Verwalten von Site Recovery Manager

Site Recovery Manager 6.0

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Grundlegendes zur VMware vCenter Site Recovery Manager - Verwaltung

VMware vCenter Site Recovery Manager (Site Recovery Manager), eine Erweiterung zu VMware vCenter Server, stellt eine Lösung für die Notfallwiederherstellung und Geschäftskontinuität bereit und unterstützt Sie beim Planen, Testen und Ausführen der Wiederherstellung von virtuellen vCenter Server-Maschinen. Site Recovery Manager kann replizierte Datenspeicher erkennen und verwalten sowie die Migration von Bestandslisten zwischen vCenter Server-Instanzen automatisieren.

Zielgruppe

Dieses Buch richtet sich an Site Recovery Manager-Administratoren, die mit vSphere und dessen Replizierungstechnologien, wie z. B. der hostbasierten Replizierung und replizierten Datenspeichern, vertraut sind. Diese Lösung hilft Administratoren, die den Schutz für die vSphere-Bestandsliste konfigurieren möchten. Sie kann auch anderen Benutzern helfen, die virtuelle Maschinen zu einer geschützten Bestandsliste hinzufügen oder überprüfen möchten, ob eine vorhandene Bestandsliste für die Verwendung mit Site Recovery Manager ordnungsgemäß konfiguriert ist.

Aktualisierte Informationen

Verwalten von Site Recovery Manager wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *Verwalten von Site Recovery Manager*.

Revision	Beschreibung
DE-001664-06	■ Funktion von `defaultMaxBootAndShutdownOpsPerCluster` und `defaultMaxBootAndShutdownOpsPerHost` wurde unter Ändern der Einstellungen, um große Site Recovery Manager-Umgebungen auszuführen geklärt. ■ Maximale Protokollgröße von Site Recovery Manager Server wurde unter Ändern der Größe und Anzahl der Site Recovery Manager Server-Protokolldateien aktualisiert. ■ Die Informationen zur Zeitüberschreitungsperiode für Synchronisierungsvorgänge für vSphere Replication wurden in den folgenden Themen aktualisiert ■ Ändern der vSphere Replication-Einstellungen ■ Einstellungen für große Site Recovery Manager-Umgebungen ■ Ändern der Einstellungen, um große Site Recovery Manager-Umgebungen auszuführen ■ Erneutes Schützen schlägt mit einem vSphere Replication-Zeitüberschreitungsfehler fehl ■ Die Aussage, dass vSphere keine Unterstützung von vSphere vMotion bei virtuellen MSCS-Maschinen bietet, wurde aus Schützen von Microsoft Cluster Server und fehlertoleranten virtuellen Maschinen entfernt. ■ Die Beschreibung der Einstellung **allowOtherSolutionTagInRecovery** wurde unter Ändern der vSphere Replication-Einstellungen aktualisiert.
DE-001664-05	■ In vSphere Replication-Schutzgruppen wurde die Empfehlung hinzugefügt, für die vSphere Replication-Replikation und Site Recovery Manager Platzhalter-VMs unterschiedliche Datenspeicher zu verwenden. ■ In Erneutes Schützen virtueller Maschinen wurde die Empfehlung hinzugefügt, dass nach dem Ausführen des Vorgangs zum erneuten Schützen der Wiederherstellungsplan-Verlauf auf Fehler überprüft werden sollte.
DE-001664-04	Die Aussage, dass vSphere keine Unterstützung von vSphere vMotion bei virtuellen MSCS-Maschinen bietet, wurde aus Schützen von Microsoft Cluster Server und fehlertoleranten virtuellen Maschinen entfernt.
DE-001664-03	■ Zuweisen von Site Recovery Manager-Rollen und -Berechtigungen wurde durch die Beschreibung der Zuweisung von detaillierteren Berechtigungen ergänzt. ■ Die Themen Organisieren von Schutzgruppen in Ordnern und Organisieren von Wiederherstellungsplänen in Ordnern wurden hinzugefügt.
DE-001664-02	Es wurde ein Verweis auf das vRealize Orchestrator Plug-In für vSphere Replication in Automatisierte Vorgänge des vRealize Orchestrator-Plug-Ins für Site Recovery Manager hinzugefügt.

Revision	Beschreibung
DE-001664-01	■ In Installieren von SRA (Storage Replication Adapter) wurde der Pfad zu SRA-Downloads auf myvmware.com korrigiert und die Möglichkeit des Downloads zertifizierter SRAs von Drittanbieter-Sites geklärt. ■ In Neukonfigurieren der Site Recovery Manager-Einstellungen wurde hinzugefügt, dass erweiterte Einstellungen bei einem Upgrade oder nach De- und Neuinstallation der gleichen Produktversion nicht aufbewahrt werden.
DE-001664-00	Erstversion.

Site Recovery Manager -Rechte, -Rollen und -Berechtigungen

1

Site Recovery Manager bietet die Notfallwiederherstellung, indem Vorgänge für Benutzer ausgeführt werden. Zu diesen Vorgängen gehört das Verwalten von Objekten, z. B. von Wiederherstellungsplänen und Schutzgruppen, sowie die Durchführung von Vorgängen, z. B. das Replizieren und Ausschalten virtueller Maschinen. Site Recovery Manager verwendet Rollen und Berechtigungen, damit nur Benutzer mit den richtigen Rollen und Berechtigungen Vorgänge ausführen können.

