur chaque site.

Installer des adaptateurs de réplication de stockage

Si vous protégez des machines virtuelles à l'aide de la réplication basée sur la baie ou de la réplication basée sur la baie avec protection de stratégie de stockage, vous devez installer un adaptateur de réplication de stockage spécifique à chaque baie de stockage que vous utilisez avec Site Recovery Manager. Un SRA est un programme qu'un fournisseur de baies met en œuvre pour permettre à Site Recovery Manager d'utiliser un type de baie spécifique.

Vous devez installer un SRA approprié sur les hôtes Site Recovery Manager Server au niveau du site protégé et du site de récupération. Si vous utilisez plusieurs types de baie de stockage, vous devez installer le SRA pour chaque type de baie sur les deux hôtes Site Recovery Manager Server.

Note Vous pouvez configurer Site Recovery Manager afin d'utiliser plusieurs types de baie de stockage. En revanche, vous ne pouvez pas stocker les disques d'une machine virtuelle sur plusieurs baies de différents fournisseurs. Vous devez stocker tous les disques d'une machine virtuelle sur une même baie.

Les adaptateurs de réplication de stockage arrivent avec leurs propres instructions d'installation. Vous devez installer la version du SRA qui correspond à une version spécifique de Site Recovery Manager. Installez la même version du SRA au niveau des deux sites. Ne mélangez pas différentes versions de SRA.

Si vous utilisez vSphere Replication, vous n'avez pas besoin d'un SRA.

Conditions préalables

- Vérifiez la disponibilité d'un SRA pour votre type de stockage en consultant le *Guide de compatibilité VMware* pour Site Recovery Manager à l'adresse <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra>.
- Téléchargez le SRA en accédant à <https://my.vmware.com/web/vmware/downloads>, en sélectionnant **VMware Site Recovery Manager > Télécharger le produit**, puis en sélectionnant **Pilotes et outils > Adaptateurs de réplication de stockage > Accéder aux téléchargements**.
- Si vous obtenez un SRA provenant du site d'un autre fournisseur, vérifiez qu'il a été certifié pour la version de Site Recovery Manager que vous utilisez en vérifiant la compatibilité de Site Recovery Manager dans le *Guide de compatibilité VMware* sur <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra>.
- Lisez la documentation fournie avec votre SRA. Les SRA ne prennent pas en charge toutes les fonctionnalités prises en charge par les baies de stockage. La documentation qui est fournie par votre SRA détaille ce qui est pris en charge et requis par le SRA. Par exemple, HP et EMC possèdent des exigences physiques détaillées qu'il faut satisfaire pour que le SRA fonctionne comme prévu.
- Installez Site Recovery Manager Server avant d'installer les SRA.

- Votre SRA peut nécessiter l'installation d'autres composants fournis par le fournisseur. Il peut être nécessaire d'installer certains de ces composants sur l'hôte Site Recovery Manager Server. D'autres composants peuvent nécessiter uniquement l'accès au réseau par Site Recovery Manager Server. Pour connaître les dernières informations propres à ces besoins, consultez les notes de mise à jour et les fichiers Lisez-moi des SRA que vous installez.
- Activez la fonction permettant à la baie de stockage de créer des copies de snapshots des périphériques répliqués. Consultez la documentation du SRA.

Procédure

- 1 Installez le SRA sur chaque hôte Site Recovery Manager Server.

Le programme d'installation installe le SRA dans `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\storage\sra`.

- 2 Dans vSphere Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Paire de sites**, accédez à **Configurer > Réplication basée sur la baie > Adaptateurs de réplication de stockage** et cliquez sur le bouton **Réanalyser les adaptateurs**.

Cette action actualise les informations des SRA, permettant ainsi à Site Recovery Manager de détecter les SRA.

Configurer les gestionnaires de baies

Après avoir couplé le site protégé et le site de récupération, configurez leurs gestionnaires de baies respectifs, de sorte que Site Recovery Manager puisse découvrir les périphériques répliqués, calculer les groupes de banques de données et initier les opérations de stockage.

Vous ne configurez généralement les gestionnaires de baies qu'une seule fois après vous être connecté aux sites. Vous n'avez pas besoin de les reconfigurer à moins que les informations de connexion et d'identification du gestionnaire de baies ne changent, ou que vous souhaitiez utiliser un ensemble de baies différent.

Conditions préalables

- Connectez les sites comme indiqué dans [Connecter le site protégé et le site de récupération](#) dans *Installation et configuration de Site Recovery Manager*.
- Installez les SRA au niveau des deux sites comme décrit dans [Installer des adaptateurs de réplication de stockage](#).

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Dans l'onglet Paire de sites, cliquez sur **Configurer > Réplication basée sur la baie > Paires de baies**.

- 4 Cliquez sur le bouton **Ajouter** pour ajouter un gestionnaire de baies.

- 5 Sélectionnez l'adaptateur de réplication de stockage que vous souhaitez que Site Recovery Manager utilise et cliquez sur **Suivant**.

Si aucun type de gestionnaire n'apparaît, effectuez une nouvelle recherche d'adaptateur de réplication de stockage (SRA) ou vérifiez que vous avez installé un adaptateur SRA sur l'hôte de Site Recovery Manager Server.

- 6 Entrez un nom pour le gestionnaire de baies local, fournissez les informations requises pour le type de SRA sélectionné et cliquez sur **Suivant**.

Utilisez un nom descriptif vous permettant d'identifier aisément le stockage associé à ce gestionnaire de baies.

Pour plus d'informations sur le remplissage de ces zones de texte, reportez-vous à la documentation fournie par le fournisseur SRA. Les zones de texte varient en fonction des SRA, mais les zones de texte communes incluent l'adresse IP, les informations de protocole, le mappage entre les noms de baie et les adresses IP, ainsi que le nom d'utilisateur et le mot de passe.

- 7 (Facultatif) Si vous ne souhaitez pas créer une paire de baies, cochez la case **Ne pas créer un gestionnaire de baies distant maintenant** et cliquez sur **Terminer**.
- 8 Entrez un nom pour le gestionnaire de baies distant, fournissez les informations requises pour le type de SRA sélectionné et cliquez sur **Suivant**.
- 9 Sur la page **Paires de baies**, sélectionnez la paire de baies à activer, puis cliquez sur **Suivant**.
- 10 Vérifiez la configuration et cliquez sur **Terminer**.

Ajouter des adaptateurs de réplication de stockage au Site Recovery Manager Appliance

Si vous prévoyez d'utiliser Site Recovery Manager pour la réplication basée sur la baie, vous devez ajouter des adaptateurs de réplication de stockage (SRA) au Site Recovery Manager Server. Les fichiers SRA sont distribués sous forme d'archives `.tar.gz`.

Vous devez installer un SRA approprié sur les hôtes Site Recovery Manager Server au niveau du site protégé et du site de récupération. Si vous utilisez plusieurs types de baie de stockage, vous devez installer le SRA pour chaque type de baie sur les deux hôtes Site Recovery Manager Server.

Conditions préalables

- Téléchargez le SRA. Accédez à <https://my.vmware.com/web/vmware/downloads>, sélectionnez **VMware Site Recovery Manager > Télécharger le produit**, puis sélectionnez **Pilotes et outils > Adaptateurs de réplication de stockage > Accéder aux téléchargements**.

- Si vous obtenez un SRA d'un site de fournisseur différent, vérifiez qu'il est certifié pour la version de Site Recovery Manager que vous utilisez. Reportez-vous au *Guide de compatibilité VMware* pour Site Recovery Manager à l'adresse <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra>.
- Activez la fonction permettant à la baie de stockage de créer des copies de snapshots des périphériques répliqués. Consultez la documentation du SRA.

Procédure

- 1 Connectez-vous à l'interface de gestion de Site Recovery Manager Appliance en tant qu'administrateur.
- 2 Dans l'interface de gestion de Site Recovery Manager Appliance, cliquez sur **Adaptateurs de réplication de stockage**, puis sur **Nouvel adaptateur**.
- 3 Cliquez sur **Télécharger**, accédez au répertoire dans lequel vous avez enregistré le fichier SRA, puis sélectionnez-le.
- 4 Une fois le processus terminé, cliquez sur **Fermer**.
La carte Adaptateur de réplication de stockage s'affiche dans l'interface de gestion de Site Recovery Manager Appliance.
- 5 Connectez-vous à vSphere Client ou à vSphere Web Client.
- 6 Cliquez sur **Site Recovery > Ouvrir Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 7 Dans l'onglet **Paire de sites**, accédez à **Configurer > Réplication basée sur la baie > Adaptateurs de réplication de stockage** et cliquez sur le bouton **Réanalyser les adaptateurs**.

Télécharger et charger les archives de configuration des adaptateurs de réplication de stockage


Si vous utilisez Site Recovery Manager Appliance avec la réplication basée sur la baie et que vous devez remplacer un adaptateur de réplication de stockage (SRA), vous pouvez télécharger l'archive de configuration de ce SRA, puis importer la configuration dans le nouveau SRA.

Conditions préalables

Pour télécharger un fichier de configuration de SRA et l'importer dans un autre SRA, vous devez utiliser des SRA obtenus auprès du même fournisseur.

Procédure

- 1 Connectez-vous à l'interface de gestion de Site Recovery Manager Appliance en tant qu'administrateur.
- 2 Cliquez sur l'onglet **Adaptateurs de réplication de stockage**.

- Sélectionnez la carte Adaptateur de réplication de stockage appropriée et cliquez sur le menu déroulant ().


Option	Description
Télécharger l'archive de la configuration	Téléchargez l'archive de la configuration pour le SRA sélectionné.
Télécharger l'archive de la configuration	<p>Importez une configuration pour le SRA sélectionné.</p> <ol style="list-style-type: none"> Accédez au répertoire dans lequel vous avez enregistré le fichier d'archive de la configuration du SRA et sélectionnez ce fichier. Les fichiers de configuration sont distribués sous forme d'archives <code>.tar.gz</code>. Cliquez sur Ouvrir.

Supprimer les adaptateurs de réplication de stockage

Vous utilisez l'interface de gestion du Site Recovery Manager Appliance pour supprimer les adaptateurs de réplication de stockage (SRA) du Site Recovery Manager Server.

Note Si vous supprimez un SRA, toutes les opérations en cours d'exécution impliquant des baies de stockage contrôlées par cet adaptateur sont interrompues. Cela inclut, sans s'y limiter, les opérations de récupération, de test, de nettoyage et de reprotection.

Procédure

- Connectez-vous à l'interface de gestion de Site Recovery Manager Appliance en tant qu'administrateur.
- Dans l'interface de gestion du Site Recovery Manager Appliance, cliquez sur **Adaptateurs de réplication de stockage**.
- Sélectionnez la carte Adaptateur de réplication de stockage appropriée et, dans le menu déroulant (), cliquez sur **Supprimer**.
- Confirmez que vous êtes informé des conséquences de la suppression de l'adaptateur et cliquez sur **Supprimer**.

Réanalyser les baies pour détecter des modifications de la configuration

Par défaut, Site Recovery Manager recherche dans les baies les modifications qui ont été apportées à la configuration des périphériques en réanalysant les baies toutes les 24 heures. Cependant, vous pouvez forcer la réanalyse d'une baie à tout moment.

Vous pouvez reconfigurer la fréquence d'analyse des baies effectuée par Site Recovery Manager en modifiant l'option `storage.minDsGroupComputationInterval` dans Paramètres avancés. Consultez [Modifier les paramètres de stockage](#).

La configuration des gestionnaires de baies provoque le calcul des groupes de banques de données par Site Recovery Manager, basé sur l'ensemble de périphériques de stockage répliqués qu'il trouve. Si vous changez la configuration de la baie sur un site pour ajouter ou supprimer des périphériques, Site Recovery Manager doit réanalyser les baies et recalculer les groupes de banques de données.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet Paire de sites, cliquez sur **Configurer > Réplication basée sur la baie > Paires de baies**.
- 4 Sélectionnez une paire de baies et cliquez sur **Paire du gestionnaire de baies > Découvrir des paires de baies** pour réanalyser les baies ou sur **Découvrir des périphériques** pour recalculer les périphériques de stockage et les groupes de cohérence.

Lorsque vous sélectionnez une paire de baies, l'onglet **Paires de baies** fournit des informations détaillées sur tous les périphériques de stockage de la baie, notamment le nom du périphérique local, le périphérique auquel il est associé, la direction de la réplication et le groupe de protection auquel il appartient. Il indique également si la banque de données est locale ou distante, et précise l'ID du groupe de cohérence pour chaque périphérique SRA.

Modifier des gestionnaires de baies

Utilisez l'assistant Modifier le gestionnaire de baies local ou l'assistant Modifier le gestionnaire de baies distant pour modifier le nom d'un gestionnaire de baies ou d'autres paramètres, tels que l'adresse IP ou le nom d'utilisateur et le mot de passe.

Pour plus d'informations sur le remplissage des champs d'adaptateur, voir la documentation fournie par le fournisseur SRA. Bien que les champs varient en fonction des SRA, les champs communs incluent l'adresse IP, les informations de protocole, le mappage entre les noms de baie et les adresses IP et les noms et mots de passe utilisateur.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet Paire de sites, cliquez sur **Configurer > Réplication basée sur la baie > Paires de baies**.
- 4 Sélectionnez une paire de baies, cliquez sur **Paire du gestionnaire de baies**, puis cliquez sur **Modifier le gestionnaire de baies local** ou **Modifier le gestionnaire de baies distant**.

5 Modifiez le nom de la baie.

Utilisez un nom descriptif vous permettant d'identifier aisément le stockage associé à ce gestionnaire de baies. Vous ne pouvez pas modifier le type de gestionnaire de baies.

6 Modifiez les informations d'adaptateur.

Ces champs sont créés par le SRA.

7 Cliquez sur **Enregistrer** pour terminer la modification du gestionnaire de baies.

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.

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. 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.

Note 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 hôtes et clusters protégés, à la fois sur le site protégé et sur le site de récupération. Tous les hôtes d'un cluster doivent avoir accès à la banque de données non répliquée. Sinon, vMotion ne fonctionne pas.

Procédure

1 Dans vSphere Client, sélectionnez **Hôtes et clusters**, sélectionnez un hôte, puis cliquez sur **Configurer**.

2 Sous **Machines virtuelles**, sélectionnez **Emplacement du fichier d'échange** et cliquez sur **Modifier**.

3 Sélectionnez **Utiliser une banque de données spécifique** et sélectionnez une banque de données non répliquée.

4 Cliquez sur **OK**.

5 Mettez hors tension, puis sous tension toutes les machines virtuelles de l'hôte.

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.

6 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.

Isolation de périphériques pour le stockage étiré pendant une récupération d'urgence

Pendant une récupération d'urgence avec un stockage étiré, la commande de basculement doit isoler les périphériques sur le site de récupération.

Si certains hôtes sur le site protégé sont toujours opérationnels et continuent d'exécuter des machines virtuelles lorsque vous initiez une récupération d'urgence, Site Recovery Manager ne peut pas mettre sous tension les machines virtuelles correspondantes sur le site de récupération en raison de fichiers verrouillés. Si la baie de stockage isole les périphériques sur le site de récupération, les hôtes ESX sur le site de récupération peuvent désactiver les verrouillages concernés et mettre sous tension les machines virtuelles.

Site Recovery Manager doit utiliser `isolation="true"` dans la commande SRA de basculement pour les périphériques étirés qui n'ont pas été désactivés sur le site protégé.

Si des machines virtuelles sont exécutées sur le site de récupération à partir du même périphérique et que le site de récupération ESXi monte le stockage depuis le site protégé, il existe un risque d'échec des opérations d'écriture lors de l'isolation. Il est recommandé que toutes les machines virtuelles sur un stockage étiré soient exécutées sur le site protégé.

Les détails de l'implémentation de l'isolation pour le stockage étiré sont spécifiques aux fournisseurs de baies. Certains fournisseurs de baies peuvent rendre les périphériques inaccessibles sur le site protégé après l'exécution de la commande SRA de basculement avec isolation. Certains fournisseurs de baies peuvent interrompre la communication entre le site source et le site cible pour un périphérique en particulier.

Utilisation de vSphere Replication avec Site Recovery Manager

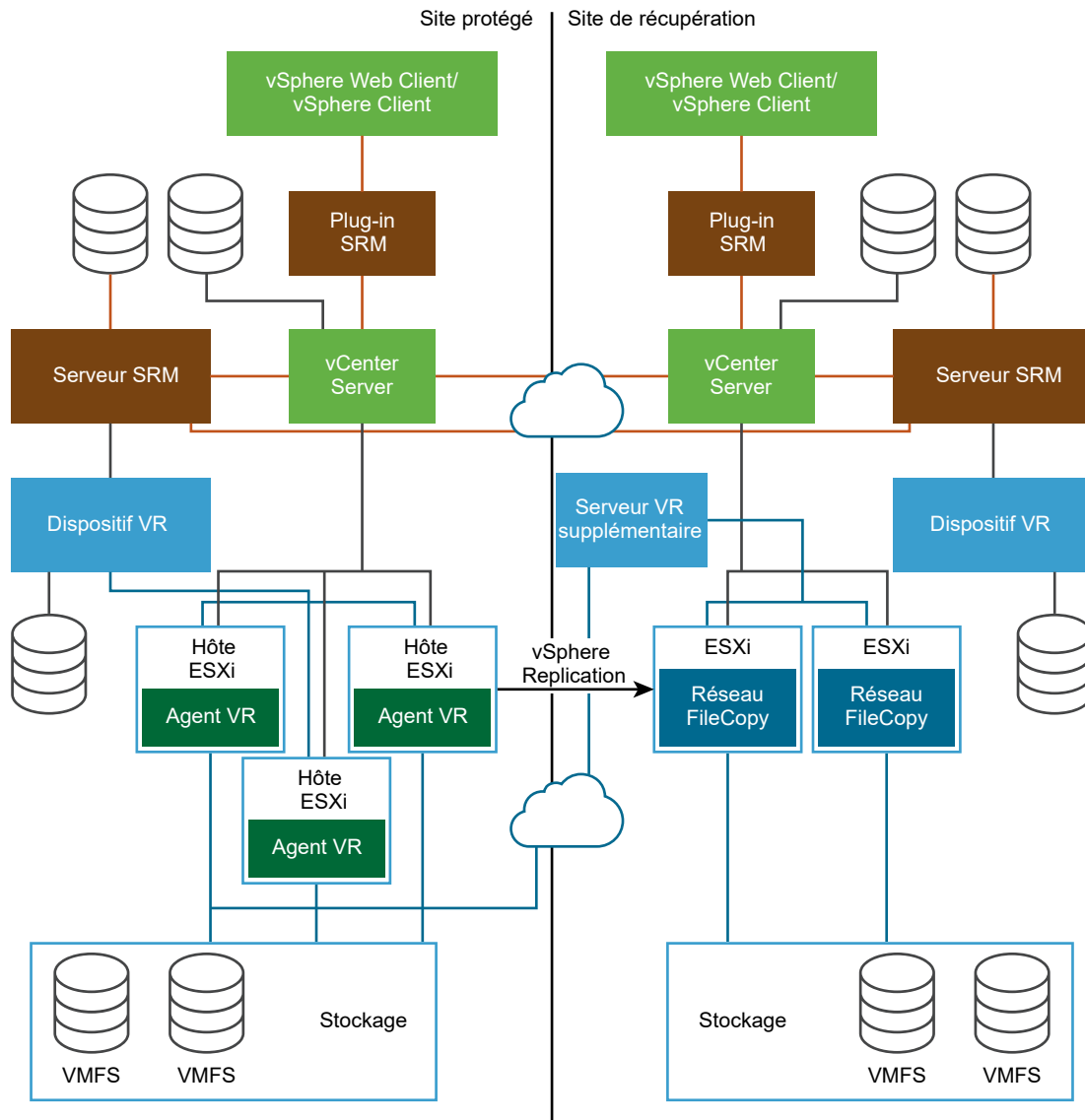
Site Recovery Manager peut utiliser vSphere Replication pour répliquer des données vers les serveurs sur le site de récupération.

Vous déployez le dispositif vSphere Replication et configurez vSphere Replication sur les machines virtuelles indépendamment de Site Recovery Manager. Reportez-vous à la documentation de vSphere Replication à l'adresse <https://www.vmware.com/support/pubs/vsphere-replication-pubs.html> pour plus d'informations sur le déploiement et la configuration de vSphere Replication.

vSphere Replication ne requiert pas de baies de stockage. La source et la cible de la réplication de stockage de vSphere Replication peuvent être n'importe quel périphérique de stockage, cela incluant, sans s'y limiter, des baies de stockage.

Vous pouvez configurer vSphere Replication pour créer et conserver à intervalles réguliers des snapshots des machines virtuelles protégées sur le site de récupération. La prise de snapshots des machines virtuelles à plusieurs moments spécifiques vous permet de conserver plusieurs répliques d'une machine virtuelle sur le site de récupération. Chaque snapshot reflète l'état de la machine virtuelle à un point précis dans le temps. Lorsque vous effectuez une récupération à l'aide de vSphere Replication, vous pouvez sélectionner les snapshots à récupérer.

Figure 2-2. Architecture de Site Recovery Manager avec vSphere Replication



Réplication 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.

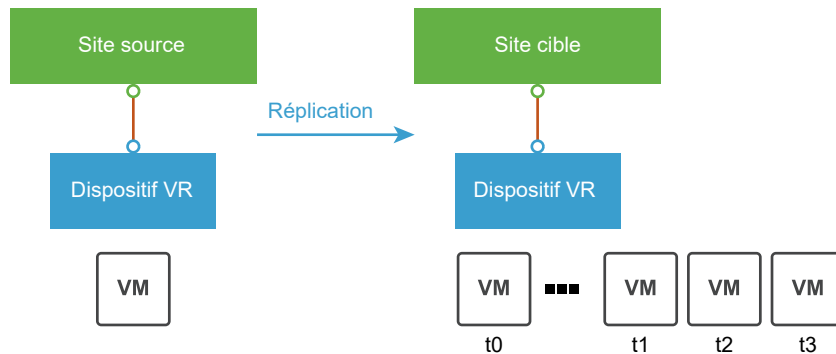
Lorsque vous configurez la réplication d'une machine virtuelle, vous pouvez activer des instances à plusieurs moments spécifiques (MPIT) dans les paramètres de récupération de l'assistant Configurer la réplication. vSphere Replication conserve un certain nombre d'instances de snapshots de la machine virtuelle sur le site cible en fonction de la stratégie de rétention que vous spécifiez. vSphere Replication ne peut pas prendre en charge plus 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 2-3. Récupération d'une machine virtuelle à différents moments spécifiques (PIT)



Utilisation de la réplication basée sur la baie et de vSphere Replication avec Site Recovery Manager

Vous pouvez associer la réplication basée sur la baie et vSphere Replication dans votre déploiement Site Recovery Manager.

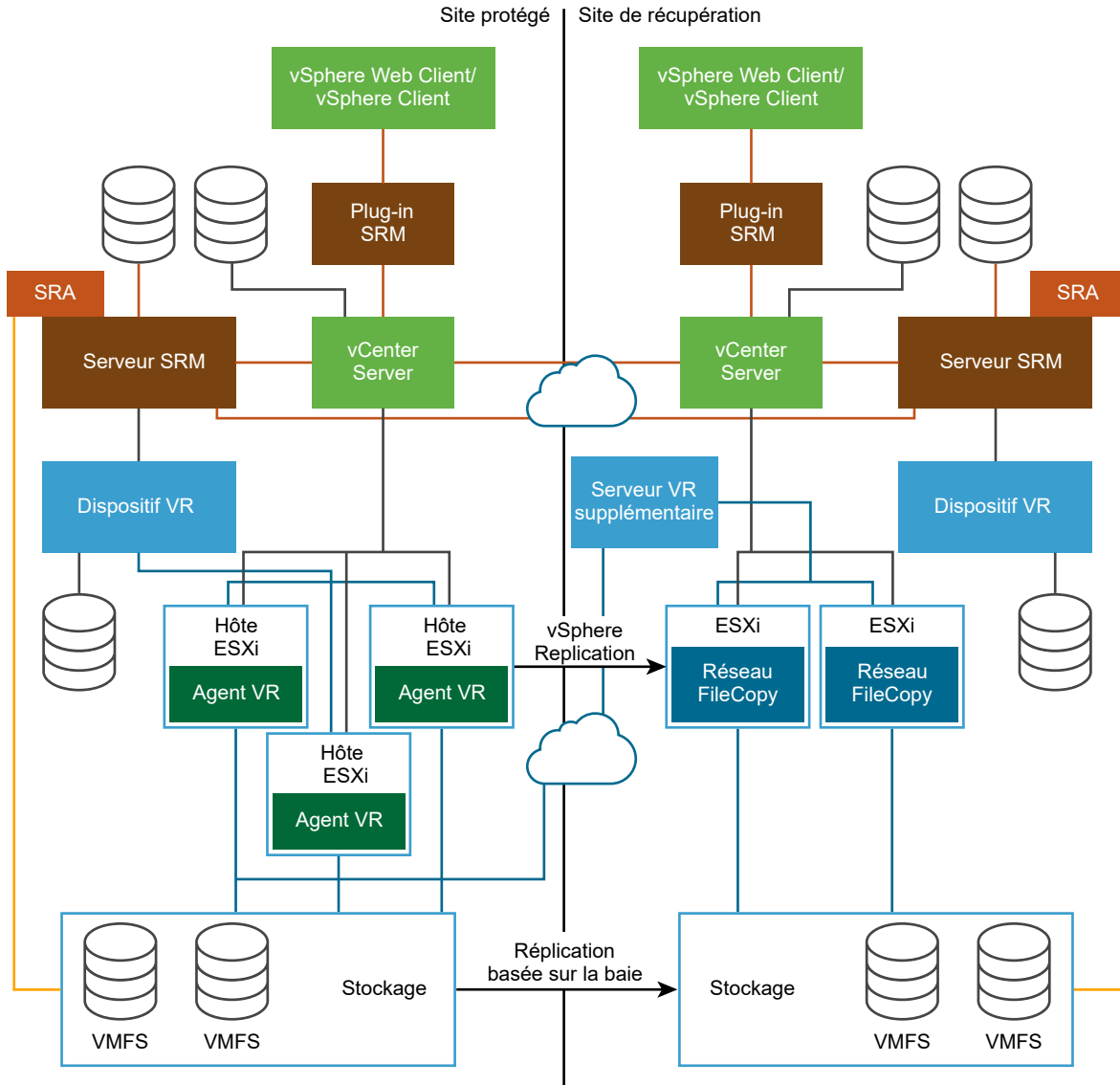
Pour créer un déploiement Site Recovery Manager mixte associant la réplication basée sur la baie et vSphere Replication, vous devez configurer les sites protégé et de récupération pour les deux types de réplication.

- Configurez et connectez les baies de stockage et installez les adaptateurs de réplication de stockage (SRA) appropriés sur les deux sites.
- Déployez les dispositifs vSphere Replication sur les deux sites et configurez la connexion entre les dispositifs.
- Configurez des machines virtuelles pour la réplication en utilisant soit la réplication basée sur la baie soit vSphere Replication, tel qu'approprié.

Note Ne tentez pas de configurer vSphere Replication sur une machine virtuelle qui réside sur une banque de donnée que vous répliquez en utilisant la réplication basée sur la baie.

Vous créez des groupes de protection basés sur la baie pour des machines virtuelles que vous configurez avec la réplication basée sur la baie, et des groupes de protection de vSphere Replication pour des machines virtuelles que vous configurez avec vSphere Replication. Vous ne pouvez pas associer les différents types de réplication dans un groupe de protection. Vous pouvez associer des groupes de protection basés sur la baie et des groupes de protection de vSphere Replication dans le même plan de récupération.

Figure 2-4. Architecture Site Recovery Manager avec une réplication basée sur la baie et vSphere Replication



Configuration des mappages

3

Les mappages vous permettent de spécifier de quelle manière Site Recovery Manager mappe les ressources de machine virtuelle sur le site protégé aux ressources sur le site de récupération.

Vous pouvez configurer des mappages à l'échelle du site pour mapper des objets dans l'inventaire de vCenter Server sur le site protégé à des objets correspondants dans l'inventaire de vCenter Server sur le site de récupération.

- Des réseaux, y compris l'option permettant de spécifier un autre réseau à utiliser pour les tests de plan de récupération
- Les dossiers des centres de données ou des machines virtuelles
- Des ressources de calcul, y compris des pools de ressources, des hôtes autonomes, des vApp ou des clusters

Pendant une récupération, lorsque des machines virtuelles démarrent sur le site de récupération, elles utilisent les ressources situées sur le site de récupération que vous spécifiez dans les mappages. Pour activer la protection et la relecture bidirectionnelles, vous pouvez configurer des mappages inversés, afin de mapper à nouveau les objets situés sur le site de récupération avec leurs objets correspondants sur le site protégé. Vous pouvez également configurer d'autres mappages dans le sens inverse, afin que les machines virtuelles récupérées sur un site utilisent des ressources différentes pour les machines virtuelles protégées de ce site.

Site Recovery Manager applique des mappages d'inventaire de manière différente selon que vous utilisez des groupes de protection basés sur la baie et des groupes de protection vSphere Replication ou des groupes de protection de stratégie de stockage. Pour plus d'informations sur les différents types d'applications des mappages d'inventaire Site Recovery Manager aux différents types de groupes de protection, reportez-vous aux sections [Mappages d'inventaire pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication](#) et [Mappages d'inventaire pour les groupes de protection de stratégie de stockage](#).

Si vous utilisez des groupes de protection de stratégie de stockage, en plus de mapper des objets d'inventaire, vous mappez des stratégies de stockage sur le site protégé à des stratégies de stockage sur le site de récupération.

Ce chapitre contient les rubriques suivantes :

- [Mappages d'inventaire pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication](#)

- [Mappages d'inventaire pour les groupes de protection de stratégie de stockage](#)
- [Configurer les mappages d'inventaire](#)
- [À propos des mappages de stratégies de stockage](#)
- [Sélectionner des mappages de stratégies de stockage](#)

Mappages d'inventaire pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication

Pour la protection basée sur la baie et la protection vSphere Replication, Site Recovery Manager applique des mappages d'inventaire à l'ensemble des machines virtuelles dans un groupe de protection lorsque vous créez ce groupe.

Site Recovery Manager crée une machine virtuelle réservée lorsque vous créez un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication. Site Recovery Manager obtient les attributions de ressources pour l'espace réservé des mappages d'inventaire à l'échelle du site.

Si vous configurez des mappages d'inventaire à l'échelle du site, vous pouvez les appliquer à un groupe de protection à chaque fois que cela s'avère nécessaire, par exemple, pour ajouter de nouvelles machines virtuelles à un groupe de protection existant.

Si vous modifiez les mappages d'inventaire à l'échelle du site pour un site, les modifications n'affectent pas les machines virtuelles que Site Recovery Manager protège déjà dans un groupe de protection existant. Site Recovery Manager applique uniquement les nouveaux mappages aux machines virtuelles protégées précédemment si vous reconfigurez la protection sur celles-ci.

Site Recovery Manager ne peut pas protéger une machine virtuelle, sauf si elle dispose de mappages d'inventaire valides. Néanmoins, la configuration de mappages d'inventaire à l'échelle du site n'est pas obligatoire pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication. Si vous créez un groupe de protection de réplication basée sur la baie ou un groupe de protection vSphere Replication sans avoir défini de mappages d'inventaire à l'échelle du site, vous pouvez configurer individuellement chaque machine virtuelle du groupe. Vous pouvez remplacer les mappages d'inventaire à l'échelle du site en configurant la protection des machines virtuelles dans un groupe de protection. Vous pouvez également créer des mappages d'inventaire à l'échelle du site après avoir créé un groupe de protection, puis appliquer ces mappages d'inventaire à l'échelle du site à celui-ci.

- Pour plus d'informations sur la configuration des mappages d'inventaires à l'échelle du site, reportez-vous à la section [Configurer les mappages d'inventaire](#).
- Pour plus d'informations sur la configuration individuelle de mappages sur des machines virtuelles, reportez-vous à la section [Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

- Pour plus d'informations sur l'application de mappages d'inventaire à l'échelle du site à un groupe de protection existant, reportez-vous à la section [Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

Il est impossible de modifier les configurations réseau de machines virtuelles à espace réservé, car elles ne prennent pas en charge les cartes réseau. Vous pouvez uniquement modifier le réseau d'une machine virtuelle à espace réservé dans les mappages d'inventaire. S'il n'existe aucun mappage pour un réseau, vous pouvez spécifier un réseau lors de la configuration de la protection d'une machine virtuelle individuelle. Les modifications apportées à la machine virtuelle à espace réservé remplacent les paramètres que vous définissez lors de la configuration de la protection de la machine virtuelle. Site Recovery Manager conserve ces modifications sur le site de récupération lors du test et de la récupération.

Mappages d'inventaire pour les groupes de protection de stratégie de stockage

Pour la protection de stratégie de stockage, Site Recovery Manager applique des mappages d'inventaire aux machines virtuelles lorsque vous exécutez un plan de récupération contenant un groupe de protection de stratégie de stockage.

Avec les groupes de protection basés sur la baie et les groupes de protection vSphere Replication, Site Recovery Manager applique des mappages d'inventaire au moment où vous configurez la protection sur une machine virtuelle. Avec les groupes de protection de stratégie de stockage, du fait que la protection de stratégie de stockage est dynamique, Site Recovery Manager applique uniquement les mappages d'inventaire au moment où vous exécutez un plan de récupération. Les décisions relatives au placement de machine virtuelle sont prises en fonction des mappages d'inventaire au moment de l'exécution du plan de récupération, afin que Site Recovery Manager ne crée pas de machines virtuelles réservées sur le site de récupération.

Du fait que Site Recovery Manager applique des mappages d'inventaire pour les groupes de protection de stratégie de stockage au moment où vous exécutez un plan de récupération, vous ne pouvez pas configurer des mappages individuels sur des machines virtuelles dans des groupes de protection de stratégie de stockage. Site Recovery Manager utilise toujours des mappages d'inventaire à l'échelle du site lorsque vous exécutez un plan de récupération avec protection de stratégie de stockage. Si les mappages d'inventaire sont manquants, le test de récupération, la migration planifiée et la récupération d'urgence des plans de récupération contenant des groupes de protection de stratégie de stockage échouent. Vous pouvez configurer Site Recovery Manager afin qu'il interroge ponctuellement les machines virtuelles faisant partie de groupes de protection de stratégie de stockage à la recherche de l'absence de mappages et

qu'il renvoie un avertissement, le cas échéant, car tout mappage manquant peut entraîner l'échec de la récupération d'un groupe. Pour plus d'informations sur la configuration de l'interrogation ponctuelle à la recherche de l'absence de mappages, reportez-vous à la section [Modifier les paramètres de réplication](#).

Note Si le mappage réseau est manquant mais que d'autres mappages sont présents et que vous exécutez un test de récupération, Site Recovery Manager utilise le réseau de test généré automatiquement et le test réussit en renvoyant un avertissement. Si un test de récupération réussit en renvoyant un avertissement sur le mappage réseau manquant, configurez le mappage réseau et réexécutez le test. La migration planifiée et la récupération d'urgence n'utilisent pas le réseau de test et échouent si le mappage réseau est manquant.

Si un plan de récupération échoue à cause de mappages manquants et que le site protégé est disponible, configurez les mappages manquants et réexécutez le plan. Pour plus d'informations sur la configuration des mappages d'inventaire à l'échelle d'un site, reportez-vous à la section [Configurer les mappages d'inventaire](#).

Mappages d'inventaire de ressources et groupes de protection de stratégie de stockage

Suite à la protection dynamique des machines virtuelles, les groupes de protection de stratégie de stockage ont des exigences et des limitations spécifiques quant à la définition des mappages d'inventaire de ressources.

- Site Recovery Manager nécessite des mappages d'inventaire de ressources existants pour toutes les ressources de calcul de niveau supérieur (clusters ou hôtes non gérés) sur le site de protection qui ont monté les banques de données protégées avec un groupe de protection de stratégie de stockage.
- Site Recovery Manager détermine la visibilité souhaitée de la banque de données récupérée en fonction des mappages de ressources de calcul de niveau supérieur et ne prend pas en compte les mappages de ressources pour les pools de ressources.
 - S'il n'existe aucun mappage de ressources pour sa ressource de calcul parent de niveau supérieur, Site Recovery Manager ne peut pas appliquer un mappage existant pour un pool de ressources.
 - Un mappage existant d'un pool de ressources de site de protection à une hiérarchie de ressources de calcul de récupération différente par rapport à son parent n'expose pas le stockage des machines virtuelles sous ce pool de ressources à la ressource de calcul mappée.

Pour une récupération réussie du groupe de protection de stratégie de stockage, vous devez respecter les règles suivantes lors de la création de mappages de ressources.

- Créez des mappages de ressources pour toutes les ressources de calcul protégées de niveau supérieur (clusters ou hôtes non gérés) qui ont des banques de données montées protégées par un groupe de protection de stratégie de stockage.

- Si vous devez créer des mappages supplémentaires pour les pools de ressources, mappez-les à une cible sous la même ressource de calcul de récupération de niveau supérieur, à laquelle leur ressource de calcul protégée parent de niveau supérieur est mappée. Par exemple, lorsque l'hôte protégé ou le cluster P est mappé vers un hôte de récupération, un cluster R ou un pool de ressources de récupération sous R, tous les pools de ressources protégés sous P doivent également être mappés à R ou à un pool de ressources de récupération sous R.

Mappages réservés temporaires pour la protection de stratégie de stockage

Site Recovery Manager applique des mappages d'inventaires pour la protection de stratégie de stockage au moment où vous exécutez un plan de récupération. Si vous exécutez un plan de récupération contenant des groupes de protection de stratégie de stockage et que vous n'avez pas configuré de mappages d'inventaire ou si les objets que vous avez mappés sont manquants, le test de récupération, la migration planifiée et la récupération d'urgence échouent.

En général, vous ne pouvez configurer des mappages d'inventaire que si le site protégé et le site de récupération sont disponibles. Si un plan de récupération avec des groupes de protection de stratégie de stockage échoue en raison de mappages manquants et que le site protégé n'est pas disponible, vous ne pouvez pas configurer les mappages manquants normalement. Lorsqu'une récupération échoue en raison de mappages manquants et de la non-disponibilité du site protégé, Site Recovery Manager crée des mappages réservés temporaires pour pallier à cette situation. Les mappages réservés temporaires vous permettent de configurer les mappages manquants afin que vous puissiez exécuter la récupération avec succès lorsque le site protégé est hors ligne. Les mappages réservés temporaires sont des mappages incomplets qui identifient des objets d'inventaire sur le site protégé contenant des machines virtuelles qui figurent dans le plan de récupération. Les mappages réservés temporaires n'incluent pas d'objets cibles sur le site de récupération. Lorsqu'une récupération échoue en raison de mappages manquants, que le site protégé n'est pas disponible et que Site Recovery Manager crée des mappages réservés temporaires, vous pouvez compléter les mappages réservés temporaires et réexécuter la récupération avec succès.

Pour plus d'informations sur la configuration des mappages réservés temporaires, reportez-vous à la section [Configurer des mappages réservés temporaires](#).

Configurer des mappages réservés temporaires

Si un plan de récupération contenant un groupe de protection de stratégie de stockage échoue en raison de mappages manquants et que le site protégé n'est pas disponible, Site Recovery Manager crée des mappages réservés temporaires. Vous réalisez ces mappages réservés temporaires pour que la récupération puisse aboutir.

Du fait que Site Recovery Manager applique des mappages d'inventaire à des machines virtuelles dans des groupes de protection de stratégie de stockage au moment où vous exécutez un plan de récupération, les groupes de protection de stratégie de stockage nécessitent des mappages d'inventaire à l'échelle du site. Si les mappages d'inventaire à l'échelle du site sont manquants, les tests de récupération, les migrations planifiées et la récupération d'urgence des plans de récupération contenant des groupes de protection de stratégie de stockage échouent.

Si un plan de récupération contenant un groupe de protection de stratégie de stockage échoue en raison de mappages manquants et que le site protégé est disponible, configurez les mappages manquants normalement et réexécutez la récupération. Pour plus d'informations sur la configuration des mappages d'inventaire à l'échelle d'un site, reportez-vous à la section [Configurer les mappages d'inventaire](#).

Si un plan de récupération contenant un groupe de protection de stratégie de stockage échoue en raison de mappages manquants et que le site protégé n'est pas disponible, vous ne pouvez pas configurer les mappages manquants normalement. Pour que la récupération aboutisse, vous devez réaliser les mappages réservés temporaires que Site Recovery Manager crée quand un plan de récupération échoue en raison de mappages manquants.

Conditions préalables

- Le site protégé n'est pas disponible.
- Vous avez exécuté une récupération d'urgence sur un plan de récupération contenant un groupe de protection de stratégie de stockage.
- La récupération a échoué en raison de mappages d'inventaire manquants.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération** et sélectionnez le plan de récupération qui a échoué.
- 4 Sélectionnez l'option **Étapes de récupération** et développez les étapes se trouvant dans un état d'erreur.
- 5 Survolez avec le pointeur de la souris un message d'erreur pour afficher le message complet.

Si les mappages d'inventaire sont manquants, une erreur sur les mappages manquants s'affiche.

Par exemple, si des mappages de ressources sont manquants, le message `Impossible d'atteindre les hôtes associés aux VM d'espaces réservés`. Le mappage du pool de ressources `address` est manquant dans les mappages de ressources.

- 6 Sélectionnez l'onglet **Paire de sites** et vérifiez la connexion SRM distante du site de récupération.

Un message s'affiche vous informant que le site protégé est hors ligne et que Site Recovery Manager a créé des mappages d'espaces réservés temporaires.

- 7 Sélectionnez chacun des onglets **Mappages de réseau**, **Mappages de dossiers**, **Mappages de ressources** et **Mappages de stratégies de stockage**.

Partout où des mappages sont manquants, Site Recovery Manager a sélectionné une ressource sur le site protégé. La ressource correspondante sur le site de récupération affiche **Mappage manquant**.

- 8 Sélectionnez le mappage réservé manquant et cliquez sur l'icône pour modifier le mappage.

- 9 Sélectionnez, sur le site de récupération, une ressource avec laquelle effectuer le mappage dans la ressource sur le site protégé que Site Recovery Manager a sélectionné et cliquez sur **OK**.

- 10 Cliquez sur l'onglet **Plans de récupération**, sélectionnez le plan de récupération ayant échoué et réexécutez le plan de récupération.

