# Storage Replication Adapter Dell EMC série ME4 pour vSphere

Guide d'utilisation

Modèle réglementaire: E09J, E10J, E11J
Type réglementaire: E09J001, E10J001, E11J001

## Remarques, précautions et avertissements

**REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.**

**PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.**

**AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.**



2018 - 08

Rév. A00

# Table des matières

1

# Installation et configuration du SRA

Le SRA (Storage Replication Adapter) Dell EMC série ME4 pour vSphere permet d'utiliser VMware vCenter Site Recovery Manager (SRM) 6.5 ou une version ultérieure avec toutes ses fonctionnalités. En combinant la fonctionnalité de réplication du système de stockage Série ME4 et vCenter SRM, le SRA fournit une solution automatisée pour la mise en œuvre et le test de la reprise après sinistre entre des sites géographiquement séparés. Il permet également d'utiliser SRM pour les migrations planifiées entre deux sites.

Sujets :



# À propos de VMware Site Recovery Manager

vCenter Site Recovery Manager (SRM) est une solution de continuité d'activité et de reprise après sinistre qui vous aide à planifier, tester et exécuter la restauration de machines virtuelles vCenter entre deux sites, à savoir le site protégé et le site de récupération.

Deux types de restauration sont disponibles : la migration planifiée et la reprise après sinistre.

## Migration planifiée

La migration planifiée consiste à mettre hors-service des machines virtuelles sur le site protégé et à mettre en service les machines équivalentes sur le site de récupération de façon organisée. Pour assurer la réussite de la migration planifiée, les deux sites doivent être entièrement opérationnels.

## Restauration après sinistre

La reprise après sinistre est similaire à la migration planifiée. Cependant, elle n'implique pas que les deux sites soient opérationnels. Au cours d'une opération de reprise après sinistre, les défaillances d'opérations sur le site protégé sont signalées. Sinon, elles sont ignorées.

SRM coordonne le processus de restauration avec les mécanismes de réplication sous-jacents suivants : les machines virtuelles sur le site protégé sont arrêtées correctement (dans la mesure où ces machines virtuelles sont toujours disponibles) et les machines virtuelles répliquées peuvent être démarrées. La restauration des machines virtuelles protégées vers le site de récupération est gérée par un plan de restauration qui spécifie l'ordre dans lequel les machines virtuelles sont démarrées. Le plan de restauration spécifie également les paramètres réseau comme les adresses IP et peut contenir des scripts spécifiés par l'utilisateur pouvant être exécutés pour effectuer des actions de restauration personnalisées.

À l'issue d'une restauration, les machines virtuelles en cours d'exécution ne sont plus protégées. Pour parer à cette réduction de la protection, SRM applique une opération de reprotection pour les machines virtuelles. Cette opération inverse les rôles des deux sites une

fois le site protégé d'origine de nouveau opérationnel. Le site qui était précédemment le site de récupération devient le site protégé et le site qui était précédemment le site protégé devient le site de récupération.

SRM vous permet de tester les plans de restauration. Vous pouvez effectuer des tests à l'aide d'une copie temporaire des données répliquées, et ce, sans perturber les opérations en cours sur les deux sites. Vous pouvez effectuer des tests à l'issue d'une reprotection pour vérifier la validité de la nouvelle configuration de site protégé/site de récupération.

# Sites protégés et sites de récupération

Dans le cadre d'une installation classique de SRM, un site protégé fournit des services de datacenter stratégiques. Il peut s'agir de n'importe quel site où vCenter est utilisé pour répondre à un besoin critique.

Le site de récupération est un site alternatif vers lequel ces services peuvent migrer. Il peut se trouver à des milliers de kilomètres de distance. Il est généralement hébergé dans une installation préservée des perturbations pouvant affecter le site protégé, notamment des perturbations environnementales et infrastructurelles.