Site Recovery Manager fügt mehrere Rollen zu vCenter Server hinzu. Jede dieser Rollen beinhaltet Rechte, um Site Recovery Manager- und vCenter Server-Aufgaben auszuführen. Sie können Benutzern Rollen zuweisen, um ihnen zu erlauben, Aufgaben in Site Recovery Manager abzuschließen.

Recht	Das Recht, eine Aktion auszuführen, z. B. einen Wiederherstellungsplan zu erstellen oder eine Schutzgruppe zu ändern.
Rolle	Eine Sammlung von Rechten. Standardrollen stellen die Rechte bereit, die bestimmte Benutzer benötigen, um mehrere Site Recovery Manager-Aufgaben auszuführen, beispielsweise Benutzer, die Schutzgruppen verwalten oder Wiederherstellungen durchführen. Ein Benutzer kann höchstens eine Rolle auf einem Objekt haben, aber Rollen können kombiniert werden, wenn der Benutzer mehreren Gruppen angehört, die alle Rollen auf dem Objekt haben.
Berechtigung	Eine Rolle, die einem bestimmten Benutzer oder einer bestimmten Benutzergruppe auf einem bestimmten Objekt zugeteilt wurde. Ein Benutzer oder eine Benutzergruppe wird auch als Prinzipal bezeichnet. Eine Berechtigung ist eine Kombination aus einer Rolle, einem Objekt und einem Prinzipal. Beispielsweise ist eine Berechtigung das Recht, eine bestimmte Schutzgruppe zu ändern.

Weitere Informationen zu den Rollen, die Site Recovery Manager zu vCenter Server hinzufügt, und zu den Rechten, die Benutzer benötigen, um Aufgaben auszuführen, finden Sie unter Rollenreferenzen für Site Recovery Manager.

Wie Site Recovery Manager Berechtigungen handhabt

Site Recovery Manager prüft, ob ein Nutzer über die Berechtigung zum Durchführen eines Vorgangs verfügt, wie z. B. zum Konfigurieren des Schutzes oder zum Ausführen der einzelnen Schritte in einem Wiederherstellungsplan. Diese Berechtigungsüberprüfung stellt die richtige Authentifizierung der Nutzer sicher, repräsentiert aber nicht den Sicherheitskontext, in dem der Vorgang durchgeführt wird.

Site Recovery Manager führt Vorgänge im Sicherheitskontext der Benutzer-ID durch, die zum Verbinden von Sites verwendet wird, oder im Kontext der ID, unter der der Site Recovery Manager-Dienst ausgeführt wird, wie beispielsweise die lokale System-ID.

Nachdem Site Recovery Manager sichergestellt hat, dass ein Benutzer über die entsprechenden Berechtigungen für die vSphere-Zielressourcen verfügt, führt Site Recovery Manager unter Verwendung der vSphere-Administratorrolle Vorgänge im Namen von Benutzern durch.

Für Vorgänge, die den Schutz auf virtuellen Maschinen konfigurieren, validiert Site Recovery Manager die Benutzerberechtigungen, wenn der Benutzer den Vorgang anfordert. Vorgänge erfordern eine zweistufige Validierung.

1 Während der Konfiguration stellt Site Recovery Manager sicher, dass der Benutzer, der das System konfiguriert, über die entsprechenden Berechtigungen zum Durchführen der Konfiguration für das vCenter Server-Objekt verfügt. Ein Benutzer muss beispielsweise über die Berechtigungen zum Schützen einer virtuellen Maschine und zum Verwenden von Ressourcen auf einer sekundären vCenter Server-Instanz verfügen, die die wiederhergestellte virtuelle Maschine verwendet.

2 Der Benutzer, der die Konfiguration durchführt, muss über die entsprechenden Berechtigungen verfügen, um den Vorgang durchzuführen, den er konfiguriert. Ein Benutzer muss z. B. über die Berechtigungen zum Ausführen eines Wiederherstellungsplans verfügen. Site Recovery Manager führt den Vorgang dann im Namen des Benutzers als vCenter Server-Administrator durch.

Folglich muss ein Benutzer, der eine bestimmte Aufgabe, z. B. eine Wiederherstellung, durchführt, nicht unbedingt über Berechtigungen zum Durchführen von Aufgaben auf vSphere-Ressourcen verfügen. Der Benutzer benötigt lediglich die Berechtigung zum Ausführen einer Wiederherstellung in Site Recovery Manager. Die Rolle autorisiert die Aktion, aber die Aktion wird von Site Recovery Manager als Administrator durchgeführt. Site Recovery Manager führt die Vorgänge anhand der Administratoranmeldedaten durch, die Sie angeben, wenn Sie den Schutz- und die Wiederherstellungs-Site verbinden.

Site Recovery Manager unterhält eine Datenbank mit Berechtigungen für interne Site Recovery Manager-Objekte, die ein Modell ähnlich dem verwendet, das vCenter Server nutzt. Site Recovery Manager überprüft seine eigenen Site Recovery Manager-Rechte – sogar für vCenter Server-Objekte. Site Recovery Manager überprüft z. B. die Berechtigung **Resource.Verwendung der Wiederherstellung** für den Zieldatenspeicher, anstatt mehrere Low-Level-Berechtigungen zu prüfen, wie z. B. **Speicher zuteilen**. Site Recovery Manager überprüft zudem die Berechtigungen auf der vCenter Server-Remoteinstanz.

Um Site Recovery Manager mit vSphere Replication zu verwenden, müssen Sie Benutzern vSphere Replication-Rollen sowie Site Recovery Manager-Rollen zuweisen. Informationen über die vSphere Replication-Rollen finden Sie unter *Verwaltung von vSphere Replication*.