Si vous avez configuré tous les mappages manquants, la récupération aboutit. Si des mappages sont toujours manquants, la récupération échoue.

- 11 Si la récupération échoue à nouveau, répétez les étapes [Étape 4](#) à [Étape 10](#) jusqu'à ce que la récupération aboutisse.

Étape suivante

Lorsque le site protégé est à nouveau disponible, configurez normalement des mappages d'inventaire à l'échelle du site et réexécutez une récupération afin que Site Recovery Manager puisse terminer la procédure de récupération sur le site protégé.

Note Site Recovery Manager ne conserve pas les mappages réservés temporaires. Les mappages réservés temporaires que vous avez configurés sont perdus si vous redémarrez Site Recovery Manager Server sur le site de récupération. Configurez toujours des mappages d'inventaire normaux après avoir exécuté une récupération dans laquelle vous avez configuré des mappages réservés temporaires.

Les utilisateurs obtiennent l'accès aux machines virtuelles après la configuration des mappages réservés temporaires

Les utilisateurs qui terminent les mappages réservés temporaires alors que le site protégé n'est pas disponible peuvent obtenir l'accès à des machines virtuelles incorrectes.

Problème

Le site protégé n'est pas disponible pendant une récupération d'urgence et Site Recovery Manager crée des mappages réservés temporaires. L'utilisateur qui exécute le plan de récupération termine les mappages réservés temporaires et réexécute le plan. Une fois la récupération terminée, l'utilisateur a accès aux machines virtuelles du site de récupération auxquelles il n'avait pas l'autorisation d'accéder sur le site protégé.

- Si le site protégé n'est pas disponible, l'utilisateur exécute une récupération d'urgence.
- L'utilisateur n'a pas l'autorisation d'accéder à tous les objets d'inventaire du site protégé.
- Site Recovery Manager détecte les mappages manquants et crée des mappages réservés temporaires incluant des objets du site protégé auxquels l'utilisateur n'a pas l'autorisation d'accéder.
- L'utilisateur configure les mappages cibles entre les objets du site protégé et les objets du site de récupération auxquels il a accès.
- Une fois la récupération terminée, du fait que les machines virtuelles récupérées utilisent des ressources sur le site de récupération auxquelles l'utilisateur a l'autorisation d'accéder, l'utilisateur peut accéder aux machines virtuelles auxquelles il n'avait pas l'autorisation d'accéder quand celles-ci se trouvaient sur le site protégé.

Cause

Si le site protégé n'est pas disponible, Site Recovery Manager ne peut pas effectuer de vérifications d'autorisation sur les objets d'inventaire du site protégé avant de les utiliser pour créer des mappages réservés temporaires.

Solution

Vérifiez que les utilisateurs qui ont l'autorisation d'exécuter des plans de récupération ont également l'autorisation d'accéder à tous les objets de deux sites.

Configurer les mappages d'inventaire

Les mappages d'inventaire fournissent des objets par défaut à l'inventaire sur le site de récupération que les machines virtuelles récupérées utilisent lorsque vous exécutez une récupération.

Pour la protection basée sur la baie et la protection vSphere Replication, si vous configurez des mappages d'inventaire à l'échelle du site avant de créer des groupes de protection, vous n'avez pas besoin de configurer la protection de manière individuelle sur chaque machine virtuelle lorsque vous créez un groupe de protection. Site Recovery Manager applique les mappages à l'échelle du site à toutes les machines virtuelles d'un groupe de protection de réplication basée sur la baie ou un groupe de protection vSphere Replication au moment où vous créez le groupe de protection.

Lorsque vous utilisez une protection de stratégie de stockage, Site Recovery Manager applique les mappages d'inventaire au moment où s'exécute un plan de récupération. Vous ne pouvez pas configurer la protection de manière individuelle sur les machines virtuelles dans un groupe de protection de stratégie de stockage. En conséquence, vous devez configurer des mappages d'inventaire à l'échelle du site si vous utilisez la protection de stratégie de stockage.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Paire de sites**, développez l'option **Configurer** et sélectionnez le type de ressource à configurer.

Option	Action
Mappages de réseau	Mappez des réseaux sur le site protégé aux réseaux sur le site de récupération.
Mappages de dossier	Mappez des centres de données ou des dossiers de machines virtuelles sur le site protégé aux centres de données ou aux dossiers de machines virtuelles sur le site de récupération.
Mappage de ressource	Mappez des pools de ressources, des hôtes autonomes, des vApps ou des clusters sur le site protégé à des pools de ressources, des hôtes autonomes, des vApps ou des clusters sur le site de récupération. Vous pouvez mapper n'importe quel type de ressources d'un site à n'importe quel type de ressources de l'autre site.
	Note Vous ne pouvez pas mapper des hôtes individuels qui font partie de clusters d'autres objets ressource.

- 4 Cliquez sur **Nouveau** pour créer un nouveau mappage.
- 5 Sélectionnez la création de mappage automatique ou manuelle, puis cliquez sur **Suivant**.

Cette étape s'applique uniquement aux mappages de réseau et aux mappages de dossiers. Le mappage automatique n'est disponible que pour les mappages de réseau et de dossiers. Vous devez configurer les mappages de ressources manuellement.

Option	Description
Automatiquement	Site Recovery Manager mappe automatiquement les réseaux et les dossiers sur le site protégé à des réseaux et des dossiers sur le site de récupération qui ont le même nom.
Manuellement	Pour mapper des réseaux et des dossiers spécifiques sur le site protégé à des réseaux, des dossiers et des ressources spécifiques sur le site de récupération.

6 Sélectionnez les éléments du site protégé pour mapper ceux du site de récupération.

- Si vous avez sélectionné le mappage automatique, développez les éléments d'inventaire de gauche pour sélectionner un nœud parent sur le site local (un centre de données ou un dossier, par exemple), puis ceux de droite pour sélectionner un nœud parent sur le site distant.
- Si vous avez sélectionné le mappage manuel, développez les éléments d'inventaire de gauche pour sélectionner un objet spécifique sur le site local, puis ceux de droite pour sélectionner l'objet sur le site distant auquel vous souhaitez mapper cet objet.

Si vous sélectionnez le mappage manuel, vous pouvez mapper plusieurs éléments sur le site local à un seul élément sur le site distant. Vous ne pouvez sélectionner qu'un seul élément à la fois sur le site distant.

Note Le mappage automatique des câbles universels NSX est pris uniquement en charge avec les groupes de protection de stratégie de stockage. Si vous utilisez des groupes de protection de machine virtuelle, vous devez configurer explicitement le mappage réseau entre deux extrémités du câble universel pour vous assurer que les machines virtuelles recouvrent le même câble universel. Reportez-vous à [Utilisation de Site Recovery Manager avec NSX Data Center for vSphere](#).

7 Cliquez sur **Ajout de mappages**.

Les mappages s'affichent en bas de la page. Si vous avez sélectionné le mappage automatique, Site Recovery Manager mappe automatiquement tous les éléments sous le nœud sélectionné sur le site protégé aux éléments qui ont le même nom sous le nœud sélectionné sur le site de récupération.

8 Cliquez sur **Suivant**.

9 (Facultatif) Si vous configurez des mappages de réseau, sur la page **Sélectionner des réseaux de test**, cliquez sur le réseau dans la colonne Réseau de test et utilisez le menu déroulant pour sélectionner le réseau à utiliser lorsque vous testez des plans de récupération.

Vous pouvez configurer Site Recovery Manager pour créer un réseau isolé sur le site de récupération pour tester un plan de récupération. La création d'un réseau de test isolé permet au test de s'exécuter sans ajouter de trafic supplémentaire au réseau de production sur le site de récupération.

- Sélectionnez **Réseau isolé (créé automatiquement)** pour créer automatiquement un réseau isolé sur le site de récupération à utiliser pour les tests. Il s'agit de l'option par défaut.
- Sélectionnez un réseau existant sur le site de récupération à utiliser pour les tests.

- 10 (Facultatif) Cliquez sur la page **Préparer des mappages inversés** et cochez la case de mappage.

La sélection de cette option permet de créer des mappages correspondants de l'élément sur le site distant à l'élément sur le site local. Vous avez besoin de mappages inversés pour établir une protection bidirectionnelle et pour exécuter des opérations de reprotection. Vous ne pouvez pas sélectionner cette option si deux ou plusieurs mappages ont la même cible sur le site distant.

- 11 Cliquez sur **Terminer** pour créer les mappages.
- 12 Répétez [Étape 3](#) jusqu'à [Étape 11](#) pour établir des mappages pour les types de ressources restants.

À propos des mappages de stratégies de stockage

Vous pouvez protéger des machines virtuelles que vous avez associées à des stratégies de stockage en les incluant à des groupes de protection de stratégie de stockage.

Les stratégies de stockage placent les machines virtuelles dans l'inventaire vCenter Server et sur des banques de données en fonction de règles et de balises que vous définissez dans vCenter Server. Les stratégies de stockage peuvent déplacer les machines virtuelles dans l'inventaire ou vers différentes banques de données, pour s'adapter aux modifications de l'environnement vCenter Server.

Si vous mappez des stratégies de stockage sur le site protégé à des stratégies de stockage sur le site de récupération, lorsque vous exécutez un plan de récupération, Site Recovery Manager place les machines virtuelles récupérées dans l'inventaire vCenter Server et sur les banques de données du site de récupération en fonction de la stratégie de stockage à laquelle vous avez effectué le mappage sur le site de récupération.

Sélectionner des mappages de stratégies de stockage

Si vous mappez des stratégies de stockage sur le site protégé à des stratégies de stockage sur le site de récupération, lorsque vous exécutez un plan de récupération, Site Recovery Manager peut placer les machines virtuelles récupérées dans l'inventaire de vCenter Server et sur les banques de données du site de récupération en fonction de la stratégie de stockage à laquelle vous avez effectué le mappage sur le site de récupération.

Conditions préalables

Vous avez créé des stratégies de stockage sur le site protégé et le site de récupération.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Paire de sites**, cliquez sur **Configurer > Mappages de stratégies de stockage**.
- 4 Sélectionnez un site et cliquez sur **Nouveau** pour créer un mappage.
- 5 Sélectionnez la création de mappage automatique ou manuelle, puis cliquez sur **Suivant**.

Option	Description
Préparer automatiquement des mappages pour les stratégies de stockage portant des noms correspondants	Site Recovery Manager mappe automatiquement les stratégies de stockage sur le site protégé à des stratégies de stockage sur le site de récupération qui ont le même nom.
Préparer des mappages manuellement	Pour mapper des stratégies de stockage spécifiques sur le site protégé à des stratégies de stockage spécifiques sur le site de récupération.

- 6 Sélectionnez les stratégies de stockage sur le site protégé à mapper à celles du site de récupération.
 - Si vous avez sélectionné le mappage automatique, Site Recovery Manager sélectionne l'une des stratégies de stockage sur le site protégé pour laquelle il existe une stratégie de stockage portant le même nom sur le site de récupération.
 - Si vous avez sélectionné le mappage manuel, sélectionnez une stratégie de stockage spécifique sur le site protégé, puis sélectionnez la stratégie de stockage sur le site de récupération à laquelle mapper cette stratégie de stockage.

Si vous sélectionnez le mappage manuel, vous pouvez mapper plusieurs stratégies de stockage sur le site local à une seule stratégie de stockage sur le site distant. Vous ne pouvez sélectionner qu'un seul élément à la fois sur le site distant.

- 7 Cliquez sur **Ajout de mappages**.
Les mappages s'affichent en bas de la page.
- 8 Cliquez sur **Suivant**.
- 9 (Facultatif) Dans la page **Mappages inversés**, cochez la case d'un mappage et cliquez sur **Suivant**.

Si vous cochez cette option, vous pouvez créer des mappages correspondants de la stratégie de stockage sur le site distant à la stratégie de stockage sur le site local. Vous avez besoin de mappages inversés pour établir une protection bidirectionnelle et pour exécuter des opérations de reprotection. Vous ne pouvez pas sélectionner cette option si deux ou plusieurs mappages ont la même cible sur le site distant.

- 10 Cliquez sur **Terminer** pour créer les mappages.

À propos des machines virtuelles à espace réservé

4

Lorsque vous créez un groupe de protection de réplication basée sur la baie contenant des groupes de banques de données ou un groupe de protection vSphere Replication contenant des machines virtuelles individuelles, Site Recovery Manager crée une machine virtuelle à espace réservé sur le site de récupération pour chacune des machines virtuelles du groupe de protection.

Une machine virtuelle à espace réservé est un sous-ensemble de fichiers d'une machine virtuelle. Site Recovery Manager utilise ce sous-ensemble de fichiers pour enregistrer une machine virtuelle avec vCenter Server au niveau du site de récupération.

Les fichiers des machines virtuelles à espace réservé sont très petits et ne représentent pas des copies complètes des machines virtuelles protégées. La machine virtuelle à espace réservé n'a aucun disque qui lui est associé. La machine virtuelle à espace réservé réserve des ressources de calcul sur le site de récupération et fournit l'emplacement dans l'inventaire de vCenter Server sur lequel la machine virtuelle protégée se restaure lorsque vous exécutez une récupération.

La présence de machines virtuelles à espace réservé dans l'inventaire du site de récupération donne une indication visuelle aux administrateurs de vCenter Server de la protection des machines virtuelles par Site Recovery Manager. Les espaces réservés indiquent également aux administrateurs de vCenter Server que les machines virtuelles peuvent mettre sous tension et commencer à consommer les ressources locales lorsque Site Recovery Manager teste ou exécute un plan de récupération.

Lorsque vous récupérez une machine virtuelle protégée en testant ou en exécutant un plan de récupération, Site Recovery Manager remplace l'espace réservé par la machine virtuelle récupérée, et la met sous tension comme indiqué par le plan de récupération. Une fois le test du plan de récupération terminé, Site Recovery Manager restaure les espaces réservés et désactive les machines virtuelles récupérées, dans le cadre du processus de nettoyage.

Note Site Recovery Manager ne crée pas de machines virtuelles à espace réservé pour les groupes de protection de stratégie de stockage. Pour plus d'informations sur la manière dont Site Recovery Manager place des machines virtuelles sur le site de récupération lorsque vous utilisez des groupes de protection de stratégie de stockage, reportez-vous aux sections [Mappages d'inventaire pour les groupes de protection de stratégie de stockage](#) et [À propos des mappages de stratégies de stockage](#).

À propos des modèles de machines virtuelles à espace réservé

Lorsque vous protégez un modèle sur le site protégé, Site Recovery Manager crée le modèle à espace réservé en créant une machine virtuelle dans le pool de ressources par défaut d'une ressource informatique, puis en désignant cette machine virtuelle comme modèle. Site Recovery Manager sélectionne la ressource de calcul de l'ensemble des ressources de calcul disponibles dans le centre de données au niveau du site de récupération sur lequel le dossier de la machine virtuelle sur le site protégé est mappé. Tous les hôtes de la ressource informatique sélectionnée doivent avoir accès à au moins une banque de données à espace réservé. Au moins un hôte de la ressource informatique doit prendre en charge la version matérielle du modèle de machine virtuelle protégée.

À propos des banques de données à espace réservé

Si vous utilisez une réplication basée sur la baie pour protéger des groupes de banques de données ou si vous utilisez vSphere Replication pour protéger des machines virtuelles individuelles, vous devez identifier une banque de données sur le site de récupération dans lequel Site Recovery Manager peut stocker les fichiers de machines virtuelles réservées.

Note Site Recovery Manager ne crée pas de machines virtuelles à espace réservé pour les groupes de protection de stratégie de stockage. Vous n'avez pas besoin d'identifier une banque de données réservée si vous utilisez uniquement des groupes de protection de stratégie de stockage.

Les fichiers de machines virtuelles à espace réservé sont très petits, la banque de données à espace réservé n'a donc pas besoin d'être suffisamment grande pour accueillir les machines virtuelles complètes.

Pour activer une migration et une reprotection planifiées, vous devez sélectionner des banques de données à espace réservé sur les deux sites.

Ce chapitre contient les rubriques suivantes :

- [Ce qui arrive aux machines virtuelles à espace réservé pendant la récupération](#)
- [Sélectionner une banque de données à espace réservé](#)

Ce qui arrive aux machines virtuelles à espace réservé pendant la récupération

Lorsque vous créez des groupes de protection basés sur la baie et des groupes de protection vSphere Replication, Site Recovery Manager crée des machines virtuelles réservées sur le site de récupération. Lorsque vous exécutez un plan de récupération contenant des groupes de

protection, Site Recovery Manager remplace les espaces réservés par des machines virtuelles réelles.

Note Site Recovery Manager ne crée pas de machines virtuelles à espace réservé pour les groupes de protection de stratégie de stockage. Cet exemple s'applique aux groupes de protection basés sur la baie et aux groupes de protection vSphere Replication. Il ne s'applique pas aux groupes de protection de stratégie de stockage. Pour plus d'informations sur la manière dont Site Recovery Manager récupère les machines virtuelles lorsque vous utilisez des groupes de protection de stratégie de stockage, reportez-vous à la section [À propos des groupes de protection de stratégie de stockage](#).

Cet exemple illustre le processus par lequel Site Recovery Manager remplace des machines virtuelles réservées sur le site de récupération par des machines virtuelles réelles lorsque vous exécutez des plans de récupération contenant des groupes de protection basés sur la baie et des groupes de protection vSphere Replication.

- 1 Les machines virtuelles se répliquent sur le site de réplication indépendamment de Site Recovery Manager, en fonction du type de réplication que vous utilisez.
 - Pour la réplication basée sur la banque de données, la baie de stockage réplique des banques de données contenant des fichiers de machine virtuelle comme du stockage brut dans la baie de stockage cible.
 - vSphere Replication réplique des machines virtuelles individuelles à l'aide de copies des machines virtuelles de la banque de données que vous configurez comme cible de vSphere Replication. Ces copies de machines virtuelles ne sont pas sous tension.
- 2 Vous désignez une banque de données sur le site de récupération que Site Recovery Manager doit utiliser pour stocker les fichiers de machine virtuelle réservée.
- 3 Lorsque vous configurez la protection Site Recovery Manager sur une machine virtuelle en ajoutant un groupe de banques de données ou une machine virtuelle individuelle à un groupe de protection, Site Recovery Manager crée un espace réservé pour la machine virtuelle de la banque de données réservée sur le site de récupération.
- 4 Lorsque vous exécutez un plan de récupération, Site Recovery Manager arrête les machines virtuelles sur le site protégé et active les machines virtuelles sur le site de réplication en fonction du type de réplication que vous utilisez.
 - Pour la réplication basée sur la banque de données, Site Recovery Manager met en évidence le stockage brut sur le site de récupération contenant les machines virtuelles répliquées en tant que banque de données vCenter Server. Site Recovery Manager enregistre la banque de données récupérée auprès de l'hôte ou du cluster ESXi auprès duquel la banque de données réservée est enregistrée.
 - vSphere Replication met sous tension les copies des machines virtuelles sur le site de récupération.

- Site Recovery Manager envoie une demande à vCenter Server pour échanger l'identité des machines virtuelles réservées pour les machines virtuelles répliquées ayant été mises en évidence sur le site de récupération.

Sélectionner une banque de données à espace réservé

Si vous utilisez des groupes de protection basés sur la baie ou des groupes de protection vSphere Replication, vous devez spécifier une banque de données à espace réservé sur le site de récupération que Site Recovery Manager peut utiliser pour stocker des machines virtuelles à espace réservé.

Vous devez configurer une banque de données à espace réservé sur les deux sites de la paire afin d'établir une protection bidirectionnelle et d'effectuer une reprotection.

Note Site Recovery Manager ne crée pas de machines virtuelles à espace réservé pour les groupes de protection de stratégie de stockage. Vous n'avez pas besoin de sélectionner une banque de données à espace réservé si vous utilisez uniquement des groupes de protection de stratégie de stockage.

Conditions préalables

- Vérifiez que vous avez connecté et couplé les sites protégé et de récupération.
- Les banques de données à espace réservé doivent répondre à certains critères.
 - Pour les clusters, les banques de données à espace réservé doivent être visibles pour tous les hôtes du cluster.
 - Vous ne pouvez pas sélectionner comme banques de données à espace réservé des banques de données répliquées à l'aide d'une réplication basée sur la baie.

Procédure

- Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- Dans l'onglet **Paire de sites**, sélectionnez **Configurer > Banques de données à espace réservé**.
- Sélectionnez un site et cliquez sur **Nouveau** pour configurer une banque de données à espace réservé.

- 5 Sélectionnez une banque de données à désigner comme emplacement des machines virtuelles réservées sur le site local et cliquez sur **OK**.

Les banques de données précédemment configurées sont affichées, mais vous ne pouvez pas les sélectionner. Si une banque de données est répliquée alors que Site Recovery Manager ne dispose pas d'un gestionnaire de baies pour cette banque de données, l'option permettant de sélectionner la banque de données répliquée peut être disponible. Ne sélectionnez pas des banques de données répliquées non gérées par Site Recovery Manager.

Important Si vous utilisez vSphere Replication, vous pouvez sélectionner une banque de données à espace réservé que vous utilisez déjà comme banque de données cible pour des répliqués. Si vous utilisez la même banque de données, Site Recovery Manager crée des VM à espace réservé en se servant des noms des cibles de répliqués et en ajoutant le suffixe(1). Pour plus d'informations sur les groupes de protection vSphere Replication, reportez-vous à [Groupes de protection vSphere Replication](#). La sélection de la même banque de données peut être source de confusion lors de la différenciation des cibles de répliqués et des VM à espace réservé. Pour éviter toute confusion, il est recommandé d'utiliser différentes banques de données.

Assurez-vous que les banques de données à espace réservé ne se trouvent pas dans le même cluster Storage DRS que les banques de données cibles répliqués de vSphere Replication.

Note Lorsque vous configurez ou reconfigurez une répliqués de machine virtuelle à l'aide de vSphere Replication, ne définissez pas le dossier de machine virtuelle à espace réservé en tant que dossier de répliqués pour la machine virtuelle.

- 6 Sélectionnez l'autre site de la paire.
- 7 Répétez les étapes [Étape 3](#) à [Étape 5](#) pour configurer une banque de données réservée sur l'autre site.

Création et gestion des groupes de protection

5

Après avoir configuré une solution de réplication, vous pouvez créer des groupes de protection. Un groupe de protection est un ensemble de machines virtuelles protégées par Site Recovery Manager.

Vous pouvez inclure un ou plusieurs groupes de protection dans un 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 pouvez configurer les machines virtuelles et créer des groupes de protection de manière différente, selon que vous utilisez une réplication basée sur la baie, vSphere Replication ou une protection de stratégie de stockage. 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 ou une protection de stratégie de stockage. Vous pouvez inclure une combinaison de groupes de protection de réplication basée sur la baie et des groupes de protection de vSphere Replication dans le même plan de récupération. Vous ne pouvez pas inclure de groupes de protection de stratégie de stockage dans le même plan de récupération que les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication.

Après avoir configuré la réplication des machines virtuelles, vous devez attribuer à chaque machine virtuelle un pool existant de ressources, un dossier et un réseau sur le site de récupération. Vous pouvez spécifier les valeurs par défaut au niveau du site pour ces affectations en sélectionnant les mappages d'inventaire. Pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication, si vous ne spécifiez pas de mappages d'inventaire, vous configurez des mappages individuellement pour chaque machine virtuelle du groupe de protection. Vous ne pouvez pas configurer de mappages individuellement pour les machines virtuelles des groupes de protection de stratégie de stockage. Vous devez donc configurer des mappages d'inventaire à l'échelle du site si vous utilisez des groupes de protection de stratégie de stockage.

Dès que vous avez créé un groupe de protection de réplication basée sur la baie ou un groupe de protection vSphere Replication, Site Recovery Manager crée des machines virtuelles réservées sur le site de récupération et applique les mappages d'inventaire à chaque machine virtuelle du groupe. Si Site Recovery Manager ne peut mapper une machine virtuelle à un dossier, un réseau et un pool de ressources au niveau du site de récupération, Site Recovery Manager définit la machine virtuelle dans l'état Mappage manquant, sans toutefois lui créer un espace réservé.

Pour les groupes de protection de stratégie de stockage, Site Recovery Manager applique des mappages d'inventaire lorsque vous exécutez un plan de récupération. Site Recovery Manager ne crée pas de machines virtuelles à espace réservé pour les groupes de protection de stratégie de stockage.

Site Recovery Manager ne peut pas protéger les machines virtuelles sur lesquelles vous n'avez pas configuré ou mal configuré la réplication. Dans le cas d'une réplication basée sur la baie, cela est vrai même si les machines virtuelles résident sur une banque de données protégée.

Ce chapitre contient les rubriques suivantes :

- À propos des groupes de protection de réplication basée sur la baie et des groupes de banques de données
- Groupes de protection vSphere Replication
- À propos des groupes de protection de stratégie de stockage
- Protection d'une machine virtuelle chiffrée
- Présentation des états des groupes de protection
- Présentation des états de protection des machines virtuelles
- Création de groupes de protection
- Organiser des groupes de protection en dossiers
- Ajouter et supprimer des groupes de banques de données ou des machines virtuelles dans un groupe de protection
- Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication
- Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication
- Modification des paramètres d'une machine virtuelle dans un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication
- Suppression de la protection d'une machine virtuelle

À propos des groupes de protection de réplication basée 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 un 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 à un groupe de protection de réplication basée sur la baie en les plaçant dans une banque de données qui appartient à un groupe de banques de données que Site Recovery Manager associe à un groupe de protection. Site Recovery Manager recalcule les groupes de banques de données quand il détecte un changement dans une machine virtuelle protégée. Par exemple, si vous ajoutez un disque dur situé sur un autre LUN à une machine virtuelle protégée, Site Recovery Manager ajoute le LUN au groupe de banques de données de ce groupe de protection. Vous devez reconfigurer la protection pour protéger le nouveau LUN. Site Recovery Manager calcule les groupes de cohérence lorsque vous configurez une paire de baies ou lorsque vous actualisez la liste de périphériques.

Vous pouvez également ajouter des machines virtuelles au groupe de protection à l'aide de Storage vMotion pour déplacer leur fichiers vers l'une des banques de données du groupe de banques de données. Vous pouvez supprimer une machine virtuelle à partir d'un groupe de protection de réplication basée sur la baie en déplaçant les fichiers de la machine virtuelle vers une autre banque de données.

Vous pouvez protéger et récupérer des machines virtuelles chiffrées en utilisant des groupes de protection de réplication basée sur la baie. La protection et la récupération des machines virtuelles chiffrées avec la réplication basée sur la baie requièrent VMware vSphere 6.7 et version ultérieure.

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.

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.

Groupes de protection vSphere Replication

Vous pouvez inclure des machines virtuelles que vous avez configurées pour vSphere Replication dans des groupes de protection vSphere Replication.

Les machines virtuelles dans l'inventaire vCenter Server qui sont configurées pour vSphere Replication peuvent être sélectionnées lorsque vous créez ou modifiez un groupe de protection vSphere Replication.

Vous sélectionnez un emplacement cible sur une banque de données du site distant lorsque vous configurez vSphere Replication sur une machine virtuelle. Lorsque vous incluez une machine virtuelle avec vSphere Replication dans un groupe de protection, Site Recovery Manager crée une machine virtuelle à espace réservé pour la récupération. La cible de réplication de vSphere Replication et la machine virtuelle à espace réservé que Site Recovery Manager crée sur les deux peuvent se trouver dans la même banque de données du site de récupération, car elles sont créées dans des dossiers distincts de la banque de données. Lorsque la cible de réplication et les machines virtuelles à espace réservé se trouvent dans la même banque de données, Site Recovery Manager crée le nom de la machine virtuelle à espace réservé en utilisant le nom de la cible de réplication avec le suffixe (1). Pour éviter toute confusion, la meilleure pratique consiste à utiliser des banques de données différentes pour la cible de réplication de vSphere Replication et pour les machines virtuelles à espace réservé de Site Recovery Manager. Site Recovery Manager applique les mappages d'inventaire à la machine virtuelle à espace réservé sur le site de récupération.

Note Lorsque vous configurez ou reconfigurez une réplication de machine virtuelle à l'aide de vSphere Replication, ne définissez pas le dossier de machine virtuelle à espace réservé en tant que dossier de réplication pour la machine virtuelle.

vSphere Replication synchronise les fichiers de disque de la machine virtuelle cible de réplication selon l'objectif de point de récupération que vous avez défini lors de la configuration de vSphere Replication sur la machine virtuelle. Lorsque vous effectuez une récupération avec Site Recovery Manager, Site Recovery Manager met sous tension la machine virtuelle cible de réplication et l'enregistre dans vCenter Server sur le site de récupération à la place de la machine virtuelle à espace réservé.

Lors de l'utilisation des groupes de protection de vSphere Replication, Site Recovery Manager dépend de vSphere Replication mais vSphere Replication ne dépend pas de Site Recovery Manager. Vous pouvez utiliser vSphere Replication indépendamment de Site Recovery Manager. Ainsi, vous pouvez utiliser vSphere Replication pour répliquer toutes les machines virtuelles dans l'inventaire vCenter Server, mais n'inclure qu'un sous-ensemble de ces machines virtuelles dans les groupes de protection. Les modifications apportées à la configuration de vSphere Replication peuvent affecter la protection fournie par Site Recovery Manager des machines virtuelles que vous choisissez d'inclure dans les groupes de protection.

- Site Recovery Manager surveille l'état des machines virtuelles de vSphere Replication dans les groupes de protection de vSphere Replication. Si la réplication ne fonctionne pas pour une machine virtuelle dans un groupe de protection, Site Recovery Manager ne peut pas récupérer la machine virtuelle.
- Si vous annulez la configuration de vSphere Replication sur une machine virtuelle, Site Recovery Manager continue d'inclure cette machine virtuelle dans des groupes de protection dans lesquels vous l'avez inclus. Site Recovery Manager ne peut pas récupérer cette machine virtuelle tant que vous n'avez pas reconfiguré la réplication. Si vous annulez la configuration de vSphere Replication sur une machine virtuelle, vous pouvez la supprimer manuellement du groupe de protection.
- Si vous avez configuré vSphere Replication sur une machine virtuelle qui réside dans une banque de données que Site Recovery Manager protège déjà avec une réplication basée sur la baie, Site Recovery Manager signale une erreur si vous essayez d'inclure cette machine virtuelle dans un groupe de protection de vSphere Replication.

Si vous supprimez une machine virtuelle avec vSphere Replication d'un groupe de protection, vSphere Replication continue de répliquer la machine virtuelle sur le site de récupération. La machine virtuelle ne récupère pas avec le reste des machines virtuelles dans le groupe de protection si vous exécutez un plan de récupération associé.

À propos des groupes de protection de stratégie de stockage

Les groupes de protection de stratégie de stockage activent la protection automatique des machines virtuelles associées à une stratégie de stockage.

Vous pouvez utiliser la réplication basée sur la baie pour répliquer les banques de données du site protégé sur le site de récupération. Si vous balisez une banque de données et que vous créez une stratégie de stockage mappée à cette balise, la banque de données est associée automatiquement à cette stratégie de stockage. Un groupe de protection de stratégie de stockage qui inclut cette stratégie de stockage protège automatiquement toutes les machines virtuelles ayant été balisées comme il se doit et résidant sur la banque de données. Si vous dissociez une machine virtuelle de la stratégie de stockage ou que vous la déplacez de la banque de données, la protection de Site Recovery Manager est annulée automatiquement.

Lorsque vous créez un groupe de protection de stratégie de stockage, Site Recovery Manager effectue les opérations suivantes :

- Il crée un objet géré représentant le groupe de protection de stratégie de stockage sur l'instance de Site Recovery Manager Server locale.
- Il associe les stratégies de stockage que vous sélectionnez avec le groupe de protection de stratégie de stockage. Site Recovery Manager protège toutes les stratégies de stockage conformes que vous incluez dans le groupe de protection de stratégie de stockage.
- Le groupe de protection de stratégie de stockage protège activement les entités de vSphere sur l'instance de vCenter Server locale et détermine la conformité des stratégies de stockage qu'il contient. La protection initiale du groupe de protection de stratégie de stockage créé récemment inclut la protection de toutes les machines virtuelles associées aux stratégies de stockage dans le groupe de protection, en fonction du dernier état connu de l'inventaire vSphere.

Note la protection initiale n'inclut pas les synchronisations de stockage des groupes de cohérence associés. Vous devez répliquer le stockage en fonction de son calendrier standard, indépendamment de vSphere et de Site Recovery Manager.

- Il démarre la surveillance de l'inventaire vSphere afin de détecter les entités de vSphere ajoutées à l'inventaire après la protection initiale. Si Site Recovery Manager ne parvient pas à protéger des entités de vSphere, la création du groupe de protection de stratégie de stockage n'échoue pas, mais des erreurs s'affichent dans les propriétés du groupe de protection.
- Il crée un objet géré par des pairs pour représenter le groupe de protection de stratégie de stockage sur l'instance de Site Recovery Manager Server sur le site de récupération. Cet objet est prêt pour la récupération immédiatement après sa création, même si le stockage sous-jacent n'est pas encore prêt pour la récupération.

Après avoir créé un groupe de protection de stratégie de stockage, vous pouvez avoir besoin de synchroniser le stockage sous-jacent pour vous assurer que les entités vSphere protégées sont récupérables. Exécutez un test de récupération avec l'option de répliquer les modifications récentes dès que possible après avoir créé le groupe de protection.

Conditions préalables pour les groupes de protection de stratégie de stockage

Lorsque vous créez des groupes de protection de stratégie de stockage, vous devez d'abord créer des stratégies de stockage et vérifier que votre environnement respecte certaines conditions préalables.

Conditions préalables

- Créez des balises de banque de données et attribuez-les aux banques de données à associer à une stratégie de stockage :
 - Si votre environnement n'utilise pas le mode Enhanced Linked Mode, créez des catégories de balises sur le site protégé et le site de récupération, puis attribuez-les aux banques de données à protéger sur le site protégé.
 - Si votre environnement utilise le mode Enhanced Linked Mode, créez des catégories de balises et des balises uniquement sur le site protégé. Les balises sont répliquées sur d'autres instances de vCenter Server dans des environnements en mode Enhanced Linked Mode.
- Créez des stratégies de stockage de machine virtuelle dans vCenter Server sur les deux sites, incluant les balises que vous avez attribuées aux banques de données à protéger. Créez des stratégies de machine virtuelle sur les deux sites même si votre environnement utilise le mode Enhanced Linked Mode. Les stratégies de stockage peuvent porter des noms différents sur chaque site.
- Associez des machines virtuelles à protéger à la stratégie de stockage correspondante sur le site protégé. Vous devez associer tous les disques de la machine virtuelle à la même stratégie de stockage.
- Configurez une réplication basée sur la baie des banques de données entre le site protégé et le site de récupération à l'aide de la technologie de réplication fournie par votre fournisseur de baie.
- Configurez les mappages d'inventaire dans Site Recovery Manager. Les groupes de protection de stratégie de stockage ont un comportement spécifique concernant l'application des mappages d'inventaire et les conditions requises pour définir les mappages d'inventaire de ressources. Par exemple, si vous utilisez des groupes de protection de stratégie de stockage et que vous ne configurez pas de mappages, la migration planifiée ou la récupération d'urgence échouent, mais Site Recovery Manager termine correctement votre opération avec des mappages réservés temporaires.
- Au démarrage de Site Recovery Manager Server, Site Recovery Manager interroge la gestion du stockage basée sur les stratégies et les services du gestionnaire de balises dans vCenter Server pour trouver des machines virtuelles associées à une stratégie de stockage. Ces services et vCenter Server doivent être en cours d'exécution lorsque vous démarrez ou redémarrez Site Recovery Manager Server. Dans le cas contraire, Site Recovery Manager Server ne démarre pas.

Pour plus d'informations sur la création de stratégies de stockage, reportez-vous à [Stratégies de stockage de machine virtuelle](#) dans la *documentation de VMware vSphere ESXi et vCenter Server 6.7*.

Pour plus d'informations sur la création de mappages d'inventaires, reportez-vous à la section [Configurer les mappages d'inventaire](#).

Pour plus d'informations sur les groupes de protection de stratégie de stockage et les mappages d'inventaire, consultez [Mappages d'inventaire pour les groupes de protection de stratégie de stockage](#).

Pour plus d'informations sur les limitations connues des groupes de protection de stratégie de stockage, reportez-vous à la section [Limitations des groupes de protection de stratégie de stockage](#).

Limitations des groupes de protection de stratégie de stockage

Les groupes de protection de stratégie de stockage font l'objet de limitations.

Protection de modèles de machine virtuelle

Les banques de données conformes aux stratégies de stockage protégé ne doivent pas contenir de modèles de machine virtuelle.

Protection de machines virtuelles avec disques RDM

Les banques de données conformes aux stratégies de stockage protégé ne doivent pas contenir de machines virtuelles avec disques RDM.

Protection des machines virtuelles et limites d'attribution de licence

- Les machines virtuelles qui ne sont pas protégées initialement en raison de limites d'attribution de licence ne sont pas protégées après que vous modifiez les groupes de cohérence et les machines virtuelles pour vous conformer à la limite d'attribution de licence.
- Les machines virtuelles qui ne sont pas protégées initialement en raison de limites d'attribution de licence ne sont pas protégées même après vous installez une licence pour un nombre supérieur de machines virtuelles.

Balises dupliquées dans des environnements en mode Enhanced Linked Mode

Dans un environnement qui utilise le mode Enhanced Linked Mode, si une partition réseau temporaire se produit entre des instances de vCenter Server, il est possible de créer une balise sur un site et de créer une autre balise portant le même nom sur un autre site. Vous pouvez ensuite baliser un ensemble de banques de données sur un site avec la première balise et un autre ensemble de banques de données sur l'autre site avec la seconde balise identique. Du fait que Site Recovery Manager recherche les balises par nom plutôt que par ID, lorsque la partition réseau est supprimée, les banques de données sur chaque site semblent être balisées avec la même

balise. Si vous supprimez l'une des balises dupliquées, Site Recovery Manager peut supprimer la protection des groupes de cohérence se trouvant dans la banque de données portant cette balise. Les machines virtuelles de ces groupes de cohérence perdent leur protection et les paramètres de récupération des machines virtuelles sont supprimés.

Pour éviter cette situation, résolvez les problèmes de conflits de balises avant de créer des groupes de protection de stratégie de stockage et de configurer des paramètres de récupération de machine virtuelle. Si vous rencontrez cette situation après avoir déjà créé des groupes de protection de stratégie de stockage, fermez temporairement le site protégé pour résoudre le conflit de balises.

Changement des états de la baie de Récupération à Reprotection

Après l'exécution d'un plan de récupération mais avant l'exécution d'une reprotection, si vous changez l'état d'un périphérique de baie, par exemple pour résoudre des problèmes d'inversion de réplication, et que vous lancez une nouvelle analyse des périphériques de stockage, Site Recovery Manager peut s'arrêter de façon inattendue. Le cas échéant, vous devez recréer les groupes de protection et plans de récupération correspondants.

Association de banques de données non répliquées à des stratégies de stockage

Il est possible d'associer une banque de données non répliquée à une stratégie de stockage que vous incluez dans un groupe de protection de stratégie de stockage. En revanche, Site Recovery Manager ne protège pas les machines virtuelles se trouvant sur une banque de données non répliquée, même si celle-ci est associée à une stratégie de stockage incluse dans un groupe de protection de stratégie de stockage. Si vous exécutez un plan de récupération qui inclut ce groupe de protection, toutes les machines virtuelles qui ont des fichiers sur une banque de données non répliquée apparaissent avec des erreurs dans le groupe de protection et ne sont pas récupérées.

Banques de données recouvrant plusieurs groupes de cohérence

Ne configurez pas les banques de données pour recouvrir plusieurs groupes de cohérence. Site Recovery Manager ne peut pas protéger ce type de banques de données sinon les machines virtuelles qui utilisent plusieurs groupes de cohérence et opérations risquent d'échouer.

- Si aucune autre banque de données sauvegardée par le groupe de cohérence ne fait partie de la stratégie de stockage, le groupe de protection peut ignorer le groupe de cohérence.
- Le groupe de protection peut ne pas signaler les problèmes liés aux banques de données.
- Les machines virtuelles utilisant des banques de données recouvrant des groupes de cohérence sont dans un état non protégé, même si elles utilisent la stratégie de stockage adéquate.
- Les banques de données recouvrant plusieurs groupes de cohérence semblent être non répliquées et ne sont pas protégées par le groupe de protection de stratégie de stockage. Ces banques de données peuvent disparaître lorsque Site Recovery Manager fait migrer le groupe de protection vers le site de récupération.

Protection de groupes de cohérence identiques dans les groupes de protection de réplication basée sur la baie et les groupes de protection de stratégie de stockage

Si vous balisez une banque de données répliquée et que vous l'associez à une stratégie de stockage, vous pouvez inclure celle-ci et les groupes de cohérence qui lui sont associés dans un groupe de protection de stratégie de stockage. Il est également possible d'inclure un groupe de banques de données contenant la banque de données balisée dans un groupe de protection de réplication basée sur la baie. Par conséquent, les groupes de cohérence peuvent se retrouver inclus dans un groupe de protection de réplication basée sur la baie et dans un groupe de protection de stratégie de stockage.

Quand un groupe de protection de stratégie de stockage et un groupe de protection de réplication basée sur la baie tentent de protéger le même groupe de cohérence, le groupe de protection de réplication basée sur la baie devient le propriétaire du groupe de cohérence et des machines virtuelles que celui-ci contient. Le groupe de protection de stratégie de stockage indique un état d'erreur pour le groupe de cohérence et les machines virtuelles. Dans ce cas, vous devez supprimer le groupe de cohérence de l'un des groupes de protection.

- Pour conserver le groupe de cohérence dans le groupe de protection de réplication basée sur la baie, dissociez les machines virtuelles concernées de la stratégie de stockage. Dissociez également le groupe de cohérence de la stratégie de stockage. Cela permet de les supprimer du groupe de protection de stratégie de stockage.
- Pour conserver le groupe de cohérence dans le groupe de protection de stratégie de stockage, modifiez le groupe de protection de réplication basée sur la baie pour supprimer la banque de données et les machines virtuelles. Cela résout automatiquement l'erreur dans le groupe de protection de stratégie de stockage.

Modification de l'état de protection des groupes de cohérence et des machines virtuelles pendant et après une récupération

Vous pouvez modifier l'état de protection des groupes de cohérence et des machines virtuelles qui appartiennent à un groupe de protection de stratégie de stockage en ajoutant des balises aux banques de données ou en les supprimant, ou en associant ou dissociant des machines virtuelles avec des stratégies de stockage. Lorsque vous modifiez l'état de protection des machines virtuelles et des groupes de cohérence, et qu'une migration ou une récupération d'urgence planifiée n'est pas en cours d'exécution, Site Recovery Manager met à jour l'état de protection des machines virtuelles et des groupes de cohérence dans le groupe de protection de stratégie de stockage.