**REMARQUE : Le SRA Série ME4 connecte VMware SRM à la fonctionnalité de réplication du système de stockage. Dans ce contexte, vous rencontrerez peut-être une terminologie différente, dont les significations sont cependant les mêmes. Par exemple, l'interface utilisateur et la documentation VMware font généralement référence aux sites protégés et aux sites de récupération. En revanche, l'interface utilisateur et la documentation de réplication du ME Storage Manager (Gestionnaire de stockage ME) (MESM) font référence aux volumes et sites principaux et secondaires.**

# SRM : prérequis

Une configuration classique de SRM inclut deux sites géographiquement séparés avec connectivité TCP/IP, le site protégé et le site de récupération. Le site protégé est le site répliqué vers le site de récupération en vue d'une reprise après sinistre. Chaque site contient un système de stockage Dell EMC série ME4, des serveurs VMware ESX, un serveur Virtual Center (vCenter) et un serveur SRM exécutant SRM.

Après avoir configuré le site protégé et le site de récupération et installé l'infrastructure nécessaire pour la communication réseau entre les deux sites, vous pouvez installer et configurer le logiciel. Pour plus d'informations, reportez-vous à la rubrique Configuration des systèmes de stockage Série ME4.

# Configuration des systèmes de stockage Série ME4

Si vos systèmes de stockage Série ME4 ne sont pas encore configurés :

1. Suivez les instructions d'installation figurant dans le *Dell EMC série ME4 Storage System Deployment Guide* (Guide de déploiement du système de stockage Dell EMC ME4 Series).
2. Assurez-vous que les deux systèmes de stockage bénéficient de la même configuration d'interface hôte (iSCSI, FC ou hybride FC/iSCSI).

# Configurer la réplication

**REMARQUE : Assurez-vous que le nom du système de stockage, les informations d'identification utilisateur et les adresses IP des deux systèmes de stockage sont définis avant de configurer le SRA. Le SRA utilise les mêmes informations d'identification utilisateur pour les systèmes de stockage local et distant. Par conséquent, si l'utilisateur avec rôle de gestionnaire utilise le même mot de passe sur les deux sites, créez un `user ID` pour le SRA avec `manage` sur les deux systèmes. Reportez-vous à la rubrique Meilleures pratiques pour plus d'informations sur la configuration.**

1. Utilisez le ME Storage Manager (Gestionnaire de stockage ME) (MESM) pour configurer le logiciel de réplication en suivant les instructions figurant dans la section du guide de l'administrateur dédiée à la réplication. Utilisez notamment les paramètres suivants pour le SRA :
   - snapshot-count : 3 (ou une valeur supérieure)

- snapshot-history : `both`
- snapshot-retention : `high`
- queue-policy : `queue-latest`
- (Facultatif) snapshot-basename : `same-as-volume-name`

**REMARQUE : Vous pourrez résoudre les problèmes plus facilement si vous définissez le nom de base comme indiqué. En effet, les instantanés de réplication seront nommés comme le volume de base, avec le suffixe `_nnnn` (indiquant le numéro de génération de la réplication).**

2 Utilisez le MESM sur chaque système pour définir l'autre système dans l'ensemble de réplication en tant que système distant.

3 Utilisez le MESM pour effectuer au moins une réplication.

4 Utilisez le MESM pour programmer des réplications depuis le site protégé vers le site de récupération. Vous vous assurerez ainsi qu'en cas de sinistre entraînant la désactivation du site protégé ou endommageant le matériel ou les fichiers, SRM peut utiliser la dernière copie répliquée sur le site de récupération en vue d'une reprise après sinistre. Lorsque vous utilisez des réplications planifiées, veillez à vérifier que la source de la réplication la plus récente était dans un état valide.

# Installer le logiciel SRM

Vous devez installer un serveur SRM sur le site protégé et sur le site de récupération. Une fois les serveurs SRM installés, téléchargez le plug-in du client SRM à partir de l'un des serveurs SRM à l'aide du menu **Manage Plugins** de vSphere Client. Utilisez le plug-in du client SRM pour configurer et gérer SRM sur chaque site.

Avant d'installer SRM, vous devez installer vCenter Server sur chaque site. Le programme d'installation de SRM doit être en mesure de se connecter à ce serveur au cours de l'installation. VMware recommande d'installer SRM sur un autre système que celui sur lequel vCenter Server est installé. L'installation de SRM et vCenter Server sur le même système peut rendre plus complexe l'exécution des tâches administratives. Lors d'une mise à niveau de SRM, seuls les groupes de protection et plans de restauration dans un état valide sont enregistrés. Les groupes de protection ou plans de restauration dans un état non valide sont rejetés.