Site Recovery Manager und die vCenter Server - Administratorrolle

Ein Benutzer oder eine Benutzergruppe mit der vCenter Server-Administratorrolle auf einer vCenter Server-Instanz erhält während der Installation von Site Recovery Manager sämtliche Site Recovery Manager-Berechtigungen.

Wenn Sie Benutzern oder Benutzergruppen die vCenter Server-Administratorrolle nach der Installation von Site Recovery Manager zuweisen, müssen Sie ihnen die Site Recovery Manager-Rollen für die Site Recovery Manager-Objekte manuell zuweisen.

Sie können Site Recovery Manager-Rollen Benutzern oder Benutzergruppen zuweisen, die nicht über die vCenter Server-Administratorrolle verfügen. In diesem Fall haben die betroffenen Benutzer die Berechtigung zur Durchführung von Site Recovery Manager-Vorgängen, nicht jedoch zur Durchführung aller vCenter Server-Vorgänge.

Site Recovery Manager - und vSphere Replication -Rollen

Bei der Installation von vSphere Replication mit Site Recovery Manager werden für die vCenter Server-Administratorrolle alle Berechtigungen aus Site Recovery Manager und vSphere Replication übernommen.

Wenn Sie einem Benutzer oder einer Benutzergruppe manuell eine Site Recovery Manager-Rolle zuweisen bzw. einem Benutzer oder einer Benutzergruppe, bei dem/der es sich nicht um einen Site Recovery Manager-Administrator handelt, eine vCenter Server-Rolle zuweisen, erhalten die betroffenen Benutzer keine vSphere Replication-Berechtigungen. Die Site Recovery Manager-Rollen schließen nicht die Berechtigungen der vSphere Replication-Rollen ein. Beispiel: Die Administratorrolle für Site Recovery Manager-Wiederherstellungen umfasst die Berechtigung zur Ausführung von Wiederherstellungsplänen, was auch Wiederherstellungspläne mit vSphere Replication-Schutzgruppen einschließt, jedoch nicht die Berechtigung zur Konfiguration von vSphere Replication auf einer virtuellen Maschine. Die Trennung der Site Recovery Manager- und der vSphere Replication-Rollen ermöglicht die Aufteilung von Zuständigkeiten auf verschiedene Benutzer. Beispiel: Ein Benutzer mit der VRM-Administratorrolle ist für die Konfiguration von vSphere Replication auf virtuellen Maschinen und ein anderer Benutzer mit der Administratorrolle für Site Recovery Manager-Wiederherstellungen für die Ausführung von Wiederherstellungen zuständig.

Es kann vorkommen, dass ein Benutzer, bei dem es sich nicht um einen vCenter Server-Administrator handelt, die Berechtigungen zur Durchführung sowohl von Site Recovery Manager- als auch von vSphere Replication-Vorgängen benötigt. Um einem einzelnen Benutzer eine Kombination aus Site Recovery Manager- und vSphere Replication-Rollen zuzuweisen, können Sie den Benutzer in zwei Benutzergruppen aufnehmen.

Beispiel: Zuweisen von Site Recovery Manager - und vSphere Replication -Rollen zu einem Benutzer

Durch Erstellung von zwei Benutzergruppen können Sie einem Benutzer die Berechtigungen sowohl einer Site Recovery Manager-Rolle als auch einer vSphere Replication-Rolle gewähren, ohne dass es sich bei diesem Benutzer um einen vCenter Server-Administrator handelt.

1 Erstellen Sie zwei Benutzergruppen.

2 Weisen Sie einer der Benutzergruppen eine Site Recovery Manager-Rolle zu, z. B. Site Recovery Manager-Administrator.

3 Weisen Sie der anderen Benutzergruppe eine vSphere Replication-Rolle zu, z. B. VRM-Administrator.

4 Nehmen Sie den Benutzer in beide Benutzergruppen auf.

Damit verfügt der Benutzer über sämtliche Berechtigungen der Site Recovery Manager-Administratorrolle und der VRM-Administratorrolle.

Verwalten von Berechtigungen in einer Konstellation mit gemeinsam genutzter Wiederherstellungs-Site

Sie können Site Recovery Manager zur Verwendung mit einer gemeinsam genutzten Wiederherstellungs-Site konfigurieren. Der vCenter Server-Administrator auf der gemeinsam genutzten Wiederherstellungs-Site muss Berechtigungen verwalten, sodass jeder Benutzer über ausreichende Berechtigungen zum Konfigurieren und Verwenden von Site Recovery Manager verfügt, aber kein Benutzer Zugriff auf Ressourcen hat, die anderen Benutzern gehören.

Im Kontext einer gemeinsam genutzten Wiederherstellungs-Site ist ein Benutzer der Besitzer eines Paars der Site Recovery Manager Server-Instanzen. Benutzer mit ausreichenden Berechtigungen müssen in der Lage sein, auf die gemeinsam genutzte Wiederherstellungs-Site zuzugreifen, um die Wiederherstellungspläne für die eigene Schutz-Site zu erstellen, zu testen und auszuführen. Der vCenter Server-Administrator auf der gemeinsam genutzten Wiederherstellungs-Site muss für jeden Benutzer eine separate Benutzergruppe erstellen. Die Benutzerkonten von Benutzern können nicht Mitglied der vCenter Server-Administratorengruppe sein. Die einzige unterstützte Konfiguration für eine gemeinsam genutzte Wiederherstellungs-Site ist für eine Organisation, um alle Schutz-Sites und die Wiederherstellungs-Site zu verwalten.