Si vous modifiez l'état de protection des machines virtuelles et des groupes de cohérence au cours d'une migration ou d'une récupération d'urgence planifiée qui utilise le groupe de protection de stratégie de stockage, l'interface utilisateur de Site Recovery Manager peut afficher les modifications sur le site de protection, mais le workflow de récupération ne peut pas être mis à jour correctement et un échec de la récupération peut survenir.

Pour une récupération réussie, ne modifiez pas l'état de protection des machines virtuelles et des groupes de cohérence du groupe de protection de stratégie de stockage au cours d'une migration ou d'une récupération d'urgence planifiée de ce groupe. Plus exactement, la fenêtre qui s'ouvre pour la première fois lorsque les modifications de protection ne sont pas prises en charge, démarre un plan de récupération contenant le groupe de protection de stratégie de stockage qui entre dans l'état Récupération en cours, jusqu'à ce qu'il passe à l'état Récupération terminée.

En effet, vous ne pouvez pas ajouter des groupes de cohérence ou des machines virtuelles à un groupe de protection de stratégie de stockage si vous avez exécuté un plan de récupération contenant ce groupe de protection, quelle que soit l'issue de l'opération (réussie ou non).

N'ajoutez pas de groupes de cohérence ou de machines virtuelles à un groupe de protection de stratégie de stockage se trouvant dans un état Récupéré ou Partiellement récupéré. En revanche, vous pouvez ajouter de nouveaux groupes de cohérence ou de nouvelles machines virtuelles à un groupe de protection de stratégie de stockage n'ayant jamais été inclus dans l'exécution d'un plan de récupération ou ayant été inclus uniquement dans des tests de récupération.

Après avoir exécuté un plan de récupération contenant un groupe de protection de stratégie de stockage, vous devez inclure tous les nouveaux groupes de cohérence ou toutes les nouvelles machines virtuelles à un nouveau groupe de protection de stratégie de stockage. Supprimez les nouveaux groupes de cohérence ou les nouvelles machines virtuelles du groupe de protection de stratégie de stockage récupéré avant de les ajouter à un nouveau groupe de protection de stratégie de stockage. Site Recovery Manager prend uniquement en charge la protection d'un objet dans un seul groupe de protection.

Conditions requises pour les mappages d'inventaire de ressources

Les groupes de protection de stratégie de stockage ont des exigences et des limitations spécifiques relatives à la définition des mappages d'inventaire de ressources. Pour plus d'informations, consultez [Mappages d'inventaire pour les groupes de protection de stratégie de stockage](#).

Groupes de protection de stratégie de stockage et machines virtuelles non protégées

Votre environnement, l'implémentation de vos stratégies de stockage et la configuration des banques de données et des machines virtuelles à protéger doivent répondre aux conditions préalables des groupes de protection de stratégie de stockage. Dans le cas contraire, Site Recovery Manager peut ne pas protéger toutes les machines virtuelles d'un groupe de protection de stratégie de stockage.

Pour en savoir plus sur les conditions préalables à satisfaire pour la protection de stratégie de stockage, reportez-vous à la section [Conditions préalables pour les groupes de protection de stratégie de stockage](#).

Par exemple, les machines virtuelles qui ne sont pas associées à une stratégie de stockage peut résider dans une banque de données balisée avec des machines virtuelles associées à une stratégie de stockage. Si vous incluez la stratégie de stockage à un groupe protection de stratégie de stockage, car ces machines virtuelles ne sont pas associées à cette stratégie de stockage, Site Recovery Manager ne les protège pas.

Les machines virtuelles non protégées peuvent s'afficher dans les groupes de protection de stratégie de stockage pour des raisons autres que la non-association des machines virtuelles à la stratégie de stockage correspondante. Pour obtenir des descriptions des autres circonstances dans lesquelles des machines virtuelles non protégées peuvent s'afficher dans des groupes de protection de stratégie de stockage, reportez-vous à la section [Limitations des groupes de protection de stratégie de stockage](#).

Si un groupe de protection de stratégie de stockage inclut des machines virtuelles non protégées, celles-ci s'affichent dans la vue **Objets associés > Machines virtuelles** du groupe de protection de stratégie de stockage. Le groupe de protection s'affiche dans un état d'erreur.

La manière dont Site Recovery Manager gère les machines virtuelles non protégées dépend du type de récupération que vous exécutez.

Note Vous pouvez uniquement tenter de protéger des machines virtuelles non protégées dans des groupes de protection de stratégie de stockage sur lesquels vous n'avez jamais exécuté de récupération. Si vous avez exécuté une opération de récupération avec succès ou non sur un groupe de protection de stratégie de stockage contenant des machines virtuelles non protégées, vous devez supprimer celles-ci du groupe de protection de stratégie de stockage.

- Si vous exécutez un test de récupération sur un groupe de protection de stratégie de stockage contenant des machines virtuelles non protégées, l'opération échoue avec des erreurs. Si un test de récupération échoue en raison de machines virtuelles non répliquées, exécutez un nettoyage avant de tenter de protéger ou de supprimer les machines virtuelles non protégées, puis réexécutez le test. Après le nettoyage, si vous n'avez jamais tenté d'exécuter une récupération sur ce groupe de protection, tentez de corriger la protection des machines virtuelles affectées, par exemple en les associant à la stratégie de stockage correspondante ou en déplaçant les fichiers de la machine virtuelles d'une banque de données non répliquées vers une banque de données répliquée.
- Si vous avez exécuté une migration planifiée sur un groupe de protection de stratégie de stockage contenant des machines virtuelles non protégées, l'opération échoue et le plan de récupération affiche l'état Récupération incomplète. Pendant l'étape de désactivation de la migration planifiée, des machines virtuelles non protégées sur le site protégé peuvent empêcher Site Recovery Manager de passer le stockage en lecture seule ou bien des machines virtuelles peuvent perdre l'accès à leurs données. Si un groupe de protection est dans l'état Récupération incomplète, vous devez supprimer les machines virtuelles non protégées de la banque de données protégée et les dissocier de la stratégie de stockage.
- Si vous exécutez une récupération d'urgence sur un groupe de protection de stratégie de stockage contenant des machines virtuelles non protégées, l'opération réussit, mais Site

Recovery Manager ne récupère pas les machines virtuelles non protégées. Lorsque le site protégé est à nouveau en ligne et que vous tentez d'exécuter une migration planifiée pour terminer la récupération, la migration planifiée échoue si les machines virtuelles non protégées sont toujours présentes sur le site protégé. Si un groupe de protection est dans l'état Récupération incomplète, vous devez supprimer les machines virtuelles non protégées de la banque de données protégée et les dissocier de la stratégie de stockage.

Protection d'une machine virtuelle chiffrée

Vous pouvez protéger et récupérer des machines virtuelles chiffrées à l'aide d'un groupe de protection de réplication basée sur la baie, d'un groupe de protection vSphere Replication ou d'un groupe de protection de stratégie de stockage (SPPG).

Après avoir créé une stratégie de stockage, vous devez modifier son ensemble de règles en appliquant la procédure suivante.

Conditions préalables

- Si vous utilisez un SPPG, remplissez les conditions préalables spécifiées dans [Conditions préalables pour les groupes de protection de stratégie de stockage](#)
- Vérifiez que les sites de récupération et les sites protégés utilisent un serveur gestionnaire de clés (KMS) ou que les clusters du serveur gestionnaire de clés des deux sites utilisent les clés de chiffrement communes. Pour plus d'informations sur la configuration d'un cluster de serveur gestionnaire de clés, reportez-vous à la documentation *VMware vSphere ESXi and vCenter Server 6.7*.

Procédure

- 1 Sur la page **Ensemble de règles** de l'assistant **Stratégie de stockage de VM**, sélectionnez **Utiliser des ensembles de règles dans la stratégie de stockage** et vérifiez que l'option de remplacement sur balise est sélectionnée pour le type de stockage.
- 2 Cliquez sur **<Ajouter une règle>**, puis sur **Balises de la catégorie**.
- 3 Dans le menu **<Sélectionner une catégorie>**, cliquez sur une catégorie.
- 4 Vérifiez que l'option **Balisé** à l'aide de l'une des valeurs suivantes est sélectionnée pour **Balises de la catégorie**.
- 5 Cliquez sur **Ajouter des balises** et sélectionnez votre balise.

Étape suivante

- 1 Créez un mappage vers la stratégie de stockage et assurez-vous que la stratégie de stockage sur le site de récupération est identique à celle du site protégé. Pour plus d'informations sur la création de mappage de stratégie de stockage, reportez-vous à la section [Sélectionner des mappages de stratégies de stockage](#).

- 2 Créez un groupe de protection de réplication basée sur la baie, un groupe de protection vSphere Replication ou un groupe de protection de stratégie de stockage. Pour plus d'informations sur la création d'un groupe de protection de réplication basée sur la baie, consultez [Créer des groupes de protection de réplication basée sur la baie](#). Pour plus d'informations sur la création d'un groupe de protection vSphere Replication, consultez [Créer des groupes de protection pour vSphere Replication](#). Pour plus d'informations sur la création de groupe de protection de stratégie de stockage, reportez-vous à la section [Créer des groupes de protection de stratégie de stockage](#).

Présentation des états des groupes de protection

Vous pouvez surveiller le statut d'un groupe de protection et déterminer l'opération autorisée dans chaque état.

Tableau 5-1. États des groupes de protection

État	Description
Chargement	S'affiche brièvement lorsque l'interface est en cours de chargement jusqu'à ce que le statut des groupes de protection apparaisse.
OK	Le groupe est inactif. Toutes les machines virtuelles sont dans l'état OK. Vous pouvez modifier le groupe.
Non configuré	Le groupe est inactif. Certaines machines virtuelles peuvent ne pas être dans l'état OK. Vous pouvez modifier le groupe.
Test	Le groupe est utilisé dans un plan qui exécute un test. Vous ne pouvez pas modifier le groupe.
Test terminé	Le groupe est utilisé dans un plan qui exécute un test. Vous ne pouvez pas modifier le groupe. Le groupe revient à l'état OK ou Non configuré une fois le nettoyage terminé.
Nettoyage	Le groupe est utilisé dans un plan qui est en cours de nettoyage après un test. Vous ne pouvez pas modifier le groupe. Le groupe revient à l'état OK ou Non configuré une fois le nettoyage terminé. En cas d'échec du nettoyage, le groupe passe à l'état Test.
Récupération	Le groupe est utilisé dans un plan qui exécute une récupération. Vous ne pouvez pas modifier le groupe. En cas de réussite de la récupération, le groupe passe à l'état Récupéré. En cas d'échec de la récupération, le statut du groupe passe à Partiellement récupéré.

Tableau 5-1. États des groupes de protection (suite)

État	Description
Partiellement récupéré	Le groupe est dans un plan qui a terminé une récupération, mais certaines machines virtuelles n'ont pas été récupérées. Vous pouvez supprimer des machines virtuelles, mais vous ne pouvez ni les configurer, ni les restaurer.
Récupéré	Le groupe est dans un plan qui a correctement terminé une récupération. Vous pouvez supprimer des machines virtuelles, mais vous ne pouvez ni les configurer, ni les restaurer.
Reprotection	Le groupe est utilisé dans un plan qui exécute une reprotection. Vous ne pouvez pas modifier le groupe. Le groupe revient à l'état OK ou Non configuré une fois la reprotection terminée. En cas d'échec de la reprotection, le groupe passe à l'état Partiellement reprotégé.
Partiellement reprotégé	Le groupe est dans un plan dont une reprotection a échoué. Vous pouvez supprimer des machines virtuelles, mais vous ne pouvez ni les configurer, ni les restaurer.
Configuration de la protection	Des opérations de protection sont en cours sur des machines virtuelles du groupe.
Suppression de la protection	La suppression de la protection des machines virtuelles du groupe est en cours.
Restauration d'espaces réservés	Une création d'espaces réservés est en cours pour les machines virtuelles du groupe.
Opérations en cours	Une combinaison d'au moins une opération de configuration de la protection et d'une opération de suppression de la protection est en cours dans le groupe.

Présentation des états de protection des machines virtuelles

Vous pouvez surveiller le statut d'une machine virtuelle dans un groupe de protection et déterminer l'opération autorisée dans chaque état.

Tableau 5-2. États de protection des machines virtuelles

État	Description
VM à espace réservé non trouvée	Vous avez supprimé la machine virtuelle réservée. L'icône Restaurer l'espace réservé est activée.
VM protégée initiale introuvable	Vous avez supprimé la machine virtuelle de production initiale après le basculement et avant la reprotection. L'icône Restaurer l'espace réservé est activée.

Tableau 5-2. États de protection des machines virtuelles (suite)

État	Description
Le <i>nom</i> de la banque de données utilisé par la VM est manquant dans le groupe	La machine virtuelle requiert une banque de données qui n'est pas dans le groupe de protection. Modifiez le groupe de protection pour inclure la banque de données.
Le <i>nom</i> de la banque de données utilisé par la VM est protégé dans un groupe différent	La machine virtuelle requiert une banque de données qui est dans un autre groupe de protection. Supprimez la banque de données de l'autre groupe de protection et modifiez le groupe de protection actuel pour y inclure la banque de données. Vous ne pouvez pas inclure une banque de données dans deux groupes de protection.
Périphérique introuvable : <i>nom du périphérique</i>	Vous avez ajouté un disque ou un périphérique non répliqué à une machine virtuelle protégée. Vous devez modifier la réplication de la machine virtuelle pour inclure ou supprimer le périphérique de la protection.
Mappage manquant : <i>Nom</i> du dossier ; <i>nom</i> du réseau ; <i>nom</i> du pool de ressources	Les mappages de dossiers, de ressources ou réseau ne sont pas configurés pour cette machine virtuelle. Corrigez les mappages d'inventaire pour le site ou configurez manuellement la machine virtuelle.
Erreur de création de VM à espace réservé : <i>chaîne d'erreur du serveur</i>	Erreur au cours de la création de la machine virtuelle réservée.
OK	La machine virtuelle protégée existe et le statut du fournisseur et de l'espace réservé sont propres.
Non valide : <i>erreur</i>	La machine virtuelle n'est pas valide parce que la banque de données interne n'est pas répliquée ou la machine virtuelle a été supprimée. La chaîne d'erreur du serveur contient les détails. Supprimez manuellement la protection des machines virtuelles.
Non configuré	Vous avez ajouté une nouvelle machine virtuelle après avoir créé le groupe de protection. Utilisez Tout configurer pour configurer la protection sur la machine virtuelle.
Erreur : <i>erreur</i>	L'erreur peut être l'une des erreurs suivantes : <ul style="list-style-type: none"> ■ Le pool de ressources, le dossier ou le réseau du site de récupération ne sont pas dans le même centre de données. ■ Banque de données réservée introuvable. ■ Toutes les erreurs de vCenter Server qui se sont produites lors de la création de l'espace réservé, telles que des problèmes de connexion ou d'autorisation.
Configuration de la protection	Opération de machine virtuelle.
Suppression de la protection	Opération de machine virtuelle.

Tableau 5-2. États de protection des machines virtuelles (suite)

État	Description
Restauration de l'espace réservé	Opération de machine virtuelle.
Chargement	S'affiche brièvement lorsque l'interface est en cours de chargement jusqu'à ce que le statut de la machine virtuelle apparaisse.
Conflit de mappage	Site Recovery Manager Server a signalé un conflit d'inventaire. Le pool de ressources et le dossier de la machine virtuelle sont dans centres de données différents.
Erreur de réplication	vSphere Replication signale une erreur concernant la machine virtuelle.
Avertissement de réplication	vSphere Replication signale un avertissement concernant la machine virtuelle.

Création de groupes de protection

Créez des groupes de protection pour permettre à Site Recovery Manager de protéger les machines virtuelles.

Lorsque vous créez des groupes de protection, attendez que les opérations se terminent comme prévu. Vérifiez que Site Recovery Manager crée le groupe de protection et que la protection des machines virtuelles du groupe a réussi.

Vous pouvez organiser les groupes de protection dans les dossiers.

Note Le nom du groupe de protection doit être différent du nom du dossier sélectionné.

Créer des groupes de protection pour vSphere Replication

Créez des groupes de protection pour vSphere Replication afin de protéger les machines virtuelles pour lesquelles vous avez configuré vSphere Replication.

Conditions préalables

Vérifiez que vous avez configuré vSphere Replication sur les machines virtuelles.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Groupes de protection**, puis cliquez sur **Nouveau** pour créer un groupe de protection.

- 4 Sur la page **Nom et direction**, entrez un nom et une description pour le groupe de protection, sélectionnez une direction et cliquez sur **Suivant**.
- 5 Dans le volet **Type de groupe de protection**, sélectionnez **VM individuelles (vSphere Replication)** et cliquez sur **Suivant**.
- 6 Dans la liste, sélectionnez les machines virtuelles à ajouter au groupe de protection et 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.

- 7 Sur la page **Plan de récupération**, vous pouvez éventuellement ajouter le groupe de protection à un plan de récupération.

Option	Description
Ajouter au plan de récupération existant	Ajoute le nouveau groupe de protection à un plan de récupération existant.
Ajouter au nouveau plan de récupération	Ajoute le groupe de protection à un nouveau plan de récupération. Si vous sélectionnez cette option, vous devez entrer un nom de plan de récupération.
Ne pas ajouter maintenant au plan de récupération	Sélectionnez cette option si vous ne souhaitez pas ajouter le groupe de protection à un plan de récupération.

- 8 Passez vos paramètres en revue et cliquez sur **Terminer**.

Résultats

Vous pouvez surveiller la progression de la création du groupe de protection dans l'onglet **Groupe de protection**.

- Si Site Recovery Manager a correctement appliqué les mappages d'inventaire aux machines virtuelles protégées, l'état de protection du groupe de protection est **OK**.
- Si vous n'avez pas configuré les mappages d'inventaire ou si Site Recovery Manager n'a pas pu les appliquer, l'état de protection du groupe de protection est **Non configuré**.

Étape suivante

Si l'état de protection du groupe de protection est **Non configuré**, appliquez les mappages d'inventaire aux machines virtuelles :

- Pour appliquer des mappages d'inventaire à l'échelle du site ou pour vérifier la validité des mappages d'inventaire déjà définis, reportez-vous à [Configurer les mappages d'inventaire](#). Pour appliquer ces mappages à l'ensemble des machines virtuelles, consultez [Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

- Pour appliquer de manière individuelle des mappages d'inventaire à chaque machine virtuelle du groupe de protection, consultez [Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

Créer des groupes de protection de stratégie de stockage

Créez des groupes de protection de stratégie de stockage afin de protéger les machines virtuelles qui sont associées à une stratégie de stockage.

Conditions préalables

Vérifiez que vous avez satisfait les conditions requises dans [Conditions préalables pour les groupes de protection de stratégie de stockage](#) et examiné [Limitations des groupes de protection de stratégie de stockage](#).

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Groupes de protection**, puis cliquez sur **Nouveau** pour créer un groupe de protection.
- 4 Sur la page **Nom et direction**, entrez un nom et une description pour le groupe de protection, sélectionnez une direction et cliquez sur **Suivant**.
- 5 Sur la page **Type de groupe de protection**, sélectionnez **Stratégies de stockage (réplication basée sur la baie)** et cliquez sur **Suivant**.
- 6 Sélectionnez les stratégies de stockage à ajouter au groupe de protection et cliquez sur **Suivant**.
- 7 Sur la page **Plan de récupération**, vous pouvez éventuellement ajouter le groupe de protection à un plan de récupération.

Option	Description
Ajouter au plan de récupération existant	Ajoute le nouveau groupe de protection à un plan de récupération existant.
Ajouter au nouveau plan de récupération	Ajoute le groupe de protection à un nouveau plan de récupération. Si vous sélectionnez cette option, vous devez entrer un nom de plan de récupération.
Ne pas ajouter maintenant au plan de récupération	Sélectionnez cette option si vous ne souhaitez pas ajouter le groupe de protection à un plan de récupération.

8 Passez vos paramètres en revue et cliquez sur **Terminer**.

Vous pouvez surveiller la progression de la création du groupe de protection dans l'onglet **Groupe de protection**.

- Si Site Recovery Manager a protégé correctement toutes les machines virtuelles associées à la stratégie de stockage, l'état de protection du groupe de protection est **OK**.
- Si Site Recovery Manager ne peut pas protéger toutes les machines virtuelles associées à la stratégie de stockage, l'état de protection du groupe de protection est **Non configuré**.

Étape suivante

Si l'état de protection du groupe de protection est **Non configuré**, vérifiez que les conditions préalables sont remplies dans [Conditions préalables pour les groupes de protection de stratégie de stockage](#), consultez la section [Limitations des groupes de protection de stratégie de stockage](#), modifiez l'implémentation de la stratégie de stockage comme il se doit et tentez de recréer le groupe de protection.

Créer des groupes de protection de réplication basée sur la baie

Créez des groupes de protection de réplication basée sur la baie pour protéger les machines virtuelles pour lesquelles vous avez configuré la réplication basée sur la baie.

Conditions préalables

Vérifiez que vous avez inclus des machines virtuelles dans les banques de données pour lesquelles vous avez configuré la réplication basée sur la baie.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Groupes de protection**, puis cliquez sur **Nouveau** pour créer un groupe de protection.
- 4 Sur la page **Nom et direction**, entrez un nom et une description pour le groupe de protection, sélectionnez une direction et cliquez sur **Suivant**.
- 5 Dans le volet **Type de groupe de protection**, sélectionnez **Groupes de banque de données (réplication basée sur la baie)**, sélectionnez une paire de baies, puis cliquez sur **Suivant**.
- 6 Sélectionnez les groupes de banques de données à ajouter au groupe de protection et cliquez sur **Suivant**.

Lorsque vous sélectionnez un groupe de banques de données, les machines virtuelles contenues dans le groupe apparaissent dans la table **Machines virtuelles**.

- 7 Sur la page **Plan de récupération**, vous pouvez éventuellement ajouter le groupe de protection à un plan de récupération.

Option	Description
Ajouter au plan de récupération existant	Ajoute le nouveau groupe de protection à un plan de récupération existant.
Ajouter au nouveau plan de récupération	Ajoute le groupe de protection à un nouveau plan de récupération. Si vous sélectionnez cette option, vous devez entrer un nom de plan de récupération.
Ne pas ajouter maintenant au plan de récupération	Sélectionnez cette option si vous ne souhaitez pas ajouter le groupe de protection à un plan de récupération.

- 8 Passez vos paramètres en revue et cliquez sur **Terminer**.

Vous pouvez surveiller la progression de la création du groupe de protection dans l'onglet **Groupe de protection**.

- Si Site Recovery Manager a correctement appliqué les mappages d'inventaire aux machines virtuelles protégées, l'état de protection du groupe de protection est **OK**.
- Si vous n'avez pas configuré les mappages d'inventaire ou si Site Recovery Manager n'a pas pu les appliquer, l'état de protection du groupe de protection est **Non configuré**.

Étape suivante

Si l'état de protection du groupe de protection est **Non configuré**, appliquez les mappages d'inventaire aux machines virtuelles :

- Pour appliquer des mappages d'inventaire à l'échelle du site ou pour vérifier la validité des mappages d'inventaire déjà définis, reportez-vous à [Configurer les mappages d'inventaire](#). Pour appliquer ces mappages à l'ensemble des machines virtuelles, consultez [Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).
- Pour appliquer de manière individuelle des mappages d'inventaire à chaque machine virtuelle du groupe de protection, consultez [Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

Organiser des groupes de protection en dossiers

Vous pouvez créer des dossiers pour y organiser des groupes de protection.

L'organisation de groupes de protection en dossiers est utile si vous avez un grand nombre de groupes de protection. Vous pouvez limiter l'accès aux groupes de protection en plaçant ces derniers dans des dossiers et en attribuant différentes autorisations aux dossiers pour différents utilisateurs ou différents groupes. Pour savoir comment attribuer des autorisations aux dossiers, reportez-vous à [Attribuer des rôles et des autorisations Site Recovery Manager](#).

Procédure

- 1 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 2 Cliquez sur l'onglet **Groupes de protection** et, dans le volet de gauche, cliquez avec le bouton droit sur **Groupes de Protection**, puis cliquez sur **Nouveau dossier**.
- 3 Entrez un nom pour le nouveau dossier, puis cliquez sur **Ajouter**.
- 4 Ajoutez au dossier des groupes de protection nouveaux ou existants.

Option	Description
Créer un groupe de protection	Cliquez avec le bouton droit sur le dossier et sélectionnez Nouveau groupe de protection .
Ajouter un groupe de protection existant	Cliquez avec le bouton droit sur un groupe de protection dans l'arborescence d'inventaire et sélectionnez Déplacer . Sélectionnez un dossier cible et cliquez sur Déplacer .

Ajouter et supprimer des groupes de banques de données ou des machines virtuelles dans un groupe de protection

Vous pouvez ajouter et supprimer des groupes de banques de données dans un groupe de protection de réplication basée sur la baie, ou bien ajouter et supprimer des machines virtuelles dans un groupe de protection vSphere Replication. Vous pouvez également modifier le nom et la description d'un groupe de protection de réplication basée sur la baie ou d'un groupe de protection vSphere Replication.

Note Vous ne pouvez pas modifier des groupes de protection de stratégie de stockage après leur création initiale. Vous ajoutez des machines virtuelles à un groupe de protection de stratégie de stockage existant ou vous les en supprimez en modifiant les associations de stratégies de stockage des machines virtuelles dans les banques de données protégées. Vous pouvez ajouter ou supprimer des machines virtuelles dans un groupe de protection de stratégie de stockage uniquement si la récupération n'a jamais été exécutée sur le groupe de protection. Pour plus d'informations, consultez [Limitations des groupes de protection de stratégie de stockage](#).

Conditions préalables

Vous avez créé un groupe de protection de réplication basée sur la baie ou un groupe de protection vSphere Replication.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Cliquez sur l'onglet **Groupes de protection**, cliquez avec le bouton droit sur un groupe de protection, puis cliquez sur **Modifier**.
- 4 (Facultatif) Modifiez le nom ou la description du groupe de protection et cliquez sur **Suivant**.
- 5 Cliquez sur **Suivant**.
- 6 Modifiez les groupes de banques de données ou les machines virtuelles contenus dans le groupe de protection.
 - Pour les groupes de protection basés sur la baie, sélectionnez ou désélectionnez des groupes de banques de données pour les ajouter ou les supprimer du groupe de protection et cliquez sur **Suivant**.
 - Pour les groupes de protection vSphere Replication, sélectionnez ou désélectionnez des machines virtuelles pour les ajouter ou les supprimer du groupe de protection et cliquez sur **Suivant**.
- 7 Consultez les paramètres, puis cliquez sur **Suivant** pour appliquer les modifications.
 Vous ne pouvez pas rétablir ou annuler des modifications pendant que Site Recovery Manager met à jour le groupe de protection.
- 8 Cliquez sur **Terminer**.

Résultats

Si vous avez configuré les mappages d'inventaire à l'échelle du site, Site Recovery Manager applique les mappages aux machines virtuelles que vous avez ajoutées au groupe de protection. En cas de succès, l'état des machines virtuelles est **OK**.

Note Lorsque vous ajoutez des banques de données ou des machines virtuelles à un groupe de protection, les mappages d'inventaire s'appliquent uniquement aux nouvelles machines virtuelles. Ainsi, si vous modifiez les mappages d'inventaire, puis ajoutez une banque de données à un groupe de protection qui est dans l'état **OK**, Site Recovery Manager applique les nouveaux mappages aux machines virtuelles nouvellement protégées qui se trouvent dans la nouvelle banque de données. Les machines virtuelles protégées précédemment continuent d'utiliser les anciens mappages.

Si vous n'avez pas configuré les mappages d'inventaire à l'échelle du site, l'état du groupe de protection est **Non configuré** et l'état des nouvelles machines virtuelles est **Mappage manquant**.

Étape suivante

Si l'état du groupe de protection est `Non configuré` et l'état des nouvelles machines virtuelles est `Mappage manquant`, appliquez des mappages d'inventaire aux machines virtuelles :

- Pour appliquer des mappages d'inventaire à l'échelle du site ou pour vérifier la validité des mappages d'inventaire déjà définis, reportez-vous à [Configurer les mappages d'inventaire](#). Pour appliquer ces mappages à l'ensemble des machines virtuelles, consultez [Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).
- Pour appliquer de manière individuelle des mappages d'inventaire à chaque machine virtuelle du groupe de protection, consultez [Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication

Si l'état de protection d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication est `Non configuré`, vous pouvez configurer la protection de l'ensemble des machines virtuelles non configurées en utilisant les mappages d'inventaire existants à l'échelle du site, en une seule étape.

L'état d'un groupe de protection peut être `Non configuré` pour plusieurs raisons :

- Vous n'avez pas configuré les mappages d'inventaire à l'échelle du site avant d'avoir créé le groupe de protection.
- Vous n'avez pas configuré les mappages de banques de données réservées avant d'avoir créé le groupe de protection.
- Vous avez ajouté des machines virtuelles à un groupe de protection après l'avoir créé.
- Des machines virtuelles ont perdu leur protection, vraisemblablement parce que vous les avez reconfigurées après les avoir ajoutées à un groupe de protection. Vous avez ajouté ou supprimé, par exemple, des disques ou des périphériques virtuels.

Conditions préalables

- Configurez ou reconfigurez des mappages d'inventaire à l'échelle du site. Pour sélectionner des mappages d'inventaire, consultez [Configurer les mappages d'inventaire](#).
- Configurez ou reconfigurez des mappages de banques de données réservées. Pour configurer une banque de données à espace réservé, consultez [Sélectionner une banque de données à espace réservé](#).

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Groupes de protection**, puis sur un groupe de protection et, dans le volet de droite, cliquez sur l'onglet **Machines virtuelles**.
- 4 Cliquez sur le bouton **Configurer toutes les VM**.

Au moins une machine virtuelle du groupe de protection doit être dans l'état Non configuré pour que le bouton **Configurer toutes les VM** soit actif.
- 5 Cliquez sur **Oui** pour confirmer que vous souhaitez appliquer des mappages d'inventaire à toutes les machines virtuelles non configurées.
- 6 Surveillez l'état des machines virtuelles. Si Site Recovery Manager n'a pas pu appliquer certains ou tous les mappages d'inventaire, ou s'il n'a pas pu créer des espaces réservés pour les machines virtuelles, vous pouvez effectuer des actions correctives.

État	Action
OK	Aucune action n'est requise
Non configuré ou mappage manquant	Vérifiez les mappages d'inventaire et cliquez à nouveau sur Configurer toutes les VM
Erreur de création de la VM à espace réservé	<p>Vérifiez le mappage de banque de données à espace réservé et essayez de recréer les machines virtuelles à espace réservé.</p> <ul style="list-style-type: none"> ■ Pour recréer l'espace réservé d'une machine virtuelle individuelle, cliquez avec le bouton droit sur une machine virtuelle et sélectionnez Recréer l'espace réservé. ■ Pour recréer l'espace réservé pour plusieurs machines virtuelles, cliquez avec le bouton droit sur le groupe de protection et sélectionnez Restaurer les VM réservées.

Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication

Il est possible de configurer de manière individuelle les mappages pour les machines virtuelles d'un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication. Vous pouvez ainsi utiliser différentes ressources sur le site de récupération pour différentes machines virtuelles.

Vous pouvez configurer de manière individuelle des mappages d'inventaire sur des machines virtuelles dans un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication, même si vous avez configuré des mappages d'inventaire à l'échelle du site. Dans ce cas, vous pouvez supprimer la protection d'une machine virtuelle individuelle et configurer les mappages de dossiers et de ressources pour remplacer les mappages à l'échelle du site. Vous pouvez modifier le mappage réseau d'une machine virtuelle individuelle sans supprimer la protection.

Vous ne pouvez pas spécifier des banques de données réservées pour des machines virtuelles individuelles. Vous devez mapper les banques de données du site protégé aux banques de données réservées du site de récupération au niveau du site. Pour configurer une banque de données à espace réservé, consultez [Sélectionner une banque de données à espace réservé](#).

Conditions préalables

Vous avez créé un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Groupes de protection**, puis cliquez sur le groupe de protection qui inclut la machine virtuelle à configurer.
- 4 Dans le volet de droite, cliquez sur l'onglet **Machines virtuelles**.
- 5 Cliquez avec le bouton droit sur la machine virtuelle, puis cliquez sur **Configurer la protection**.
- 6 Pour configurer des mappages d'inventaire en développant les ressources, cochez la case **Remplacer les mappages de sites** et sélectionnez des ressources sur le site de récupération. Cliquez sur **OK**.

Vous pouvez modifier uniquement les mappages de dossiers, de pools de ressources et réseau.

- 7 Surveillez l'état des machines virtuelles. Si Site Recovery Manager n'a pas pu appliquer certains ou tous les mappages d'inventaire, ou s'il n'a pas pu créer des espaces réservés pour les machines virtuelles, vous pouvez effectuer des actions correctives.

État	Action
OK	Aucune action n'est requise
Non configuré ou Mappage manquant	Cliquez à nouveau sur Configurer la protection et vérifiez les mappages d'inventaire.
Erreur de création de la VM à espace réservé	Vérifiez le mappage de banque de données à espace réservé au niveau du site, cliquez sur la machine virtuelle avec le bouton droit de la souris, puis cliquez sur Recréer l'espace réservé .

Modification des paramètres d'une machine virtuelle dans un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication

La modification des paramètres d'une machine virtuelle protégée et l'ajout ou la modification de périphériques de stockage, tels que des disques durs ou des lecteurs de DVD, peuvent affecter la protection de cette machine virtuelle.

Note Vous pouvez modifier les paramètres d'une machine virtuelle que vous protégez dans un groupe de protection de stratégie de stockage.

Si vous utilisez la réplication basée sur la baie, l'ajout ou la modification de périphériques sur une machine virtuelle protégée affecte la protection suivant le mode de création du périphérique.

- Si le nouveau périphérique se trouve sur une banque de données répliquée qui ne fait pas partie d'un groupe de protection, le groupe de protection contenant la machine virtuelle passe à l'état **Non configuré**. Reconfigurez le groupe de protection afin d'ajouter la banque de données contenant le nouveau périphérique au groupe de protection.
- Si le nouveau périphérique se trouve sur une banque de données répliquée protégée par un autre groupe de protection, la protection de la machine virtuelle n'est pas valide.
- Si le nouveau périphérique se trouve sur une banque de données non répliquée, vous devez répliquer cette dernière ou supprimer la protection du périphérique.
- Si vous utilisez Storage vMotion pour déplacer une machine virtuelle vers une banque de données non répliquée ou vers une banque de données répliquée sur une baie pour laquelle Site Recovery Manager ne possède pas d'adaptateur de réplication de stockage (SRA), la protection de la machine virtuelle n'est pas valide. Vous pouvez utiliser Storage vMotion pour transférer une machine virtuelle vers une banque de données faisant partie d'un autre groupe de protection.

Si vous ajoutez un périphérique à une machine virtuelle que vous protégez en utilisant vSphere Replication, vous devez reconfigurer vSphere Replication sur la machine virtuelle pour sélectionner les options de réplication pour le nouveau périphérique. Pour plus d'informations sur la reconfiguration des paramètres de vSphere Replication, reportez-vous à la documentation de vSphere Replication à l'adresse <https://docs.vmware.com/fr/vSphere-Replication/index.html>.

Après avoir modifié les machines virtuelles dans des groupes de protection basés sur la baie ou des groupes de protection vSphere Replication, vous devez reconfigurer la protection de toutes les machines virtuelles dont l'état est `Non configuré`, `Périphérique non trouvé`, `Périphériques non résolus` ou `Mappage manquant`. Reportez-vous à la section [Appliquer les mappages d'inventaire à tous les membres d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#) et [Configurer des mappages d'inventaire pour une machine virtuelle individuelle d'un groupe de protection basé sur la baie ou d'un groupe de protection vSphere Replication](#).

Suppression de la protection d'une machine virtuelle

Vous pouvez souhaiter supprimer la protection d'une machine virtuelle pour différentes raisons : La suppression de la protection d'une machine virtuelle affecte les groupes de protection de façon différente.

La suppression de la protection supprime la machine virtuelle réservée sur le site de récupération. Si vous supprimez la protection d'une machine virtuelle dans une réplication basée sur la baie ou un groupe de protection vSphere Replication, les états de la machine virtuelle et du groupe de protection sont définis sur `Non configuré`. L'exécution d'un plan de récupération contenant le groupe de protection réussit pour les machines virtuelles protégées, mais Site Recovery Manager ne récupère pas les machines virtuelles ou les groupes de protection dont l'état est `Non configuré`. Si vous exécutez une migration planifiée, le plan passe à l'état `Récupération incomplète`.

Note Vous ne pouvez pas supprimer temporairement la protection des machines virtuelles dans des groupes de protection de stratégie de stockage.

Dans une réplication basée sur la baie, il existe une distinction entre la protection de Site Recovery Manager d'une machine virtuelle et la gestion de stockage de Site Recovery Manager pour cette machine virtuelle. Si vous supprimez la protection d'une machine virtuelle dans un groupe de protection de réplication basée sur la baie, Site Recovery Manager ne récupère plus la machine virtuelle, mais continue à surveiller et à gérer le stockage de ses fichiers.

Vous pouvez supprimer la protection d'une machine virtuelle pour différentes raisons :

- Vous utilisez vSphere Replication et vous souhaitez exclure une machine virtuelle protégée dans un groupe de protection.
- Vous utilisez la réplication basée sur la baie, et une personne déplace une machine virtuelle que vous ne souhaitez pas protéger vers une banque de données répliquée. Si vous supprimez la protection de la machine virtuelle, le groupe de protection affiche l'état `Non`

configuré. Le test de récupération et la migration planifiée échouent pour l'ensemble du groupe. La récupération d'urgence réussit, mais uniquement pour les machines virtuelles protégées du groupe et certaines opérations sont ignorées sur le site protégé. Le plan de récupération passe à l'état *Récupération requise*. Dans ce cas, déplacez la machine virtuelle hors de la banque de données protégée.

- Vous utilisez la réplication basée sur la baie et une machine virtuelle dispose de périphériques qui sont stockés sur une banque de données non répliquée. Vous pouvez supprimer la protection de la machine virtuelle de façon que la récupération s'effectue correctement pour toutes les autres machines virtuelles du groupe pendant que vous déplacez les fichiers de périphériques.

La suppression de la protection d'une machine virtuelle affecte les groupes de protection différemment, selon que vous utilisez une réplication basée sur la baie ou vSphere Replication.

- Si vous supprimez la protection d'une machine virtuelle qui fait partie d'un groupe de protection de réplication basée sur la baie, vous devez déplacer 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 que Site Recovery Manager a inclus dans un groupe de banques de données, le test de récupération et la migration planifiée échouent pour l'ensemble du groupe de banques de données. La récupération d'urgence réussit, mais uniquement pour les machines virtuelles protégées du groupe de banques de données et vous devez déplacer la machine virtuelle non protégée avant de pouvoir exécuter une migration planifiée pour terminer la récupération.
- Si vous désactivez vSphere Replication sur une machine virtuelle que vous avez incluse dans un groupe de protection, la récupération échoue pour cette machine virtuelle, mais réussit pour toutes les machines virtuelles configurées correctement dans le groupe de protection. Vous devez supprimer la protection de la machine virtuelle et supprimer celle-ci du groupe de protection, soit en modifiant le groupe de protection, soit en cliquant sur **Supprimer la VM**. Reportez-vous à [Ajouter et supprimer des groupes de banques de données ou des machines virtuelles dans un groupe de protection](#).

Supprimer la protection d'une machine virtuelle

Vous pouvez supprimer temporairement la protection d'une machine virtuelle répliquée dans une réplication basée sur la baie ou un groupe de protection vSphere Replication sans la supprimer de son groupe de protection.

Note Vous ne pouvez pas supprimer temporairement la protection des machines virtuelles dans des groupes de protection de stratégie de stockage.

Procédure

- 1 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 2 Cliquez sur l'onglet **Groupes de protection**, sélectionnez un groupe de protection et, dans le volet de droite, cliquez sur l'onglet **Machines virtuelles**.
- 3 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Supprimer la protection**.
- 4 Cliquez sur **Oui** pour confirmer la suppression de la protection de la machine virtuelle.

Création, test, et exécution de plans de récupération

6

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 pour gérer une migration planifiée des services à partir du site protégé vers le site de récupération pour l'ensemble de l'organisation, et un autre ensemble de plans pour chaque département. Dans cet exemple, avoir ces plans de récupération différents référençant un groupe de protection vous permet de choisir la façon d'effectuer la récupération.

Vous ne pouvez exécuter qu'un seul plan de récupération à la fois pour récupérer un groupe de protection particulier. Si vous testez ou exécutez un plan de récupération avec un groupe de protection qui est partagé dans d'autres plans de récupération, les autres plans de récupération modifient l'état du groupe de protection sur `Groupes de protection en cours d'utilisation` et vous ne pouvez pas les exécuter.

- **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. Si le site protégé subit un événement imprévu pouvant entraîner une perte de données, vous pouvez également exécuter un plan de récupération dans des circonstances imprévues.

- **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.

- **Exécution d'une récupération test 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.

- **Créer, tester et exécuter un plan de récupération**

Vous pouvez personnaliser les actions de Site Recovery Manager lors de la récupération en créant, testant et exécutant des plans de récupération.

- **Désactiver la récupération d'une machine virtuelle dans un groupe de protection de stratégie de stockage**

Vous pouvez désactiver la récupération d'une machine virtuelle faisant partie d'un groupe de protection de stratégie de stockage sans la supprimer du groupe.

- **Désactiver la récupération d'un groupe de cohérence dans un groupe de protection de stratégie de stockage**

Vous pouvez désactiver la récupération d'un groupe de cohérence faisant partie d'un groupe de protection de stratégie de stockage sans le supprimer du groupe.

- **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 un rapport 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.

- **Supprimer un plan de récupération**

Si vous n'avez pas besoin d'un plan de récupération, vous pouvez le supprimer.

- **Présentation des états des plans de récupération**

Vous pouvez surveiller le statut d'un plan de récupération et déterminer l'opération autorisée dans chaque état. Les états des groupes de protection au sein d'un plan de récupération déterminent l'état du plan.