Pour installer le logiciel SRM :

1 Configurez vCenter Server sur chaque site.

2 Créez un datacenter unique dans chaque instance de vCenter Server.

3 Ajoutez les hôtes locaux à ce datacenter.

4 Téléchargez le logiciel VMware Site Recovery Manager à l'aide du lien Download Product figurant sur le site Web de VMware à l'adresse suivante :

https://my.vmware.com/web/vmware/downloads

5 Installez VMware Site Recovery Manager 6.5 (ou une version ultérieure) sur chaque site en suivant les instructions du guide VMware *Administration de Site Recovery Manager*.

Pour trouver le guide et les notes de mise à jour correspondant à votre version de SRM, reportez-vous au site Web de documentation VMware :
https://docs.vmware.com/en/Site-Recovery-Manager/index.html

6 Ne configurez pas SRM pour le moment. Pour commencer, Installer le logiciel SRA.

# Installer le logiciel SRA

Téléchargez et installez le logiciel SRA Dell EMC série ME4 correspondant à votre version de VMware SRM :

1 Rendez-vous sur https://www.dell.com/support.

2 Localisez le logiciel SRA sur la page de support des systèmes de stockage de la Série ME4.

3 Ouvrez et exécutez le fichier de configuration du SRA.

Une fois le SRA installé sur chaque site, vous pouvez configurer SRM. Le plug-in pourra alors détecter les volumes répliqués entre les sites.

# Configurer SRM

Une fois SRM et le SRA installés, vous pouvez configurer SRM étape par étape à l'aide de l'onglet **Getting Started** (Prise en main) de la fenêtre principale de SRM. Pour obtenir des instructions détaillées sur la configuration de SRM, reportez-vous au guide VMware *Administration de Site Recovery Manager*.

Vous devez disposer des informations suivantes pour configurer les systèmes de stockage Série ME4 dans SRM :

- Les adresses IP des systèmes de stockage Série ME4
- Le nom d'utilisateur et le mot de passe pour chaque système de stockage, correspondant à ceux configurés dans le MESM

Apportez les modifications suivantes à vos paramètres SRM :

- Définissez `storageProvider.autoResignatureMode` sur `1` (requis).
- Définissez `storageProvider.hostRescanRepeatCnt` sur `2` (requis).
- Définissez `Storage.commandTimeout` sur `1200` secondes (recommandé).

2

# Utilisation de SRM pour la reprise après sinistre

Après avoir configuré la réplication du système de stockage et le logiciel VMware SRM sur les sites local et distant et après avoir configuré au moins un ensemble de réplication, utilisez le MESM pour planifier les réplications. Utilisez ensuite SRM pour créer et tester un ou plusieurs plans de restauration. À ce stade, SRM est en mesure s'assurer la reprise après sinistre, le basculement et le retour arrière, ainsi que les opérations reprotection.

Le guide VMware *Administration de Site Recovery Manager* offre des instructions et des informations détaillées concernant ces opérations. Ce guide est disponible sur le site web de support VMware.

Sujets :



## Détection de volume

SRM obtient des informations sur les volumes en cours de réplication auprès du SRA. SRM compare ensuite cette liste aux volumes qu'il reconnaît dans un environnement VMware.

Pour les migrations SRM planifiées, dans le cadre de scénarios n'impliquant pas de sinistre, SRM peut lancer une réplication pour garantir que les données répliquées sont à jour.

Dans le cadre de scénarios de reprise après sinistre, SRM tente de créer une réplication actuelle. Si ce n'est pas possible (par exemple, parce que le site protégé est hors ligne), SRM utilise la réplication la plus récente disponible sur le site distant.

Utilisez l'outil de planification des réplications pour effectuer des réplications régulières et ainsi minimiser la perte de données en cas de sinistre, ou créez régulièrement des migrations SRM planifiées. Dans tous les cas, assurez-vous que les volumes à répliquer à partir du site protégé sont dans un état valide, de sorte que la réplication la plus récente disponible sur le site distant puisse être utilisée en production.

Pour obtenir des instructions sur la configuration des planifications de réplication, reportez-vous au chapitre sur l'utilisation de la réplication du *Dell EMC série ME4 Storage System Administrator's Guide* (Guide administrateur du système de stockage Dell EMC ME4 Series).