Vorsicht Bestimmte Site Recovery Manager-Rollen ermöglichen Benutzern, Befehle auf einem Site Recovery Manager Server auszuführen, sodass Sie diese Rollen nur vertrauenswürdigen Benutzern auf Administratorebene zuweisen sollten. Unter Rollenreferenzen für Site Recovery Manager finden Sie die Liste der Site Recovery Manager-Rollen, die auf dem Site Recovery Manager Server Befehle ausführen.

Auf einer gemeinsam genutzten Wiederherstellungs-Site verwenden mehrere Kunden eine einzelne vCenter Server-Instanz zusammen. In einigen Fällen können mehrere Kunden zusammen einen einzelnen ESXi-Host auf der Wiederherstellungs-Site verwenden. Sie können die Ressourcen auf den Schutz-Sites den gemeinsam genutzten Ressourcen auf der gemeinsam genutzten Wiederherstellungs-Site zuordnen. Sie nutzen Ressourcen auf der Wiederherstellungs-Site möglicherweise gemeinsam, wenn Sie nicht alle virtuellen Maschinen des Kunden getrennt halten müssen, beispielsweise wenn alle Kunden zu derselben Organisation gehören.

Sie können isolierte Ressourcen ebenfalls auf der gemeinsam genutzten Wiederherstellungs-Site verwenden und die Ressourcen auf den Schutz-Sites ihren eigenen dedizierten Ressourcen auf der gemeinsam genutzten Wiederherstellungs-Site zuordnen. Sie verwenden diese Konfiguration möglicherweise, wenn Sie alle virtuellen Maschinen der Kunden voneinander getrennt halten müssen, beispielsweise wenn alle Kunden zu verschiedenen Unternehmen gehören.

Richtlinien zum Freigeben von Benutzerressourcen

Befolgen Sie diese Richtlinien, wenn Sie Berechtigungen zur Freigabe von Benutzerressourcen auf der gemeinsam genutzten Wiederherstellungs-Site konfigurieren:

- Alle Benutzer müssen auf der gemeinsam genutzten Wiederherstellungs-Site über Lesezugriff auf alle Ordner von vCenter Server verfügen.

- Erteilen Sie einem Benutzer nicht die Berechtigung, das Datencenter oder den Host umzubenennen, zu verschieben oder zu löschen.
- Erteilen Sie einem Benutzer nicht die Berechtigung, virtuelle Maschinen außerhalb der Ordner und Ressourcenpools, die für den Benutzer reserviert sind, zu erstellen.
- Erteilen Sie einem Benutzer nicht die Berechtigung, Rollen zu ändern oder Berechtigungen für Objekte zuzuweisen, die nicht für die eigene Verwendung des Benutzers reserviert sind.
- Um die ungewollte Weitergabe von Berechtigungen für unterschiedliche Organisationsressourcen zu verhindern, geben Sie auf der gemeinsam genutzten Wiederherstellungs-Site keine Berechtigungen für Root-Ordner, Datencenter und Hosts des vCenter Server weiter.

Richtlinien zum Isolieren von Benutzerressourcen

Befolgen Sie diese Richtlinien, wenn Sie Berechtigungen zum Isolieren von Benutzerressourcen auf der gemeinsam genutzten Wiederherstellungs-Site konfigurieren:

- Weisen Sie jedem Benutzer einen separaten Ordner der virtuellen Maschine in der vCenter Server-Bestandsliste zu.
  - Legen Sie die Berechtigungen für diesen Ordner fest, um das Platzieren virtueller Maschinen anderer Benutzer in diesen Ordner zu verhindern. Legen Sie beispielsweise die Administratorrolle fest und aktivieren Sie die Option „Weitergeben“ für einen Benutzer für den Ordner dieses Benutzers. Diese Konfiguration verhindert „Doppelter Name“-Fehler, die ansonsten möglicherweise auftreten, wenn mehrere Benutzer virtuelle Maschinen schützen, die identische Namen haben.
  - Platzieren Sie alle Platzhalter-VMs des Benutzers in diesen Ordner, sodass sie seine Berechtigungen übernehmen können.
  - Weisen Sie Zugriffsberechtigungen für diesen Ordner nicht anderen Benutzern zu.
- Weisen Sie allen Benutzern dedizierte Ressourcenpools, Datenspeicher und Netzwerke zu und konfigurieren Sie Berechtigungen auf dieselbe Weise wie für Ordner.

Vorsicht Eine Bereitstellung, in der Sie Benutzerressourcen isolieren, geht weiterhin davon aus, dass die vSphere-Sites untereinander vertrauenswürdig sind. Obwohl Sie Benutzerressourcen isolieren können, können Sie die Benutzer selbst nicht isolieren. Wenn Sie alle Benutzer vollständig voneinander trennen müssen, ist dies keine geeignete Bereitstellung.

Anzeigen von Aufgaben und Ereignissen in einer Konfiguration der gemeinsam genutzten Wiederherstellungs-Site

Im Fenster „Kürzlich bearbeitete Aufgaben“ des vSphere Client können Benutzer Aufgaben sehen, die andere Benutzer in Zusammenhang mit dem Objekt starten (sofern sie über die Berechtigungen verfügen, ein Objekt zu sehen). Alle Benutzer können alle Aufgaben sehen, die andere Benutzer auf einer freigegebenen Ressource durchführen. Alle Benutzer können beispielsweise die Aufgaben sehen, die auf einem freigegebenen Host, Datencenter oder auf dem vCenter Server-Root-Ordner ausgeführt werden.