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 et pour les récupérations réelles. 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 et conserve les modifications accumulées dans les journaux sur les disques de la machine virtuelle.

Si vous utilisez une réplication basée sur la baie, lorsque vous testez un plan de récupération, les machines virtuelles sur le site protégé sont toujours répliquées sur les fichiers de disque des machines virtuelles de réplication sur le site de récupération. Lors d'un test de récupération, la baie crée un snapshot des volumes hébergeant les fichiers de disque des machines virtuelles sur le site de récupération. La réplication de la baie continue normalement alors que le test est en cours. Lorsque vous effectuez un nettoyage après l'exécution d'un test, la baie supprime les snapshots qui ont été créés précédemment dans le cadre du workflow du test 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.

Avant d'exécuter un basculement ou un autre test, vous devez exécuter avec succès une opération de nettoyage. Reportez-vous à [Nettoyage après l'essai d'un plan de récupération](#).

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

Tester les réseaux et les réseaux de centre de données

Lorsque vous testez un plan de récupération, Site Recovery Manager peut créer un réseau de test 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 isolé 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. Un réseau de test isolé ne recouvre pas les hôtes. Vous devez configurer un réseau de test pour chaque réseau qu'un plan de récupération utilise lors de la récupération.

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.

Un réseau de centre de données est un réseau existant sur le site de récupération. Vous pouvez sélectionner un réseau de centre de données à utiliser comme réseau de test. 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 si le protocole DHCP est configuré correctement. Les autres machines virtuelles peuvent nécessiter des étapes de personnalisation d'adresse IP et de plan de récupération supplémentaire pour appliquer la personnalisation.

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. Si le site protégé subit un événement imprévu pouvant entraîner une perte de données, vous pouvez également exécuter un plan de récupération dans des circonstances imprévues.

Note Lorsque vous exécutez un plan de récupération pour effectuer une migration planifiée et une récupération d'urgence, Site Recovery Manager apporte des modifications (dont l'inversion nécessite beaucoup de temps et de charge de travail) aux deux sites. 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.

Migration planifiée

Au cours d'une migration planifiée, Site Recovery Manager synchronise les données des machines virtuelles sur le site de récupération avec celles du site protégé.

Site Recovery Manager tente d'arrêter normalement les machines protégées, exécute une synchronisation finale afin de ne pas perdre de données, puis met sous tension les machines virtuelles sur le site de récupération.

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.

Récupération d'urgence

Pendant une récupération d'urgence, Site Recovery Manager tente d'abord de synchroniser le stockage. Si cela réussit, Site Recovery Manager utilise l'état du stockage synchronisé pour restaurer les machines virtuelles sur le site de récupération à leur état disponible le plus récent, conformément à l'objectif de point de récupération (RPO) que vous définissez lorsque vous configurez la réplication.

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 pas arrêter les machines virtuelles, Site Recovery Manager va tout de même mettre sous tension les copies sur le site de récupération.

Dans le cas où le site protégé revient en ligne après la récupération d'urgence, le plan de récupération passe à un état incohérent dans lequel les machines virtuelles de production sont en cours d'exécution sur les deux sites. Ce scénario est connu sous le nom de Split-Brain. Site Recovery Manager détecte cet état et vous pouvez relancer le plan pour mettre les machines virtuelles hors tension sur le site protégé. Le plan de récupération revient ensuite à un état cohérent et vous pouvez exécuter la reprotection.

Si Site Recovery Manager détecte que la banque de données d'un site protégé est dans l'état APD (Tous chemins hors service) et que, par conséquent, elle empêche une machine virtuelle de s'éteindre, Site Recovery Manager attend un certain temps avant de tenter 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.

Utilisation de VMware Tools

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. VMware Tools est également utilisé pour l'arrêt normal du système d'exploitation invité des machines virtuelles protégées. C'est pourquoi il est recommandé d'installer 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 sorte qu'il n'attende pas le démarrage de VMware Tools sur les machines virtuelles récupérées et qu'il ignore l'étape d'arrêt du système d'exploitation invité. Reportez-vous à [Modifier les paramètres de récupération](#).

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

Si le site protégé est hors ligne et si Site Recovery Manager ne peut pas effectuer ses tâches en temps opportun, cela fait augmenter le RTO jusqu'à un niveau inacceptable. Dans ce cas, vous pouvez exécuter un plan de récupération avec 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.

À quel moment utiliser la récupération forcée ?

Vous pouvez utiliser la récupération forcée dans les cas où l'infrastructure échoue au niveau du site protégé et où, en conséquence, les machines virtuelles protégées sont ingérables et ne peuvent pas 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.

Forcer la récupération ne termine pas le processus de mise hors tension des machines virtuelles sur le site protégé. En conséquence, un scénario Split-Brain se produit, mais la récupération peut se terminer plus rapidement.

Récupération forcée avec vSphere Replication

Lors de l'exécution de la récupération d'urgence à l'aide de vSphere Replication, Site Recovery Manager prépare le stockage de vSphere Replication à la reprotection et vous n'avez pas besoin de vérifier la mise en miroir comme vous le faites avec la réplication basée sur la baie.

Récupération forcée avec réplication basée sur la baie

Exécuter une récupération d'urgence avec une réplication basée sur la baie lorsque la baie de stockage du site protégé est hors ligne ou indisponible peut affecter 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 alors que le stockage de site protégé est toujours disponible, 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.

Activation de la récupération forcée

Pour sélectionner la récupération forcée lors de l'exécution de la récupération d'urgence, vous devez activer l'option `recovery.forceRecovery` dans Paramètres avancés sur le serveur de Site Recovery Manager du site de récupération. Pour plus d'informations, reportez-vous à la section [Modifier les paramètres de récupération](#).

Dans l'assistant d'**exécution d'un plan de récupération**, vous pouvez sélectionner l'option de récupération forcée uniquement en mode de récupération d'urgence. Cette option n'est pas disponible pour une migration planifiée.

Migration planifiée après une récupération forcée

Lorsque vous exécutez une migration planifiée après l'exécution d'une récupération forcée, l'arrêt de machines virtuelles sur le site protégé risque d'échouer si les banques de données sous-jacentes sont en lecture seule ou ne sont pas disponibles. Dans ce cas, connectez-vous à vCenter Server sur le site protégé et mettez les machines virtuelles hors tension manuellement. Une fois les machines virtuelles hors tension, exécutez de nouveau la migration planifiée.

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 6-1. 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 l'autorisation Site Recovery Manager.Plans de récupération.Test .	Nécessite l'autorisation Site Recovery Manager.Plans de récupération.Récupération .
Effet sur les machines virtuelles du site protégé	aucune	Site Recovery Manager arrête les machines virtuelles dans l'ordre inverse de leur priorité et restaure toutes les machines virtuelles qui sont suspendues sur le site protégé.
Effet sur les machines virtuelles du site de récupération	Si le plan de récupération l'exige, Site Recovery Manager interrompt les machines virtuelles locales. Site Recovery Manager redémarre les machines virtuelles suspendues après avoir nettoyé les résultats du test.	Si le plan de récupération l'exige, Site Recovery Manager interrompt les machines virtuelles locales.

Tableau 6-1. Différences entre test et exécution d'un plan de récupération (suite)

Point de divergence	Tester un plan de récupération	Exécuter un plan de récupération
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 la baie, 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 des sites protégés en cas d'échec.
Réseau	Si vous affectez explicitement les réseaux test, Site Recovery Manager connecte les machines virtuelles récupérées à un réseau test. Si l'attribution réseau de la machine virtuelle est Réseau isolé (créé automatiquement) et qu'il n'existe aucun mappage au niveau du site, Site Recovery Manager attribue les machines virtuelles à des réseaux temporaires qui ne sont connectés à aucun réseau physique.	Site Recovery Manager connecte les machines virtuelles récupérées au réseau de centre de données spécifié par l'utilisateur.
Interruption d'un plan de récupération	Vous pouvez annuler un test à tout moment.	Vous pouvez annuler la récupération à tout moment.

Exécution d'une récupération test 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 **Utiliser un mappage au niveau du site** et qu'aucun mappage n'est défini au niveau du site, alors les machines virtuelles qui sont récupérées entre les hôtes sont placées dans leur propre réseau de test pendant les tests de plan de récupération. Chaque commutateur de test est isolé entre les hôtes. Ainsi, les machines virtuelles d'un même plan de récupération sont isolées à la fin de la récupération test. 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.

Créer, tester et exécuter un plan de récupération

Vous pouvez personnaliser les actions de Site Recovery Manager lors de la récupération en créant, testant et exécutant des plans 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 Organiser des plans de récupération en dossiers

Pour contrôler l'accès de différents utilisateurs ou groupes aux plans de récupération, vous pouvez organiser vos plans de récupération dans des dossiers.

3 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.

4 Tester un plan de récupération

Lorsque vous testez un plan de récupération, Site Recovery Manager exécute les machines virtuelles du plan de récupération sur un réseau de test et sur 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. Vous devez terminer l'opération de nettoyage avant de pouvoir exécuter un basculement ou un autre test.

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 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 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.

8 Annuler un test ou une récupération

Vous pouvez annuler un test du plan de récupération lorsque l'état est Test en cours ou Basculement en cours.

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.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez sur **Nouveau** pour créer un plan de récupération.
- 4 Entrez un nom, une description et une direction pour le plan, sélectionnez un dossier, puis cliquez sur **Suivant**.

Note Le nom du plan de récupération doit être différent du nom du dossier sélectionné.

- 5 Sélectionnez le type de groupe dans le menu.

Option	Action
Groupes de protection pour des VM individuelles ou groupes de banques de données	Sélectionnez cette option pour créer un plan de récupération contenant une réplication basée sur la baie et des groupes de protection vSphere Replication.
Groupes de protection de stratégie de stockage	Sélectionnez cette option pour créer un plan de récupération contenant des groupes de protection de stratégie de stockage. Si vous utilisez un stockage étiré, sélectionnez cette option.

- 6 Sélectionnez un ou plusieurs groupes de protection pour le plan à récupérer et cliquez sur **Suivant**.

- 7 Dans le menu déroulant **Réseau de test**, sélectionnez un réseau à utiliser lors du test de récupération, puis cliquez sur **Suivant**.

S'il n'y a aucun mappage au niveau du site, l'option par défaut **Utiliser un mappage au niveau du site** crée automatiquement un réseau de test isolé.

- 8 Consultez les informations récapitulatives et cliquez sur **Terminer** pour créer le plan de récupération.

Organiser des plans de récupération en dossiers

Pour contrôler l'accès de différents utilisateurs ou groupes aux plans de récupération, vous pouvez organiser vos plans de récupération dans des dossiers.

L'organisation de plans de récupération en dossiers est utile si vous avez un grand nombre de plans de récupérations. Vous pouvez limiter l'accès aux plans de récupération en plaçant ces derniers dans des dossiers et en attribuant différentes autorisations aux dossiers pour différents utilisateurs ou groupes. Pour savoir comment attribuer des autorisations aux dossiers, reportez-vous à [Attribuer des rôles et des autorisations Site Recovery Manager](#).

Procédure

- 1 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 2 Cliquez sur l'onglet **Plans de récupération** et, dans le volet de gauche, cliquez avec le bouton droit sur **Plans de récupération**, puis cliquez sur **Nouveau dossier**.
- 3 Entrez un nom pour le dossier à créer, puis cliquez sur **Ajouter**.
- 4 Ajoutez au dossier des plans de récupération nouveaux ou existants.

Option	Description
Créer un plan de récupération	Cliquez avec le bouton droit sur le dossier et sélectionnez Nouveau plan de récupération .
Ajouter un plan de récupération existant	Cliquez avec le bouton droit sur un plan de récupération dans l'arborescence d'inventaire et cliquez sur Déplacer . Sélectionnez un dossier cible et cliquez sur Déplacer .

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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération, puis cliquez sur **Modifier**.
- 4 (Facultatif) Modifiez le nom ou la description du plan, puis cliquez sur **Suivant**.
Vous ne pouvez pas modifier la direction et l'emplacement du plan de récupération.
- 5 (Facultatif) Sélectionnez ou désélectionnez un ou plusieurs groupes de protection pour les ajouter au plan ou les en supprimer, puis cliquez sur **Suivant**.
- 6 (Facultatif) Dans le menu déroulant, sélectionnez un autre réseau de test sur le site de récupération, puis 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**.

Tester un plan de récupération

Lorsque vous testez un plan de récupération, Site Recovery Manager exécute les machines virtuelles du plan de récupération sur un réseau de test et sur 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 prendre 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 constatez un ralentissement des temps de réponse lorsque vous testez des 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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération, puis cliquez sur **Tester**.

Vous pouvez également exécuter un test en cliquant sur l'icône **Tester** dans la vue **Étapes de récupération** du plan de récupération.

- 4 (Facultatif) Sélectionnez **Répliquer les changements récents vers le site de récupération**.

La sélection de cette case à cocher permet de s'assurer que le site de récupération possède la copie la plus récente des machines virtuelles protégées, mais que la synchronisation peut demander plus de temps.

- 5 Cliquez sur **Suivant**.

- 6 Examinez les informations du test et cliquez sur **Terminer**.

- 7 Cliquez sur l'onglet **Étapes de récupération** dans l'onglet du plan de récupération pour surveiller la progression du test et répondre aux messages.

L'onglet **Étapes de récupération** affiche la progression des étapes individuelles. La tâche Test dans la zone Tâches récentes suit la progression globale.

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. Vous devez terminer l'opération de nettoyage avant de pouvoir exécuter un basculement ou un autre test.

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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération et sélectionnez **Nettoyage**.

Vous pouvez également exécuter un test en cliquant sur l'icône **Nettoyage** dans la vue **Étapes de récupération** du plan de récupération.

- 4 Passez en revue les informations de nettoyage et cliquez sur **Suivant**.

- 5 Cliquez sur **Terminer**.

- 6 (Facultatif) Si le nettoyage se termine avec des erreurs, cochez la case **Forcer le nettoyage** pour ignorer les erreurs au cours de l'opération de nettoyage et relancez le nettoyage. Si nécessaire, exécutez un nettoyage plusieurs fois, jusqu'à ce qu'il se termine sans erreur.

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 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. 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](#).
- Vérifiez que vous avez configuré les mappages d'inventaire complets. Si vous avez configuré uniquement les mappages d'inventaire réservés temporaires et que vous exécutez une migration planifiée avec l'option **Activer l'opération vMotion des VM éligibles**, la migration planifiée échoue, même si les deux sites sont en cours d'exécution.
- Pour utiliser l'option **Activer l'opération vMotion des VM éligibles** avec la migration planifiée, activez vMotion sur les machines virtuelles. Pour obtenir des instructions sur l'activation de vMotion sur les machines virtuelles, reportez-vous à la section [Activer vSphere vMotion pour la migration planifiée](#).

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération, puis cliquez sur **Exécuter**.
- 4 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**.
- 5 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. Si votre baie prend en charge le stockage étiré, cochez la case Activer l'opération vMotion des VM éligibles .
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.

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

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

- 7 Cliquez sur **Suivant**.
- 8 Vérifiez les informations sur la récupération et cliquez sur **Terminer**.
- 9 Pour surveiller la progression des étapes individuelles, cliquez sur le plan de récupération et cliquez sur l'onglet **Étapes de récupération**.

Résultats

Le panneau **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 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.

Conditions préalables

- 1 Pour configurer Site Recovery Manager afin qu'il conserve les anciens snapshots PIT, définissez la valeur de l'option **vrReplication.preserveMpitImagesAsSnapshots** dans **Paramètres avancés** sur `true`. Pour plus d'informations, reportez-vous à [Modifier les paramètres de vSphere Replication](#) et [Réplication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques](#).

- 2 Configurez la réplication de la machine virtuelle avec vSphere Replication.
- 3 Ajoutez la machine virtuelle à un groupe de protection vSphere Replication et incluez le groupe de protection dans un plan de récupération.

Procédure

- 1 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.

- 2 Dans la vue **VM et modèles**, cliquez avec le bouton droit de la souris sur la machine virtuelle récupérée et sélectionnez **Snapshots > Gérer les snapshots**.

- 3 Sélectionnez l'un des snapshots PIT de cette machine virtuelle et cliquez sur **Restaurer**.

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

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

Annuler un test ou une récupération

Vous pouvez annuler un test du plan de récupération lorsque l'état est Test en cours ou Basculement en cours.

Lorsque vous annulez un test ou une récupération, Site Recovery Manager ne démarre aucun processus et utilise certaines règles pour arrêter les processus en cours. L'annulation d'un basculement vous oblige à le réexécuter.

- Les processus ne pouvant être arrêtés, tels que la mise sous tension ou l'attente d'un signal de pulsation, continuent jusqu'à ce qu'ils soient achevés avant que l'annulation ne soit effectuée.
- Les processus ajoutant ou supprimant des périphériques de stockage sont annulés par le nettoyage.

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

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Sélectionnez l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération et sélectionnez **Annuler**. Vous pouvez également annuler le plan dans l'onglet **Étapes de récupération**.

Étape suivante

Exécutez un nettoyage après l'annulation d'un test.

Désactiver la récupération d'une machine virtuelle dans un groupe de protection de stratégie de stockage

Vous pouvez désactiver la récupération d'une machine virtuelle faisant partie d'un groupe de protection de stratégie de stockage sans la supprimer du groupe.

Si vous exécutez un plan de récupération qui ne peut pas se terminer sans erreurs, vous pouvez désactiver la récupération des machines virtuelles qui génèrent les erreurs. Vous devez recommencer la procédure pour chaque machine virtuelle impliquée.

Conditions préalables

Si vous souhaitez utiliser l'option Désactiver la récupération, le groupe de protection de stratégie de stockage doit être partiellement récupéré.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Groupes de protection**, cliquez sur un groupe de protection de stratégie de stockage, puis cliquez sur l'onglet **Machines virtuelles**.
- 4 Sélectionnez une machine virtuelle, puis cliquez sur le bouton **Désactiver la récupération**.
- 5 Cliquez sur **Oui** pour confirmer.

Résultats

Lors de la prochaine exécution du plan de récupération, cette machine virtuelle sera ignorée.

Étape suivante

Exécutez à nouveau le plan de récupération.

Désactiver la récupération d'un groupe de cohérence dans un groupe de protection de stratégie de stockage

Vous pouvez désactiver la récupération d'un groupe de cohérence faisant partie d'un groupe de protection de stratégie de stockage sans le supprimer du groupe.

Si un groupe de cohérence génère des erreurs lors de l'exécution du plan de récupération d'un groupe de protection de stratégie de stockage, vous pouvez désactiver la récupération de ce groupe de cohérence. Vous devez recommencer la procédure pour chaque groupe de cohérence impliqué.

Conditions préalables

Si vous souhaitez utiliser l'option Désactiver la récupération, le groupe de protection de stratégie de stockage doit être partiellement récupéré, et l'une des conditions suivantes doit s'appliquer au groupe de cohérence :

- il n'est pas affiché sur le site de récupération ;
- il est affiché sur le site de récupération, mais il est vide ;
- il est affiché sur le site de récupération, mais toutes les machines virtuelles du groupe ont des erreurs.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Sélectionnez l'onglet **Groupes de protection**, cliquez sur un groupe de protection de stratégie de stockage, puis sélectionnez l'onglet **Groupes de cohérence**.
- 4 Sélectionnez un groupe de cohérence, puis cliquez sur le bouton **Désactiver la récupération**.
- 5 Cliquez sur **Oui** pour confirmer.

Résultats

Lors de la prochaine exécution du plan de récupération, ce groupe de cohérence sera ignoré.

Étape suivante

Exécutez à nouveau le plan de récupération. Reportez-vous à [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.

Conditions préalables

Vérifiez qu'aucun test de récupération ou aucune récupération réelle n'est en cours.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez sur un plan de récupération.
- 4 (Requis) Cliquez sur l'onglet **Étapes de récupération** et, dans le menu déroulant **Afficher**, sélectionnez le mode pour les étapes de récupération.

Option	Description
Étapes de test	Exporte les étapes de test de récupération.
Étapes de récupération	Exporte les étapes de récupération.
Étapes de nettoyage	Exporte les étapes de nettoyage.
Étapes de reprotection	Exporte les étapes de reprotection.

Note L'option qui permet de sélectionner le mode pour les étapes de récupération peut ne pas être disponible selon l'état du plan de récupération.

- 5 Cliquez sur l'icône **Exporter les étapes**.

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

- 6 Cliquez sur **Télécharger** et fermez la fenêtre.

En outre, vous pouvez ouvrir le rapport des étapes du plan de récupération dans un nouvel onglet.

Afficher et exporter un rapport 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.

Le rapport 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 pouvez exporter un rapport historique à tout moment, mais celui-ci ne contient que les entrées des opérations terminées. Si une opération est en cours, le rapport historique apparaît après la fin de l'opération.

Site Recovery Manager préserve l'historique des plans de récupération supprimés. Vous pouvez exporter des rapports d'historique pour des plans existants et supprimés.

Pour exporter un rapport d'historique pour un plan existant, procédez comme suit :

Conditions préalables

Vous avez exécuté ou testé un plan de récupération ou vous avez effectué un nettoyage après un test.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Paire de sites**, cliquez sur **Historique des plans de récupération**.
- 4 (Facultatif) Pour exporter la totalité de l'historique des plans de récupération pour une période donnée, cliquez sur **Tout exporter**.
- 5 (Facultatif) Sélectionnez un élément dans l'historique des plans de récupération et cliquez sur **Exporter le rapport** pour obtenir l'historique du plan de récupération pour une période donnée, une exécution de plan de récupération, un test, un nettoyage ou une opération de reprotection.
- 6 Sélectionnez un format pour le fichier généré, puis cliquez sur **Télécharger** ou **Ouvrir dans un nouvel onglet**.

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

Supprimer un plan de récupération

Si vous n'avez pas besoin d'un plan de récupération, vous pouvez le supprimer.

Conditions préalables

Vérifiez que le plan de récupération se trouve dans un état cohérent.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez avec le bouton droit sur le plan de récupération à supprimer et cliquez sur **Supprimer**.

Présentation des états des plans de récupération

Vous pouvez surveiller le statut d'un plan de récupération et déterminer l'opération autorisée dans chaque état. Les états des groupes de protection au sein d'un plan de récupération déterminent l'état du plan.

Tableau 6-2. États de récupération

État	Description
Prêt	<p>Les étapes de récupération sont effacées.</p> <p>Pour les groupes de protection de stratégie de stockage, les étapes de récupération n'affichent pas les machines virtuelles et les groupes de cohérence quand un plan de récupération est dans cet état.</p> <p>Vous pouvez vérifier les machines virtuelles protégées dans un plan de récupération dans l'onglet Machines virtuelles.</p>
Test en cours	L'annulation d'un test fait passer le plan à l'état Annulation en cours .
Test terminé	Le test s'est terminé avec ou sans erreurs. Si un échec se produit pendant le test, le plan passe à l'état Test interrompu .
Test interrompu	Le serveur est tombé en panne au cours de l'exécution d'un test.
Nettoyage en cours	<p>Après un nettoyage réussi, l'état du plan passe à Prêt.</p> <p>Si le nettoyage est incomplet, l'état passe à Nettoyage incomplet.</p> <p>Si vous définissez l'option Forcer le nettoyage, l'état passe à Prêt après une erreur.</p> <p>En cas de panne pendant le nettoyage, l'état passe à Nettoyage incomplet.</p>
Nettoyage incomplet	<p>Des erreurs se sont produites pendant le nettoyage.</p> <p>Vous pouvez relancer le nettoyage.</p> <p>Lors de l'exécution du nettoyage dans cet état, l'assistant de nettoyage propose une option qui permet d'ignorer les erreurs.</p>
Nettoyage interrompu	<p>Site Recovery Manager a échoué pendant le nettoyage.</p> <p>Vous ne pouvez pas modifier les options de récupération.</p>
Récupération en cours	Si vous annulez la récupération, l'état passe à Annulation en cours .
Récupération d'urgence terminée	<p>Au cours d'une récupération sur le site protégé, les machines virtuelles n'ont pas pu être arrêtées, probablement parce que les sites n'étaient pas connectés en raison d'un Split-Brain.</p> <p>Une invite système vous avertit de la présence d'un Split-Brain et vous invite à relancer la récupération dès que les sites seront reconnectés.</p> <p>Une fois les sites connectés, l'état passe à Récupération requise (Split-Brain).</p>
Récupération démarrée	<p>Une récupération a démarré sur le site homologue, mais si les sites ne sont pas connectés l'état exact est inconnu.</p> <p>Connectez-vous au site de récupération ou reconnectez les sites pour obtenir l'état actuel.</p>

Tableau 6-2. États de récupération (suite)

État	Description
Récupération requise (Split-Brain)	<p>Les sites ont été déconnectés pendant la récupération. Un scénario Split-Brain a été détecté lorsque les sites se sont reconnectés.</p> <p>Le système vous invite à relancer la récupération afin de synchroniser les sites.</p> <p>Pour les groupes de protection de stratégie de stockage, les étapes de récupération n'affichent pas les machines virtuelles et les groupes de cohérence quand un plan de récupération est dans cet état.</p> <p>Vous pouvez vérifier les machines virtuelles protégées dans un plan de récupération dans l'onglet Machines virtuelles.</p>
Récupération terminée	<p>En cas d'erreurs, toutes les machines virtuelles sont récupérées, mais il existe des erreurs. La réexécution de la récupération ne corrige pas les erreurs.</p> <p>Le plan passe à cet état une fois la récupération du Split-Brain résolue.</p> <p>Vous pouvez voir les étapes de récupération de la dernière exécution de récupération.</p> <p>Pour les groupes de protection de stratégie de stockage, les étapes de récupération n'affichent pas les machines virtuelles et les groupes de cohérence quand un plan de récupération est dans cet état.</p> <p>Vous pouvez vérifier les machines virtuelles protégées dans un plan de récupération dans l'onglet Machines virtuelles.</p> <p>Les sites ont été déconnectés pendant la récupération. L'état de la connexion est la seule propriété qui déclenche cet état.</p>
Récupération incomplète	<p>Récupération annulée ou erreur de banque de données. Relancez la récupération.</p> <p>Vous devez résoudre les erreurs et relancer la récupération ou supprimer la protection des machines virtuelles qui possèdent des erreurs. Le plan détecte la résolution des erreurs en effectuant l'une de ces deux méthodes et met à jour l'état sur <i>Récupération terminée</i>.</p>
Récupération partielle	<p>Seulement une partie des groupes de protection a été récupérée par un plan de chevauchement.</p>
Récupération interrompue	<p>Une panne qui s'est produite lors de la récupération provoque son interruption. Pour continuer, cliquez sur Exécuter. Vous ne pouvez pas modifier les options de récupération.</p>
Annulation en cours	<p>L'annulation d'un test entraîne l'état <i>Test terminé</i> avec le dernier résultat annulé.</p> <p>L'annulation d'une récupération entraîne l'état <i>Récupération incomplète</i> avec le dernier résultat annulé.</p> <p>Si l'opération est annulée suffisamment tôt, cela peut entraîner un état <i>Prêt</i>.</p>
Reprotection en cours	<p>En cas d'échec du serveur pendant cet état, l'état passe à <i>Reprotection interrompue</i>.</p>

Tableau 6-2. États de récupération (suite)

État	Description
Reprotection partielle	<p>Le plan de chevauchement a été reprotégé.</p> <p>Les groupes déjà reprotégés passent à l'état Prêt, mais cela est correct puisque les autres groupes sont dans l'état Récupéré.</p>
Reprotection incomplète	<p>La reprotection n'a pas terminé les opérations de stockage. Les sites doivent être connectés pour que la reprotection réussisse lors de la nouvelle exécution.</p> <p>La reprotection a terminé les opérations de stockage, mais pas la création de machines virtuelles fantômes. Vous pouvez réexécuter la reprotection, même si le site exécutant les machines virtuelles est déconnecté, puis passer à la récupération immédiatement après.</p>
Reprotection interrompue	<p>En cas de panne de Site Recovery Manager Server pendant une reprotection, relancez la reprotection pour continuer et nettoyer l'état correctement.</p>
Attente des entrées de l'utilisateur	<p>Le test est mis en pause. Fermez l'invite pour reprendre le test.</p> <p>La récupération est mise en pause. Fermez l'invite pour reprendre la récupération.</p>
Groupes de protection en cours d'utilisation	<p>Le plan contient des groupes qui sont utilisés par un autre plan pour un test. Cet état se produit également lorsque l'autre plan a terminé une opération de test sur les groupes sans exécuter de nettoyage.</p> <p>Attendez que l'autre plan termine le test ou le nettoyage, ou modifiez le plan pour supprimer les groupes.</p>
Erreur de direction	<p>Les groupes sont dans un état mixte, qui est un état non valide. Le plan contient différents groupes qui sont Prêts dans des directions opposées. Sélectionnez une direction qui sera correcte et supprimez les groupes de protection dirigés dans le sens opposé.</p> <p>Cette erreur se produit lorsque des plans de chevauchement ont exécuté et reprotégé certains groupes du plan.</p>
En cours de suppression	<p>Le plan passe à ce bref état tout en attendant la suppression d'un plan homologue. Le plan s'exécute automatiquement lorsque l'autre plan est supprimé.</p>

Tableau 6-2. États de récupération (suite)

État	Description
Plan hors synchronisation	<p>Cet état peut se produire dans des circonstances différentes :</p> <ul style="list-style-type: none"> ■ Entre une récupération de test réussie et une opération de nettoyage. Si vous ne pouvez pas modifier le plan qui affiche cet état, exécutez le nettoyage pour ramener le plan à l'état <code>Prêt</code>. Pour autoriser le nettoyage, vous devrez peut-être ouvrir le plan dans l'interface utilisateur de VMware Site Recovery pour l'autre site. Si le plan reste dans l'état <code>Plan hors synchronisation</code>, modifiez-le. ■ Vous pouvez modifier le plan au cours d'une opération normale. <p>L'ouverture du plan pour modifier et enregistrer les modifications force la synchronisation par Site Recovery Manager des données internes de Site Recovery Manager pour le plan entre les serveurs Site Recovery Manager de protection et de récupération, faisant disparaître l'état <code>Plan hors synchronisation</code>.</p>
Aucun groupe de protection	<p>Le plan ne contenant aucun groupe de protection, il ne peut pas être exécuté.</p> <p>Vous pouvez modifier le plan incluant le site de récupération.</p> <p>Vous pouvez créer des plans vides via l'API ou l'interface utilisateur ou en supprimant des groupes de protection.</p>
Erreur interne	<p>Un groupe de protection figurant dans le plan a un état inconnu ou une autre erreur inattendue s'est produite.</p> <p>Vous ne pouvez pas exécuter le plan, mais vous pouvez le supprimer.</p>

Configuration d'un plan de récupération

7

Vous pouvez configurer un plan de récupération pour exécuter des commandes sur Site Recovery Manager Server ou sur une machine virtuelle, afficher des messages nécessitant une réponse lorsque le plan s'exécute sur le serveur Site Recovery Manager Server ou dans le système d'exploitation invité, 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.

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.

Lorsqu'un plan de récupération est en cours d'exécution, son état reflète celui de l'exécution du plan de récupération, plutôt que celui des groupes de protection qu'il contient.

Étapes d'un plan de récupération

Un plan de récupération exécute une série d'étapes devant être effectuées dans un ordre spécifique pour un workflow spécifique, tel qu'une migration planifiée ou une reprotection. 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.

- Certaines étapes s'exécutent uniquement avec un stockage étiré.

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, Site Recovery Manager effectue les opérations suivantes :

- 1 Site Recovery Manager désactive les machines virtuelles en fonction de la priorité que vous avez définie ; ainsi, les machines virtuelles à priorité élevée sont les dernières à être mises hors tension. Site Recovery Manager ignore cette étape lorsque vous testez un plan de récupération.
- 2 Site Recovery Manager met sous tension des groupes de machines virtuelles du site de récupération suivant l'ordre de priorité que vous avez défini. Pour qu'un groupe de priorité puisse démarrer, toutes les machines virtuelles du groupe à priorité plus élevée suivant doivent avoir été récupérées, ou leur récupération doit avoir échoué.

Pendant la récupération, les dépendances entre les machines virtuelles dans les différents groupes de priorité sont ignorées. 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.

Étapes de la récupération pour le stockage étiré

L'assistant du plan de récupération fournit une option à utiliser dans tout vSphere vMotion pour effectuer un basculement pour toutes les machines virtuelles protégées et sous tension se trouvant sur un stockage étiré du site protégé. Quand cette option est sélectionnée, deux étapes supplémentaires ont lieu pendant la récupération, immédiatement avant la mise hors tension des machines virtuelles du site protégé.

- **Préparation du stockage pour la migration des VM.** Site Recovery Manager modifie la préférence au site de récupération pour chaque groupe de cohérence.
- **Migration des VM.** Si la machine virtuelle de production n'est pas sous tension, l'étape échoue. Si la machine virtuelle de production est sous tension, Site Recovery Manager initie une migration vSphere vMotion pour migrer la machine virtuelle vers le site de récupération.

Attention Les machines virtuelles qui sont éligibles pour la migration ne sont pas migrées si elles sont une priorité plus faible que les machines virtuelles non admissibles ou si elles ont des dépendances sur des machines virtuelles non éligibles.

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 Site Recovery Manager Server ou dans une machine virtuelle faisant partie du plan de récupération.

Lorsque vous ajoutez des étapes de récupération personnalisées, elles sont partagées entre le workflow de test et le workflow d'exécution. Vous ne pouvez pas exécuter des étapes personnalisées sur les machines virtuelles à suspendre.

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.

Toutefois, s'il existe des étapes personnalisées qui exécutent des commandes contenant des informations spécifiques au site, telles que les configurations réseau, vous devrez peut-être modifier ces étapes après une nouvelle protection.

Vous pouvez configurer des commandes et des invites dans les étapes du plan de récupération pour définir l'achèvement d'une opération particulière. Vous ne pouvez pas ajouter des commandes et des invites avant l'étape Configurer des réseaux de test.

Vous ne pouvez pas ajouter des commandes et des invites aux étapes de niveau supérieur relatives aux groupes de protection de stratégie de stockage suivantes :

- Test de récupération des groupes de cohérence de stockage terminé
- Test de récupération des VM terminé
- Test de récupération des groupes de protection terminé
- Migration en direct des groupes de protection terminée
- Terminer les opérations du groupe de protection sur le site protégé
- Récupération des groupes de cohérence de stockage terminée
- Récupération des VM terminée
- Récupération des groupes de protection terminée

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

Les commandes de niveau supérieur s'exécutent sur Site Recovery Manager Server. Vous pouvez utiliser ces commandes pour mettre sous tension des périphériques physiques ou rediriger le trafic réseau.

Commandes par machine virtuelle

Site Recovery Manager associe les commandes par machine virtuelle avec les machines virtuelles nouvellement récupérées lors du processus de récupération. Vous pouvez utiliser ces commandes pour effectuer des 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 Site Recovery Manager Server ou la machine virtuelle nouvellement récupérée. Les commandes qui s'exécutent sur la machine virtuelle nouvellement récupérée le font dans le contexte du compte d'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 effectuer en réponse directe à une invite est de fermer le message, ce qui permet à la récupération de continuer.

Étapes d'exécution de commandes et d'invites

Pour les groupes de protection de stratégie de stockage, si vous ajoutez une commande ou une invite avant les machines virtuelles dont la priorité est la plus grande, Site Recovery Manager exécute la commande ou l'invite après que l'étape **Appliquer les stratégies de VM** se termine pour toutes les machines virtuelles.

Pour les groupes de protection de réplication basée sur la baie et les groupes de protection vSphere Replication, la première étape de commande ou d'invite (ou personnalisée) ajoutée entre **Créer un snapshot du stockage inscriptible** et le premier groupe de machines virtuelles non vide démarre parallèlement à l'étape **Créer un snapshot du stockage inscriptible** pour traiter les scénarios d'échec.

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. Au lieu de cela, le plan de récupération est mis en pause jusqu'à ce que vous fermiez l'invite.

Instructions pour l'écriture des étapes de commande

Tous les fichiers de commandes, les scripts 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 Site Recovery Manager Server sur le site de récupération avant de l'ajouter au plan.

Site Recovery Manager pour Windows

- 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 Site Recovery Manager Server, 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 se termine 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.

Site Recovery Manager Appliance

- Vous devez copier le script dans le répertoire de base de l'utilisateur **admin** `/home/admin`.
- Vous devez modifier l'autorisation d'accès du script pour que l'utilisateur **srm** puisse l'exécuter. Par exemple, pour un script de dépistage, utilisez la ligne de commande suivante :

```
chmod 755 Myscript.sh
```

- Lorsque vous exécutez le script, vous devez utiliser le chemin d'accès complet sur l'hôte local. Par exemple, pour exécuter un script de dépistage, utilisez la commande suivante :

```
/bin/sh /home/admin/Myscript.sh
```

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 sur Site Recovery Manager Server s'exécutent avec l'identité du compte de service Site Recovery Manager. Dans la configuration par défaut, les étapes de commande sur une machine virtuelle récupérée s'exécutent avec l'identité du compte de service VMware Tools. Vous pouvez modifier la configuration par défaut des machines virtuelles compatibles avec le paramètre **recovery.autoDeployGuestAlias**. Pour plus d'informations sur le paramètre **recovery.autoDeployGuestAlias**, reportez-vous à la section [Modifier les paramètres de récupération](#).

Site Recovery Manager définit les variables d'environnement uniquement pour la durée de l'étape de commande. Les variables d'environnement publiques n'existent pas dans Site Recovery Manager Server et le SE invité de la machine virtuelle récupérée si la commande est exécutée.

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
<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 Site Recovery Manager Server 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 Server 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_GuestNom</i>	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 d'accès au fichier VMX de la machine virtuelle.	[datastore-123] jquser-vm2/jquser-vm2.vmx

Tableau 7-3. Variables d'environnement disponibles pour les étapes de commande par machine virtuelle exécutées sur les machines virtuelles récupérées

Nom	Valeur et description	Exemple
<i>VMware_GuestOp_OutputFile</i>	<p>La valeur du chemin d'accès à un fichier de sortie de commande.</p> <p>Si la commande crée le fichier, Site Recovery Manager télécharge le contenu du fichier et l'ajoute à l'historique du plan de récupération et aux journaux du serveur.</p> <p>Site Recovery Manager ajoute les derniers 4 Ko du fichier de sortie de commande à l'historique du plan de récupération et aux journaux de serveur. Si les scripts génèrent une sortie supérieure à 4 Ko, elle doit être enregistrée dans un emplacement personnalisé.</p> <p>À la fin de la commande, Site Recovery Manager supprime le fichier de sortie de commande.</p>	C:\Windows\TEMP\vmware0\srmStdOut.log

Exemple : Commandes exécutables sur Site Recovery Manager

Pour Site Recovery Manager pour Windows, vous pouvez créer un fichier `myServerScript.bat` dont le contenu est le suivant.

```
@echo off
echo %DATE% %TIME% : Recovery Plan %VMware_RecoveryName% ran in %VMware_RecoveryMode% mode"
:: some more custom actions
```

Pour exécuter le fichier `myServerScript.bat`, utilisez le contenu de commande suivant.

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myServerScript.bat > %VMware_GuestOp_OutputFile%
2>&1
```

Pour Site Recovery Manager Appliance, vous pouvez créer un script `myServerScript.sh` dont le contenu est le suivant.

```
clear
echo "$(date "+%Y-%m-%d %H:%M:%S") : Recovery Plan $VMware_RecoveryName ran in
$VMware_RecoveryMode mode"
# some more custom actions
```

Note N'utilisez pas les symboles de barre verticale (|) et de guillemet simple (') lors de l'écriture des commandes dans le script.

Pour exécuter le script `myServerScript.sh`, utilisez le contenu de commande suivant.

```
/bin/sh /home/admin/myServerScript.sh
```

Exemple : Contenu pour les commandes exécutées sur une machine virtuelle récupérée

Pour les systèmes d'exploitation invités Windows, vous pouvez créer un fichier `myGuestScript.bat` dont le contenu est le suivant.

```
@echo off
echo %DATE% %TIME% : VM %VMware_VM_Name% recovered by RP %VMware_RecoveryName% ran in
%VMware_RecoveryMode% mode
echo %DATE% %TIME% : Configured with the following FQDN: %VMware_VM_GuestName% and IP:
%VMware_VM_GuestIp%
:: some more custom actions
```

Pour exécuter le fichier `myGuestScript.bat`, utilisez le contenu de commande suivant.

```
C:\Windows\System32\cmd.exe /c C:\myScripts\myGuestScript.bat > %VMware_GuestOp_OutputFile%
2>&1
```

Pour les systèmes d'exploitation invités Linux et Unix, vous pouvez créer un fichier `myGuestScript.sh` dont le contenu est le suivant.

```
echo $(date) : VM $VMware_VM_Name recovered by $VMware_RecoveryName ran
echo $(date) : Configured with the following FQDN: $VMware_VM_GuestName and IP:
$VMware_VM_GuestIp
# some more custom actions
```

Pour exécuter le fichier `myGuestScript.sh`, utilisez le contenu de commande suivant.