## Créer un plan de restauration

Créez un plan de restauration pour établir le mode de restauration des machines virtuelles. Un plan de restauration de base inclut les étapes (basées sur des valeurs par défaut) permettant de contrôler le mode de restauration des machines virtuelles d'un groupe de protection sur le site de récupération. Vous pouvez personnaliser le plan selon vos besoins. Les plans de restauration sont différents des groupes de protection. Ils indiquent la façon dont les machines virtuelles d'un ou plusieurs groupes de protection sont restaurées sur le site de récupération.

L'onglet **Recovery** de la fenêtre principale de SRM vous permet de créer, tester et exécuter un plan de restauration étape par étape. Pour obtenir des instructions détaillées, reportez-vous au guide VMware *Administration de Site Recovery Manager*.

# Tester un plan de restauration

Vous pouvez créer automatiquement un environnement de test isolé n'entraînant aucune interruption sur le site de récupération en utilisant la réplication et en connectant les machines virtuelles à votre réseau de test isolé. Vous pouvez également enregistrer les résultats des tests et les consulter ou les exporter à tout moment.

Le test d'un plan de restauration permet d'en évaluer presque tous les aspects, malgré plusieurs concessions visant à éviter l'interruption des opérations en cours. Si le test d'un plan de restauration n'a aucun effet durable sur les sites, l'exécution effective du plan a, quant à elle, des effets importants sur les deux sites.

Exécutez des restaurations de test aussi souvent que nécessaire. Le test d'un plan de restauration n'affecte pas la réplication ni les opérations en cours sur les sites (même s'il peut interrompre temporairement les machines virtuelles locales sélectionnées sur le site de récupération, si les restaurations ont été configurées à cette fin). Vous pouvez annuler un test de plan de restauration à tout moment.

Dans le cas de migrations planifiées, une restauration arrête la réplication après une synchronisation finale de la source et de la cible. Pour les reprises après sinistre, notez que les machines virtuelles sont restaurées selon leur dernier état disponible, tel que déterminé par l'objectif de point de restauration. Une fois la réplication finale effectuée, SRM apporte aux deux sites des modifications dont l'inversion requiert beaucoup de temps et d'efforts. Par conséquent, il convient d'attribuer séparément le privilège permettant de tester un plan de restauration et le privilège permettant de l'exécuter.

Lorsque des basculements SRM de test vers le site de récupération sont demandés, SRM effectue les actions suivantes :

1 Il détermine le dernier point de restauration pour chaque volume répliqué.

2 Il crée un instantané de test inscriptible pour chaque point de restauration avec un nom de type **sra***nnnnnn* où *nnnnnn* est un chiffre qui augmente de façon monotone.

3 Il mappe les instantanés de test avec les hôtes ESXi appropriés sur le site de récupération.

À l'arrêt des tests, les instantanés de test sont démappés et supprimés.

# Basculement et restauration

Le processus de retour arrière consiste à rétablir l'environnement de réplication à son état d'origine sur le site protégé avant le basculement. Le retour arrière avec SRM est un processus automatisé qui se produit après la restauration. En cas de migration planifiée, le processus de retour arrière des machines virtuelles protégées est ainsi simplifié. Si l'ensemble de l'environnement SRM reste intact après la restauration, le retour arrière s'effectue comme suit : les étapes de reprotection sont exécutées avec SRM, puis le plan de restauration est de nouveau exécuté. Les machines virtuelles configurées dans leurs groupes de protection sont alors retransférées vers le site SRM protégé d'origine.

Dans les scénarios de sinistre, les étapes de retour arrière varient selon le degré de défaillance du site protégé. Par exemple, le basculement peut être dû à une panne du système de stockage ou à la perte de l'ensemble du datacenter. La configuration manuelle du retour arrière est importante, car le site protégé peut présenter une configuration matérielle ou SAN différente après un sinistre. Avec SRM, une fois le retour arrière configuré, il peut être géré et automatisé comme n'importe quel basculement SRM planifié. Les étapes de restauration peuvent varier selon les conditions du dernier basculement. Si le retour arrière suit un basculement non planifié, une remise en miroir complète des données entre les deux sites peut être nécessaire. C'est généralement dans un scénario de retour arrière que cette étape prend le plus de temps.