Ereignisse, die alle Instanzen des Site Recovery Manager Server auf einer gemeinsam genutzten Wiederherstellungs-Site generieren, verfügen über identische Berechtigungen. Alle Benutzer, die Ereignisse aus einer Instanz des Site Recovery Manager Server sehen können, können Ereignisse aus allen Site Recovery Manager Server-Instanzen sehen, die auf der gemeinsam genutzten Wiederherstellungs-Site ausgeführt werden.

Zuweisen von Site Recovery Manager -Rollen und -Berechtigungen

Während der Installation von Site Recovery Manager wird Benutzern mit der vCenter Server-Administratorrolle auch die Administratorrolle für Site Recovery Manager gewährt. Zu diesem Zeitpunkt können sich nur vCenter Server-Administratoren bei Site Recovery Manager anmelden, sofern sie nicht explizit anderen Benutzern Zugriff gewähren.

Damit andere Benutzer auf Site Recovery Manager zugreifen können, müssen vCenter Server-Administratoren diesen auf der Site Recovery Manager-Benutzeroberfläche im vSphere Web Client Berechtigungen gewähren. Sie führen Site-weite Berechtigungszuweisungen pro Site durch. Sie müssen auf beiden Sites entsprechende Berechtigungen hinzufügen.

Site Recovery Manager benötigt Berechtigungen für vCenter Server- und Site Recovery Manager-Objekte. Um Berechtigungen auf der Remoteinstallation von vCenter Server zu konfigurieren, starten Sie eine weitere Instanz des vSphere Web Client. Nach dem Verbinden der Schutz- und der Wiederherstellungs-Site können Sie auf beiden Sites die Site Recovery Manager-Berechtigungen über die gleiche vSphere Web Client-Instanz ändern.

Site Recovery Manager erweitert die vCenter Server-Rollen und -Berechtigungen um zusätzliche Berechtigungen, die eine detaillierte Steuerung der Site Recovery Manager-spezifischen Aufgaben und Vorgänge ermöglichen. Informationen zu den Berechtigungen jeder Site Recovery Manager-Rolle finden Sie unter Rollenreferenzen für Site Recovery Manager.

Sie können Benutzern detailliertere Berechtigungen zuweisen, indem Sie ihnen Berechtigungen für bestimmte Site Recovery Manager-Objekte zuweisen, einschließlich individueller Array-Manager, Schutzgruppen und Wiederherstellungspläne. Sie können einem Benutzer auch den Zugriff auf bestimmte Gruppen von Schutzgruppen, Wiederherstellungsplänen und Array-Managern ermöglichen, indem Sie Schutzgruppen- und Wiederherstellungsplan-Ordnern sowie allen Array-Managern für eine Site Berechtigungen zuweisen.

Vorgehensweise

1 Wählen Sie in vSphere Web Client die Objekte aus, denen Sie Berechtigungen zuweisen möchten.

Option	Beschreibung
Siteweite Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
Individueller Schutzgruppe Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung**, erweitern Sie **Bestandslisten**, klicken Sie auf **Schutzgruppen** und wählen Sie eine Schutzgruppe aus.

Option	Beschreibung
Einem Schutzgruppen-Ordner Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung**, erweitern Sie **Bestandslistenstrukturen**, klicken Sie auf **Schutzgruppen** und wählen Sie einen Schutzgruppen-Ordner aus. Sie können dem Root-Ordner oder einem Unterordner Berechtigungen zuweisen.
Individuellem Wiederherstellungsplan Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung**, erweitern Sie **Bestandslisten**, klicken Sie auf **Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
Einem Wiederherstellungsplan-Ordner Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung**, erweitern Sie **Bestandslistenstrukturen**, klicken Sie auf **Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan-Ordner aus. Sie können dem Root-Ordner oder einem Unterordner Berechtigungen zuweisen.
Individuellem Array-Manager Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung > Array-basierte Replizierung** und wählen Sie einen Array-Manager aus.
Sämtlichen Array-Managern für eine Site Berechtigungen zuweisen	Klicken Sie auf **Site-Wiederherstellung**, erweitern Sie **Bestandslistenstrukturen**, klicken Sie auf **Array-basierte Replizierung** und wählen Sie einen Site-Ordner aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Berechtigungen** und dann auf das Symbol **Berechtigung hinzufügen**.

3 Identifizieren Sie einen Benutzer oder eine Gruppe für die Rolle.

   a Klicken Sie in der Spalte „Benutzer und Gruppen“ auf **Hinzufügen**.

   b Wählen Sie im Dropdown-Menü **Domäne** die Domäne aus, die den Benutzer oder die Gruppe enthält.

   c Geben Sie einen Benutzer- oder Benutzergruppennamen im Textfeld **Suchen** ein oder wählen Sie in der Liste **Benutzer/Gruppe** einen Namen aus.

   d Klicken Sie auf **Hinzufügen** und anschließend auf **OK**.

4 Wählen Sie im Dropdown-Menü **Zugewiesene Rolle** eine Rolle aus, um sie dem bzw. der in Schritt 3 ausgewählten Benutzer bzw. ausgewählten Benutzergruppe zuzuweisen.

   Das Dropdown-Menü **Zugewiesene Rolle** enthält sämtliche Rollen, die in vCenter Server und dessen Plug-Ins zur Verfügung stehen. Site Recovery Manager fügt mehrere Rollen zu vCenter Server hinzu.