```
/bin/sh myGuestScript.sh &>$VMware_GuestOp_OutputFile
```

Créer des étapes de commande ou des invites de messages de niveau supérieur

Vous pouvez ajouter les étapes de récupération de niveau supérieur n'importe où dans le plan de récupération. Les étapes de commande de niveau supérieur sont des commandes ou scripts exécutés sur Site Recovery Manager Server pendant une récupération. Vous pouvez également ajouter des étapes qui affichent des invites de messages qu'un utilisateur doit avaliser pendant une récupération.

Conditions préalables

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

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Plans de récupération**, sélectionnez un plan de récupération, puis cliquez sur **Étapes de récupération**.
- 4 Utilisez le menu déroulant **Afficher** pour sélectionner le type d'étape que vous souhaitez ajouter.

Option	Description
Étapes de test	Ajoutez une étape à exécuter lors du test d'un plan de récupération.
Étapes de récupération	Ajoutez une étape à exécuter lors d'une migration planifiée ou d'une récupération d'urgence.

Vous ne pouvez pas ajouter d'étapes aux opérations de nettoyage ou de reprotection.

- 5 Sélectionnez l'emplacement où vous voulez ajouter l'étape.
 - Pour ajouter une étape avant une autre étape, cliquez avec le bouton droit sur l'étape et sélectionnez **Ajouter une étape avant**.

- Pour ajouter une étape après la dernière étape, cliquez avec le bouton droit sur la dernière étape et sélectionnez **Ajouter une étape après**.
- 6 Sélectionnez **Commande sur SRM Server** ou **Invite**.
 - 7 Dans la zone de texte **Nom**, entrez un nom pour l'étape.
Le nom de l'étape apparaît dans la liste des étapes dans la vue **Étapes de récupération**.
 - 8 Dans la zone de texte **Contenu**, entrez une invite de commande, de script ou de message.
 - Si vous avez sélectionné **Commande sur SRM Server**, entrez la commande ou le script à exécuter.
 - Si vous avez sélectionné **Invite**, entrez le texte du message à afficher pendant l'exécution du plan de récupération.
 - 9 (Facultatif) Modifiez le paramètre **Délai d'expiration** pour la commande à exécuter sur Site Recovery Manager Server.
Cette option n'est pas disponible si vous créez une étape d'invite.
 - 10 Cliquez sur **Ajouter** pour ajouter l'étape au plan de récupération.

Étape suivante

Vous pouvez cliquer avec le bouton droit sur l'étape créée récemment et sélectionner les options permettant de modifier, supprimer ou ajouter des étapes avant et après celle-ci.

Créer des invites de messages ou des étapes de commande pour des machines virtuelles individuelles

Vous pouvez créer des étapes de récupération personnalisées pour inviter les utilisateurs à effectuer des tâches ou pour que Site Recovery Manager effectue des tâches sur une machine virtuelle avant ou après que Site Recovery Manager l'ait mise sous tension.

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 plusieurs plans de récupération contiennent la même machine virtuelle, Site Recovery Manager inclut les commandes et les invites dans tous les plans de récupération.

Conditions préalables

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

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Dans l'onglet **Plans de récupération**, sélectionnez un plan de récupération, puis cliquez sur **Étapes de récupération**.
- 4 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Configurer la récupération**.
- 5 Dans l'onglet **Propriétés de récupération**, cliquez sur **Étapes précédant la mise sous tension** ou **Étapes suivant la mise sous tension**.
- 6 Cliquez sur l'icône représentant le signe plus pour ajouter une étape.
- 7 Sélectionnez le type d'étape à créer.

Option	Description
Invite	Invite les utilisateurs à effectuer une tâche ou à fournir des informations que l'utilisateur doit aviser avant que le plan passe à l'étape suivante. Cette option est disponible pour des étapes de pré-mise sous tension ou de post-mise sous tension.
Commande sur le serveur SRM	Exécute une commande sur Site Recovery Manager Server. Cette option est disponible pour des étapes de pré-mise sous tension ou de post-mise sous tension.
Commande sur la VM récupérée	Exécute une commande sur la machine virtuelle récupérée. Cette option est uniquement disponible pour les étapes de post-mise sous tension.

- 8 Dans la zone de texte **Nom**, entrez un nom pour l'étape.
Le nom de l'étape apparaît dans la liste des étapes dans la vue **Étapes de récupération**.
- 9 Dans la zone de texte **Contenu**, entrez une invite de commande, de script ou de message.
 - Si vous avez sélectionné **Commande sur SRM Server** ou **Commande sur la VM récupérée**, entrez la commande ou le script à exécuter.
 - Si vous avez sélectionné **Invite**, entrez le texte du message à afficher pendant l'exécution du plan de récupération.
- 10 (Facultatif) Modifiez le paramètre **Délai d'expiration** pour la commande à exécuter sur Site Recovery Manager Server.
Cette option n'est pas disponible si vous créez une étape d'invite.
- 11 Pour ajouter l'étape au plan de récupération, cliquez sur **Ajouter**.
- 12 Pour reconfigurer la machine virtuelle afin qu'elle exécute la commande avant ou après activation, cliquez sur **OK**.

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. Site Recovery Manager reprend les machines virtuelles interrompues lors d'un basculement lorsque le basculement s'exécute dans le sens opposé.

Vous pouvez uniquement ajouter des machines virtuelles pour suspendre au niveau du site de récupération.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez sur un plan de récupération, puis sur **Étapes de récupération**.
- 4 Cliquez avec le bouton droit sur **Interrompre les VM non critiques sur le site de récupération**, puis cliquez sur **Ajouter ou supprimer une VM non critique**.
- 5 Sélectionnez les machines virtuelles sur le site de récupération à interrompre lors d'une récupération.
- 6 Cliquez sur **Enregistrer**.

Résultats

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

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. La priorité de récupération détermine l'ordre dans lequel les machines virtuelles sont arrêtées et mises sous tension.

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.

Attention Si une machine virtuelle éligible pour la migration de stockage est tirée à une priorité inférieure à celle d'une machine virtuelle qui est non éligible pour la migration de stockage tirée, la machine virtuelle éligible n'est pas migrée.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez sur un plan de récupération et sur **Machines virtuelles**.
- 4 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Groupe de priorité**.
- 5 Sélectionnez une nouvelle priorité pour la machine virtuelle.
1 représente la priorité la plus élevée et 5 la plus faible.
- 6 Pour confirmer le changement de priorité, cliquez sur **Oui**.

Configuration des dépendances de machines virtuelles

Si une machine virtuelle dépend de services exécutés sur une autre machine virtuelle du même groupe de protection, vous pouvez configurer une dépendance entre les machines virtuelles. En configurant une dépendance, vous pouvez garantir que les machines virtuelles démarrent sur le site de récupération dans le bon ordre. Les dépendances sont uniquement valides si les machines virtuelles ont la même priorité.

Attention Les machines virtuelles qui sont éligibles pour la migration de stockage tirée ne sont pas migrées si elles dépendent de machines virtuelles qui ne sont pas admissibles pour la migration de stockage tirée.

Lors de l'exécution d'un plan de récupération, Site Recovery Manager démarre les machines virtuelles dont dépendent d'autres machines virtuelles avant de démarrer les machines virtuelles avec les dépendances. Si Site Recovery Manager ne peut pas démarrer une machine virtuelle dont une autre machine virtuelle dépend, le plan de récupération continue avec un avertissement. Vous ne pouvez configurer des dépendances qu'entre des machines virtuelles se trouvant dans le même groupe de priorité de récupération. Si vous configurez une machine virtuelle pour qu'elle dépende d'une machine virtuelle se trouvant dans un groupe disposant d'une priorité plus faible, Site Recovery Manager ignore la dépendance et démarre en premier la machine virtuelle du groupe dont la priorité est la plus élevée.

Si vous supprimez du plan de récupération un groupe de protection qui contient la machine virtuelle dépendante, l'état du groupe de protection est défini sur **Pas dans ce plan** dans les dépendances pour la machine virtuelle avec la dépendance. Si la machine virtuelle configurée dispose d'une priorité différente de celle de la machine virtuelle dont elle dépend, l'état de la machine virtuelle dépendante est défini sur **Priorité inférieure** ou **Priorité supérieure**.

Conditions préalables

Vérifiez que la machine virtuelle dépendante et la machine virtuelle dont elle dépend font partie du même plan de récupération et du même groupe de priorité de récupération.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez sur un plan de récupération et sur **Machines virtuelles**.
- 4 Cliquez avec le bouton droit sur une machine virtuelle qui dépend d'une ou de plusieurs autres machines virtuelles, puis cliquez sur **Configurer la récupération**.
- 5 Développez **Dépendances de la VM**.
- 6 Dans le menu déroulant, sélectionnez **Afficher tout**.
- 7 Sélectionnez une ou plusieurs machines virtuelles dans la liste de toutes les machines virtuelles du plan de récupération sélectionné.

Les machines virtuelles sélectionnées sont ajoutées à la liste des dépendances.

- 8 Vérifiez que les machines virtuelles de la liste **Dépendances de la VM** sont activées et que l'état des dépendances est **OK**.
- 9 (Facultatif) Pour supprimer une dépendance, sélectionnez **Afficher les dépendances de VM** dans le menu déroulant, sélectionnez une machine virtuelle dans la liste des machines virtuelles dont dépend cette machine virtuelle, puis cliquez sur **Supprimer**.
- 10 Cliquez sur **OK**.

Activer vSphere vMotion pour la migration planifiée

La migration d'une machine virtuelle à l'aide de vSphere vMotion est uniquement disponible pour une migration planifiée. Vous pouvez activer ou désactiver vSphere vMotion dans la boîte de dialogue **Propriétés de récupération**.

Conditions préalables

- Avant d'exécuter une migration vSphere vMotion, vérifiez que la machine virtuelle fait partie d'un groupe de protection de stratégie de stockage, qu'elle est placée sur un stockage étiré et qu'elle est sous tension.
- Vérifiez que vous avez configuré les mappages d'inventaire complets. Si vous avez configuré uniquement les mappages d'inventaire réservés temporaires et que vous exécutez une migration planifiée avec l'option **Activer l'opération vMotion des VM éligibles**, la migration planifiée échoue, même si les deux sites sont en cours d'exécution.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez sur un plan de récupération, puis cliquez sur l'onglet **Machines virtuelles**.
- 4 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Configurer la récupération**.

Sélectionnez **Utiliser vMotion pour la migration planifiée (la VM doit être sous tension)**.

- 5 Cliquez sur **OK**.

Résultats

Il ne se produit aucun cycle d'alimentation pendant la migration planifiée. Les actions d'arrêt ou de démarrage configurées ou les étapes configurées avant la mise sous tension sont ignorées. Les étapes configurées après la mise sous tension sont exécutées.

Configurer les options de démarrage et d'arrêt de machine virtuelle

Vous pouvez configurer la façon dont une machine virtuelle démarre et s'arrête sur le site de récupération lors d'une récupération.

Vous pouvez configurer si le système d'exploitation invité d'une machine virtuelle doit s'arrêter avant qu'elle ne soit mise hors tension sur le site protégé. Vous pouvez configurer si une machine virtuelle doit être mise sous tension sur le site de récupération. Vous pouvez également configurer des délais après mise sous tension d'une machine virtuelle pour permettre à VMware Tools et à d'autres applications de démarrer sur la machine virtuelle récupérée avant que le plan de récupération ne se poursuive.

Conditions préalables

Vous avez créé un plan de récupération.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez sur un plan de récupération et sur **Machines virtuelles**.
- 4 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Configurer la récupération**.
- 5 Développez **Action Arrêt** et sélectionnez le mode d'arrêt pour cette machine virtuelle.

Option	Description
Arrêter le système d'exploitation invité avant la mise hors tension	Arrête progressivement la machine virtuelle avant de la mettre hors tension. Vous pouvez définir un délai d'expiration pour l'opération d'arrêt. La définition du délai d'expiration sur 0 équivaut à l'option Mettre hors tension. Cette option requiert l'exécution de VMware Tools sur la machine virtuelle. Note La machine virtuelle se met hors tension à l'expiration du délai. Si l'arrêt du système d'exploitation de la machine virtuelle n'est pas terminé à l'expiration du délai, des données risquent d'être perdues. Dans le cas d'une grande machine virtuelle qui nécessite davantage de temps pour s'arrêter normalement, réglez un délai de mise hors tension suffisamment long.
Mettre hors tension	Met hors tension la machine virtuelle sans arrêter le système d'exploitation invité.

- 6 Développez **Action de démarrage** et sélectionnez si la machine virtuelle doit être mise sous tension après une récupération.

Option	Description
Mettre sous tension	Met sous tension la machine virtuelle sur le site de récupération.
Ne pas mettre sous tension	Récupère la machine virtuelle, mais ne la met pas sous tension.

- 7 (Facultatif) Sélectionnez ou désélectionnez la case à cocher **Attendre VMware Tools**.

Cette option est uniquement disponible si vous avez sélectionné **Mettre sous tension** dans [Étape 6](#).

Si vous sélectionnez **Attendre VMware Tools**, Site Recovery Manager attend jusqu'à ce que VMware Tools démarre après la mise sous tension de la machine virtuelle, avant que le plan de récupération ne passe à l'étape suivante. Vous pouvez définir un délai d'expiration avant le démarrage de VMware Tools.

- 8 (Facultatif) Sélectionnez ou désélectionnez la case à cocher **Délai supplémentaire avant d'exécuter les étapes suivant la mise sous tension et de démarrer les machines virtuelles dépendantes** et spécifiez la durée du délai supplémentaire.

Cette option est uniquement disponible si vous avez sélectionné **Mettre sous tension** dans [Étape 6](#).

Par exemple, vous pouvez spécifier un délai supplémentaire après avoir mis sous tension une machine virtuelle pour autoriser les applications dont une autre machine virtuelle dépend à démarrer.

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 à fonctionner sans interrompre les applications et les systèmes d'exploitation invités 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`.

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. Par conséquent, les snapshots ne sont plus disponibles après récupération, sauf si vous configurez vSphere Replication pour qu'il conserve plusieurs snapshots à un moment donné. Pour plus d'informations sur la récupération d'anciens snapshots à l'aide de plusieurs snapshots à un moment donné avec vSphere Replication, voir [Réplication d'une machine virtuelle et activation d'instances à plusieurs moments spécifiques](#).

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. Le paramètre de **réserve de l'intégrité de la mémoire d'invité (totalement verrouillée)** est la seule exception, s'il était activé sur la machine virtuelle protégée.

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 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 la baie.

- Site Recovery Manager ne prend pas en charge le stockage des composants de machines virtuelles s'étendant sur plusieurs baies du site protégé qui sont répliqués sur une seule baie du site de récupération.
- Site Recovery Manager ne prend pas en charge le stockage des composants de machines virtuelles s'étendant sur plusieurs baies du site protégé qui sont répliqués sur 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.

Par conséquent, 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.

Personnalisation des propriétés IP des machines virtuelles

8

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.

Si vous ne personnalisez pas les propriétés IP d'une machine virtuelle, Site Recovery Manager utilise les paramètres IP du site de récupération lors d'une récupération ou d'un test de passage du site de protection vers le site de récupération. Site Recovery Manager utilise les paramètres IP du site de protection après la reprotection, durant la récupération ou lors d'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 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.

Note Vous ne configurez qu'une adresse IP par carte réseau.

Pour obtenir la liste des systèmes d'exploitation invités pour lesquels Site Recovery Manager prend en charge la personnalisation IP, consultez *Matrices de compatibilité pour Site Recovery Manager 8.2* à l'adresse <https://docs.vmware.com/fr/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html>.

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 le site de récupération, la carte réseau continue à utiliser les paramètres IP du site protégé, et vice versa, et Site Recovery Manager n'applique pas la personnalisation IP à la machine virtuelle lors de la récupération.

Vous pouvez appliquer des personnalisations IP à une seule machine virtuelle ou à plusieurs à la fois.

Si vous configurez une personnalisation IP sur des machines virtuelles, Site Recovery Manager ajoute des 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 pour s'assurer que les modifications s'appliquent et que les services du système d'exploitation 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.

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>.

- **Personnalisation manuelle des propriétés IP pour une machine virtuelle individuelle**
Vous pouvez personnaliser manuellement les paramètres IP pour des machines virtuelles individuelles du site protégé et du site de récupération.
- **Personnalisation des propriétés IP pour plusieurs machines virtuelles**
Vous pouvez personnaliser les propriétés IP de plusieurs machines virtuelles sur les sites protégés et de récupération en utilisant DR IP Customizer et en définissant des règles de mappage IP de niveau sous-réseau.

Personnalisation manuelle des propriétés IP pour une machine virtuelle individuelle

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

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Cliquez sur l'onglet **Plans de récupération**, puis cliquez sur un plan de récupération et sur **Machines virtuelles**.
- 4 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Configurer la récupération**.
- 5 Cliquez sur l'onglet **Personnalisation IP** et sélectionnez l'option **Personnalisation IP manuelle** dans le menu déroulant.
- 6 Sélectionnez la carte réseau dont vous allez modifier les paramètres IP.
- 7 Cliquez sur **Configurer** pour le site protégé ou le site de récupération, selon la valeur des paramètres IP que vous souhaitez configurer.
- 8 Pour configurer les paramètres IPv4, cliquez sur l'onglet **IPv4**.
 - Sélectionnez DHCP ou, 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, vous pouvez également cliquer sur **Extraire** pour importer les paramètres actuels configurés sur la machine virtuelle.
- 9 Pour configurer les paramètres IPv6, cliquez sur l'onglet **IPv6**.
 - Sélectionnez DHCP ou, 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, vous pouvez cliquer sur **Extraire** pour importer les paramètres actuels configurés sur la machine virtuelle.
- 10 Pour configurer les paramètres DNS, cliquez sur l'onglet **DNS**.

■ **Tableau 8-1. Paramètres DNS**

Configuration	Options
Serveur DNS	Choisissez comment trouver les serveurs DNS : <ul style="list-style-type: none"> ■ Utilisez DHCP pour obtenir automatiquement une adresse DNS. ■ Spécifiez un serveur DNS préféré et un serveur DNS secondaire.
Suffixe DNS	Entrez un suffixe DNS puis cliquez sur Ajouter , ou sélectionnez un suffixe DNS existant puis cliquez sur Supprimer , Monter ou Descendre .

- Si la machine virtuelle est activée et dispose de VMware Tools, vous pouvez cliquer sur **Extraire** pour importer les paramètres actuels configurés sur la machine virtuelle.
- 11 (Requis) 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.

- 12 Répétez les étapes de [Étape 7](#) à [Étape 10](#) pour configurer les paramètres du site protégé ou du site de récupération, si nécessaire.
- 13 Répétez le processus de configuration pour d'autres cartes réseau, si nécessaire.

Résultats

Les paramètres du site de récupération sont appliqués pendant la récupération. Les paramètres du site protégé sont appliqués pendant la restauration.

Note Les machines virtuelles dotées de la personnalisation IP définie manuellement ne sont pas soumises à l'évaluation des règles de mappage IP durant la récupération. La configuration IP définie manuellement est prioritaire sur les règles de mappages IP.

Appliquer des règles de personnalisation IP à une machine virtuelle

Vous pouvez appliquer une règle de personnalisation IP aux paramètres de récupération d'une machine virtuelle protégée.

Lorsque vous appliquez une règle de personnalisation IP, vous spécifiez une règle de mappage IP de sous-réseau unique à chaque mappage de réseau.

Si vous définissez l'option de paramètre avancé `recovery.useIpMapperAutomatically` sur la valeur `True` et configurez la règle de mappage IP pour les réseaux virtuels, Site Recovery Manager évalue les règles de mappage IP de sous-réseau lors de la récupération pour personnaliser les machines virtuelles. Si vous définissez cette option sur `False`, Site Recovery Manager n'évalue pas les règles de mappage IP lors de la récupération. Vous pouvez modifier l'impact de cette option pour chaque machine virtuelle à l'aide de l'option **Personnalisation IP**.

L'option par défaut de `recovery.useIpMapperAutomatically` est `True`. Si vous la définissez sur `Auto`, Site Recovery Manager personnalise la machine virtuelle à l'aide de la règle Personnalisation IP.

Conditions préalables

Pour obtenir la liste des systèmes d'exploitation invités pour lesquels Site Recovery Manager prend en charge la personnalisation IP, consultez *Matrices de compatibilité pour Site Recovery Manager 8.2* à l'adresse <https://docs.vmware.com/fr/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html>.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Sélectionnez l'onglet **Plans de récupération**, cliquez sur un plan de récupération et sélectionnez **Machines virtuelles**.

- 4 Cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Configurer la récupération**.
- 5 Dans la liste de modes **Personnalisation IP**, sélectionnez **Utiliser les règles de personnalisation IP, le cas échéant**, puis cliquez sur **OK**.

Personnalisation des propriétés IP pour plusieurs machines virtuelles

Vous pouvez personnaliser les propriétés IP de plusieurs machines virtuelles sur les sites protégés et de récupération en utilisant DR IP Customizer et en définissant des règles de mappage IP de niveau sous-réseau.

Dans les versions précédentes de Site Recovery Manager, vous personnalisez les propriétés IP pour plusieurs machines virtuelles à l'aide de l'outil DR IP Customizer. Outre DR IP Customizer, vous pouvez personnaliser les propriétés IP de plusieurs machines virtuelles en définissant des règles de personnalisation IP de niveau sous-réseau.

Vous pouvez utiliser des règles de personnalisation IP de niveau sous-réseau avec DR IP Customizer.

- DR IP Customizer permet de rapidement définir des paramètres de personnalisation IP explicites pour plusieurs machines virtuelles en utilisant un fichier CSV.
- Vous pouvez appliquer des règles de personnalisation IP de niveau sous-réseau à des machines virtuelles à l'aide de vSphere Web Client.

Les machines virtuelles que vous configurez à l'aide de DR IP Customizer ne sont pas soumises aux règles de personnalisation IP du niveau sous-réseau. Vous pouvez obtenir les mêmes résultats de personnalisation IP en utilisant DR IP Customizer ou des règles de sous-réseau IP.

Personnalisation des propriétés IP pour plusieurs machines virtuelles à l'aide de l'outil DR IP Customizer

L'outil DR IP Customizer permet de définir des paramètres de personnalisation IP explicites pour plusieurs machines virtuelles sur le site protégé et le site de récupération.

Outre la définition de règles de mappage IP de sous-réseau, vous pouvez utiliser l'outil DR IP Customizer pour appliquer des paramètres réseau personnalisés à des machines virtuelles lors de leur démarrage sur le site de récupération. Vous fournissez les paramètres IP personnalisés à l'outil DR IP Customizer dans 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 sur les machines protégées pour appliquer le fichier CSV contenant les configurations de la mise en 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.

Vous pouvez personnaliser les paramètres IP du site protégé et du site de récupération afin que Site Recovery Manager utilise les configurations appropriées lors des opérations de reprotection.

Pour obtenir la liste des systèmes d'exploitation invités pour lesquels Site Recovery Manager prend en charge la personnalisation IP, consultez *Matrices de compatibilité pour Site Recovery Manager 8.2* à l'adresse <https://docs.vmware.com/fr/Site-Recovery-Manager/8.2/rn/srm-compat-matrix-8-2.html>.

- **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.

- **Syntaxe de l'outil DR IP Customizer**

L'outil DR IP Customizer comprend des options permettant de recueillir des informations 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.

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 Server pour chaque site lors de l'exécution de la commande.

Procédure

- 1 Connectez-vous à l'hôte Site Recovery Manager Server sur le site protégé ou de récupération et ouvrez une invite de commande.
- 2 Remplacez le répertoire de travail par :
 - Pour Windows, C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin.
 - Pour Linux, /opt/vmware/srm/bin/.
- 3 Exécutez la commande `dr-ip-reporter`.
 - Si vous disposez de Platform Services Controller avec une seule instance de vCenter Server, exécutez la commande suivante :
 - Pour Windows :

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

- Pour Linux :

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out path_to_report_file.xml
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Cet exemple indique `dr-ip-reporter` sur le fichier `vmware-dr.xml` de Site Recovery Manager Server et génère le fichier de rapport pour l'instance de vCenter Server qui est associé à Platform Services Controller sur `https://Platform_Services_Controller_address`.

- Si vous disposez de Platform Services Controller qui inclut plusieurs instances de vCenter Server, vous devez spécifier l'ID de vCenter Server du paramètre `--vcid`.

- Pour Windows :

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

- Pour Linux :

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Cet exemple indique `dr-ip-reporter` sur le fichier `vmware-dr.xml` de Site Recovery Manager Server et génère le fichier de rapport pour l'instance de vCenter Server avec l'ID `vCenter_Server_ID`.

Note L'ID de vCenter Server n'est pas identique au nom de vCenter Server.

- Pour limiter la liste de réseaux à ceux uniquement requis par un plan de récupération spécifique, incluez l'option `--plan` dans la ligne de commande :

- Pour Windows :

```
dr-ip-reporter.exe --cfg "SRM_install_dir\config\vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--plan recovery_plan_name
```

- Pour Linux :

```
/opt/vmware/srm/bin/dr-ip-reporter --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--out "path_to_report_file.xml"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--plan recovery_plan_name
```

Syntaxe de l'outil DR IP Customizer

L'outil DR IP Customizer comprend des options permettant de recueillir des informations 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.

Note Site Recovery Manager vous permet de définir des règles de mappage au niveau du sous-réseau IP pour personnaliser les paramètres IP sur des machines virtuelles à l'aide de l'outil de personnalisation DR IP Customizer. Vous pouvez utiliser des règles de mappage au niveau du sous-réseau IP en association avec l'outil DR IP Customizer. Pour plus d'informations sur les moyens d'utiliser des règles de mappage au niveau du sous-réseau IP avec l'outil DR IP Customizer, reportez-vous à [Personnalisation des propriétés IP pour plusieurs machines virtuelles](#).

- Si vous utilisez Site Recovery Manager pour Windows, le fichier exécutable `dr-ip-customizer.exe` se trouve sous `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin` sur la machine hôte Site Recovery Manager Server.
- Si vous utilisez le dispositif Site Recovery Manager Virtual Appliance, le fichier `dr-ip-customizer` se trouve dans le répertoire `/opt/vmware/srm/bin/` sur le dispositif.

Lorsque vous exécutez `dr-ip-customizer.exe` ou `dr-ip-customizer`, vous spécifiez différentes options selon que vous générez ou appliquez un fichier à valeurs séparées par des virgules (CSV).

```
dr-ip-customizer.exe
--cfg SRM Server configuration XML
--cmd apply/drop/generate
[--csv Name of existing CSV File]
[--out Name of new CSV file to generate]
--uri https://host[:port]/lookupservice/sdk
--vcid UUID
[--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 8-2. Options de DR IP Customizer

Option	Description	Obligatoire
<code>-h [--help]</code>	Affiche des informations sur l'utilisation de <code>dr-ip-customizer.exe</code> ou <code>dr-ip-customizer</code> .	Non
<code>--cfg arg</code>	Chemin d'accès au fichier de configuration XML de l'application, <code>vmware-dr.xml</code> .	Oui

Tableau 8-2. 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>apply</code> applique les paramètres de personnalisation réseau aux plans de récupération sur les instances de Site Recovery Manager Server 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.	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>--uri arg</code>	<p>URL de Lookup Service sur Platform Service Controller au format <code>https://host[:port]/lookupservice/sdk</code>. Si le port n'est pas 443, spécifiez-le. L'instance de Site Recovery Manager associe cette adresse au nœud infra du site principal.</p> <p>Utilisez 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>--vcid arg</code>	UUID d'instance de vCenter Server du site principal.	Facultatif, sauf si l'infrastructure de site principal contient plus d'une instance de vCenter Server.
<code>-i [--ignore-thumbprint]</code>	Ignorer l'invite de confirmation de l'empreinte vCenter Server.	Non

Tableau 8-2. Options de DR IP Customizer (suite)

Option	Description	Obligatoire
-e [--extra-dns-columns]	Doit être spécifié si le fichier CSV d'entrée contient des colonnes supplémentaires pour les informations DNS.	Non
-v [--verbose]	Permettre une sortie détaillée. Vous pouvez inclure une option --verbose sur toute ligne de commande dr-ip-customizer.exe ou dr-ip-customizer pour journaliser d'autres messages de diagnostic.	Non

L'outil peut imprimer l'UUID sur l'instance de Lookup Service chaque fois que la valeur --vcid n'est pas spécifiée, comme dans cet exemple :

■ Pour Windows :

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml" -i --cmd generate -o "c:\tmp\output.csv" --uri https://service.company.com:443/lookupservice/sdk --vcid ?
```

■ Pour Linux :

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml" -i --cmd generate -o "/home/admin/output.csv" --uri https://service.company.com:443/lookupservice/sdk --vcid ?
```

Le message d'erreur qui en résulte inclut l'UUID d'instance de vCenter Server suivie du nom d'hôte DNS de vCenter Server pour chaque instance de vCenter Server enregistrée avec Lookup Service :

```
ERREUR : impossible de trouver l'instance de VC. Utilisez l'une des instances de VC connues suivantes : e07c907e-cd41-4fe7-b38a-f4c0e677a18c vc.company.com
```

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.

Note Site Recovery Manager vous permet de définir des règles de mappage au niveau du sous-réseau IP pour personnaliser les paramètres IP sur des machines virtuelles à l'aide de l'outil de personnalisation DR IP Customizer. Vous pouvez utiliser des règles de mappage au niveau du sous-réseau IP en association avec l'outil DR IP Customizer. Pour plus d'informations sur les moyens d'utiliser des règles de mappage au niveau du sous-réseau IP avec l'outil DR IP Customizer, reportez-vous à [Personnalisation des propriétés IP pour plusieurs machines virtuelles](#).

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 8-3. Colonnes 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. Il est identique à l'ID de machine virtuelle que l'instance de vCenter Server utilise s'il est présent, ou à l'ID du BIOS si ce n'est pas le cas.	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 8-3. 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 primaires	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 8-3. 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 statique. Si le champ n'est pas défini sur une adresse statique spécifique, vous devez le définir 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 de réseau virtuel avec une adresse IPv6 statique. Si le champ n'est pas défini sur une adresse statique spécifique, vous devez le définir sur DHCP.</p> <p>Si vous exécutez Site Recovery Manager Server sur Windows Server 2003 et personnalisez les adresses IPv6 d'une machine virtuelle, vous devez activer IPv6 sur les instances de Site Recovery Manager Server. Site Recovery Manager effectue la validation des adresses IP pendant la personnalisation, ce qui nécessite l'activation d'IPv6 sur Site Recovery Manager Server si vous personnalisez les adresses IPv6. Le protocole IPv6 est activé par défaut sur les versions les plus récentes de Windows Server.</p>
Longueur de préfixe de sous-réseau IPv6	Longueur de préfixe du sous-réseau IPv6 à utiliser.	Personnalisable. Peut être vide.
Passerelle(s) IPv6	Passerelle(s) IPv6 pour cet adaptateur.	Personnalisable. Peut être vide.

Tableau 8-3. 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.

Note Site Recovery Manager vous permet de définir des règles de mappage au niveau du sous-réseau IP pour personnaliser les paramètres IP sur des machines virtuelles à l'aide de l'outil de personnalisation DR IP Customizer. Vous pouvez utiliser des règles de mappage au niveau du sous-réseau IP en association avec l'outil DR IP Customizer. Pour plus d'informations sur les moyens d'utiliser des règles de mappage au niveau du sous-réseau IP avec l'outil DR IP Customizer, reportez-vous à [Personnalisation des propriétés IP pour plusieurs machines virtuelles](#).

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 peut contenir plusieurs adaptateurs et chaque adaptateur peut 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 une adresse IP pour un adaptateur réseau sur chacun des sites protégés et de récupération, ou pour spécifier plusieurs adresses de serveur DNS, ajoutez une nouvelle ligne pour chaque 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` ou `dr-ip-customizer` avec la commande `--cmd generate`. Modifiez le fichier CSV pour personnaliser les paramètres IP des machines virtuelles protégées.

Note Site Recovery Manager vous permet de définir des règles de mappage au niveau du sous-réseau IP pour personnaliser les paramètres IP sur des machines virtuelles à l'aide de l'outil de personnalisation DR IP Customizer. Vous pouvez utiliser des règles de mappage au niveau du sous-réseau IP en association avec l'outil DR IP Customizer. Pour plus d'informations sur les moyens d'utiliser des règles de mappage au niveau du sous-réseau IP avec l'outil DR IP Customizer, reportez-vous à [Personnalisation des propriétés IP pour plusieurs machines virtuelles](#).

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)
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-B,0,,,,,,,,,,,,,
103b9e8b-1f90-faca-8028-13820b8f236e,vm-3-win,vcenter-server-site-A,0,,,,,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,,,,,
834c1a9b-1f91-fbca-1028-43820d8f236d,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 8-4. 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
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							eng.example.com

Tableau 8-4. Configuration des adresses IPv4 statiques dans 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
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
103b9e8b-1f90-faca-8028-13820b8f236e		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 8-5. 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
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0							eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	

Tableau 8-5. 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
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcenter-server-site-A	1			dhcp				
103b9e8b-1f90-faca-8028-13820b8f236e		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 8-6. Configuration des adresses IPv4 et IPv6 DHCP statiques sur un fichier CSV modifié

ID de la VM	Nom de VM	vCenter Serv	ID de l'adaptateur	WINS primaire	WINS secondaire	Masque de sous-réseau	Adresse IP	Passerelle(s)	Adresse IPv6	Longueur de préfixe de sous-réseau IPv6	Passerelle(s) IPv6	Serveur(s) DNS	Suffixe(s) DNS
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0										example.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcenter-server-site-B	0										eng.example.com

Tableau 8-6. 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	WIN S primaires	WIN S 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
103b9e8b-1f90-faca-8028-13820b8f236e		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	
103b9e8b-1f90-faca-8028-13820b8f236e		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-10301	vm-3-win	vcen-ter-server-site-A	0										exemple.com
103b9e8b-1f90-faca-8028-13820b8f236e	vm-3-win	vcen-ter-server-site-A	0										eng.example.com
103b9e8b-1f90-faca-8028-13820b8f236e		vcen-ter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	

Tableau 8-6. Configuration des adresses IPv4 et IPv6 DHCP statiques sur un fichier CSV modifié (suite)

ID de la VM	Nom de la 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
103b9e8b-1f90-faca-8028-13820b8f236e		vcen-ter-server-site-A	1									::ffff:192.168.0.251	
103b9e8b-1f90-faca-8028-13820b8f236e		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.

Note Site Recovery Manager vous permet de définir des règles de mappage au niveau du sous-réseau IP pour personnaliser les paramètres IP sur des machines virtuelles à l'aide de l'outil de personnalisation DR IP Customizer. Vous pouvez utiliser des règles de mappage au niveau du sous-réseau IP en association avec l'outil DR IP Customizer. Pour plus d'informations sur les moyens d'utiliser des règles de mappage au niveau du sous-réseau IP avec l'outil DR IP Customizer, reportez-vous à [Personnalisation des propriétés IP pour plusieurs machines virtuelles](#).

Conditions préalables

- Utilisez l'outil DR IP Customizer sur un ordinateur ayant accès aux instances de vCenter Server de votre environnement.
- Si vous utilisez Site Recovery Manager pour Windows, le compte d'utilisateur que vous avez utilisé pour exécuter l'outil DR IP Customizer requiert au minimum le rôle d'administrateur des plans de récupération de Site Recovery Manager.
- Si vous utilisez le dispositif Site Recovery Manager Virtual Appliance, vous devez utiliser le protocole SSH avec l'utilisateur Admin.

Procédure

- 1 Connectez-vous à l'hôte Site Recovery Manager Server et ouvrez un interpréteur de commande.
- 2 Remplacez le répertoire de travail par :
 - Pour Windows, `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin`.
 - Pour Linux, `/opt/vmware/srm/bin/`.
- 3 Exécutez la commande `dr-ip-customizer` afin de générer un fichier CSV (comma-separated-value) contenant des informations sur les machines virtuelles protégées.
 - Si vous avez une instance de Platform Services Controller avec une seule instance de vCenter Server

Pour Windows, exécutez la commande suivante :

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml"
--cmd generate --out "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Pour Linux, exécutez la commande suivante :

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd generate --out "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Cet exemple indique `dr-ip-customizer` sur le fichier `vmware-dr.xml` de Site Recovery Manager Server et génère le fichier CSV pour l'instance de vCenter Server qui est associé à Platform Services Controller sur `https://Platform_Services_Controller_address`.

- Si vous disposez de Platform Services Controller qui inclut plusieurs instances de vCenter Server, vous devez spécifier l'ID de vCenter Server du paramètre `--vcid`. Si vous ne spécifiez pas `--vcid`, ou si vous fournissez un ID incorrect, l'outil répertorie toutes les instances disponibles de vCenter Server.

Pour Windows, exécutez la commande suivante :

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml"
--cmd generate --out "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Pour Linux, exécutez la commande suivante :

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd generate --out "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Cet exemple indique `dr-ip-customizer` sur le fichier `vmware-dr.xml` de Site Recovery Manager Server et génère le fichier CSV pour l'instance de vCenter Server avec l'ID `vCenter_Server_ID`.

Note L'ID de vCenter Server n'est pas identique au nom de vCenter Server.

- 4 (Requis) Vérifiez l'empreinte de vCenter Server et entrez **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` 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.

- Si vous avez une instance de Platform Services Controller avec une seule instance de vCenter Server

Pour Windows, exécutez la commande suivante :

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml"
--cmd apply --csv "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Pour Linux, exécutez la commande suivante :

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd apply --csv "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
```

Cet exemple indique `dr-ip-customizer` sur le fichier `vmware-dr.xml` de Site Recovery Manager Server et applique les personnalisations au fichier CSV sur vCenter Server qui est associé à Platform Services Controller sur `https://Platform_Services_Controller_address`.

- Si vous disposez de Platform Services Controller qui inclut plusieurs instances de vCenter Server, vous devez spécifier l'ID de vCenter Server du paramètre `--vcid`.

Pour Windows, exécutez la commande suivante :

```
dr-ip-customizer.exe --cfg "C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml"
--cmd apply --csv "C:\tmp\output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Pour Linux, exécutez la commande suivante :

```
/opt/vmware/srm/bin/dr-ip-customizer --cfg "/opt/vmware/srm/conf/vmware-dr.xml"
--cmd apply --csv "/home/admin/output.csv"
--uri "https://Platform_Services_Controller_address[:port]/lookupservice/sdk"
--vcid vCenter_Server_ID
```

Cet exemple indique `dr-ip-customizer` sur le fichier `vmware-dr.xml` de Site Recovery Manager Server et applique les personnalisations au fichier CSV sur l'instance de vCenter Server avec l'ID `vCenter_Server_ID`.

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.

Personnaliser les propriétés IP pour plusieurs machines virtuelles en définissant des règles de personnalisation

Vous pouvez spécifier une seule règle de mappage IP au niveau du sous-réseau pour un mappage de réseau virtuel configuré spécifique sur les sites protégés et de récupération.

Grâce au mappage au niveau du sous-réseau, il n'est plus nécessaire de définir un mappage IP exact au niveau de l'adaptateur. À la place, spécifiez une règle de personnalisation IP que Site Recovery Manager applique aux adaptateurs appropriés. La règle de personnalisation IP est utilisée pour les workflows de test et de récupération. Vous ne pouvez pas réutiliser les règles de personnalisation IP d'un mappage réseau à l'autre.

Important

- Les règles de mappage de sous-réseau IP prennent uniquement en charge le protocole IPv4.
 - La personnalisation IPv6 basée sur les règles n'est pas prise en charge dans Site Recovery Manager.
 - Lorsque vous appliquez les règles de mappage de sous-réseau IP à des machines virtuelles Windows sur lesquelles l'adresse IPv6 est activée, les paramètres, le protocole DHCP ou l'adresse statique IPv6 restent inchangés après la récupération. Pour les machines virtuelles Linux, les paramètres IPv6 sont réinitialisés sur DHCP.
 - Site Recovery Manager n'évalue pas les règles de mappage IP pour les machines virtuelles configurées pour utiliser la personnalisation IP manuelle.
-

La règle de personnalisation IP s'applique aux machines virtuelles basculées d'un sous-réseau IPv4 de site protégé vers un sous-réseau IPv4 de site de récupération, par exemple de 10.17.23.0/24 vers 10.18.22.0/24. La règle de personnalisation IP indique que, pendant la récupération, Site Recovery Manager évalue la configuration IP existante des cartes réseau de la machine virtuelle récupérée et reconfigure les cartes réseau statiques trouvées sur le sous-réseau 10.17.23.0/24 pour le sous-réseau 10.18.22.0/24.

Si la règle correspond, Site Recovery Manager établit la nouvelle adresse IPv4 statique à partir de l'ancienne en conservant les bits d'hôte de l'adresse IPv4 d'origine et en les plaçant sur le sous-réseau cible. Par exemple, si l'adresse du site protégé d'origine est 10.17.23.55/24, la nouvelle adresse est 10.18.22.55/24.

Si la zone de texte de passerelle par défaut est vide, Site Recovery Manager dérive le nouveau paramètre de passerelle à partir de celui d'origine en conservant les bits d'hôte de l'adresse IPv4 d'origine et en les plaçant dans le sous-réseau cible. Par exemple, si la passerelle du site protégé d'origine est 10.17.23.1, la nouvelle passerelle est 10.18.22.1. Si vous spécifiez un paramètre de passerelle explicite, Site Recovery Manager vérifie que la syntaxe de l'adresse IPv4 est correcte et l'applique exactement.

Site Recovery Manager applique le DNS et d'autres paramètres, tels que spécifiés. Les cartes réseau sur lesquelles DHCP est activée ne peuvent pas être personnalisées, car leur configuration réseau reste inchangée pendant la récupération.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Paire de sites**, cliquez sur **Configurer > Mappages de réseau**.
- 4 Sélectionnez un mappage de réseau pour lequel définir une règle de personnalisation.
- 5 Pour définir une règle, cliquez sur **Ajouter une règle de personnalisation IP**.
- 6 Spécifiez les plages d'IP de sous-réseau à mapper aux sites protégé et de récupération.
- 7 Spécifiez les paramètres réseau pour le réseau du site de récupération.
- 8 Cliquez sur **Ajouter** pour enregistrer vos modifications.

Reprotection des machines virtuelles après une récupération

9

Après une récupération, le site de récupération devient le site principal, mais les machines virtuelles ne sont pas encore protégées. Si le site protégé d'origine est opérationnel, vous pouvez inverser la direction de protection afin d'utiliser le site protégé d'origine comme nouveau site de récupération.

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 comporte une fonction de reprotection qui permet d'inverser la protection de manière automatisée.

Dès que Site Recovery Manager effectue une récupération, les machines virtuelles démarrent sur le site de récupération. 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 lancer le processus de reprotection uniquement si la récupération se termine sans erreur. 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.

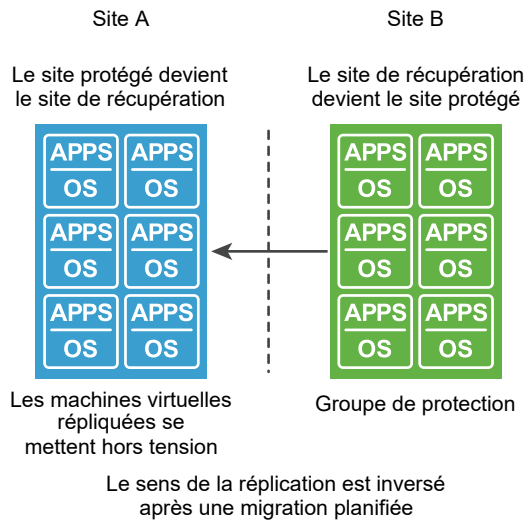
Vous pouvez effectuer la reprotection sur des plans de récupération contenant des groupes de protection de réplication basée sur la baie, des groupes de protection vSphere Replication et des groupes de protection de stratégie de stockage.