Tous les plans de restauration dans SRM incluent une tentative initiale de synchronisation des données entre les sites de protection et de récupération, même dans le cadre d'un scénario de reprise après sinistre.

Au cours de la reprise après sinistre, le processus tente d'abord d'arrêter les machines virtuelles du groupe de protection et d'établir une synchronisation finale entre les sites. Le but est alors de garantir que les machines virtuelles sont statiques et font l'objet d'un arrêt en douceur avant l'exécution du plan de restauration, et ce, afin de minimiser autant que possible la perte de données. Si le site protégé n'est plus disponible, le plan de restauration continuera de s'exécuter jusqu'à son terme, même si des erreurs se produisent.

Ce nouvel attribut minimise le risque de perte de données lors d'une reprise après sinistre en établissant le juste compromis entre la nécessité d'assurer la cohérence des machines virtuelles et la capacité à atteindre des objectifs de point de restauration agressifs.

# Basculement automatique

SRM automatise l'exécution des plans de restauration pour en garantir la précision et la cohérence. vCenter Server vous offre une visibilité et un contrôle complets sur le processus (état de chaque étape, indicateurs de progression, description détaillée de toutes les erreurs, etc.).

En cas de sinistre, lorsqu'un basculement SRM réel est demandé, le SRA exécute les actions suivantes :

1 Il sélectionne les volumes répliqués.
2 Il identifie et supprime les copies à distance incomplètes en cours et présente la copie à distance complète la plus récente en tant que volume principal.
3 Il convertit les volumes distants en volumes principaux et configure l'authentification pour les hôtes ESXi en vue de leur montage.

Si, pour quelque raison que ce soit, un basculement réel ne s'exécute pas complètement, son exécution peut être retentée via des appels multiples. Par exemple, si la restauration d'un seul volume a échoué de par la présence d'un instantané normal, l'instantané peut être supprimé manuellement et le basculement peut être à nouveau demandé.

# Reprotection

Après l'exécution d'un plan de restauration ou d'une migration planifiée, l'environnement doit rester protégé contre les défaillances, et ce, dans de nombreux cas, notamment pour assurer sa résilience ou pour répondre à l'ensemble des objectifs de reprise après sinistre.

Extension de SRM pour les plans de restauration, la reprotection peut être utilisée uniquement avec la réplication de système de stockage. Elle permet à l'environnement sur le site de récupération d'établir la réplication synchronisée et la protection de l'environnement d'origine.

Si vous optez pour la reprotection de l'environnement après le basculement du site de récupération, le processus établit la synchronisation et tente de répliquer les données entre les groupes de protection s'exécutant sur le site de récupération et sur le site principal précédemment protégé.

Cette capacité à reprotéger un environnement garantit la protection des environnements contre les défaillances même après un scénario de restauration de site. Cela permet également d'entreprendre un retour arrière automatisé vers un site principal après une migration ou un basculement.

# Retour arrière automatisé

Vous pouvez configurer un workflow de retour arrière automatisé pour retransférer l'ensemble de l'environnement vers le site principal à partir du site de récupération.

Le retour arrière se produit lorsque le processus de reprotection a vérifié que la réplication et la synchronisation des données sont établies sur le site principal d'origine.

Le retour arrière automatisé applique le même workflow que celui utilisé pour faire migrer l'environnement vers le site protégé. Il garantit que les systèmes critiques encapsulés par le plan de restauration sont retransférés vers leur environnement d'origine. Le workflow s'exécute uniquement si la reprotection s'est correctement déroulée. Le retour arrière est disponible uniquement avec la réplication de système de stockage.

Le retour arrière garantit que :

- toutes les machines virtuelles qui ont initialement migré vers le site de récupération sont retransférées vers le site principal ;
- les environnements exigeant que les tests de reprise après sinistre soient effectués avec des environnements de production et des migrations réelles peuvent être retransférés vers le site initial ;
- des processus de restauration simplifiés permettent un retour aux opérations standard après une défaillance ;

- le basculement peut être effectué en cas de sinistre ou de migration planifiée.