Option	Aktion
Genehmigt einem Benutzer oder einer Benutzergruppe die Durchführung aller Site Recovery Manager-Konfigurations- und -Verwaltungsvorgänge.	Weist die Rolle **SRM-Administrator** zu.
Genehmigt einem Benutzer oder einer Benutzergruppe die Verwaltung und Modifizierung von Schutzgruppen und die Schutzkonfiguration auf virtuellen Maschinen.	Weist die Rolle **Administrator für SRM-Schutzgruppen** zu.

Option	Aktion
Genehmigt einem Benutzer oder einer Benutzergruppe die Durchführung und das Testen von Wiederherstellungen.	Weist die Rolle **Administrator für SRM-Wiederherstellungen** zu.
Genehmigt einem Benutzer oder einer Benutzergruppe das Erstellen, Modifizieren und Testen von Wiederherstellungsplänen.	Weist die Rolle **Administrator für SRM-Wiederherstellungspläne** zu.
Genehmigt einem Benutzer oder einer Benutzergruppe das Testen von Wiederherstellungsplänen.	Weist die Rolle **Administrator für SRM-Wiederherstellungstest** zu.

Wenn Sie eine Rolle auswählen, werden die Berechtigungen für diese Rolle in einer hierarchischen Liste angezeigt. Klicken Sie auf eine Berechtigung in der hierarchischen Liste, um eine Beschreibung dieser Berechtigung anzuzeigen. Sie können die Liste der Berechtigungen einzelner Rollen nicht ändern.

5 Wenn die ausgewählte Rolle auf alle untergeordneten Objekte der von dieser Rolle betroffenen Bestandslistenobjekte angewendet werden soll, wählen Sie **An untergeordnete Objekte weitergeben** aus.

   Wenn z. B. eine Rolle Berechtigungen zum Ändern von Ordnern einschließt, werden durch Auswahl dieser Option die Berechtigungen auf alle virtuellen Maschinen in einem Ordner ausgeweitet. Sie können diese Option deaktivieren, um eine komplexere Berechtigungshierarchie zu erstellen. Deaktivieren Sie z. B. diese Option zur Außerkraftsetzung der Berechtigungen, die vom Stamm eines bestimmten Knotens in der Hierarchiestruktur weitergegeben werden, ohne jedoch die Berechtigungen der untergeordneten Objekte dieses Knotens außer Kraft zu setzen.

6 Klicken Sie auf **OK**, um die Rolle und deren zugehörige Berechtigungen dem Benutzer oder der Benutzergruppe zuzuweisen.

7 Wiederholen Sie die Schritte Schritt 2 bis Schritt 6, um Benutzern bzw. Benutzergruppen auf der anderen Site Recovery Manager-Site Rollen und Berechtigungen zuzuweisen.

Sie haben einem Benutzer bzw. einer Benutzergruppe eine bestimmte Site Recovery Manager-Rolle zugewiesen. Dieser Benutzer bzw. diese Benutzergruppe verfügt über Berechtigungen zur Durchführung der Aktionen, die die Rolle für die Objekte auf der von Ihnen konfigurierten Site Recovery Manager-Site definiert.

Beispiel: Kombinieren von Site Recovery Manager -Rollen

Sie können einem Benutzer oder einer Benutzergruppe jeweils nur eine Rolle zuweisen. Wenn ein Benutzer, bei dem es sich nicht um einen vCenter Server-Administrator handelt, die Berechtigungen mehrerer Site Recovery Manager-Rollen benötigt, können Sie mehrere Benutzergruppen einrichten. Angenommen, ein Benutzer benötigt die Berechtigungen zur Verwaltung von Wiederherstellungsplänen und zur Ausführung von Wiederherstellungsplänen.

1 Richten Sie zwei Benutzergruppen ein.

2 Weisen Sie einer Gruppe die Rolle **Administrator für SRM-Wiederherstellungspläne** zu.

3 Weisen Sie der anderen Gruppe die Rolle **Administrator für SRM-Wiederherstellungen** zu.

4 Nehmen Sie den Benutzer in beide Gruppen auf.

Wenn ein Benutzer Mitglied von Gruppen ist, in denen die beiden Rollen **Administrator für SRM-Wiederherstellungspläne** und **Administrator für SRM-Wiederherstellungen** vorhanden sind, kann er Wiederherstellungspläne sowohl verwalten als auch ausführen.

Rollenreferenzen für Site Recovery Manager

Site Recovery Manager enthält mehrere Rollen. Jede Rolle enthält mehrere Rechte, sodass Benutzer mit diesen Rollen verschiedene Aktionen ausführen können.

Rollen können über mehrere überlappende Rechte und Aktionen verfügen. Beispielsweise verfügen die Rolle Site Recovery Manager-Administrator und der Administrator von Site Recovery Manager-Schutzgruppen über das Recht **Erstellen** für Schutzgruppen. Mit diesem Recht kann der Benutzer einen Aspekt der Aufgaben abschließen, die die Verwaltung von Schutzgruppen ausmachen.

Weisen Sie Benutzern Rollen für Site Recovery Manager-Objekte konsistent an beiden Sites zu, sodass Schutz- und Wiederherstellungsobjekte über identische Berechtigungen verfügen.

Alle Benutzer benötigen mindestens die Berechtigung **System.Lesen** für die Root-Ordner von vCenter Server und die Site Recovery Manager-Root-Knoten an beiden Sites.