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 se met hors ligne, exécutez le workflow de récupération d'urgence sur le plan de récupération pour mettre en ligne les machines virtuelles sur le site B. Après la récupération, les machines virtuelles protégées du site A démarrent sur le site B, sans protection.

Lorsque le site A revient en ligne, vous terminez la récupération en effectuant une migration planifiée, car les machines virtuelles et les banques de données du site A doivent être mises hors tension et démontées avant l'inversion de la protection. Lancez ensuite 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 la réplication du site B vers le site A.

Figure 9-1. Processus de reprotection de Site Recovery Manager



- **Reprotection par Site Recovery Manager des machines virtuelles avec la réplication basée sur la baie**

Au cours du processus de reprotection avec la réplication basée sur la baie, Site Recovery Manager inverse la direction de la protection, puis force une synchronisation du stockage du nouveau site protégé vers le nouveau site de récupération.

- **Comment Site Recovery Manager reprotège les machines virtuelles avec vSphere Replication**

Au cours du processus de reprotection à l'aide de vSphere Replication, Site Recovery Manager inverse la direction de la protection, puis force une synchronisation du stockage du nouveau site protégé vers le nouveau site de récupération.

- **Reprotection de machines virtuelles par Site Recovery Manager avec une protection de stratégie de stockage**

Au cours du processus de reprotection à l'aide d'une protection de stratégie de stockage, Site Recovery Manager inverse la direction de la réplication et protège les machines virtuelles associées aux stratégies de stockage correspondantes sur ce qui était précédemment le site de récupération. Site Recovery Manager rétablit la protection de l'entité vSphere et la surveillance sur le nouveau site protégé.

- **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. Après une opération de reprotection, vous pouvez restaurer les machines virtuelles sur leur site initial à l'aide d'un workflow de migration planifiée.

■ Présentation des états de reprotection

Le processus de reprotection peut passer par plusieurs états qui s'affichent dans le plan de récupération dans l'interface utilisateur de Site Recovery.

Reprotection par Site Recovery Manager des machines virtuelles avec la réplication basée sur la baie

Au cours du processus de reprotection avec la réplication basée sur la baie, Site Recovery Manager inverse la direction de la 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 sous-jacentes d'inverser le sens de réplication. Après l'inversion de la réplication, Site Recovery Manager crée des machines virtuelles à espace réservé sur le nouveau site de récupération (qui était le site protégé initial, avant l'opération de reprotection).

Lors de la création des machines virtuelles réservées sur le nouveau site protégé, Site Recovery Manager utilise l'emplacement de la machine virtuelle protégée initiale pour déterminer l'emplacement dans lequel créer la machine virtuelle réservée. Site Recovery Manager utilise l'identité de la machine virtuelle protégée initiale pour créer l'espace réservé. 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 réservées. Vous devez configurer les mappages d'inventaire sur les deux sites avant d'exécuter le processus de reprotection, sous peine d'échec du processus.

Lors de la reprotection de machines virtuelles à l'aide de la réplication basée sur la baie, Site Recovery Manager place les fichiers des machines virtuelles réservées dans la banque de données réservée 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 le processus de reprotection est terminé.

Comment Site Recovery Manager reprotège les machines virtuelles avec vSphere Replication

Au cours du processus de reprotection à l'aide de vSphere Replication, Site Recovery Manager inverse la direction de la protection, puis force une synchronisation du stockage du nouveau site protégé vers le nouveau site de récupération.

Lors de la reprotection à l'aide de vSphere Replication, Site Recovery Manager utilise les fichiers VMDK d'origine en tant que 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.

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 le processus de reprotection est terminé.

Pour configurer manuellement la réplication inverse sur une machine virtuelle protégée vSphere Replication, utilisez l'interface utilisateur de Site Recovery pour forcer l'arrêt du groupe de réplication entrante sur l'ancien site de récupération, qui est désormais le site protégé. Si vous supprimez simplement la machine virtuelle sur le site protégé d'origine, la reprotection échouera.

Reprotection de machines virtuelles par Site Recovery Manager avec une protection de stratégie de stockage

Au cours du processus de reprotection à l'aide d'une protection de stratégie de stockage, Site Recovery Manager inverse la direction de la réplication et protège les machines virtuelles associées aux stratégies de stockage correspondantes sur ce qui était précédemment le site de récupération. Site Recovery Manager rétablit la protection de l'entité vSphere et la surveillance sur le nouveau site protégé.

L'inversion de la réplication d'un groupe de protection de stratégie de stockage est identique à l'inversion de la réplication d'un groupe de protection de réplication basée sur la baie, car elle n'affecte que le stockage sous-jacent. Lorsque vous effectuez une reprotection sur un plan de récupération incluant un groupe de protection de stratégie de stockage, la technologie de réplication fournie par vos baies de stockage inverse la réplication de tous les groupes de cohérence associés aux stratégies de stockage contenues dans le groupe de protection.

Si les baies de stockage échouent à inverser la réplication de l'un des groupes de cohérence dans le groupe de protection, le plan de protection passe à l'état Reprotection incomplète. Dans cet état, vous devez résoudre les problèmes de stockage et réexécuter la reprotection. La réexécution de la reprotection sur un groupe de protection de stratégie de stockage affecte uniquement la direction de la réplication des groupes de cohérence pour lesquels l'opération de reprotection précédente a échoué.

Une fois que les baies de stockage ont inversé la direction de la réplication, Site Recovery Manager rétablit la protection et la surveillance de l'entité vSphere. Les conditions du rétablissement de la protection et de la surveillance de l'entité vSphere pendant la reprotection sont moins strictes que celles de l'établissement de la protection et de la surveillance de l'entité vSphere pendant la création d'un groupe de protection de stratégie de stockage :

- Site Recovery Manager vérifie la conformité des stratégies de stockage du nouveau site protégé. Si les stratégies de stockage du nouveau site protégé ne sont pas conformes, la reprotection n'échoue pas, mais Site Recovery Manager ne peut pas protéger les machines virtuelles associées à cette stratégie de stockage. Pour plus d'informations sur la conformité, reportez-vous aux sections [Conditions préalables pour les groupes de protection de stratégie de stockage](#) et [Limitations des groupes de protection de stratégie de stockage](#).
- Site Recovery Manager redémarre la surveillance de l'entité vSphere sur le nouveau site protégé.
- Site Recovery Manager démarre la protection de toutes les machines virtuelles conformes. Cet ensemble de machines virtuelles peut être différent de celui qui a été récupéré lorsque vous avez exécuté le plan de récupération initial, car vous-même ou un autre utilisateur avez peut-être associé davantage de machines virtuelles à la stratégie de stockage sur le nouveau site protégé. La reprotection n'échoue pas si Site Recovery Manager ne parvient pas à protéger une machine virtuelle sur le nouveau site protégé.
- Le groupe de protection de stratégie de stockage est prêt pour la récupération entre le nouveau site protégé et 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.

Vous pouvez effectuer la reprotection sur des plans de récupération contenant des groupes de protection de réplication basée sur la baie, des groupes de protection vSphere Replication et des groupes de protection de stratégie de stockage.

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 de vCenter Server, les serveurs ESXi, les instances de Site Recovery Manager Server 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. Après une opération de reprotection, vous pouvez restaurer les machines virtuelles sur leur site initial à l'aide d'un workflow de migration planifiée.

Conditions préalables

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

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Cliquez sur l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération, puis cliquez sur **Reprotéger**.
- 4 Cochez la case pour confirmer que vous comprenez que l'opération de reprotection est irréversible.
- 5 (Facultatif) Pour ignorer les erreurs au cours de l'opération de nettoyage sur le site de récupération, sélectionnez la case à cocher **Forcer le nettoyage**, puis cliquez sur **Suivant**.
L'option **Forcer le nettoyage** est disponible uniquement quand vous avez effectué une opération de reprotection initiale au cours de laquelle des erreurs se sont produites.
- 6 Vérifiez les informations sur la reprotection et cliquez sur **Terminer**.

- 7 Pour surveiller la progression de l'opération de reprotection, sélectionnez le plan de récupération et cliquez sur onglet **Étapes de récupération**.
- 8 Lorsque l'opération de reprotection est terminée, sélectionnez le plan de récupération, cliquez sur **Historique**, puis sur le bouton **Exporter le rapport pour l'élément d'historique sélectionné**.

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.

Présentation des états de reprotection

Le processus de reprotection peut passer par plusieurs états qui s'affichent dans le plan de récupération dans l'interface utilisateur de Site Recovery.

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

Tableau 9-1. États de reprotection

État	Description	Mesure corrective
Reprotection en cours	Site Recovery Manager exécute la reprotection.	aucune
Reprotection partielle	Elle se produit lorsque plusieurs plans de récupération partagent les mêmes groupes de protection et que certains groupes de protection ont été reprotégés sans erreur dans un autre plan.	Exécutez une nouvelle reprotection des plans reprotégés en partie.

Tableau 9-1. États de reprotection (suite)

État	Description	Mesure corrective
Reprotection incomplète	Apparaît à cause d'échecs lors de la reprotection. Par exemple, cet état peut survenir en raison d'un échec de réplication inverse ou d'un échec de création de machines virtuelles à espace réservé.	<ul style="list-style-type: none"> ■ Si une opération de reprotection n'a pas pu effectuer une réplication inverse, assurez-vous que les sites sont connectés, vérifiez la progression de la reprotection dans l'interface utilisateur de Site Recovery, puis redémarrez la tâche de reprotection. Si la reprotection ne réussit toujours pas, exécutez-la à nouveau à l'aide de l'option Forcer le nettoyage. ■ Si la création de machines virtuelles réservées par Site Recovery Manager échoue, il est toujours possible de procéder à une récupération. Vérifiez les étapes de reprotection dans l'interface utilisateur de Site Recovery, corrigez les problèmes et réexécutez la reprotection.
Reprotection interrompue	Ce problème se produit si 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 relancez la tâche de reprotection.
Prêt	Cet état apparaît lorsque l'opération de reprotection se termine sans erreur.	Aucune.

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

10

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 9 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 Pour arrêter les machines virtuelles du site protégé et démarrer les machines virtuelles du site de récupération, effectuez une migration planifiée. Pour éviter les ruptures de disponibilité des machines virtuelles, il peut être judicieux d'effectuer un test avant 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.

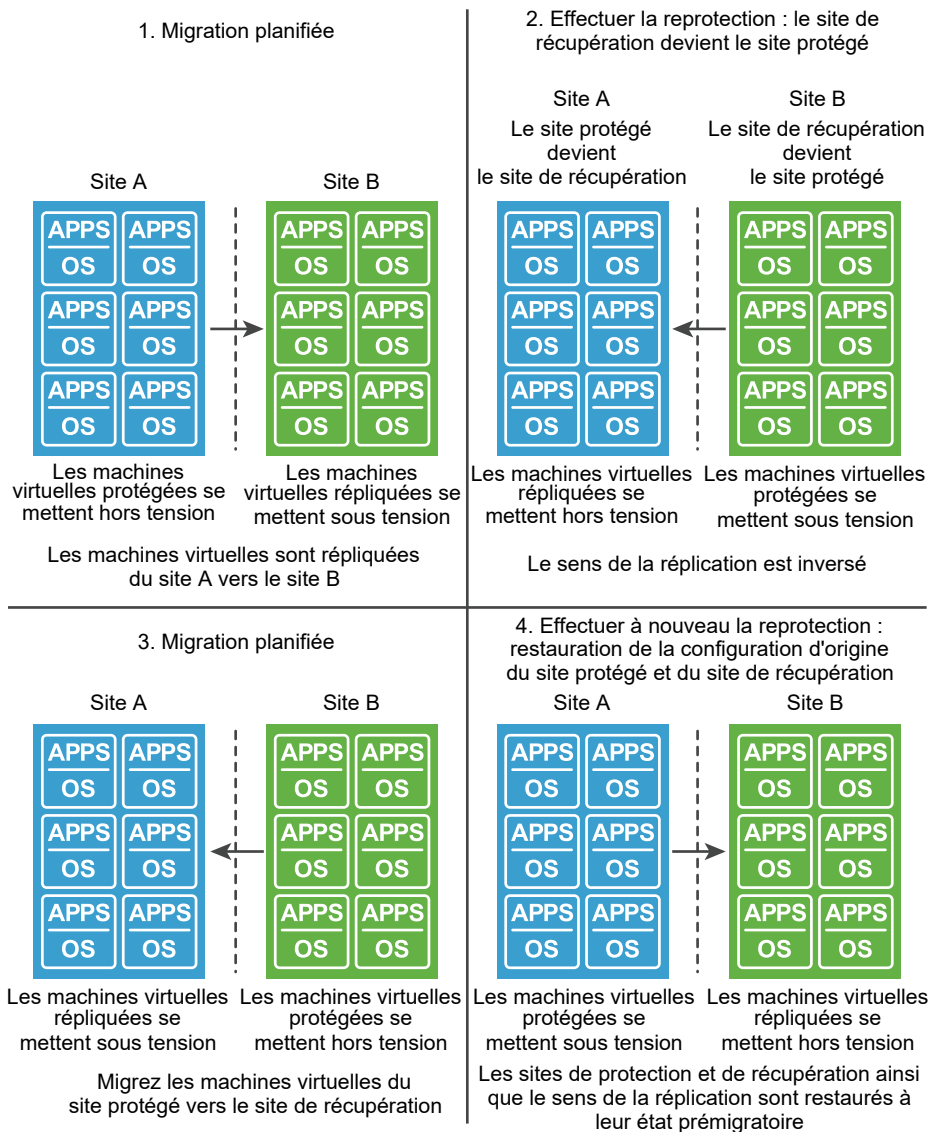
Vous pouvez configurer et exécuter un retour arrière lorsque vous êtes prêt à rétablir les services pour le site protégé d'origine, après l'avoir ramené en ligne après un incident.

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.

- 1 Les machines virtuelles se répliquent du site A vers le site B.
- 2 Effectuer une reprotection. Le site B, précédemment site de récupération, devient le site protégé. Site Recovery Manager utilise les informations de protection pour établir la protection du site B. Le site A devient le site de récupération.
- 3 Pour récupérer les machines virtuelles protégées du site B vers le site A, effectuez une migration planifiée.
- 4 Effectuez une deuxième reprotection. Le site A devient le site protégé et le site B le site de récupération.

Figure 10-1. Processus de retour arrière de 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.

Après une récupération du site A vers le site B, les machines virtuelles récupérées sont en cours d'exécution sur le site B sans protection.

Conditions préalables

- 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.
- Vous n'avez effectué aucune reprotection depuis la récupération.
- Si vous avez procédé à une récupération d'urgence, vous devez effectuer une migration planifiée lorsque les hôtes et les banques de données du site protégé d'origine sont à nouveau en cours d'exécution.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Plans de récupération**, cliquez avec le bouton droit sur un plan de récupération, puis cliquez sur **Reprotéger**.
- 4 Cochez la case pour confirmer que vous comprenez que l'opération de reprotection est irréversible.
- 5 Déterminez s'il convient d'activer l'option **Forcer le nettoyage** et cliquez sur **Suivant**.
L'option **Forcer le nettoyage** est uniquement disponible une fois l'exécution de la reprotection terminée et en cas d'erreur. L'activation de cette option force la suppression des machines virtuelles, en ignorant les erreurs, et renvoie le plan de récupération à l'état **Prêt**.
- 6 Vérifiez les informations sur la reprotection et cliquez sur **Terminer**.
- 7 Sélectionnez le plan de récupération et cliquez sur **Étapes de récupération** pour surveiller l'opération de reprotection jusqu'à ce qu'elle se termine.
- 8 (Requis) 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 inverse la réplication, de sorte que le site de récupération d'origine, le site B, est dorénavant le site protégé.
- 9 Pour exécuter le plan de récupération en tant que migration planifiée, cliquez avec le bouton droit sur le plan de récupération, puis cliquez sur **Récupération**.
- 10 Sélectionnez le plan de récupération et cliquez sur **Étapes de récupération** pour surveiller la migration planifiée jusqu'à ce qu'elle se termine.
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 avec le bouton droit sur le plan de récupération, puis cliquez sur **Reprotéger** et suivez les instructions de l'assistant pour effectuer une seconde opération de reprotection.

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.

Interoperabilité de Site Recovery Manager avec d'autres logiciels

11

Site Recovery Manager Server fonctionne en tant qu'extension de vCenter Server sur un site. Site Recovery Manager est compatible avec d'autres solutions VMware et des logiciels tiers.

Vous pouvez exécuter d'autres solutions VMware, telles que vCenter Update Manager, vCenter Server Heartbeat, VMware Fault Tolerance, vSphere Storage vMotion et vSphere Storage DRS dans des déploiements que vous protégez à l'aide de Site Recovery Manager. Soyez vigilant avant de connecter d'autres solutions VMware à l'instance vCenter Server auquel Site Recovery Manager Server est connecté. Le fait de connecter d'autres solutions VMware à la même instance vCenter Server que Site Recovery Manager peut générer des problèmes lors de la mise à niveau de Site Recovery Manager ou vSphere. Vérifiez la compatibilité et l'interopérabilité des versions de ces solutions avec votre version de Site Recovery Manager en consultant les *matrices d'interopérabilité des produits VMware*.

Ce chapitre contient les rubriques suivantes :

- Site Recovery Manager et vCenter Server
- Utilisation de Site Recovery Manager avec le stockage VMware vSAN et vSphere Replication
- Interaction de Site Recovery Manager avec DPM et DRS lors d'une récupération
- Interaction entre Site Recovery Manager et Storage DRS ou Storage vMotion
- Interaction entre Site Recovery Manager et vSphere High Availability
- Interaction de Site Recovery Manager avec le stockage étiré
- Utilisation de Site Recovery Manager avec NSX Data Center for vSphere
- Site Recovery Manager et vSphere PowerCLI
- Site Recovery Manager et chiffrement des machines virtuelles
- Site Recovery Manager et vRealize Orchestrator
- Protection de machines virtuelles MSCS (Microsoft Cluster Server) et tolérantes aux pannes
- Utilisation de Site Recovery Manager avec les banques de données SIOC
- Utilisation de Site Recovery Manager avec des clusters de contrôle d'admission
- Site Recovery Manager et machines virtuelles associées aux périphériques de disque RDM
- Site Recovery Manager et contrôleurs de domaine Active Directory

Site Recovery Manager et vCenter Server

Site Recovery Manager exploite les services de vCenter Server, tels que la gestion de stockage, l'authentification, l'autorisation et la personnalisation de l'invité. Site Recovery Manager utilise également l'ensemble standard d'outils d'administration de vSphere pour gérer ces services.

Étant donné que Site Recovery Manager Server dépend de vCenter Server pour certains services, vous devez installer et configurer vCenter Server sur un site avant d'installer Site Recovery Manager.

Vous pouvez utiliser Site Recovery Manager et vSphere Replication avec vCenter Server Appliance ou avec une installation standard de vCenter Server. Vous pouvez avoir une installation de vCenter Server Appliance sur un site et une installation standard de vCenter Server sur l'autre site.

Effet des modifications de l'inventaire vCenter Server sur Site Recovery Manager

Étant donné que les groupes de protection Site Recovery Manager s'appliquent à un sous-ensemble de l'inventaire vCenter Server, les modifications apportées à l'inventaire protégé par les administrateurs et les utilisateurs de vCenter Server peuvent affecter l'intégrité de la protection et de la récupération de Site Recovery Manager. Site Recovery Manager dépend de la disponibilité de certains objets, tels que les machines virtuelles, les dossiers, les pools de ressources et les réseaux, dans l'inventaire vCenter Server sur les sites protégé et de récupération. La suppression de ressources, telles que des dossiers ou réseaux référencés par les plans de récupération, peut invalider le plan. Le changement de nom ou le déplacement d'objets dans l'inventaire vCenter Server n'affecte pas Site Recovery Manager, à moins que cela n'entraîne l'inaccessibilité des ressources au cours du test ou de la récupération.

Dans le cas de la réplication basée sur la baie et de vSphere Replication, Site Recovery Manager peut tolérer certaines modifications sur le site protégé sans interruption.

- Suppression de machines virtuelles protégées.
- Suppression d'un objet pour lequel un mappage d'inventaire existe.

Site Recovery Manager peut tolérer un certain nombre de modifications sur le site de récupération, sans interruption.

- Déplacement des machines virtuelles à espace réservé vers un dossier ou pool de ressources différent.
- Suppression d'un objet pour lequel un mappage d'inventaire existe.

Note Les groupes de protection de stratégie de stockage gèrent les modifications différemment. Reportez-vous à [Mappages d'inventaire pour les groupes de protection de stratégie de stockage](#).

Site Recovery Manager et base de données vCenter Server

Si vous mettez à jour l'installation de vCenter Server étendue par Site Recovery Manager, ne réinitialisez pas la base de données vCenter Server au cours de cette mise à jour. Site Recovery Manager stocke les informations d'identification concernant tous les objets vCenter Server dans la base de données Site Recovery Manager. Si vous réinitialisez la base de données vCenter Server, les données d'identification que Site Recovery Manager a stockées ne correspondront plus aux informations d'identification dans la nouvelle instance de vCenter Server et les objets seront introuvables.

Utilisation de Site Recovery Manager avec le stockage VMware vSAN et vSphere Replication

Vous pouvez utiliser le stockage VMware vSAN avec Site Recovery Manager et vSphere Replication.

Site Recovery Manager prend en charge vSphere Replication avec vSAN. Vous ne pouvez pas utiliser le stockage vSAN avec une réplication basée sur la baie.

Pour plus d'informations sur les versions compatibles de vSphere Replication et vSAN, reportez-vous à la section *Matrices d'interopérabilité des produits VMware* à l'adresse https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Pour plus d'informations sur l'utilisation de vSphere Replication avec vSAN, reportez-vous à la section *Utilisation de vSphere Replication avec le stockage VMware vSAN* dans *Administration de vSphere Replication*.

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 les clusters sur le site de récupération et vérifie que tous les hôtes qui se trouvent dans le cluster sont mis sous tension au début de la récupération ou de la récupération test. Cela garantit une capacité d'hôte suffisante lors de la récupération des machines virtuelles. Une fois la récupération ou le test terminé, Site Recovery Manager rétablit les valeurs initiales des paramètres DPM sur le cluster du site de récupération.

Pour les opérations de migration planifiée et de reprotection, Site Recovery Manager désactive également DPM sur les clusters concernés du site protégé et vérifie que tous les hôtes du cluster sont mis sous tension. Site Recovery Manager peut ainsi exécuter des opérations au niveau de l'hôte, par exemple le démontage des banques de données ou le nettoyage du stockage après une opération de reprotection. Une fois l'opération de migration planifiée ou de récupération terminée, Site Recovery Manager restaure les paramètres DPM sur le cluster sur le site protégé à leurs valeurs d'origine.

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.

Pour plus d'informations sur la manière dont Site Recovery Manager gère le balisage des banques de données pour Storage DRS, consultez <http://kb.vmware.com/kb/2108196>.

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.

- Storage DRS tient compte du statut de protection et de réplication des banques de données lors du calcul des recommandations de placement pour réaliser une migration automatique ou manuelle. Storage DRS vérifie si la banque de données est répliquée, dans le cadre d'un groupe de cohérence ou d'un groupe de protection, puis attribue les balises adéquates à la banque de données. Pour plus d'informations sur la façon dont Site Recovery Manager gère le balisage des [banques de données](#), reportez-vous à .

- Site Recovery Manager prend en charge les clusters de Storage DRS qui contiennent des banques de données provenant de différents groupes de cohérence. Si vous migrez une machine virtuelle vers une banque de données qui ne fait pas partie d'un groupe de protection, vous devrez reconfigurer le groupe de protection de manière à inclure cette banque de données.
- Site Recovery Manager prend en charge Storage vMotion sans limitation entre les banques de données non répliquées et les banques de données répliquées au sein du même groupe de cohérence. Dans ces cas spécifiques, Storage DRS peut réaliser automatiquement Storage vMotion dans des clusters en mode automatique, ou émettre des recommandations pour Storage vMotion dans des clusters en mode manuel.
- Des considérations spéciales s'appliquent à Storage vMotion entre une banque de données répliquée et une banque de données non répliquée, ou entre des banques de données répliquées de différents groupes de cohérence. Dans ces cas spécifiques, Storage DRS n'initie pas ou ne recommande pas automatiquement Storage vMotion. L'initialisation manuelle de Storage vMotion génère un message d'avertissement détaillant l'impact possible.
- 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.

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

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

- vSphere Replication est compatible avec vSphere Storage DRS sur le site protégé et le site de récupération. Sur le site protégé, vous pouvez utiliser Storage DRS pour déplacer les fichiers de disque des machines virtuelles protégées par vSphere Replication sans incidence sur la réplication en cours. Sur le site de récupération, vous pouvez inscrire le dispositif vSphere Replication auprès du service vCenter Single Sign-On de sorte que Storage DRS puisse identifier les fichiers de disque de réplication sur le cluster Storage DRS et générer des recommandations de migration. Vous pouvez utiliser Storage DRS pour migrer des fichiers de disque de réplication sans incidence sur la récupération suivante. Reportez-vous à la section *Inscrire le dispositif vSphere Replication Appliance avec vCenter Single Sign-On* de la documentation de vSphere Replication pour plus de détails.
- vSphere Replication est compatible avec Storage vMotion sur le site protégé. Vous pouvez utiliser Storage vMotion pour déplacer les fichiers de disque des machines virtuelles répliquées sur le site protégé sans incidence sur la réplication en cours.
- Site Recovery Manager détecte les modifications et bascule vers la machine virtuelle avec succès.
- Site Recovery Manager prend en charge les clusters de Storage DRS sur le site de récupération avec les banques de données contenant les disques de réplication de vSphere Replication.
- 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 la génération par Storage DRS de recommandations de migration ou le déclenchement direct de Storage vMotion si Storage DRS est exécuté en mode entièrement automatique. Ce phénomène a lieu si les règles DRS sont extrêmement agressives ou si un grand nombre de machines virtuelles effectuent simultanément une synchronisation complète. 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.

- Lorsque vous utilisez Storage DRS en mode manuel sur des banques de données de machines virtuelles protégées, des recommandations caduques peuvent exister après un basculement. Après la reprotection des machines virtuelles basculées vers le site d'origine, si vous appliquez ces recommandations caduques de Storage DRS, la VM à espace réservé de Site Recovery Manager se corrompt, entraînant l'échec de la récupération suivante du site d'origine sur les VM pour lesquelles les recommandations de Storage DRS étaient appliquées. Si vous appliquez ces mises à jour caduques, désinscrivez la VM à espace réservé et utilisez l'opération de réparation de Site Recovery Manager pour recréer un espace réservé valide. Pour éviter ce problème, supprimez toutes les recommandations issues d'un basculement précédent depuis ce site en régénérant les recommandations de Storage DRS pour le cluster concerné de Storage DRS une fois la reprotection réalisée avec succès.

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.

Interaction de Site Recovery Manager avec le stockage étiré

La prise en charge du stockage étiré est disponible pour la réplication basée sur la baie.

Site Recovery Manager prend en charge le stockage étiré actif-actif entre le site protégé et le site de récupération à l'aide de Cross vCenter Server vMotion pour effectuer des migrations planifiées, ce qui élimine le temps d'arrêt prolongé du service. La récupération d'urgence et le test de récupération continuent d'utiliser la fonctionnalité de récupération basée sur le LUN existant.

Important Le stockage étiré est pris en charge uniquement dans les environnements vCenter Single Sign-On en mode Enhanced Linked Mode. La migration planifiée avec Cross vCenter Server vMotion échoue si les sites ne sont pas au mode Enhanced Linked Mode. Le stockage étiré est requis lorsque vous utilisez une migration vMotion entre plusieurs serveurs vCenter Server pendant une migration planifiée.

Groupes de protection

Important Les groupes de protection pour le stockage étiré doivent être créés en tant que groupes de protection de stratégie de stockage. Vous devez créer et utiliser des profils de stockage pour protéger et récupérer des périphériques de stockage étiré.

- Les groupes de protection comportant des périphériques étirés doivent avoir une direction préférée du site protégé au site de récupération. La direction préférée doit correspondre à la préférence de site que la baie conserve pour les périphériques correspondants. Si la baie prend en charge la préférence de site, le site protégé doit donc avoir la préférence de site.
- Les machines virtuelles étirées et non étirées et les groupes de cohérence peuvent être dans les mêmes groupes de protection et le même plan de récupération.
- Les machines virtuelles étirées doivent se situer sur une banque de données étirée et être sous tension sur le site protégé.
- Vous ne pouvez pas créer deux groupes de protection dans un sens opposé en utilisant la même paire de périphériques étirés. Vous pouvez placer des machines virtuelles sur les périphériques étirés du site de récupération qui correspondent aux périphériques protégés sur le site protégé, mais si le site de récupération ESXi monte le stockage du site protégé, un il existe un risque d'endommagement des données. Vous ne pouvez pas protéger ces machines virtuelles, mais elles sont protégées automatiquement pendant le processus de reprotection.

Migration planifiée

- L'assistant **Exécuter le plan de récupération** dispose d'une option permettant d'utiliser Cross vCenter Server vMotion pour effectuer une migration planifiée. Si l'option est sélectionnée, Cross vCenter Server vMotion est utilisé pour toutes les machines virtuelles sous tension et protégées sur le stockage étiré du site protégé. Si l'option n'est pas sélectionnée, le workflow de récupération standard est utilisé pour les réplicas de LUN, y compris le stockage étiré.
- Si Cross vCenter Server vMotion échoue, quelle qu'en soit la raison, le plan de récupération s'arrête à l'étape Migration des VM et ne continue pas. Si vous ne pouvez pas résoudre le problème qui empêche Site Recovery Manager d'utiliser Cross vCenter Server vMotion, réexécutez le plan de récupération avec l'option vSphere vMotion désactivée. La migration peut ensuite utiliser le workflow de récupération standard pour les réplicas de LUN.

- Pendant l'étape de désactivation, les périphériques étirés restent montés sur le site protégé, même si vMotion n'est pas utilisé. Site Recovery Manager ignore les répliques de machines virtuelles non protégées sur les périphériques étirés sur le site protégé et n'annule pas leur enregistrement.

Test de récupération

- Le test de récupération est effectué à l'aide du workflow de test de récupération standard pour les répliques de périphériques, y compris les périphériques étirés. Des vérifications de compatibilité de vMotion sont effectuées pour chaque machine virtuelle située sur les périphériques étirés.
- Si la baie ne prend pas en charge la création de snapshots en lecture-écriture pour les périphériques étirés, Site Recovery Manager ne vous autorise pas à effectuer un test de récupération pour ces périphériques.

Opération de migration vMotion entre plusieurs serveurs vCenter Server

Cross vCenter Server vMotion n'est pas pris en charge pour la migration d'un groupe de ports vSphere Distributed Switch vers un réseau de commutation standard. Dans cette instance, toute tentative de migration d'une machine virtuelle à l'aide de Cross vCenter Server vMotion entraîne ces messages d'erreur.

- Impossible de trouver un hôte dans le cluster <cluster-name> qui soit compatible avec l'instance de Cross vCenter Server vMotion de la machine virtuelle <vm-name> du groupe de protection <PG-name>.
- L'interface réseau connectée actuellement, <network-adapter-name>, ne peut pas utiliser le réseau <network-name>, car le type du réseau de destination n'est pas pris en charge pour vMotion en fonction du type du réseau source.

Cross vCenter Server vMotion ne fonctionne pas dans les cas suivants :

- Si le DRS est désactivé pour le cluster
- Si la machine virtuelle a des snapshots
- Si la machine virtuelle est un clone lié

La configuration requise pour l'opération de migration vMotion entre plusieurs serveurs vCenter Server dans vSphere est traitée dans la documentation d'*ESXi et vCenter Server 6.7*.

Utilisation de Site Recovery Manager avec NSX Data Center for vSphere

Site Recovery Manager peut protéger les machines virtuelles associées aux réseaux NSX présentes sur le site protégé et le site de récupération sans devoir configurer de mappages d'inventaire.

NSX Data Center for vSphere prend en charge les commutateurs logiques universels qui permettent la création de réseaux de couche 2 qui étendent les limites du système vCenter Server. Lorsque vous utilisez des commutateurs logiques universels avec NSX, un groupe de ports virtuels situé sur le site protégé et sur le site de récupération se connecte au même réseau de couche 2. Cela signifie que lorsque vous utilisez des groupes de protection de stratégie de stockage et un commutateur logique universel, vous n'avez pas besoin de spécifier de mappage réseau. Site Recovery Manager fonctionne avec NSX Data Center for vSphere pour mapper automatiquement la machine virtuelle au réseau correct du site de récupération.

Vous pouvez remplacer le mappage automatique en configurant manuellement des mappages sur les réseaux étirés. Les topologies Enhanced Linked Mode et non-Enhanced Linked Mode sont prises en charge.

Limitations

- Le mappage automatique des câbles universels NSX est **uniquement** pris en charge avec les groupes de protection de stratégie de stockage et les commutateurs logiques universels.
- Le mappage automatique de réseau pour les groupes de protection de stratégie de stockage n'est pas pris en charge sur VMware NSX-T™ Data Center.
- Pour les groupes de protection de machine virtuelle, vous devez configurer explicitement le mappage réseau entre deux extrémités du câble universel pour vous assurer que les machines virtuelles sont récupérées sur le même câble universel.
- Cette fonctionnalité est prise en charge uniquement pour une récupération complète. Le basculement de test doit être effectué manuellement.

Consultez [Configurer les mappages d'inventaire](#) pour plus d'informations.

Site Recovery Manager et vSphere PowerCLI

VMware vSphere PowerCLI fournit une interface Windows PowerShell pour l'accès à la ligne de commande pour les tâches Site Recovery Manager.

vSphere PowerCLI expose les API Site Recovery Manager. Vous pouvez utiliser vSphere PowerCLI pour administrer Site Recovery Manager ou pour créer des scripts qui automatisent les tâches Site Recovery Manager.

Pour plus d'informations sur la gestion de Site Recovery Manager à l'aide de vSphere PowerCLI, consultez la documentation vSphere PowerCLI à l'adresse <https://www.vmware.com/support/developer/PowerCLI/>.

Site Recovery Manager et chiffrement des machines virtuelles

Vous pouvez utiliser Site Recovery Manager pour protéger et récupérer des machines virtuelles chiffrées avec des groupes de protection basés sur la baie, des groupes de protection de stratégie de stockage et des groupes de protection vSphere Replication.

Le chiffrement protège non seulement votre machine virtuelle, mais également les disques de machine virtuelle et autres fichiers. Vous configurez une connexion approuvée entre l'instance de vCenter Server et un serveur de gestion des clés (KMS). L'instance de vCenter Server peut ensuite récupérer les clés auprès du serveur de gestion des clés si nécessaire. Vous devez utiliser un cluster KMS enregistré avec le même nom sur les sites protégés et de récupération. Pour plus d'informations, reportez-vous à la section *Configurer le cluster KMS* du guide *Administration de VMware vSAN*.

Pour effectuer une personnalisation d'invité des machines virtuelles chiffrées, Site Recovery Manager requiert ESXi 6.5 ou version ultérieure.

Pour plus d'informations sur le chiffrement des machines virtuelles, reportez-vous à la section [Chiffrement de la machine virtuelle](#) dans la documentation de *Sécurité vSphere*.

Pour plus d'informations sur les groupes de protections de stratégie de stockage et les machines virtuelles chiffrées, reportez-vous à la section [Protection d'une machine virtuelle chiffrée](#).

Pour plus d'informations sur vSphere Replication et les machines virtuelles chiffrées, reportez-vous à la section [Réplication de machines virtuelles chiffrées](#) dans la documentation *Administration de vSphere Replication*.

Site Recovery Manager et vRealize Orchestrator

Le vRealize Orchestrator Plug-in pour Site Recovery Manager vous permet d'automatiser certaines opérations de Site Recovery Manager en les incluant dans les workflows de vRealize Orchestrator.

Le vRealize Orchestrator Plug-in pour Site Recovery Manager inclut des actions et des workflows qui exécutent des opérations de Site Recovery Manager. Si vous êtes un administrateur de vRealize Orchestrator, vous pouvez créer des workflows qui incluent les actions et les workflows à partir du plug-in Site Recovery Manager. En incluant les actions et les workflows de Site Recovery Manager dans les workflows de vRealize Orchestrator, vous pouvez combiner des opérations de Site Recovery Manager avec les opérations automatisées que d'autres plug-in vRealize Orchestrator fournissent.

Vous pouvez créer par exemple un workflow qui utilise les actions et les workflows du plug-in vRealize Orchestrator pour vCenter Server pour créer et configurer des machines virtuelles et les enregistrer avec vCenter Server. Dans le même workflow, vous pouvez utiliser les actions et les workflows du plug-in Site Recovery Manager pour créer des groupes de protection et protéger les machines virtuelles dès leur création. Vous pouvez utiliser également des actions et des workflows de Site Recovery Manager pour configurer certains des paramètres de récupération pour les machines virtuelles protégées. La combinaison des actions et des workflows de vCenter Server et de Site Recovery Manager dans un workflow vRealize Orchestrator vous permet ainsi d'automatiser le processus de création et de protection des machines virtuelles.

Vous pouvez utiliser le vRealize Orchestrator Plug-in pour Site Recovery Manager dans une configuration du site de récupération partagée dans laquelle vous connectez plusieurs instances de Site Recovery Manager en une instance unique de vCenter Server. Vous pouvez également utiliser le vRealize Orchestrator Plug-in pour Site Recovery Manager avec plusieurs instances de Site Recovery Manager sur plusieurs instances de vCenter Server connectées sur le même serveur vCenter Single Sign-On.

Pour obtenir des informations sur la création des workflows en utilisant vRealize Orchestrator, consultez la [documentation de vRealize Orchestrator](#).

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 répllication basée sur la baie. La protection de machines virtuelles MSCS avec vSphere Replication n'est pas prise en charge.
- La protection et la reprotction de machines virtuelles MSCS ou tolérantes aux pannes requièrent VMware High Availability (HA) et VMware Distributed Resource Scheduler (DRS) sur le site protégé et le site de récupération. Lorsque vous transférez des machines virtuelles MSCS ou tolérantes aux pannes entre leurs sites principaux et secondaires au cours de la reprotction, 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](#).
- Vous pouvez utiliser la répllication basée sur la baie pour protéger plusieurs machines virtuelles à tolérance de panne (SMP-FT) avec vCPU. Les fichiers de disque des machines virtuelles à tolérance de panne principale et secondaire doivent résider sur des LUN répliqués, et tous les LUN doivent faire partie du même groupe de cohérence.
- Site Recovery Manager tente de basculer uniquement l'instance principale de la machine virtuelle SMP-FT et n'essaye pas de revenir sur la machine virtuelle SMP-FT secondaire si un élément est incorrect dans les fichiers de la machine virtuelle SMP-FT principale.
- Site Recovery Manager ne produit pas d'avertissement lorsqu'une machine virtuelle SMP-FT est protégée et que son stockage ne respecte pas la configuration requise pour la répllication.

- Une machine virtuelle SMP-FT ne peut être protégée que par un seul groupe de protection.
- Site Recovery Manager ne prend pas en charge les machines virtuelles SMP-FT répliquées par vSphere Replication.
- Site Recovery Manager ne prend pas en charge les machines virtuelles SMP-FT dans des groupes de protection de stratégie de stockage. SMP-FT ne prend pas en charge les profils de stockage.
- Lors de la reprotection, Site Recovery Manager ne conserve pas la configuration SMP-FT sur le site protégé d'origine.
- Lorsque vous effectuez le basculement, la machine virtuelle de destination est sous tension en tant que machine virtuelle sans tolérance de panne. Elle peut être configurée en tant que machine virtuelle SMP-FT après le basculement à l'aide d'outils en dehors de Site Recovery Manager.

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 hôte ESXi. Vous pouvez disposer d'un maximum de cinq nœuds MSCS sur un hôte ESXi.

Cluster sur boîtiers

Vous pouvez répartir le cluster MSCS sur un maximum de cinq instances d'hôte ESXi. Vous pouvez uniquement protéger un seul nœud de machine virtuelle d'un cluster MSCS sur une instance d'hôte ESXi. 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).

- 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 Cluster sur boîtiers (cluster-across-boxes) 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.

Utilisation de Site Recovery Manager avec les banques de données SIOC

Site Recovery Manager offre la prise en charge intégrale de Storage I/O Control (SIOC).

Migration planifiée des machines virtuelles sur des banques de données utilisant SIOC

Dans les versions précédentes de Site Recovery Manager, vous deviez désactiver Storage I/O Control (SIOC) sur les banques de données que vous aviez incluses dans un plan de récupération avant d'exécuter une migration planifiée. Cette version de Site Recovery Manager offre la prise en charge intégrale de SIOC, et vous n'avez donc pas besoin de désactiver SIOC avant d'exécuter une migration planifiée.

Récupération d'urgence et reprotection des machines virtuelles sur des banques de données utilisant SIOC

Dans les versions précédentes de Site Recovery Manager, si vous exécutiez une récupération d'urgence et que SIOC était activé, la récupération réussissait avec des erreurs. Après la récupération, vous deviez désactiver manuellement SIOC sur le site protégé et exécuter de nouveau une récupération de la migration planifiée. Vous ne pouviez exécuter la fonction de reprotection qu'après avoir exécuté avec succès une migration planifiée. Cette version de Site Recovery Manager offre la prise en charge intégrale de SIOC ; par conséquent, la récupération réussit sans erreurs et vous pouvez exécuter la migration planifiée et la reprotection après une récupération d'urgence sans devoir désactiver SIOC.

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 -HAAdmissionControlEnabled:$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 -HAAdmissionControlEnabled:$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.

Site Recovery Manager et machines virtuelles associées aux périphériques de disque 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 utilisez une réplication basée sur la baie ou vSphere Replication.

Note Site Recovery Manager ne prend pas en charge la protection de machines virtuelles attachées à des périphériques RDM dans des groupes de protection de stratégie de stockage.

- La réplication basée sur la baie prend en charge les périphériques RDM en mode de compatibilité physique et en mode de compatibilité virtuelle. Si vous utilisez Site Recovery Manager avec la réplication basée sur la baie, vous pouvez protéger et récupérer les machines virtuelles qui utilisent RDM en mode de compatibilité physique ou en mode de compatibilité virtuelle.
- vSphere Replication prend en charge des périphériques RDM en mode virtuel uniquement, pour les périphériques source et cible. Si vous utilisez vSphere Replication, vous ne pouvez pas protéger et récupérer les machines virtuelles qui utilisent RDM en mode de compatibilité physique.
- Si vous utilisez à la fois la réplication basée sur la baie et vSphere Replication, vous ne pouvez protéger et récupérer que les machines virtuelles qui utilisent RDM en mode de compatibilité physique à l'aide de la réplication basée sur la baie. Vous pouvez protéger et récupérer les machines virtuelles qui utilisent RDM en mode de compatibilité virtuelle à l'aide de la réplication basée sur la baie ou de vSphere Replication.