# 3

# Dépannage

VMware vCenter Server utilise le SRA pour afficher un message d'erreur détaillé chaque fois qu'une étape de restauration échoue.

Le SRA crée également un fichier journal appelé `sra.log` qui affiche chaque événement SRM et chaque commande CLI qui se produit sur les systèmes de stockage de la Série ME4. Les messages d'erreur et de ce fichier journal fournissent souvent suffisamment d'informations pour corriger les erreurs. Pour obtenir de l'aide supplémentaire, contactez VMware.

**Tableau 1. Messages d'erreurs du SRA et actions conseillées**

| Numéro de message | Message | Solution suggérée |
|---|---|---|
| 1002 | VMware Site Recovery Manager version 6.5 n'a pas été trouvé sur ce système. | Installez VMware SRM 6.5 ou une version ultérieure, puis ré-exécutez la procédure d'installation du SRA. |
| 1003 | La sortie XML vers {file} a échoué : {error} | Assurez-vous que l'emplacement du fichier spécifié existe, qu'il dispose d'un espace libre suffisant et qu'il est inscriptible. |
| 1004 | L'option d'installation n'est pas prise en charge sur ce système. | Reportez-vous aux instructions d'installation du SRA. |
| 1005 | Une version native de Perl doit être utilisée pour utiliser cette option. | Assurez-vous d'utiliser la version `Perl.exe` installée avec le logiciel SRM VMware. |
| 1006 | Délai d'attente expiré pour que le volume {volume} apparaisse sur le système de stockage {arrayname} à {file} :{line}. | Vérifiez que le volume spécifié a été créé sur le système de stockage et réessayez l'opération. |
| 1007 | L'utilisation du système de stockage {systemName} n'est pas autorisée avec ce SRA. | Contactez votre fournisseur de systèmes de stockage pour vérifier que ce système est pris en charge et pour demander une réplication et des clés de licence SRA. |
| 1008 | Aucun WWN trouvé pour le volume {primary}. | Vérifiez que le volume spécifié est configuré pour la réplication. |
| 1009 | discoverDevices : Impossible de déterminer le WWN pour le snapshot temporaire {serialNumber} ({name}). | Vérifiez si le snapshot spécifié a été conservé après un test précédent et peut être supprimé. |
| 1010 | Ne peut pas trouver de point de restauration pour le snapshot temporaire {serialNumber} ({name}). | Vérifiez si le snapshot spécifié a été conservé après un test précédent et peut être supprimé. |
| 1011 | discoverDevices : ne trouve pas le WWN pour le volume promu {secondaryName} ({secondary}). | Vérifiez le statut du volume spécifié et l'intégrité du système de stockage, puis relancez l'opération. |
| 1013 | Il n'existe aucun point de synchronisation valide pour {volume}. | Dans le MESM, utilisez le tableau Snapshots pour vérifier que le volume spécifié a été complètement répliqué à partir du site protégé. Pour plus d'informations, consultez le Guide de l'administrateur. |
| 1014 | Impossible d'exporter un snapshot pour le volume {vol}. | Un snapshot précédemment créé par le SRA existe déjà pour le volume spécifié. Un seul instantané exporté est autorisé par volume cible de la réplication. Supprimez le snapshot existant et relancez l'opération. |
| 1018 | Paramètre PeerId {PeerId} inconnu ou manquant dans la requête {command}. | Assurez-vous que chaque système de stockage communique correctement le nom de son homologue de réplication et que les noms des systèmes de stockage n'ont pas changé depuis que le SRM a été configuré. Si le |