Hinweis Bei Deinstallation von Site Recovery Manager Server entfernt Site Recovery Manager die standardmäßigen Site Recovery Manager-Rollen, die Site Recovery Manager-Berechtigungen werden hingegen beibehalten. Sie können nach der Deinstallation von Site Recovery Manager weiterhin Site Recovery Manager-Berechtigungen in anderen Rollen anzeigen und zuweisen. Dies ist standardmäßiges Verhalten von vCenter Server. Berechtigungen werden nicht entfernt, wenn Sie die Registrierung einer Erweiterung auf vCenter Server aufheben.

Tabelle 1-1. Site Recovery Manager -Rollen

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
Site Recovery Manager-Administrator	Der Site Recovery Manager-Administrator gewährt die Berechtigung zur Durchführung aller Site Recovery Manager-Konfigurations- und -Verwaltungsvorgänge. ■ Erweiterte Einstellungen konfigurieren. ■ Verbindungen konfigurieren. ■ Konfigurieren der Einstellungen für Bestandslisten. ■ Konfigurieren von Platzhalterdatenspeichern. ■ Konfigurieren von Array-Managern. ■ Schutzgruppen verwalten. ■ Wiederherstellungspläne verwalten. ■ Vorgänge zum erneuten Schutz durchführen. ■ Konfigurieren von Schutz auf virtuellen Maschinen. ■ Schutzgruppen bearbeiten. ■ Schutzgruppen entfernen. Benutzer mit dieser Rolle können keine Wiederherstellungen ausführen. Wiederherstellungen können ausschließlich von Benutzern mit der Administratorrolle für Site Recovery Manager-Wiederherstellungen ausgeführt werden.	**Site Recovery Manager.Erweiterte Einstellungen.Ändern** **Site Recovery Manager.Array-Manager.Konfigurieren** **Site Recovery Manager.DiagnosticsExport.Diagnose.Export** **Site Recovery Manager.Bestandslistenvoreinstellungen.Ändern** **Site Recovery Manager.Platzhalterdatenspeicher.Konfigurieren** **Site Recovery Manager.DiagnoseExport** **Site Recovery Manager.Schutzgruppe.Einem Plan zuweisen** **Site Recovery Manager.Schutzgruppe.Erstellen** **Site Recovery Manager.Schutzgruppe.Ändern** **Site Recovery Manager.Schutzgruppe.Entfernen** **Site Recovery Manager.Schutzgruppe.Aus Plan entfernen** **Site Recovery Manager.Wiederherstellungsverlauf.Gelöschte Pläne anzeigen** **Site Recovery Manager.Wiederherstellungsplan.Konfigurieren** **Site Recovery Manager.Wiederherstellungsplan.Erstellen** **Site Recovery Manager.Wiederherstellungsplan.Ändern** **Site Recovery Manager.Wiederherstellungsplan.Entfernen** **Site Recovery Manager.Wiederherstellungsplan.Neu schützen** **Site Recovery Manager.Wiederherstellungsplan .Testen** **Site Recovery Manager.Remote-Site.Ändern** **Datenspeicher.Replizierung.Schützen** **Datenspeicher.Replizierung.Schutz aufheben.Beenden** **Ressource.Verwendung der Wiederherstellung**	■ Virtuelle Maschinen ■ Datenspeicher ■ vCenter Server-Ordner ■ Ressourcenpools ■ Site Recovery Manager-Dienstinstanzen ■ Netzwerke ■ Site Recovery Manager-Ordner ■ Schutzgruppen ■ Wiederherstellungspläne ■ Array-Manager

Tabelle 1-1. Site Recovery Manager -Rollen (Fortsetzung)

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
		Virtuelle Maschine.SRM-Schutz.Schützen **Virtuelle Maschine.SRM-Schutz.Beenden**	
Administrator für Site Recovery Manager-Schutzgruppen	Mit der Administratorrolle für Site Recovery Manager-Schutzgruppen können Benutzer Schutzgruppen verwalten. ■ Erstellen von Schutzgruppen. ■ Ändern von Schutzgruppen. ■ Hinzufügen von virtuellen Maschinen zu Schutzgruppen. ■ Löschen von Schutzgruppen. ■ Konfigurieren von Schutz auf virtuellen Maschinen. ■ Entfernen des Schutzes aus virtuellen Maschinen. Benutzer mit dieser Rolle können weder Wiederherstellungen durchführen oder testen noch Wiederherstellungspläne erstellen oder ändern.	**Site Recovery Manager.Schutzgruppe.Erstellen** **Site Recovery Manager.Schutzgruppe.Ändern** **Site Recovery Manager.Schutzgruppe.Entfernen** **Datenspeicher.Replizierung.Schützen** **Datenspeicher.Replizierung.Schutz aufheben.Beenden** **Ressource.Verwendung der Wiederherstellung** **Virtuelle Maschine.SRM-Schutz.Schützen** **Virtuelle Maschine.SRM-Schutz.Beenden**	■ Site Recovery Manager-Ordner ■ Schutzgruppen

Tabelle 1-1. Site Recovery Manager -Rollen (Fortsetzung)