Site Recovery Manager et contrôleurs de domaine Active Directory

Site Recovery Manager peut prendre en charge la protection des machines virtuelles qui servent de contrôleurs de domaine Active Directory comme toutes les autres applications prises en charge par Site Recovery Manager.

Au lieu de la technologie de réplication Active Directory native et du mode de restauration, vous pouvez utiliser Site Recovery Manager pour protéger l'infrastructure Active Directory en cas de catastrophe. Si vous rencontrez des problèmes, ils peuvent être liés à des configurations réseau et des interdépendances de contrôleur de domaine spécifiques.

Configuration avancée de Site Recovery Manager

12

La configuration par défaut de Site Recovery Manager permet de réaliser un certain nombre de scénarios de récupération simples. Les utilisateurs avancés peuvent personnaliser Site Recovery Manager afin de répondre à un plus grand nombre de besoins en termes de récupération de site.

Ce chapitre contient les rubriques suivantes :

- [Reconfigurer les paramètres de Site Recovery Manager](#)
- [Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager](#)

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 des connexions

Site Recovery Manager communique avec d'autres services.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Connexions**.

- 4 Sélectionnez un site, puis cliquez sur **Modifier** pour modifier les paramètres.

Option	Action
Modifiez le nombre d'échecs des commandes Ping avant qu'un événement d'arrêt du site ne soit émis. La valeur par défaut est 5.	Entrez une nouvelle valeur dans la zone de texte <code>connections.hmsPanicDelay</code> .
Modifiez le nombre de tentatives de contrôle de l'état (tests Ping) avant que le résultat du contrôle ne soit déclaré comme un échec. La valeur par défaut est 2.	Entrez une nouvelle valeur dans la zone de texte <code>connections.hmsPingFailedDelay</code> .
Modifiez la valeur du délai d'expiration pour le temps d'attente des mises à jour en provenance de serveurs. La valeur par défaut est de 900 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>connections.waitForUpdatesTimeout</code> .

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

Modifier le paramètre de collecte du rapport d'historique de Site Recovery Manager

Les rapports d'historique de Site Recovery Manager sont utiles pour diagnostiquer le comportement de Site Recovery Manager Server avant et après une panne. Vous pouvez modifier le nombre de rapports d'historique à exporter.

Lorsque vous exécutez des opérations de basculement, de test, de nettoyage et de reprotection, le site A étant le site protégé et le site B étant le site de récupération, vous pouvez exporter les rapports d'historique de ces opérations lorsque vous collectez des bundles de support pour le site B, le site de récupération. L'historique le plus récent est récupéré directement à partir de la base de données Site Recovery Manager.

Après la reprotection, le site A devient le nouveau site de récupération et le site B devient le site protégé. Lorsque vous exécutez des opérations de basculement, de test, de nettoyage et de reprotection, vous pouvez exporter des rapports d'historique lorsque vous collectez un bundle de support pour le site A, le site de récupération.

Conditions préalables

- Vérifiez que vous disposez d'informations d'identification d'administrateur.
- Site Recovery Manager doit être connecté à une base de données Site Recovery Manager à laquelle vous pouvez accéder avec des informations d'identification de base de données valides.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Exporter l'historique**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres.
- 5 Remplacez la valeur de **exportHistory.numReports** si nécessaire.
Vous pouvez entrer une valeur comprise entre 0 et 50. La valeur par défaut est 5.
- 6 Si vous ne souhaitez pas exporter de rapports, définissez la valeur sur zéro (0).
- 7 Cliquez sur **OK** pour enregistrer vos modifications.

Modifier les paramètres du site local

Site Recovery Manager surveille la consommation des ressources sur l'hôte de Site Recovery Manager Server 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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > État du site local**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres.

Option	Action
Modifiez la différence de temps selon laquelle Site Recovery Manager contrôle l'utilisation du CPU, l'espace disque et la mémoire disponible sur le site local. La valeur par défaut est 60 secondes.	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.checkInterval .
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 disponible sur le site local. La valeur par défaut est 600 secondes.	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.eventFrequency .
Modifiez la différence de temps maximale autorisée entre les horloges du serveur. La valeur par défaut est 20 (secondes).	Entrez une nouvelle valeur dans la zone de texte localSiteStatus.maxClockSkew . Si l'heure de l'horloge du serveur détectée et celle de Site Recovery Manager Server diffèrent d'un nombre de secondes supérieur à la valeur définie, Site Recovery Manager génère un événement.

Option	Action
Modifiez le pourcentage d'utilisation du CPU qui provoque l'émission d'un événement d'utilisation élevé du CPU par Site Recovery Manager. La valeur par défaut est 70.	Entrez une nouvelle valeur dans la zone de texte <code>localSiteStatus.maxCpuUsage</code> .
Modifiez le nombre de jours précédant Site Recovery Manager l'expiration du certificat avant l'émission d'un événement d'expiration de certificat. La valeur par défaut est de 30 jours.	Entrez une nouvelle valeur dans la zone de texte <code>localSiteStatus.minCertRemainingTime</code> .
Modifiez le pourcentage d'espace disque disponible qui provoque l'émission d'un événement d'espace disque faible par Site Recovery Manager. La valeur par défaut est de 100 Mo.	Entrez une nouvelle valeur dans la zone de texte <code>localSiteStatus.minDiskSpace</code> .
Modifiez la quantité de mémoire disponible provoquant l'émission d'un événement de mémoire insuffisante par Site Recovery Manager. La valeur par défaut est 32 Mo.	Entrez une nouvelle valeur dans la zone de texte <code>localSiteStatus.minMemory</code> .

- 5 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 Site Recovery Manager Server.

Site Recovery Manager Server effectue une rotation des journaux. Lorsque vous redémarrez le Site Recovery Manager Server ou qu'un fichier journal devient trop volumineux, le Site Recovery Manager Server crée un fichier journal et écrit tous les messages suivants dans ce nouveau fichier. Lorsque Site Recovery Manager Server 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 Site Recovery Manager Server, 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 Site Recovery Manager Server.

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.

détaillé

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.

Note Définissez ce niveau de journalisation seulement lorsque vous y êtes invité par le support technique de VMware pour aider à résoudre un problème.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Gestionnaire de journaux**.

4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres 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
Définissez le niveau de journalisation pour tous les composants qui ne disposent pas d'une entrée dans logManager. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Default .
Définissez le niveau de journalisation pour le module API externe. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.ExternalAPI .
Définissez le niveau de journalisation pour vSphere Replication. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.HbrProvider .
Définissez le niveau de journalisation pour l'outil IP Customizer. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.IPCustomizer .
Définissez le niveau de journalisation pour le mappage d'inventaire. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.InventoryMapper .
Définissez le niveau de journalisation pour les problèmes de licence. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Licensing .
Définissez le niveau de journalisation pour les problèmes de persistance. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Persistence .
Définissez le niveau de journalisation pour les opérations de récupération. La valeur par défaut est trivia.	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Recovery . Par défaut, la journalisation de la récupération est définie sur trivia .
Définissez le niveau de journalisation pour les opérations de configuration de récupération. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.RecoveryConfig .
Définissez le niveau de journalisation pour les opérations de réplication basée sur la baie. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Replication .

Option	Description
Définissez le niveau de journalisation pour les problèmes d'autorisation entre Site Recovery Manager Server et vCenter Server. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.ServerAuthorization .
Définissez le niveau de journalisation pour la gestion des sessions. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.SessionManager .
Définissez le niveau de journalisation pour l'adaptateur de services Web SOAP. La valeur par défaut est info.	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 .
Définissez le niveau de journalisation pour les problèmes de stockage. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.Storage .
Définissez le niveau de journalisation pour les messages provenant du fournisseur de stockage basé sur la baie. La valeur par défaut est verbose (journal détaillé).	Sélectionnez un niveau de journalisation dans le menu déroulant logManager.StorageProvider .

5 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 Site Recovery Manager Server, 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 pendant les 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.

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

- `recovery.autoDeployGuestAlias`
- `recovery.defaultPriority`
- `recovery.powerOnTimeout`
- `recovery.powerOnDelay`

- `recovery.customizationShutdownTimeout`
- `recovery.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

Site Recovery Manager garde une copie des paramètres de récupération de machine virtuelle sur chaque site Site Recovery Manager. Si les paramètres avancés de récupération sont différents sur les sites de protection et de récupération, Site Recovery Manager initialise les paramètres de récupération pour une machine virtuelle avec des valeurs différentes sur chacun des sites. Lorsque Site Recovery Manager récupère la machine virtuelle du site A vers le site B, il applique les paramètres de récupération locaux pour le site B. Lors d'une récupération du site B vers le site A, Site Recovery Manager applique les paramètres de récupération locaux pour le site A. Cette condition persiste jusqu'à ce que vous modifiiez explicitement et enregistriez chacun des paramètres de récupération des machines virtuelles dans l'onglet Machines virtuelles du plan de récupération. Les paramètres de récupération pour la machine virtuelle concernée sont synchronisés et deviennent identiques sur les deux sites Site Recovery Manager.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Récupération**.

- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres du site de récupération.

Option	Action
<p>Activez ou désactivez la configuration automatique des mappages d'utilisateurs invités. Cette option est uniquement disponible pour les machines virtuelles qui utilisent une version compatible de VMware Tools. La valeur par défaut est true.</p> <p>Pour plus d'informations sur les versions compatibles de VMware Tools, reportez-vous à <i>Matrices de compatibilité pour Site Recovery Manager 8.2</i>.</p>	<p>Sélectionnez la valeur de recovery.autoDeployGuestAlias pour activer ou désactiver la configuration automatique des mappages d'utilisateurs invités.</p> <p>Si la valeur est définie sur true, Site Recovery Manager crée des mappages d'utilisateurs invités dans le système d'exploitation invité de toutes les VM lors de la récupération et les supprime lorsque le processus de récupération est terminé. Pour utiliser cette option, vous devez installer une version compatible de VMware Tools et configurer la personnalisation IP ou les appels d'hôte sur les VM à récupérer. Avant d'exécuter la récupération, veillez à la synchronisation temporelle entre les hôtes ESXi et le serveur vCenter Single Sign-On sur le site de récupération.</p> <p>Si la valeur est définie sur false, vous devez mapper manuellement l'utilisateur local de la solution Site Recovery Manager du site de récupération à un compte d'utilisateur invité sur la VM protégée. L'utilisateur du système d'exploitation invité doit disposer des autorisations nécessaires pour exécuter des commandes et doit accéder aux fichiers dans le système d'exploitation invité. Si vous configurez une personnalisation IP ou des appels d'hôte, vous devez veiller à la synchronisation temporelle entre le système d'exploitation invité de la VM protégée et les serveurs vCenter Single Sign-On sur le site de récupération.</p> <p>Si vos sites Site Recovery Manager reposent sur le mode Enhanced Linked Mode, vous pouvez utiliser vSphere Web Client pour configurer les mappages d'utilisateurs invités.</p> <p>Pour plus d'informations sur la configuration des mappages d'utilisateurs invités, reportez-vous au chapitre <i>Configuration des mappages d'utilisateurs sur des systèmes d'exploitation invités</i> de la documentation <i>VMware vSphere ESXi et vCenter Server</i>.</p> <p>Si vos sites Site Recovery Manager ne sont pas en mode Enhanced Linked Mode, vous devez utiliser l'API vSphere API pour configurer les mappages d'utilisateurs invités et faire en sorte que le certificat d'alias soit mappé. Il est recommandé d'utiliser les certificats de signature du serveur vCenter Single Sign-On. Pour plus d'informations sur l'API vSphere, reportez-vous à la documentation <i>VMware vSphere API Reference</i>.</p>
<p>Modifiez le délai d'expiration de la mise hors tension de la machine virtuelle dans la rubrique de personnalisation de l'adresse IP. La valeur par défaut est de 300 secondes.</p>	<p>Entrez une nouvelle valeur dans la zone de texte recovery.customizationShutdownTimeout. Cette valeur est le délai d'expiration minimal en secondes de la mise hors tension de la machine virtuelle utilisé uniquement dans le workflow de personnalisation de l'adresse IP. Si vous spécifiez le délai d'expiration de la mise hors tension dans les paramètres de récupération de la machine virtuelle, la plus grande des deux valeurs est prioritaire.</p>
<p>Modifier l'expiration de la personnalisation d'IP. La valeur par défaut est 600 secondes.</p>	<p>Entrez une nouvelle valeur dans la zone de texte recovery.customizationTimeout. Cette valeur est le délai d'expiration utilisé dans la préparation des scripts de personnalisation de l'adresse IP sur l'instance de Site Recovery Manager Server. Vous avez rarement besoin de changer cette valeur.</p>
<p>Modifier la priorité par défaut pour la récupération d'une machine virtuelle. La valeur par défaut est 3.</p>	<p>Entrez une nouvelle valeur dans la zone de texte recovery.defaultPriority.</p>

Option	Action
Activer ou désactiver la récupération forcée. La valeur par défaut est false .	Cochez ou décochez la case recovery.forceRecovery . Activez la récupération forcée si une absence de connectivité au site protégé affecte sérieusement RTO. Ce paramètre supprime uniquement la restriction pour sélectionner la récupération forcée lors de l'exécution d'un plan de récupération. Pour activer de fait la récupération forcée, sélectionnez-la lorsque vous exécutez un plan.
Modifier le délai d'expiration pour la mise sous tension des hôtes dans un cluster. La valeur par défaut est 1200 secondes.	Entrez une nouvelle valeur dans la zone de texte recovery.hostPowerOnTimeout .
Modifiez la valeur du délai d'attente avant la fin de l'arrêt client précédant la mise hors tension des machines virtuelles. La valeur par défaut est de 300 secondes.	<p>Entrez une nouvelle valeur dans la zone de texte recovery.powerOffTimeout. Cette valeur définit le délai d'attente du système d'exploitation invité avant la tentative de mise hors tension, en dernier recours, pour arrêter les machines virtuelles.</p> <p>Note Les machines virtuelles se mettent hors tension à l'expiration du délai. Si l'arrêt du système d'exploitation de la machine virtuelle n'est pas terminé à l'expiration du délai, des données risquent d'être perdues. Dans le cas d'une grande machine virtuelle qui nécessite davantage de temps pour s'arrêter normalement, réglez le délai de mise hors tension du système d'exploitation invité individuellement pour cette machine virtuelle comme décrit dans Configurer les options de démarrage et d'arrêt de machine virtuelle.</p>
Modifier le délai après la mise sous tension d'une machine virtuelle avant le lancement des tâches dépendantes. La valeur par défaut est 0.	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.
Modifier le délai d'attente de VMware Tools lors de la mise sous tension des machines virtuelles. La valeur par défaut est de 300 secondes.	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 des machines virtuelles protégées, définissez cette valeur sur 0 pour ignorer le délai d'attente de VMware Tools lors de la mise sous tension de ces machines virtuelles et éviter une erreur de délai d'attente dans SRM.

Option	Action
Activer ou désactiver l'évitement de l'arrêt du système d'exploitation client. La valeur par défaut est false.	<p>Cochez ou décochez la case recovery.skipGuestShutdown.</p> <p>Si skipGuestShutdown=true, Site Recovery Manager ne tente pas d'arrêter le système d'exploitation invité sur les machines virtuelles du site de protection, mais les met directement hors tension. Dans ce cas, la valeur définie pour recovery.powerOffTimeout n'a aucun effet associé à ce paramètre. Si VMware Tools n'est pas installé sur la machine virtuelle, activez ce paramètre pour éviter une erreur d'arrêt du système d'exploitation invité dans Site Recovery Manager.</p> <p>Vous pouvez également activer l'option permettant de mettre directement hors tension des machines virtuelles sans délai d'attente avant l'arrêt en contournant le système d'exploitation invité. Reportez-vous à Configurer les options de démarrage et d'arrêt de machine virtuelle.</p>
Activez ou désactivez la personnalisation IP VM automatique lors de la récupération. La valeur par défaut est true.	<p>Cochez ou décochez la case recovery.uselpMapperAutomatically. Si vous sélectionnez l'option et que les règles de mappage IP sont configurées pour les réseaux virtuels, alors Site Recovery Manager évalue ces règles pendant la récupération afin de personnaliser les VM. Si vous désactivez l'option, les règles de mappage IP ne sont pas évaluées lors de la récupération. Vous pouvez remplacer l'option pour chaque VM en Mode de personnalisation IP Paramètres de récupération de VM.</p>

5 Cliquez sur **OK** pour enregistrer vos modifications.

Étape suivante

Pour appliquer les modifications aux machines virtuelles que vous avez protégées précédemment, vous devez reconfigurer ces machines virtuelles. 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 appliquer des modifications dans les plans de récupération ou dans les groupes de protection.

Reportez-vous à la section [Appliquer des paramètres de récupération à des machines virtuelles dans un plan de récupération](#) et [Appliquer des paramètres de récupération à des machines virtuelles dans un groupe de protection](#).

Appliquer des paramètres de récupération à des machines virtuelles dans un plan de récupération

Si vous modifiez des paramètres de récupération avancée sur une machine virtuelle protégée, vous devez reconfigurer la machine virtuelle pour que les paramètres s'appliquent.

Pour configurer des paramètres de récupération dans un plan de récupération de manière plus efficace, ciblez un seul paramètre ou une seule machine virtuelle. Dans certains cas, vous pouvez appliquer un paramètre de cette façon uniquement. Par exemple, si vous modifiez les paramètres dans un scénario de récupération d'urgence ou de récupération incomplète.

Procédure

- 1 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 2 Sélectionnez l'onglet **Plans de récupération** et cliquez sur le plan de récupération auquel appartient la machine virtuelle.
- 3 Dans l'onglet **Machines virtuelles**, cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Configurer la récupération**.
- 4 Apportez les modifications de votre choix aux paramètres des propriétés de récupération.
- 5 Cliquez sur **OK**.

Étape suivante

Pour appliquer des paramètres de récupération à des machines virtuelles dans un groupe de protection, reportez-vous à la section [Appliquer des paramètres de récupération à des machines virtuelles dans un groupe de protection](#).

Appliquer des paramètres de récupération à des machines virtuelles dans un groupe de protection

Si vous modifiez des paramètres de récupération avancée pour des machines virtuelles protégées, les nouveaux paramètres s'appliquent uniquement lorsque les machines virtuelles sont reconfigurées.

Il est plus simple pour vous de mettre à jour les paramètres de récupération à l'aide de la fonctionnalité Groupes de protection lorsque vous les appliquez à plusieurs machines virtuelles, bien qu'elle puisse être utilisée pour une seule machine virtuelle. Vous pouvez sélectionner toutes les machines virtuelles d'un groupe de protection et mettre à jour tous les paramètres à la fois.

Procédure

- 1 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 2 Sélectionnez l'onglet **Groupes de protection** et cliquez sur le groupe de protection auquel appartient la machine virtuelle.
- 3 Dans l'onglet **Machines virtuelles**, cliquez avec le bouton droit sur une machine virtuelle, puis cliquez sur **Supprimer la protection**.
L'état de la machine virtuelle passe à Non configuré.
- 4 Cliquez sur **Configurer toutes les VM** pour reconfigurer toutes les machines virtuelles du groupe de protection, ou sélectionnez une machine virtuelle et cliquez sur **Configurer la protection** pour reconfigurer uniquement cette machine virtuelle.

Étape suivante

Pour appliquer des paramètres de récupération à une machine virtuelle dans un plan de récupération, reportez-vous à la section [Appliquer des paramètres de récupération à des machines virtuelles dans un plan de récupération](#).

Modifier les paramètres du gestionnaire distant

Si vous exécutez des tâches dont l'exécution est longue, le délai d'expiration par défaut sur le site distant peut s'écouler avant la fin des tâches. Vous pouvez configurer des délais d'expiration supplémentaires pour permettre à de longues tâches de se terminer.

Une tâche longue peut être la récupération test ou le nettoyage d'une grande machine virtuelle. Si une machine virtuelle dispose de disques volumineux, l'exécution d'une récupération test ou d'une récupération complète peut prendre longtemps. Le délai d'expiration par défaut surveille la connectivité entre les sites. Si une tâche prend plus de temps que le délai d'expiration par défaut et n'envoie pas de notifications à l'autre site pendant son exécution, SRM peut expirer. Dans ce cas, vous pouvez modifier les paramètres du gestionnaire distant de sorte que Site Recovery Manager n'expire pas avant la fin d'une longue tâche.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Gestionnaire distant**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres du gestionnaire distant.

Option	Action
Configurez le temps d'attente maximal pour terminer une opération distante. La valeur par défaut est de 900 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.defaultTimeout</code> .
Marquez une machine virtuelle comme protégée par Site Recovery Manager. La valeur par défaut est <code>true</code> .	Cochez la case <code>remoteManager.enableCustomFields</code> .
Définissez une période d'attente pour les demandes à ajouter au site distant. La valeur par défaut est de 2 000 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.powerOnAggregationInterval</code> .
Configurez le temps d'attente maximal pour arrêter les tâches annulées. La valeur par défaut est de 300 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.taskCancelDefaultTimeout</code> .

Option	Action
Configurez un délai d'expiration supplémentaire pour terminer les tâches sur le site distant. La valeur par défaut est de 900 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.taskDefaultTimeout</code> .
Configurez le nombre de secondes à attendre pour rapporter la progression d'une tâche distante. Si la mise à jour de la progression est reçue dans ce délai, plus de temps est attribué au traitement de la tâche. La valeur par défaut est 180 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.taskProgressDefaultTimeout</code> .
Configurez le nombre de tentatives de mise sous tension d'une machine virtuelle en cas de panne. La valeur par défaut est de 5 tentatives.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.vmPowerOnRetryCount</code> .
Configurez le nombre de tentatives d'arrêt du SE invité d'une machine virtuelle en cas de panne. La valeur par défaut est de 5 tentatives.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.vmGuestShutDownRetryCount</code> .
Configurez le nombre de tentatives de reconfiguration des paramètres d'une machine virtuelle en cas de panne. La valeur par défaut est de 5 tentatives.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.vmReconfigureRetryCount</code> .
Configurez le nombre de secondes à attendre pour l'expiration de xVC-vMotion. La valeur par défaut est de 3 600 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>remoteManager.xVcVMotionTimeout</code> .

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

Modifier les paramètres du site distant

Vous pouvez modifier les valeurs par défaut utilisées par Site Recovery Manager Server sur le site protégé pour déterminer si Site Recovery Manager Server 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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.

- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > État du site distant**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres.

Option	Action
Modifiez le nombre d'échecs des commandes Ping avant qu'un événement d'arrêt du site ne soit émis. La valeur par défaut est 5.	Entrez une nouvelle valeur dans la zone de texte <code>remoteSiteStatus.drPanicDelay</code> .
Modifiez le nombre de tentatives de contrôle de statut du site distant (commandes Ping) avant que le résultat du contrôle ne soit déclaré comme un échec. La valeur par défaut est 2.	Entrez une nouvelle valeur dans la zone de texte <code>remoteSiteStatus.drPingFailedDelay</code> .

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

Modifier les paramètres de réplication

Vous pouvez modifier les paramètres de réplication pour changer le temps d'attente de Site Recovery Manager lors de la création des espaces réservés de machines virtuelles. Vous pouvez également modifier l'intervalle d'interrogation des machines virtuelles des groupes de protection de stratégie de stockage.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Réplication**.
- 4 Sélectionnez un site, puis cliquez sur **Modifier** pour modifier les paramètres.

Option	Action
Ignorer la vérification des répliques de machines virtuelles non protégées tout en désactivant le site de protection pendant la migration planifiée. La valeur par défaut est false.	Cochez la case pour activer la valeur <code>replication.disablePiggybackVmsCheckDuringDeactivate</code> .
Modifier le délai d'attente en secondes lors de la création d'une machine virtuelle à espace réservé. La valeur par défaut est de 300 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>replication.placeholderVmCreationTimeout</code> .

Option	Action
Interroger ponctuellement les machines virtuelles des groupes de protection de stratégie de stockage à la recherche de l'absence de mappages et renvoyer un avertissement, le cas échéant, car tout mappage manquant peut entraîner un échec de la récupération d'un groupe. La valeur par défaut est false.	Cochez la case pour remplacer la valeur de <code>replication.pollForMissingInventoryMappings</code> par true.
Modifier le délai d'attente en secondes pour la réplication des informations sur le groupe de cohérence sur le site distant avant de démarrer une synchronisation en ligne sur ce site. La valeur par défaut est 900 (secondes).	Entrez une nouvelle valeur dans la zone de texte <code>replication.protectionInfoSyncTimeout</code> .
Modifier l'intervalle d'interrogation en secondes pour rechercher dans les groupes de protection de stratégie de stockage l'absence de mappages d'inventaire. La valeur par défaut est 120 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>replication.protectionPollInterval</code> . Note Avant de mettre à jour l'intervalle d'interrogation, estimez les modifications apportées à votre environnement, leur fréquence et les performances de l'environnement.

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

Modifier le paramètre SSO

Vous pouvez modifier le paramètre Single Sign-On de Site Recovery Manager pour renouveler les jetons SSO.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > SSO**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier le paramètre `sso.sts.tokenLifetime` afin de spécifier le nombre de secondes disponibles pour utiliser les jetons SSO avant leur renouvellement.

La valeur par défaut est de 28 800 secondes (8 heures).

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

Modifier les paramètres de stockage

Vous pouvez ajuster les paramètres 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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Stockage**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres de stockage.

Option	Action
Modifiez la durée d'attente, en secondes, avant toute tentative d'association de balises aux banques de données récupérées. La valeur par défaut est de 30 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>storage.attachTagsDelaySec</code> .
Modifiez le délai d'expiration en secondes pour exécuter une commande SRA. La valeur par défaut est de 300 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>storage.commandTimeout</code> .
Modifiez le délai en secondes entre les opérations associées à la surveillance des banques de données. La valeur par défaut est de 30 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>storage.datastoreMonitoringPollingInterval</code> .
Autorisez Site Recovery Manager à créer des catégories de balises et la balise Répliqué que la compatibilité du DRS de stockage requiert. La valeur par défaut est true.	Cochez la case <code>storage.enableSdrsStandardTagCategoryCreation</code> .
Autorisez Site Recovery Manager à créer et à joindre automatiquement des balises aux banques de données répliquées ou protégées pour la compatibilité du DRS de stockage. La valeur par défaut est true.	Cochez la case <code>storage.enableSdrsTagging</code> . Si vous décochez la case, Site Recovery Manager supprime l'ensemble des balises et des catégories de balises, puisrompt la compatibilité avec le DRS de stockage.
Autoriser Site Recovery Manager à réparer les balises manquantes ou incorrectes des banques de données répliquées ou protégées pour la compatibilité du DRS de stockage. La valeur par défaut est true.	Cochez la case <code>storage.enableSdrsTaggingRepair</code> .

Option	Action
Modifiez le nombre maximal d'opérations SRA simultanées. La valeur par défaut est 5.	Entrez une nouvelle valeur dans la zone de texte storage.maxConcurrentCommandCnt .
Modifiez la longueur maximale en octets de la sortie de la console de commande SRA à consigner. La valeur par défaut est 1 048 576 octets (1 Mo).	Entrez une nouvelle valeur dans la zone de texte storage.maxSraCommandOutputLength . <ul style="list-style-type: none"> ■ La valeur 0 signifie qu'il n'y a aucun journal de sortie SRA. ■ La valeur -1 représente une longueur illimitée. ■ Si vous entrez une valeur qui est différente de 0 ou -1, et qu'elle n'est pas comprise dans l'intervalle entre 512 octets et 10 Mo, la valeur est automatiquement définie sur la valeur par défaut, soit 1 Mo.
Modifiez le délai minimum en secondes entre les calculs du groupe de banques de données. La valeur par défaut est 0.	Entrez une nouvelle valeur dans la zone de texte storage.minDsGroupComputationInterval .
Modifiez l'intervalle entre les mises à jour de l'état pour les opérations de synchronisation de données courantes. La valeur par défaut est de 30 secondes.	Entrez une nouvelle valeur dans la zone de texte storage.querySyncStatusPollingInterval .
Modifiez l'intervalle entre les opérations associées au balisage du DRS de stockage. La valeur par défaut est 50 secondes.	Entrez une nouvelle valeur dans la zone de texte storage.sdrsTaggingPollInterval .
Modifiez l'intervalle entre les contrôles de détection de baie de stockage. La valeur par défaut est 86 400 secondes (24 heures).	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. La valeur par défaut est 86 400 secondes (24 heures).	Entrez une nouvelle valeur dans la zone de texte storage.syncTimeout .

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

Modifier les paramètres de stratégie de stockage de la réplication basée sur la baie

Vous pouvez modifier le paramètre de stratégie de stockage de la réplication basée sur la baie pour spécifier l'intervalle (en secondes) auquel exécuter la détection automatique de banques de données correspondant à une stratégie de stockage de machine virtuelle.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.

- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Stratégie de stockage ABR**.
- 4 Sélectionnez un site, puis cliquez sur **Modifier**.
- 5 Remplacez la valeur de **storagePolicyAbrReplication.policyDatastorePollInterval** si nécessaire. La valeur par défaut est 20 secondes.
- 6 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 en secondes. Pour plus d'informations sur ces valeurs, consultez la documentation SRA de votre fournisseur de baies.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Fournisseur de stockage**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres du fournisseur de stockage.

Option	Action
Faire essayer à Site Recovery Manager de détacher et rattacher les LUN avec des volumes dupliqués. La valeur par défaut est true.	Cochez la case storageProvider.autoDetachLUNsWithDuplicateVolume .
Définir l'indicateur IVM.EnableResignature sur les hôtes ESXi pendant le test et la récupération. La valeur par défaut est 0.	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 signe à nouveau 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 signe uniquement les volumes de snapshots VMFS qu'il gère.

Option	Action
Modifiez le délai d'attente en secondes pour attendre que l'opération d'attachement par lot du LUN se termine sur chaque hôte ESXi. La valeur par défaut est de 3 600 secondes.	Entrez une valeur dans la zone de texte storageProvider.batchAttachTimeoutSec.
Modifiez le délai d'attente en secondes pour attendre que l'opération de détachement par lot du LUN se termine sur chaque hôte ESXi. La valeur par défaut est de 3 600 secondes.	Entrez une valeur dans la zone de texte storageProvider.batchDetachTimeoutSec.
Changer l'intervalle pendant lequel Site Recovery Manager attend le montage de volumes VMFS. La valeur par défaut est de 3 600 secondes.	Entrez une nouvelle valeur dans la zone de texte storageProvider.batchMountTimeoutSec. 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.
Changer l'intervalle pendant lequel Site Recovery Manager attend le démontage de volumes VMFS. La valeur par défaut est de 3 600 secondes.	Entrez une nouvelle valeur dans la zone de texte storageProvider.batchUnmountTimeoutSec. Changez cette valeur si vous subissez des expirations de délai d'attente se produisant lorsque Site Recovery Manager vérifie des volumes VMFS dont le démontage est trop long. Ce paramètre est disponible dans Site Recovery Manager 5.5.1 et versions ultérieures.
Définir le nombre de tentatives pour les volumes VMFS/NFS de démontage par lot. La valeur par défaut est 3 tentatives.	Entrez une nouvelle valeur dans la zone de texte storageProvider.datastoreUnmountRetryCount.
Modifier l'intervalle pendant lequel Site Recovery Manager attend avant la tentative de démontage de la banque de données. La valeur par défaut est 1 seconde.	Entrez une nouvelle valeur dans la zone de texte storageProvider.datastoreUnmountRetryDelaySec.
Modifiez la durée d'attente, en secondes, avant l'extraction des banques de données sur les hôtes ESXi après la réception d'une réponse du SRA pendant le test et la récupération. Ce paramètre s'applique uniquement lorsqu'il n'y a pas de périphérique SCSI. La valeur par défaut est 0.	Entrez une nouvelle valeur dans la zone de texte storageProvider.fetchDatastoreDelaySec.
Dès qu'une récupération est réussie, forcer la suppression du préfixe snap-xx appliqué aux noms de banques de données récupérées. La valeur par défaut est false.	Cochez la case storageProvider.fixRecoveredDatastoreNames.

Option	Action
Modifier l'intervalle pendant lequel Site Recovery Manager attend avant la suppression du préfixe <code>snap-xx</code> appliqué aux noms de banques de données récupérées. La valeur par défaut est 0 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>storageProvider.fixRecoveredDatastoreNamesDelaySec</code> .
Retarder les analyses d'hôtes au cours des tests et de la récupération. La valeur par défaut est 0 secondes.	<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 <code>storageProvider.hostRescanDelaySec</code>. Ne modifiez cette valeur que si vous rencontrez des problèmes avec des banques de données indisponibles.</p>
Répéter des analyses d'hôtes pendant le test et la récupération. La valeur par défaut est 1.	Entrez une nouvelle valeur dans la zone de texte <code>storageProvider.hostRescanRepeatCnt</code> . Certaines baies de stockage nécessitent plusieurs réanalyses, par exemple, pour découvrir les snapshots des LUN basculées. Dans les versions précédentes, vous avez peut-être utilisé le paramètre <code>storageProvider.hostRescanRepeatCnt</code> pour introduire un délai dans les récupérations. Utilisez plutôt le paramètre <code>storageProvider.hostRescanDelaySec</code> .
Modifier l'intervalle pendant lequel Site Recovery Manager attend que chaque nouvelle analyse HBA soit terminée. La valeur par défaut est de 300 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>storageProvider.hostRescanTimeoutSec</code> .
Définir le nombre de fois où Site Recovery Manager tente de procéder à la resignature d'un volume VMFS. La valeur par défaut est 1.	Entrez une nouvelle valeur dans la zone de texte <code>storageProvider.resignatureFailureRetryCount</code> .
Définir un délai d'expiration pour la resignature d'un volume VMFS. La valeur par défaut est de 900 secondes.	Entrez une nouvelle valeur dans la zone de texte <code>storageProvider.resignatureTimeoutSec</code> . Si vous modifiez le paramètre <code>storageProvider.hostRescanTimeoutSec</code> , augmentez le paramètre <code>storageProvider.resignatureTimeoutSec</code> en définissant la même valeur de délai d'expiration que vous avez utilisée pour <code>storageProvider.hostRescanTimeoutSec</code> .

Option	Action
Identifier les chemins de fichiers VMX que Site Recovery Manager ne doit pas considérer comme des candidats potentiels de fichiers VMX après Storage vMotion. La valeur par défaut est <code>.snapshot</code> .	Certaines baies créent des chemins de fichiers VMX que l'algorithme de recherche <code>storageProvider.storageVmotionVmxSearch</code> doit ignorer. Entrez une liste de chaînes séparées par une virgule dans la zone de texte <code>storageProvider.storageVmotionVmxFilePathsToSkip</code> , 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.
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. La valeur par défaut est <code>true</code> .	L'option est sélectionnée par défaut. Décochez la case <code>storageProvider.storageVmotionVmxSearch</code> pour désactiver cette option.
Définir le délai d'attente en secondes pour que les périphériques étirés locaux correspondent aux périphériques étirés distants. La valeur par défaut est 300 (secondes).	Entrez la nouvelle valeur dans la zone de texte <code>storageProvider.stretchedDevicesMatchTimeout</code> .
Définir le nombre de demandes xVC-vMotion parallèles par hôte. Cette limite s'applique aux hôtes sources et cibles. La valeur par défaut est 2.	Entrez la nouvelle valeur dans la zone de texte <code>storageProvider.vmMigrationLimitPerHost</code> .
Définir le délai d'attente en secondes pour attendre que les banques de données récemment détectées deviennent accessibles. La valeur par défaut est 60 secondes.	Entrez la nouvelle valeur dans la zone de texte <code>storageProvider.waitForAccessibleDatastoreTimeoutSec</code> .
Activer le délai d'attente avant que Site Recovery Manager découvre des banques de données après récupération.	Cochez la case <code>storageProvider.waitForDeviceRediscovery</code> .
Activez le délai d'attente avant que Site Recovery Manager découvre des banques de données après le basculement.	Cochez la case <code>storageProvider.waitForDeviceRediscoveryAfterPrepareFailover</code> .

Option	Action
Définir le délai d'attente en secondes pour attendre que Virtual Center signale des banques de données récemment détectées. La valeur par défaut est de 30 secondes.	Entrez la nouvelle valeur dans la zone de texte <code>storageProvider.waitForRecoveredDatastoreTimeoutSec</code> .
Définir le délai d'attente en secondes pendant lequel Site Recovery Manager attend le montage de volumes VMFS. La valeur par défaut est de 30 secondes.	Entrez la nouvelle valeur dans la zone de texte <code>storageProvider.waitForVmfsVolumesMountedStateTimeoutSec</code> .

- 5 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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > vSphere Replication**.
- 4 Sélectionnez un site et cliquez sur **Modifier** pour 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 <code>vrReplication.allowOtherSolutionTagInRecovery</code> .
Conserver les anciens snapshots multiples générés à un moment précis au cours de la récupération. La valeur par défaut est true.	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 <code>vrReplication.preserveMpitImagesAsSnapshots</code> .

Option	Description
Modifier le délai d'expiration pour l'inversion de la réplication au cours des opérations de reprotection	Entrez une nouvelle valeur dans la zone de texte vrReplication.reverseReplicationTimeout . La valeur saisie doit être égale à la moitié du délai d'expiration que vous voulez définir. La valeur par défaut est de 7 200 secondes 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.
Modifiez le délai d'expiration des opérations de synchronisation de vSphere Replication La valeur par défaut est de 7 200 secondes.	Entrez une nouvelle valeur dans la zone de texte vrReplication.synchronizationTimeout . La valeur saisie doit être égale à la moitié du délai d'expiration que vous voulez définir. La valeur par défaut est de 7 200 secondes 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 synchronise les machines virtuelles sur le site de récupération.
Modifier le paramètre RPO par défaut pour les répliquions La valeur par défaut est de 240 secondes.	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 répliquions, 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.

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

Modifier les paramètres de télémétrie

Vous pouvez modifier les paramètres de télémétrie de Site Recovery Manager pour spécifier un hôte proxy à utiliser lors de l'envoi des rapports de télémétrie.

Procédure

- 1 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Télémétrie**.

- 4 Sélectionnez un site, puis cliquez sur **Modifier** pour modifier les paramètres.

Option	Description
Spécifiez le nom d'hôte du proxy HTTP à utiliser lors de l'envoi des rapports de télémétrie.	Entrez le nom du proxy HTTP dans la zone de texte <code>telemetry.proxyHost</code> .
Spécifiez le port du proxy HTTP à utiliser lors de l'envoi des rapports de télémétrie.	Entrez le numéro de port dans la zone <code>telemetry.proxyPort</code> .
Spécifiez si le protocole SSL doit être utilisé pour la connexion au proxy HTTP lors de l'envoi des rapports de télémétrie. La valeur par défaut est false.	Déplacez le curseur pour définir le paramètre <code>telemetry.proxyUseSsl</code> sur true.

- 5 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 menus **Paramètres avancés** de vSphere Web Client ou dans le plug-in client de Site Recovery Manager. Pour modifier d'autres paramètres, vous modifiez le fichier de configuration `vmware-dr.xml` sur Site Recovery Manager Server ou sur le Site Recovery Manager Virtual Appliance. Modifiez toujours les paramètres à l'aide des menus du client lorsqu'une telle option existe. Si vous modifiez les paramètres, vous devez apporter les mêmes modifications aux instances de Site Recovery Manager et de vCenter Server, sur le site protégé et sur le site de récupération.

Pour une description des paramètres modifiables, référez-vous à [Paramètres pour grands environnements Site Recovery Manager](#).

Procédure

1 Dans vSphere Web Client ou vSphere Client, sélectionnez un cluster.

2 Dans l'onglet **Gérer**, sélectionnez **Services > vSphere DRS**.

Si vous utilisez vCenter Server 6.0 Update 3, dans l'onglet **Gérer**, sélectionnez **Services > vSphere DRS**

3 Cliquez sur **Edit**.

4 Dans **Options avancées**, définissez le paramètre `srmMaxBootShutdownOps`.

Option	Description
Zone de texte Option	Entrez <code>srmMaxBootShutdownOps</code> .
Zone de texte Valeur	Entrez le nombre maximal d'opérations simultanées de démarrage et d'arrêt. Si, par exemple, vous définissez une valeur égale à 32, cela signifie que les machines virtuelles 1 à 32 démarrent ou s'arrêtent ensemble et que la machine virtuelle 33 démarre ou s'arrête dès que l'une des machines virtuelles du premier lot a terminé. La machine virtuelle 34 démarre lorsque la deuxième machine virtuelle du premier lot a terminé, et ainsi de suite.

5 Cliquez sur **OK** pour enregistrer vos modifications.

6 Ouvrez une session sur l'hôte Site Recovery Manager Server.

7 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.

- Si vous utilisez Site Recovery Manager pour Windows, le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` sur la machine hôte Site Recovery Manager Server.
- Si vous utilisez le Site Recovery Manager Virtual Appliance, le fichier `vmware-dr.xml` se trouve dans le répertoire `/opt/vmware/srm/conf/` sur le dispositif.

8 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, l'invité suivant démarre ou s'arrête dès que l'un du premier lot de 24 a terminé. Cela signifie que les machines virtuelles 1 à 24 démarrent toutes simultanément, puis que la machine virtuelle 25 démarre une fois que l'une des machines virtuelles du premier lot a terminé. La machine virtuelle 26 démarre lorsque la deuxième machine virtuelle du premier lot a terminé, et ainsi de suite.

- 9 Pour appliquer les nouveaux paramètres, redémarrez Site Recovery Manager Server.
- 10 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 11 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 12 Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > vSphere Replication** et augmentez les paramètres `vrReplication.synchronizationTimeout` et `vrReplication.reverseReplicationTimeout`.

La valeur par défaut est de 7 200 secondes et correspond à un délai d'expiration de synchronisation de 14 400 secondes.
- 13 Sélectionnez **Paramètres avancés > Stockage** et augmentez le paramètre `storage.commandTimeout`.

La valeur par défaut est de 300 secondes.
- 14 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 menus **Paramètres avancés** de vSphere Web Client ou dans le plug-in client de Site Recovery Manager. Pour modifier d'autres paramètres, vous modifiez le fichier de configuration `vmware-dr.xml` sur Site Recovery Manager Server ou sur le Site Recovery Manager Virtual Appliance. Modifiez toujours les paramètres à l'aide des menus du client lorsqu'une telle option existe. Si vous modifiez les paramètres, vous devez apporter les mêmes modifications aux instances de Site Recovery Manager et de vCenter Server, sur le site protégé et sur le site de récupération.