| Numéro de message | Message | Solution suggérée |
|---|---|---|
| | | nom du système de stockage a été modifié, supprimez et recréez les entrées du système distant sur chaque système de stockage si nécessaire. Si le problème persiste après le redémarrage du SRM, recréez la configuration de la paire de systèmes de stockage dans le SRM. |
| 1020 | N'a pas trouvé de volume homologue pour le volume local {localsn}. | Assurez-vous que le volume spécifié a été défini comme faisant partie d'un ensemble de réplication. |
| 1021 | Paramètres incorrects ou manquants dans la requête SRM {cmd} reçue par le SRA. | Vérifiez que les ensembles de réplication, les systèmes distants, et la configuration de SRM sont corrects. |
| 1022 | Valeur Arrayld {Arrayld} dans la requête {cmd} invalide ou inconnue. | Assurez-vous que les noms et adresses IP du système de contrôleur de stockage n'ont pas été reconfigurés depuis la configuration du SRM. |
| 1023 | Échec de l'ouverture du fichier verrou {filename}. | Vérifiez les permissions des fichiers et des répertoires pour le nom de fichier spécifié. |
| 1 024 | Paramètre Deviceld inconnu ou manquant {Deviceld} dans la requête {command}. | Vérifiez que le SRM et le SRA sont configurés correctement. Vérifiez également l'intégrité du système de stockage et les chemins d'accès au réseau entre le SRM hôte et les deux systèmes de stockage. |
| 1025 | Aucun point de synchronisation valide n'a été trouvé pour le volume {vol} pendant l'opération {command}. | L'opération a échoué sur ce volume, car il n'existe aucun point de synchronisation pour ce volume. Dans le MESM, utilisez le tableau Snapshots pour vérifier que le volume spécifié a été complètement répliqué à partir du site protégé. Pour plus d'informations, consultez le Guide de l'administrateur. |
| 1026 | Délai d'attente expiré pour que la réplication définie pour le volume {volume} passe en état de conflit sur le système de stockage {arrayname} à {file}:{line}. | Vérifiez que le volume spécifié a été créé sur le système de stockage et réessayez l'opération. |
| 1027 | La commande SRA syncOnce temporise l'attente des images de réplication pour le ou les volumes [{volumes}] à démarrer sur le système de stockage. | Vérifiez que le système de stockage est intègre et répétez l'opération si nécessaire pour vous assurer que les volumes sont répliqués. |
| 1028 | Aucun snapshot SRA trouvé pour le volume {Deviceld} dans la requête {command}. | Le SRA n'a pas réussi à exporter le snapshot dans une précédente opération testFailoverStart, le snapshot a déjà été supprimé, ou le snapshot a été perdu en raison d'un problème de communication avec le logiciel de gestion sur le port du stockage. |
| 1029 | Un snapshot SRA existant {snapshot} doit être supprimé avant que la fonction testFailoverStart puisse être exécutée sur {volume}. | Supprimez le volume du snapshot {snapshot} avant d'essayer à nouveau testFailoverStart. |
| 1030 | La réplication inverse ne peut pas être effectuée sur le volume cible {volume}, car le volume protégé original {cible} est toujours mappé sur le système de stockage distant {remoteArray}. | Assurez-vous que les systèmes de stockage ({localArray} et {remoteArray}) et leurs serveurs SRM correspondants fonctionnent et peuvent être gérés sur le réseau. |
| 1101 | Échec de la connexion au système de stockage à {url} ({response}) | Assurez-vous que les adresses IP du système de stockage sont correctement configurées et que le système de stockage est accessible depuis l'hôte SRM. De plus, si les adresses IP d'un système de stockage ont changé, il peut être nécessaire de supprimer et de recréer les définitions du système distant sur un ou les deux systèmes de stockage. |

| Numéro de message | Message | Solution suggérée |
|---|---|---|
| 1102 | L'exécution de la commande {cmd} a échoué sur le système de stockage à l'adresse {ipAddr) : {err} | Si le message d'erreur n'indique pas la raison de l'échec, ouvrez l'adresse spécifiée avec un navigateur Web pour vérifier l'intégrité du système de stockage. |
| 1103 | Aucune adresse IP spécifiée pour MC pour la commande {cmd} | Vérifiez que les adresses IP pour le système de stockage sont configurées correctement sur le système de stockage et sur l'hôte. |
| 1104 | La réponse du système de stockage à {ipAddr} ne comprenait pas d'indication d'état. | Vérifiez l'intégrité du système de stockage et redémarrez le contrôleur de gestion si nécessaire. |
| 1105 | Échec de l'exécution de la commande {cmd} sur le système de stockage à {system} : {err} | Vérifiez la configuration d'adresse IP sur le système de stockage et sur l'hôte, et vérifiez la connectivité réseau. |
| 2001 | Le volume {volume} ({name}) est déjà non adressé. | Le SRM a demandé qu'un volume soit préparé pour le basculement, mais le volume est déjà préparé. |
| 2002 | Aucune donnée trouvée pour l'image de réplication de {volume} {imageSn} ({err}). | Vérifiez que la réplication a démarré pour le volume {volume}. |
| 2003 | querySyncStatus : aucune donnée trouvée pour l'image de réplication {imageSn} du volume {vol} ({err}). | Vérifiez que la réplication a démarré pour le volume spécifié. |

**REMARQUE : Vous pouvez vous attendre à voir certaines erreurs dans le fichier journal lorsque les commandes sont exécutées pour vous assurer que les volumes sont dans un état particulier si les volumes sont déjà dans cet état. Ces erreurs sont -3395 `(Replication is not active on this secondary volume)` et -10306 `(Unable to set the specified volume as the primary volume because the specified volume is already a primary volume)`. Vous pouvez en toute sécurité ne pas tenir compte de ces messages d'erreur dans les circonstances mentionnées ci-dessus.**

# 4

# Meilleures pratiques

Voici quelques consignes et recommandations spécifiques à l'utilisation du SRA et du logiciel de réplication conjointement avec la solution de reprise après sinistre VMware SRM :

- Préparez à l'avance un plan couvrant la façon dont vous allez réétablir les planifications de réplication en cas de basculement de site. Après une opération de réplication inverse, vous devez configurer les planifications de réplication pour assurer une réplication périodique des données des nouveaux volumes source vers le site source d'origine. Le cas échéant, vous pouvez également lancer la réplication manuellement.
- Dans la mesure où la réplication s'effectue volume par volume, essayez de grouper les machines virtuelles dont les exigences de sauvegarde et planifications sont similaires sur le même volume de magasin de données. Par exemple, si certaines machines virtuelles ne requièrent pas de réplication sur un site distant ou doivent être répliquées moins fréquemment, ne les stockez pas sur le même volume de magasin de données que des machines virtuelles qui doivent être répliquées fréquemment. Vous éviterez ainsi les réplications de données superflues.
- Le SRA ne prend en charge que la réplication entre modèles matériels identiques. Par exemple, la réplication entre un système iSCSI uniquement et un système hybride FC/iSCSI n'est pas prise en charge.
- Évitez de mapper des volumes de réplication sur le LUN 0 pour parer aux problèmes liés au mappage et au démappage dynamiques des LUN, dus à la fonctionnalité de gestion spéciale attribuée au LUN 0. Vous pouvez mapper des volumes sur le LUN 0 si ces volumes ne sont pas supposés être mappés et démappés automatiquement comme les volumes de réplication (magasins de données locaux non répliqués, par exemple).
- Les volumes de réplication doivent être mappés avec le même LUN sur tous les hôtes.
- N'utilisez pas le même LUN pour différents volumes mappés sur des hôtes différents.
- À la suite d'opérations de reprise, les mappages d'hôte en lecture-écriture des volumes de réplication seront convertis en lecture seule. La restauration de la réplication convertira tous les mappages en lecture seule du même volume en lecture-écriture. Veillez à ne pas créer de mappages de volumes de réplication en lecture seule à des fins d'analyse des données, par exemple. Si un mappage de volume de réplication en lecture seule est nécessaire, envisagez de créer un instantané matériel ou logiciel non répliqué du volume.
- Le SRA peut créer des entrées hôtes sur le système de stockage pour assurer le suivi des adresses IP ou FC distantes. Ne supprimez pas les entrées hôtes dont le nom commence par « SRA ». Cependant, vous pouvez leur affecter des noms plus descriptifs.
- Pour permettre l'ajout de suffixes lors de la création des instantanés de réplication, les noms de base des ensembles de réplication pour les volumes répliqués (attribués lors de la création des ensembles de réplication) ne doivent pas dépasser 23 octets. Cette limite de 23 octets permet d'utiliser jusqu'à 23 caractères ASCII. En revanche, les caractères non-ASCII UTF-8 requièrent plus d'un octet chacun.
- Ne modifiez pas le nom des instantanés de réplication ni les noms de base des ensembles de réplication, sauf pour vous conformer aux meilleures pratiques. Le SRA s'appuie sur la cohérence entre les noms de base des ensembles de réplication et les noms des instantanés.