Pour modifier les paramètres, voir [Modifier des paramètres pour exécuter de grands environnements Site Recovery Manager](#).

Tableau 12-1. 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 Web Client ou vSphere Client en cliquant avec le bouton droit sur un cluster et en sélectionnant Paramètres . Cliquez sur vSphere DRS , puis sur Modifier > Options avancées . Tapez l'option qui doit remplacer la valeur defaultMaxBootAndShutdownOpsPerCluster que vous pouvez définir dans le fichier <code>vmware-dr.xml</code> . Vous pouvez définir une valeur defaultMaxBootAndShutdownOpsPerCluster dans le fichier <code>vmware-dr.xml</code> , puis définir d'autres valeurs srmMaxBootShutdownOps pour chacun des clusters dans vSphere Web Client ou 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 Web Client remplace la valeur defaultMaxBootAndShutdownOpsPerCluster . Vous pouvez définir une valeur defaultMaxBootAndShutdownOpsPerCluster globale dans le fichier <code>vmware-dr.xml</code> , puis définir d'autres valeurs srmMaxBootShutdownOps pour chacun des clusters dans vSphere Web 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 12-2. Paramètres de modification des périodes d'expiration

Option	Description
<code>vrReplication.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 l'interface utilisateur de Site Recovery. Dans l'onglet Accueil de Site Recovery, sélectionnez une paire de sites et cliquez sur Afficher les détails . Dans le volet de gauche, sélectionnez Configurer > Paramètres avancés > vSphere Replication . La valeur par défaut est de 7 200 secondes et correspond à un délai d'expiration de synchronisation de 14 400 secondes.
<code>vrReplication.reverseReplicationTimeout</code>	Délai d'expiration pour l'inversion de la réplication au cours des opérations de reprotection. Modifiez cette option dans l'interface utilisateur de Site Recovery. Dans l'onglet Accueil de Site Recovery, sélectionnez une paire de sites et cliquez sur Afficher les détails . Dans le volet de gauche, sélectionnez Configurer > Paramètres avancés > vSphere Replication . La valeur par défaut est de 7 200 secondes et correspond à un délai d'expiration de synchronisation de 14 400 secondes.
<code>storage.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 l'interface utilisateur de Site Recovery. Dans l'onglet Accueil de Site Recovery, sélectionnez une paire de sites et cliquez sur Afficher les détails . Dans le volet de gauche, sélectionnez Configurer > Paramètres avancés > Stockage . La valeur par défaut est de 300 secondes.

Évènements et alarmes Site Recovery Manager

13

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.

Ce chapitre contient les rubriques suivantes :

- [Contrôle des connexions entre sites par Site Recovery Manager](#)
- [Créer des alarmes 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. Il enregistre également les événements lorsque le site distant cesse de répondre.

Lorsque Site Recovery Manager établit la connexion entre deux instances couplées de Site Recovery Manager Server, le système Site Recovery Manager Server ayant initié la connexion envoie un événement `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.

- Le moniteur de connexion saute un nombre de pings qui ont échoués. Vous pouvez configurer ce nombre en paramétrant la valeur `remoteSiteStatus.drPingFailedDelay`. Le niveau par défaut est 2.
- Lorsque le nombre de tests Ping ignorés ayant échoué excède la valeur du paramètre `remoteSiteStatus.drPingFailedDelay`, Site Recovery Manager envoie un événement `RemoteSitePingFailedEvent`.

- Lorsque le nombre de tests Ping 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 définissant le paramètre `remoteSiteStatus.drPanicDelay`. Le niveau par défaut est 5.
- Site Recovery Manager continue d'envoyer des événements `RemoteSiteDownEvent` jusqu'à ce que la connexion soit rétablie.
- Lorsqu'une connexion au site distant du serveur Site Recovery Manager est rétablie, Site Recovery Manager envoie des événements `RemoteSiteUpEvent`.

Créer des 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 **Définitions des alarmes** répertorie toutes les alarmes de 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.

Note Dans un environnement comportant plusieurs systèmes vCenter Server, Site Recovery Manager affiche tous les événements des serveurs Site Recovery Manager qui sont enregistrés comme des extensions, même si vous sélectionnez des événements pour un système vCenter Server spécifique.

Conditions préalables

Pour que les alarmes envoient des notifications par e-mail, configurez les paramètres de **Messagerie** dans le menu **Paramètres de vCenter Server**. Consultez la *Documentation ESXi et vCenter Server*.

Procédure

- 1 Dans vSphere Client, cliquez sur une instance de vCenter Server.
- 2 Sous l'onglet **Configurer**, développez le nœud **Plus**, puis cliquez sur **Définitions des alarmes** afin d'afficher la liste des alarmes vCenter Server.
- 3 Cliquez sur **Ajouter** pour ajouter une nouvelle alarme.
- 4 Sur la page **Nom**, entrez un nom d'alarme, une description et cliquez sur **Suivant**.
- 5 Sur la page **Cibles**, sélectionnez une cible dans le menu déroulant et cliquez sur **Suivant**.

- 6 Sur la page **Règle pour les alarmes**, sélectionnez un événement dans le menu déroulant et l'état correspondant.

Si vous voyez des événements répétés dans la liste, chaque événement représente une instance de Site Recovery Manager et déclenche une alarme pour l'extension dans laquelle elle est inscrite. Par exemple, dans un scénario comportant plusieurs instances de Site Recovery Manager, vous pouvez utiliser `RecoveryPlanCreated (SRM 1)` et `RecoveryPlanCreated (SRM 2)` pour le même événement sur les deux extensions.

- 7 Pour ajouter une condition qui déclenche l'alarme, cliquez sur **Argument**, sélectionnez un argument dans le menu déroulant, l'opérateur et le passage de la condition avertissement à la condition critique.
- 8 (Facultatif) Choisissez d'envoyer des notifications par e-mail, des interruptions SNMP ou d'exécuter un script.
- 9 Cliquez sur **Suivant**.
- 10 Sur la page **Vérifier**, choisissez d'activer l'alarme et cliquez sur **Créer**.

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 13-1. Événements de statut du site

Nom de l'événement	Type d'événement	Description de l'événement	Catégorie
État inconnu	<code>UnknownStatusEvent</code>	L'état de Site Recovery Manager Server n'est pas disponible	Info
Site distant en panne	<code>RemoteSiteDownEvent</code>	Site Recovery Manager Server a perdu sa connexion avec l'instance distante de Site Recovery Manager Server.	Erreur
Échec du test ping du site distant	<code>RemoteSitePingFailedEvent</code>	Échecs au niveau du site distant ou problèmes de connectivité réseau.	Avertissement
Site distant créé	<code>RemoteSiteCreatedEvent</code>	Le site local a été couplé au site distant.	Info
Site distant en service	<code>RemoteSiteUpEvent</code>	Site Recovery Manager Server rétablit sa connexion avec l'instance distante de Site Recovery Manager Server.	Info
Site distant supprimé	<code>RemoteSiteDeletedEvent</code>	Le site Site Recovery Manager distant a été supprimé.	Info

Tableau 13-1. Événements de statut du site (suite)

Nom de l'événement	Type d'événement	Description de l'événement	Catégorie
Une machine virtuelle vSphere Replication répliquée est ajoutée à un groupe de protection	HbrGroupVmAssociatedEvent	Une machine virtuelle répliquée par vSphere Replication est ajoutée à un groupe de protection.	Info
Une machine virtuelle vSphere Replication est supprimée d'un groupe de protection	HbrGroupVmDisassociatedEvent	Une machine virtuelle répliquée par vSphere Replication est supprimée d'un groupe de protection.	Info
Le serveur vSphere Replication local est en panne	LocalHmsConnectionDownEvent	Des tentatives de connexion répétées à vSphere Replication échouent.	Erreur
La connexion au serveur vSphere Replication local a été restaurée	LocalHmsConnectionUpEvent	La connexion à vSphere Replication a réussi.	Info
Le serveur vSphere Replication local ne répond pas	LocalHmsPingFailedEvent	Impossible d'établir une connexion au serveur vSphere Replication local	Avertissement
Espace disque faible	LowDiskSpaceEvent	L'espace disque disponible sur le site local est faible.	Avertissement
Mémoire faible	LowMemoryEvent	La mémoire disponible sur le site local est faible.	Avertissement
Certificat de SRM Server pas encore valide	SrmCertificateNotValidEvent	Le certificat SSL/TLS pour le SRM Server spécifié est ultérieur.	Erreur
Expiration du certificat de SRM Server	SrmCertificateExpiringEvent	Le certificat SSL/TLS pour le SRM Server spécifié expire dans le nombre de jours spécifiés.	Info
Le certificat de SRM Server a expiré	SrmCertificateExpiredEvent	Le certificat SSL/TLS pour le SRM Server spécifié a expiré.	Erreur

Événements de groupe de protection

Les événements de groupe de protection fournissent des informations sur les actions et l'état des groupes de protection.

Tableau 13-2. Événements de réplication de groupe de protection

Événement	Description	Cause	Catégorie
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.	Info
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.	Info
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.	Info
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.	Info
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.	Info
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.	Info
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	Paramètres d'emplacement de récupération reconfigurés pour machine virtuelle.	Posté sur le site protégé vCenter Server uniquement lors de l'exécution complète de la reconfiguration des paramètres d'emplacement de récupération pour une machine virtuelle protégée.	Info
PlaceholderVmCreatedEvent	La machine virtuelle à espace réservé a été créée dans l'inventaire vCenter Server.	La machine virtuelle à espace réservé publiée sur le site de récupération vCenter Server est créée suite à une opération de réparation et de protection.	Info
PlaceholderVmCreatedFromOldProductionVmEvent	La machine virtuelle à espace réservé a été créée dans l'inventaire vCenter Server avec l'identité de l'ancienne machine virtuelle protégée.	La machine virtuelle à espace réservé publiée sur le site de récupération vCenter Server est créée après un remplacement de l'ancienne machine virtuelle protégée par une machine virtuelle à espace réservé lors d'une opération de reprotection.	Info
VmFullyProtectedEvent	Machine virtuelle dans un groupe : tous les périphériques non résolus ont été résolus.	Les périphériques précédemment non résolus d'une machine virtuelle protégée ont tous été résolus.	Avertissement

Tableau 13-2. Événements de réplication de groupe de protection (suite)

Événement	Description	Cause	Catégorie
VmNotFullyProtectedEvent	Machine virtuelle dans un groupe : un ou plusieurs dispositifs doivent être configurés pour la protection.	Publié 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 reprotection d'une machine virtuelle.	Avertissement
PlaceholderVmUnexpectedlyDeletedEvent	Machine virtuelle dans un groupe : la machine virtuelle réservée a été supprimée de l'inventaire vCenter Server	Publié sur le site de récupération vCenter Server lorsque Site Recovery Manager détecte que la machine virtuelle à espace réservé a été supprimée ou retirée de l'inventaire vCenter Server de manière imprévue.	Avertissement
ProductionVmDeletedEvent	Machine virtuelle dans un groupe : la machine virtuelle protégée a été supprimée de l'inventaire vCenter Server de la machine virtuelle.	Publié si une machine virtuelle protégée est supprimée ou retirée de l'inventaire vCenter Server.	Erreur
ProductionVmInvalidEvent	Machine virtuelle dans un groupe : Impossible de résoudre les emplacements de fichier de la machine virtuelle protégée pour réplication.	Publié si le fournisseur de réplication ne trouve pas les fichiers de la machine virtuelle protégée pour les répliquer.	Erreur

Événements de récupération

Les événements de récupération fournissent des informations sur les actions et l'état des processus de récupération Site Recovery Manager.

Tableau 13-3. Événements de récupération

Nom de l'événement	Type d'événement	Description de l'événement	Catégorie
Le plan de récupération a commencé à récupérer la machine virtuelle spécifiée.	RecoveryVmBegin	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.	Info
Le plan de récupération a terminé la récupération de la machine virtuelle.	RecoveryVmEnd	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.	Info

Tableau 13-3. Événements de récupération (suite)

Nom de l'événement	Type d'événement	Description de l'événement	Catégorie
Le plan de récupération [data.Plan] a échoué à l'enregistrement de la machine virtuelle [data.Vm].	RecoveryVmRegisterFailed	Signalé dans le cas de groupes de protection de stratégie de stockage après qu'une machine virtuelle récupérée a échoué à s'enregistrer auprès du VC du site de récupération. Si le plan est exécuté sur le VC local, [data.local] est vrai.	Info
Le plan de récupération <i>hostname</i> a été créé.	PlanCreated	Signalé lorsqu'un plan est créé. Il est envoyé à chaque instance de vCenter Server sur laquelle le plan est hébergé.	Info
Le plan de récupération a été détruit.	PlanDestroy	Signalé lorsqu'un plan a été supprimé du site. Notez que sur le site où la suppression du plan a été requise, il peut y avoir un délai d'attente significatif pour supprimer le plan de l'autre site. Il sera envoyé à chaque instance vCenter Server où le plan est hébergé.	Info
Le plan de récupération a été modifié.	PlanEdit	Signalé lorsqu'un plan existant est modifié.	Info
Le plan de récupération a commencé un test.	PlanExecTestBegin	Signalé sur un site de récupération lorsqu'un test de récupération est lancé.	Info
Le plan de récupération a terminé un test.	PlanExecTestEnd	Signalé sur un site de récupération lorsqu'un test de récupération est terminé.	Info
Le plan de récupération a commencé un nettoyage test.	PlanExecCleanupBegin	Signalé sur un site de récupération lorsqu'un nettoyage test est lancé.	Info
Le plan de récupération a terminé un nettoyage test.	PlanExecCleanupEnd	Signalé sur le site de récupération lorsqu'un nettoyage test est terminé.	Info
Le plan de récupération a commencé une récupération.	PlanExecBegin	Signalé sur un site de récupération lorsqu'une récupération est lancée.	Info
Le plan de récupération a terminé une récupération.	PlanExecEnd	Signalé sur un site de récupération lorsqu'une récupération est terminée.	Info
Le plan de récupération a commencé une opération de reprotection.	PlanExecReprotectBegin	Signalé sur le site de récupération lorsqu'une reprotection est lancée.	Info

Tableau 13-3. Événements de récupération (suite)

Nom de l'événement	Type d'événement	Description de l'événement	Catégorie
Le plan de récupération a terminé une opération de reprotection.	PlanExecReprotectEnd	Signalé sur le site de récupération lorsqu'une reprotection est terminée.	Info
Le plan de récupération affiche une invite et attend la saisie de l'utilisateur.	PlanPromptDisplay	Signalé sur le site de récupération lorsqu'une étape d'invite a lieu. La clé est un identifiant unique pour l'invite.	Info
Le plan de récupération a reçu une réponse à son invite.	PlanPromptResponse	Signalé sur le site de récupération lorsqu'une étape d'invite est fermée.	Info
Le plan de récupération a démarré pour exécuter une commande sur la machine Site Recovery Manager Server.	PlanServerCommandBegin	Signalé sur le site de récupération lorsque Site Recovery Manager a commencé à exécuter une commande de légende sur la machine Site Recovery Manager Server.	Info
Le plan de récupération a terminé l'exécution d'une commande sur la machine Site Recovery Manager Server.	PlanServerCommandEnd	Signalé sur le site de récupération lorsque Site Recovery Manager a terminé l'exécution d'une commande de légende sur la machine Site Recovery Manager Server.	Info
Le plan de récupération a commencé l'exécution d'une commande sur une machine virtuelle récupérée.	PlanVmCommandBegin	Signalé sur le site de récupération lorsque Site Recovery Manager a commencé à exécuter une commande de légende sur une machine virtuelle récupérée.	Info
Le Plan de récupération a terminé l'exécution d'une commande sur une machine virtuelle récupérée.	PlanVmCommandEnd	Signalé sur le site de récupération lorsque Site Recovery Manager a terminé l'exécution d'une commande de légende sur une machine virtuelle récupérée.	Info

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 13-4. Événements de SRA

Événement	Description	Cause	Catégorie
StorageAdaptLoadEvent	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.	Info
StorageAdaptReloadFailEvent	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.	Erreur
StorageAdaptChangeEvent	A chargé une nouvelle version du SRA spécifié.	Site Recovery Manager a détecté que l'adaptateur SRA connu précédemment a été mis à niveau.	Info

Tableau 13-5. Événements du gestionnaire de baies

Événement	Description	Cause	Catégorie
SAManagerAddedEvent	A créé le gestionnaire de baies spécifié en utilisant le SRA spécifié.	L'utilisateur a ajouté un gestionnaire de baies.	Info
SAManagerRemovedEvent	A supprimé le gestionnaire de baies spécifié.	L'utilisateur a supprimé un gestionnaire de baies.	Info
SAManagerReconfigEvent	A reconfiguré le gestionnaire de baies spécifié.	L'utilisateur a modifié les propriétés du gestionnaire de baies.	Info
SAManagerPingOkEvent	Envoi réussi d'un ping au gestionnaire de baies spécifié.	Site Recovery Manager Server a correctement envoyé un test Ping au gestionnaire de baies.	Info
SAManagerPingFailEvent	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.	Erreur

Tableau 13-6. Événements de paire de baies

Événement	Description	Cause	Catégorie
SAPairDiscoveredEvent	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.	Info
SAPairEnabledEvent	A activé une paire de baies répliquées avec le gestionnaire de baies.	L'utilisateur a activé une paire de baies.	Info

Tableau 13-6. Événements de paire de baies (suite)

Événement	Description	Cause	Catégorie
SAPairDisabledEvent	A désactivé une paire de baies répliquées avec le gestionnaire de baies.	L'utilisateur a désactivé une paire de baies.	Info
SAPairPingOkEvent	Envoi réussi d'un ping à une paire de baies répliquées.	Site Recovery Manager Server a correctement envoyé un test Ping à la paire de baies.	Info
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.	Erreur

Tableau 13-7. Événements de banque de données

Événement	Description	Cause	Catégorie
StorageDsDiscoveredEvent	A identifié une banque de données répliquée.	Site Recovery Manager Server a identifié une banque de données répliquée.	Info
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.	Info
StorageRdmDiscoveredEvent	A identifié des RDM répliqués joints à la machine virtuelle spécifiée.	Site Recovery Manager Server a identifié un mappage RDM répliqué. Cet élément est déclenché lorsque vous ajoutez un disque RDM à une machine virtuelle protégée.	Info
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.	Info

Tableau 13-8. Événements de protection

Événement	Description	Cause	Catégorie	Événement cible
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.	Info	Banque de données
SPDsUnprotEvent	Banque de données spécifiée non protégée.	L'utilisateur a supprimé la banque de données 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.	Info	Banque de données

Tableau 13-8. Événements de protection (suite)

Événement	Description	Cause	Catégorie	Événement cible
SPVmdiscoveredEvent	A identifié une machine virtuelle répliquée.	L'utilisateur a créé une machine virtuelle sur une banque de données répliquée.	Info	Machine virtuelle
SPVmlostEvent	La machine virtuelle spécifiée n'est plus répliquée.	L'utilisateur a migré la machine virtuelle hors de la banque de données répliquée.	Info	Machine virtuelle
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.	Avertissement	Banque de données
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.	Erreur	Banque de données
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.	Erreur	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.	Info	Groupe protection
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.	Avertissement	Banque de données

Tableau 13-8. Événements de protection (suite)

Événement	Description	Cause	Catégorie	Événement cible
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.	Erreur	Banque de données
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.	Erreur	Banque de données
SPVmdsProtRestoredEvent	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.	Info	Machine virtuelle
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.	Erreur	Banque de données
SPCgDsMissingProtEvent	La banque de données provenant du groupe de cohérence spécifié doit être incluse dans le groupe de protection spécifié.	Voir la description.	Erreur	Banque de données

Tableau 13-8. Événements de protection (suite)

Événement	Description	Cause	Catégorie	Événement cible
SPDspansConsistentGroupEvent	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.	Erreur	Banque de données
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.	Erreur	Banque de données

Événements de licence

Les événements de licence fournissent des informations sur les modifications des statuts de licence Site Recovery Manager.

Tableau 13-9. Événements de licence

Événement	Description	Cause
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 13-9. Événements de licence (suite)

Événement	Description	Cause
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 13-10. Événements d'autorisations

Événement	Description	Cause
PermissionsAddedEvent	Autorisations créées pour l'entité sur 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 sur Site Recovery Manager.	L'autorisation pour l'entité a été supprimée.
PermissionsUpdatedEvent	Autorisation modifiée pour l'entité sur 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 vSphere Web Client. 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.

Tableau 13-11. 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 Site Recovery Manager Server.	Nom du site Site Recovery Manager, nom du plan de récupération, type de récupération, état d'exécution, nom de la commande.

Tableau 13-11. 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 Site Recovery Manager Server.	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.

Collecte des fichiers journaux de Site Recovery Manager

14

Pour mieux identifier les causes des problèmes que vous pouvez rencontrer pendant l'exécution au quotidien de Site Recovery Manager, vous pourrez être amené à collecter les fichiers journaux de Site Recovery Manager pour les étudier ou les envoyer au support VMware.

Site Recovery Manager crée plusieurs fichiers journaux 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 journaux.

Site Recovery Manager Server et son client utilisent des fichiers journaux différents.

Les fichiers journaux de Site Recovery Manager Server contiennent des informations sur la configuration du serveur et des messages liés aux opérations de ce dernier. Le bundle de journaux de Site Recovery Manager Server contient également des informations système et des rapports d'historique des dernières exécutions de plan de récupération.

Les fichiers journaux des clients Site Recovery Manager contiennent des informations sur la configuration du client et des messages liés aux opérations du plug-in du client. Le bundle Site Recovery Manager inclut également des fichiers journaux du programme d'installation et le contenu du sous-répertoire SRA (storage replication adapters) du répertoire des journaux.

Les fichiers journaux des instances de vCenter Server et des instances de ESXi qui font partie de votre système Site Recovery Manager peuvent également inclure des informations utiles pour diagnostiquer d'éventuels problèmes de Site Recovery Manager.

Le fichier journal de Site Recovery Manager collecte et récupère les fichiers et les place dans un fichier compressé à l'emplacement de votre choix.

Les erreurs rencontrées lors des opérations de Site Recovery Manager s'affichent dans des boîtes de dialogue d'erreur ou dans la fenêtre **Tâches récentes**. La plupart des erreurs génèrent également une entrée dans un fichier journal de Site Recovery Manager. Vérifiez les tâches récentes et les fichiers de journalisation pour le site de récupération et le site protégé.

Collecter les fichiers journaux de Site Recovery Manager à l'aide de l'interface de Site Recovery Manager

Vous pouvez télécharger des journaux pour Site Recovery Manager à 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 Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- 2 Sur l'onglet d'accueil de **Site Recovery**, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- 3 Dans l'onglet **Paire de sites**, cliquez sur **Résumé**, puis sur **Nom** dans la zone Site Recovery Manager.
- 4 Sélectionnez un serveur et cliquez sur **Exporter les journaux**.
- 5 Cliquez sur **Télécharger** pour télécharger les journaux.

Collectez manuellement les fichiers journaux de Site Recovery Manager

Vous pouvez télécharger les fichiers journaux de Site Recovery Manager Server dans un ensemble de journaux généré manuellement. La collecte manuelle des fichiers journaux 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

- ◆ Pour collecter les fichiers journaux de Site Recovery Manager, utilisez l'une des méthodes suivantes :

Tâche	Action
Générer un bundle de journaux à partir de la machine hôte Windows Site Recovery Manager Server à l'aide de l'invite de commande	<ol style="list-style-type: none"> Connectez-vous à l'hôte Site Recovery Manager Server et ouvrez une invite de commande. Modifiez le répertoire de travail en <code>C:\Program Files\VMware\VMware vCenter Site Recovery Manager\bin</code>. Exécutez la commande suivante : <code>cscript srm-support.wsf</code> Les fichiers de journalisation individuels sont recueillis dans un fichier nommé <code>srm-support-MM-JJ-AAAA-HH-MM.zip</code>, où <code>MM-JJ-AAAA-HH-MM</code> indique le mois, le jour, l'année, l'heure et la minute auxquels les fichiers de journalisation ont été créés. Par défaut, le bundle de journaux est enregistré sur le bureau.
Générez un bundle de journaux à partir de la machine hôte Windows Site Recovery Manager Server à l'aide du menu Démarrer	<ol style="list-style-type: none"> Ouvrez une session sur l'hôte Site Recovery Manager Server. Sélectionnez Démarrer > Programmes > VMware > VMware Site Recovery Manager > Générer un bundle de journaux VMware vCenter Site Recovery Manager.
Générer un bundle de journaux à partir du Site Recovery Manager Appliance	<ol style="list-style-type: none"> Connectez-vous à la machine hôte Site Recovery Manager Appliance et ouvrez une invite de commande. Modifiez le répertoire de travail en <code>/opt/vmware/srm/bin/</code>. Exécutez la commande suivante : <ol style="list-style-type: none"> ■ Si vous êtes connecté en tant qu'utilisateur Admin : <code>sudo ./srm-support-linux.sh</code>. ■ Si vous êtes connecté en tant qu'utilisateur racine : <code>./srm-support-linux.sh</code>.

Modifier la taille et le nombre des fichiers journaux de Site Recovery Manager Server

Vous pouvez modifier la taille, le nombre et l'emplacement des fichiers journaux de Site Recovery Manager Server.

Vous pouvez modifier les paramètres de journalisation de Site Recovery Manager dans le fichier de configuration `vmware-dr.xml` sur Site Recovery Manager Server.

Procédure

- Ouvrez une session sur l'hôte Site Recovery Manager Server.
- Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.
 - Si vous utilisez Site Recovery Manager pour Windows, le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` sur la machine hôte Site Recovery Manager Server.

- Si vous utilisez le Site Recovery Manager Virtual Appliance, le fichier `vmware-dr.xml` se trouve dans le répertoire `/opt/vmware/srm/conf/` sur le dispositif.

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 10485760 octets.

```
<log>
  <maxFileSize>10485760</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 20.

```
<log>
  <maxFileNum>20</maxFileNum>
</log>
```

6 (Facultatif) Modifiez l'emplacement sur Site Recovery Manager Server dans lequel stocker les fichiers journaux en modifiant la section `<directory>` dans la section `<log>`.

Note Si vous modifiez l'emplacement des fichiers journaux, vous devez vérifier que votre compte d'utilisateur Site Recovery Manager dispose des autorisations nécessaires pour écrire dans le nouveau répertoire.

- Si vous utilisez Site Recovery Manager pour Windows, le chemin d'accès par défaut aux journaux est `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs`.
- Si vous utilisez le dispositif Site Recovery Manager Appliance, l'emplacement par défaut des fichiers journaux est `/var/log/vmware/srm`.

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, détaillé et trivia. Si vous définissez le niveau sur trivia, vous remarquerez un effet négatif sur les performances.

```
<log>
  <level>info</level>
</log>
```

9 (Facultatif) Définissez le niveau de journalisation de composants Site Recovery Manager Server.

Vous pouvez définir des niveaux de journalisation spécifiques de composants en modifiant les sections `<level>` appropriées. Par exemple, vous pouvez définir le niveau de journalisation du composant de récupération sur trivia.

```
<level id="Recovery">
  <logName>Recovery</logName>
  <logLevel>trivia</logLevel>
</level>
```

10 (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.

```
<level id="SraCommand">
  <logName>SraCommand</logName>
  <logLevel>trivia</logLevel>
</level>
```

11 Redémarrez le service Site Recovery Manager Server pour appliquer les modifications.

Configurer les vidages de mémoire de Site Recovery Manager

Vous pouvez configurer les paramètres de vidage de mémoire de Site Recovery Manager pour modifier l'emplacement des fichiers de vidage de mémoire et les compresser.

Vous pouvez modifier les paramètres de vidage de mémoire de Site Recovery Manager dans le fichier de configuration `vmware-dr.xml` sur Site Recovery Manager Server.

Procédure

- 1 Ouvrez une session sur l'hôte Site Recovery Manager Server.
- 2 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.
 - Si vous utilisez Site Recovery Manager pour Windows, le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` sur la machine hôte Site Recovery Manager Server.
 - Si vous utilisez le Site Recovery Manager Virtual Appliance, le fichier `vmware-dr.xml` se trouve dans le répertoire `/opt/vmware/srm/conf/` sur le dispositif.
- 3 Modifiez l'emplacement sur Site Recovery Manager Server dans lequel stocker les vidages de mémoire en modifiant la section `<coreDump>` du fichier `vmware-dr.xml`.

Note Si vous modifiez l'emplacement des fichiers de vidage de mémoire, vous devez vérifier que votre compte d'utilisateur Site Recovery Manager dispose des autorisations nécessaires pour écrire dans le nouveau répertoire.

- Si vous utilisez Site Recovery Manager pour Windows, le chemin d'accès par défaut au vidage de mémoire est `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles`, sauf si cet emplacement n'existe pas ou n'est pas accessible en écriture. Dans ce cas, Site Recovery Manager Server utilise `C:\ProgramData\VMware`.
- Si vous utilisez le Site Recovery Manager Appliance, l'emplacement par défaut du vidage de mémoire est `/var/log/vmware/srm/DumpFiles`.

- 4 Utilisez les paramètres système de vidage de mémoire pour limiter le nombre de fichiers de vidage de mémoire créés et compressés.

```
<debug>
  <dumpCoreCompression>true,false</dumpCoreCompression>
  <dumpFullCore>true,false</dumpFullCore>
</debug>
```

Paramètre	Description
dumpCoreCompression	Si aucune valeur n'est spécifiée, la valeur par défaut est <i>false</i> . Site Recovery Manager Server ne compresse pas les précédents fichiers de vidage de mémoire, car il en crée de nouveaux. Si vous spécifiez la valeur <i>true</i> , Site Recovery Manager Server compresse tous les vidages de mémoire plus anciens lorsqu'il en génère un nouveau.
dumpFullCore	Si aucune valeur n'est spécifiée, la valeur par défaut est <i>false</i> . Site Recovery Manager Server génère un fichier de vidage de mémoire de plusieurs Mo et offre une assistance en cas de problème. Si vous définissez cette valeur sur <i>true</i> , Site Recovery Manager Server génère un fichier de vidage de mémoire complet pouvant comporter plusieurs gigaoctets, selon la charge de travail induite par le vidage de la mémoire. Ce fichier plus volumineux permet de fournir davantage d'aide en cas de problème. Si l'espace disque le permet, définissez cette valeur sur <i>true</i> .

- 5 Pour modifier le nombre maximal de fichiers de vidage de mémoire, ajoutez une ligne à la section `<debug>`.

```
<maxCoreDumpFiles>max_files</maxCoreDumpFiles>
```

Si aucune valeur n'est spécifiée, la valeur par défaut est 4. Cette valeur spécifie le nombre maximal de fichiers de vidage de mémoire qui sont conservés dans le répertoire de vidage de mémoire. Lorsque Site Recovery Manager Server crée des vidages de mémoire, Site Recovery Manager Server supprime les fichiers plus anciens (si nécessaire) pour éviter une consommation excessive de l'espace disque ou de dépasser sa taille maximale, notamment lorsque la valeur `dumpFullCore` est *true*.

Dépannage de Site Recovery Manager

15

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/>.

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 code ou de paramètres de codes 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 Ouvrez une session sur l'hôte Site Recovery Manager Server.
- 2 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.
 - Si vous utilisez Site Recovery Manager pour Windows, le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` sur la machine hôte Site Recovery Manager Server.
 - Si vous utilisez le Site Recovery Manager Virtual Appliance, le fichier `vmware-dr.xml` se trouve dans le répertoire `/opt/vmware/srm/conf/` sur le dispositif.
- 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.

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 et renvoie une erreur si vous n'avez pas mappé les périphériques de la machine virtuelle.

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 mappé les périphériques de la machine virtuelle sur le site protégé aux périphériques correspondants sur le site de récupération.

Solution

Configurez les paramètres de protection de la machine virtuelle comme décrit dans la section [Modification des paramètres d'une machine virtuelle dans un groupe de protection basé sur la baie ou un groupe de protection vSphere Replication](#).

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 les paramètres de réplication](#).

Vous n'avez pas besoin de redémarrer le Site Recovery Manager Server après la modification de ce paramètre. Site Recovery Manager appliquera le paramètre la prochaine fois que vous configurez la protection sur une machine virtuelle.

Échec de la suppression rapide et de la recréation d'espaces réservés

Si vous supprimez toutes les machines virtuelles à espace réservé d'une banque de données, démontez puis remontez la banque de données, la création de nouvelles machines virtuelles à espace réservé peut échouer.

Problème

La création de nouveaux espaces réservés trop rapidement après avoir démonté la banque de données peut entraîner l'erreur `NoCompatibleHostFound`.

Cause

Les associations entre hôtes ESXi et banques de données sont mises à jour à intervalles de 10 minutes. Si vous créez les nouveaux espaces réservés après avoir démonté et remonté la banque de données mais avant la prochaine mise à jour, l'hôte est introuvable.

Solution

Patiencez pendant plus de 10 minutes après avoir démonté et remonté la banque de données avant de créer de nouvelles machines virtuelles à espace réservé.

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.

La migration planifiée échoue en raison d'une synchronisation infructueuse du groupe de protection de stratégie de stockage

Lorsque vous tentez d'exécuter une migration planifiée d'un plan de récupération contenant un groupe de protection de stratégie de stockage, le plan de récupération échoue en raison d'une synchronisation inachevée des modifications apportées au groupe de protection.

Problème

Lorsque vous tentez d'exécuter une migration planifiée d'un plan de récupération contenant un groupe de protection de stratégie de stockage, le message d'erreur suivant s'affiche : `Le site homologue n'a pas terminé la synchronisation des modifications apportées au groupe de protection.`

Cause

Lorsque vous exécutez une migration planifiée d'un plan de récupération contenant un groupe de protection de stratégie de stockage, Site Recovery Manager vérifie que les groupes de protection sont synchronisés sur le site protégé et le site de récupération avant d'exécuter le plan de récupération.

Si le groupe de protection est synchronisé sur les deux sites, la migration planifiée commence. Si le groupe de protection n'est pas synchronisé sur les deux sites, le message d'erreur s'affiche.

Solution

- 1 Fermez le message d'erreur et cliquez de nouveau sur **Terminer**.
- 2 (Facultatif) Si l'erreur persiste, annulez la migration planifiée, attendez un instant et tentez de réexécuter 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 une récupération, 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.
- Le cluster sur le site de récupération connaît une importante utilisation des ressources lors de la récupération simultanée de plusieurs machines virtuelles. Dans ce cas, vous pouvez augmenter certains paramètres de délai d'expiration pour accorder plus de temps à l'exécution des tâches. Reportez-vous à [Modifier les paramètres de récupération](#).

Solution

- 1 Vérifiez que VMware Tools est installé sur la machine virtuelle faisant l'objet d'une récupération.
- 2 Vérifiez la capacité disponible du site de récupération.

Si le site de récupération connaît une importante utilisation des ressources, l'augmentation du délai d'expiration pour la personnalisation d'invité peut résoudre le problème.

- a Dans vSphere Client ou vSphere Web Client, cliquez sur **Site Recovery > Ouvrir Site Recovery**.
- b Dans l'onglet Accueil de Site Recovery, sélectionnez une paire de sites et cliquez sur **Afficher les détails**.
- c Dans le volet de gauche, cliquez sur **Configurer > Paramètres avancés > Récupération**.
- d Sélectionnez un site et cliquez sur **Modifier** pour modifier les paramètres du site de récupération.
- e Augmentez le paramètre `recovery.customizationTimeout` de la valeur par défaut à 600 secondes.
- f Augmentez le paramètre `recovery.powerOnTimeout` de la valeur par défaut à 300 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

Site Recovery Manager Server 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 Site Recovery Manager Server peut nécessiter jusqu'à 15 minutes. Si le Site Recovery Manager Server a dans son cache le mauvais état d'inventaire de l'hôte, une récupération ou un test de récupération peut échouer.

Solution

Patiencez 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 les valeurs de délai d'expiration `vrReplication.synchronizationTimeout` et `vrReplication.reverseReplicationTimeout` dans l'option 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 synchronisation des groupes de protection vSphere Replication

Lors de la récupération test, de la migration planifiée et de la reprotection des plans de récupération qui contiennent des groupes de protection vSphere Replication, l'étape de synchronisation des machines virtuelles échoue avec une erreur.

Problème

La synchronisation des machines virtuelles dans un groupe de protection vSphere Replication échoue avec le message d'erreur `Erreur - Échec lors de la synchronisation VR pour le groupe VRM <Non disponible>`. Cet objet a déjà été supprimé ou n'a pas été entièrement créé.

Cause

Le trafic d'E/S excessif sur une ou plusieurs des machines virtuelles du groupe de protection entraîne l'expiration de la synchronisation avant qu'elle ne se termine. Cela est probablement dû au trafic important. Par exemple, la définition du niveau de journalisation sur le mode trivia peut entraîner un trafic d'E/S élevé.

Solution

- 1 Ouvrez une session sur l'hôte Site Recovery Manager Server.

2 Ouvrez le fichier `vmware-dr.xml` dans un éditeur de texte.

- Si vous utilisez Site Recovery Manager pour Windows, le fichier `vmware-dr.xml` se trouve dans le dossier `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config` sur la machine hôte Site Recovery Manager Server.
- Si vous utilisez le Site Recovery Manager Virtual Appliance, le fichier `vmware-dr.xml` se trouve dans le répertoire `/opt/vmware/srm/conf/` sur le dispositif.

3 Ajoutez un élément `<topology><drTaskCleanupTime>` au fichier `vmware-dr.xml`.

Vous pouvez ajouter l'élément `<topology>` n'importe où au plus haut niveau des balises `<Config>`. Définissez la valeur de `<drTaskCleanupTime>` sur au moins 300 secondes. Si vous définissez le niveau de journalisation sur `trivia`, définissez `<drTaskCleanupTime>` sur 1000 secondes.

```
<topology>
  <drTaskCleanupTime>1000</drTaskCleanupTime>
</topology>
```

4 Enregistrez et fermez le fichier `vmware-dr.xml`.

5 Redémarrez Site Recovery Manager Server pour appliquer les nouveaux paramètres.

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 réplication 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`.

La récupération s'interrompt à 36 % lors d'une migration planifiée

Si vous arrêtez le service Site Recovery Manager sur le site protégé lors d'une migration planifiée, l'opération se bloque à 36 %.

Problème

Lors d'une migration planifiée, si vous arrêtez le service Site Recovery Manager sur le site protégé, lorsque le workflow exécute l'étape 15 **Démonter le stockage du site protégé**, il est possible que la récupération n'échoue pas normalement mais plutôt qu'elle se bloque à 36 %.

Solution

Cliquez sur **Annuler** pour annuler le workflow, puis exécutez-le de nouveau.

Les opérations échouent en renvoyant une erreur concernant un fichier de configuration non répliqué

Lorsque vous exécutez plusieurs opérations de récupération ou de reprotection simultanément dans les deux directions, les opérations échouent et renvoient une erreur de fichier de configuration de machine virtuelle non répliquée.

Problème

Lorsque vous exécutez plusieurs plans de récupération simultanément contenant des groupes de protection de réplication basée sur la baie ou des groupes de protection de stratégie de stockage, avec certaines opérations s'exécutant du site A au site B, et certaines opérations s'exécutant du site B au site A, une partie ou tous les plans échouent et renvoient l'erreur Impossible de protéger la machine virtuelle « *virtual_machine_name* », car son fichier de configuration « *virtual_machine_config_file.vmx* » est situé sur une banque de données non répliquée ou non protégée.

Cause

Ce problème peut se produire du fait que le calcul de la banque de données sur un site est retardé par les opérations de récupération en cours d'exécution dans la direction opposée.

Solution

Attendez que certaines opérations se terminent pour réexécuter l'opération sur les plans de récupération ayant échoué. Sinon, exécutez les migrations planifiées simultanément dans la même direction. Une fois les migrations planifiées terminées, exécutez les migrations planifiées dans la direction opposée.

Échec de la récupération en raison d'autorisations d'utilisateur limitées

Il se peut qu'un message d'erreur soit généré pendant le processus de récupération si l'utilisateur de la solution Site Recovery Manager ne dispose pas des autorisations nécessaires pour effectuer une personnalisation IP ou des appels de système d'exploitation invité.

Problème

Si l'utilisateur de la solution Site Recovery Manager ne dispose pas des autorisations appropriées pour accéder au système d'exploitation invité de la VM récupérée, il se peut que les messages d'erreur suivants soient émis pendant le processus de récupération.

```
GuestPermissionDenied
```

```
CannotAccessFile
```

Cause

Le problème survient lorsque l'utilisateur de la solution Site Recovery Manager est mappé à un utilisateur du système d'exploitation invité qui n'a pas accès à un fichier dans le système d'exploitation invité ou qui ne dispose pas des autorisations nécessaires pour exécuter des commandes.

Solution

- 1 Si vous utilisez Site Recovery Manager pour configurer les mappages d'utilisateurs invités, assurez-vous que l'utilisateur du système d'exploitation invité qui exécute le service VMware Tools est autorisé à accéder à un fichier ou dispose des autorisations nécessaires pour exécuter des commandes.

Pour plus d'informations sur l'activation ou la désactivation de la configuration automatique des mappages d'utilisateurs invités, reportez-vous à [Modifier les paramètres de récupération](#).

- 2 (Facultatif) Si vous configurez manuellement les mappages d'utilisateurs invités, mappez l'utilisateur local de la solution Site Recovery Manager du site de récupération à l'utilisateur du système d'exploitation invité disposant des autorisations appropriées.
- 3 Exécutez à nouveau le plan de récupération.

Échec de la récupération en raison d'une combinaison de VMware Tools et ESXi non prise en charge

Il se peut que le processus de récupération échoue si la version de VMware Tools installée sur votre VM et la version de l'hôte ESXi du site de récupération sont incompatibles avec Site Recovery Manager.

Problème

Il se peut que le message d'erreur suivant soit généré pendant le processus de récupération.

```
OperationNotSupportedByGuest
```

Cause

Le problème peut survenir si vous utilisez des versions incompatibles de VMware Tools et ESXi. Pour plus d'informations sur la compatibilité entre Site Recovery Manager, VMware Tools et ESXi, reportez-vous à *Matrices de compatibilité pour Site Recovery Manager 8.2*.

Solution

- ◆ Assurez-vous que les versions de VMware Tools et ESXi soient compatibles avec votre instance de Site Recovery Manager.