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
Site Recovery Manager-Wiederherstellungs-Administrator	Die Administratorrolle für Site Recovery Manager-Wiederherstellungen ermöglicht Benutzern die Durchführung von Wiederherstellungen und Vorgängen zum erneuten Schützen. ■ Schutzgruppen aus Wiederherstellungsplänen entfernen. ■ Wiederherstellungspläne testen. ■ Wiederherstellungspläne ausführen. ■ Vorgänge zum erneuten Schützen durchführen. ■ Benutzerdefinierte Befehlsschritte auf virtuellen Maschinen konfigurieren. ■ Gelöschte Wiederherstellungspläne anzeigen. ■ Wiederherstellungseigenschaften von virtuellen Maschinen bearbeiten. Benutzer mit dieser Rolle können weder den Schutz auf virtuellen Maschinen konfigurieren noch Wiederherstellungspläne erstellen oder ändern.	**Site Recovery Manager.Schutzgruppe.Aus Plan entfernen** **Site Recovery Manager.Wiederherstellungsplan.Ändern** **Site Recovery Manager.Wiederherstellungsplan .Testen** **Site Recovery Manager.Wiederherstellungsplan.Wiederherstellen** **Site Recovery Manager.Wiederherstellungsplan.Neu schützen** **Site Recovery Manager.Wiederherstellungsplan.Konfigurieren.Befehle konfigurieren** **Site Recovery Manager.Wiederherstellungsverlauf.Gelöschte Pläne anzeigen**	■ Schutzgruppen ■ Wiederherstellungspläne ■ Site Recovery Manager-Dienstinstanzen

Tabelle 1-1. Site Recovery Manager -Rollen (Fortsetzung)

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
Administrator für Site Recovery Manager-Wiederherstellungspläne	Die Administratorrolle für Site Recovery Manager-Wiederherstellungspläne ermöglicht Benutzern das Erstellen und Testen von Wiederherstellungsplänen. ■ Schutzgruppen zu Wiederherstellungsplänen hinzufügen. ■ Schutzgruppen aus Wiederherstellungsplänen entfernen. ■ Benutzerdefinierte Befehlsschritte auf virtuellen Maschinen konfigurieren. ■ Erstellen von Wiederherstellungsplänen. ■ Wiederherstellungspläne testen. ■ Tests von Wiederherstellungsplänen abbrechen. ■ Wiederherstellungseigenschaften von virtuellen Maschinen bearbeiten. Benutzer mit dieser Rolle können weder den Schutz auf virtuellen Maschinen konfigurieren noch Wiederherstellungen oder Vorgänge zum erneuten Schützen durchführen.	**Site Recovery Manager.Schutzgruppe.Einem Plan zuweisen** **Site Recovery Manager.Schutzgruppe.Aus Plan entfernen** **Site Recovery Manager.Wiederherstellungsplan.Befehle konfigurieren** **Site Recovery Manager.Wiederherstellungsplan.Erstellen** **Site Recovery Manager.Wiederherstellungsplan.Ändern** **Site Recovery Manager.Wiederherstellungsplan.Entfernen** **Site Recovery Manager.Wiederherstellungsplan .Testen** **Ressource.Verwendung der Wiederherstellung**	■ Schutzgruppen ■ Wiederherstellungspläne ■ vCenter Server-Ordner ■ Datenspeicher ■ Ressourcenpools ■ Netzwerke
Administrator für Site Recovery Manager-Tests	Die Administratorrolle für Site Recovery Manager-Tests ermöglicht Benutzern lediglich das Testen von Wiederherstellungsplänen. ■ Wiederherstellungspläne testen.	**Site Recovery Manager.Wiederherstellungsplan.Ändern** **Site Recovery Manager.Wiederherstellungsplan .Testen**	Wiederherstellungspläne

Tabelle 1-1. Site Recovery Manager -Rollen (Fortsetzung)

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
	■ Tests von Wiederherstellungsplänen abbrechen. ■ Wiederherstellungseigenschaften von virtuellen Maschinen bearbeiten. Benutzer mit dieser Rolle können keinen Schutz auf virtuellen Maschinen konfigurieren, keine Schutzgruppen oder Wiederherstellungspläne einrichten und keine Wiederherstellungen oder Vorgänge zum erneuten Schützen durchführen.		

Replizieren von virtuellen Maschinen

2

Vor dem Erstellen von Schutzgruppen müssen Sie die Replizierung auf den zu schützenden virtuellen Maschinen konfigurieren.

Sie können virtuelle Maschinen replizieren, indem Sie entweder die Array-basierte Replizierung, vSphere Replication oder eine Kombination von beiden verwenden.

Dieses Kapitel behandelt die folgenden Themen:

Verwenden der Array-basierten Replizierung mit Site Recovery Manager

Bei der Verwendung der Array-basierten Replizierung replizieren ein oder mehrere Speicher-Arrays der Schutz-Site Daten auf Peer-Arrays der Wiederherstellungs-Site. Speicherreplizierungsadapter (SRAs) ermöglichen die Integration von Site Recovery Manager mit einer Vielzahl von Arrays.

Wenn Sie die Array-basierte Replizierung mit Site Recovery Manager verwenden möchten, müssen Sie zuerst die Replizierung einrichten, bevor Sie Site Recovery Manager konfigurieren können.

Sofern Ihr Speicher-Array Konsistenzgruppen unterstützt, ist Site Recovery Manager mit vSphere Storage DRS und vSphere Storage vMotion kompatibel. Sie können mit Storage DRS und Storage vMotion Dateien von virtuellen Maschinen innerhalb einer von Site Recovery Manager geschützten Konsistenzgruppe verschieben. Falls Ihr Speicher-Array keine Konsistenzgruppen unterstützt, können Sie Storage DRS oder Storage vMotion nicht in Verbindung mit Site Recovery Manager verwenden.

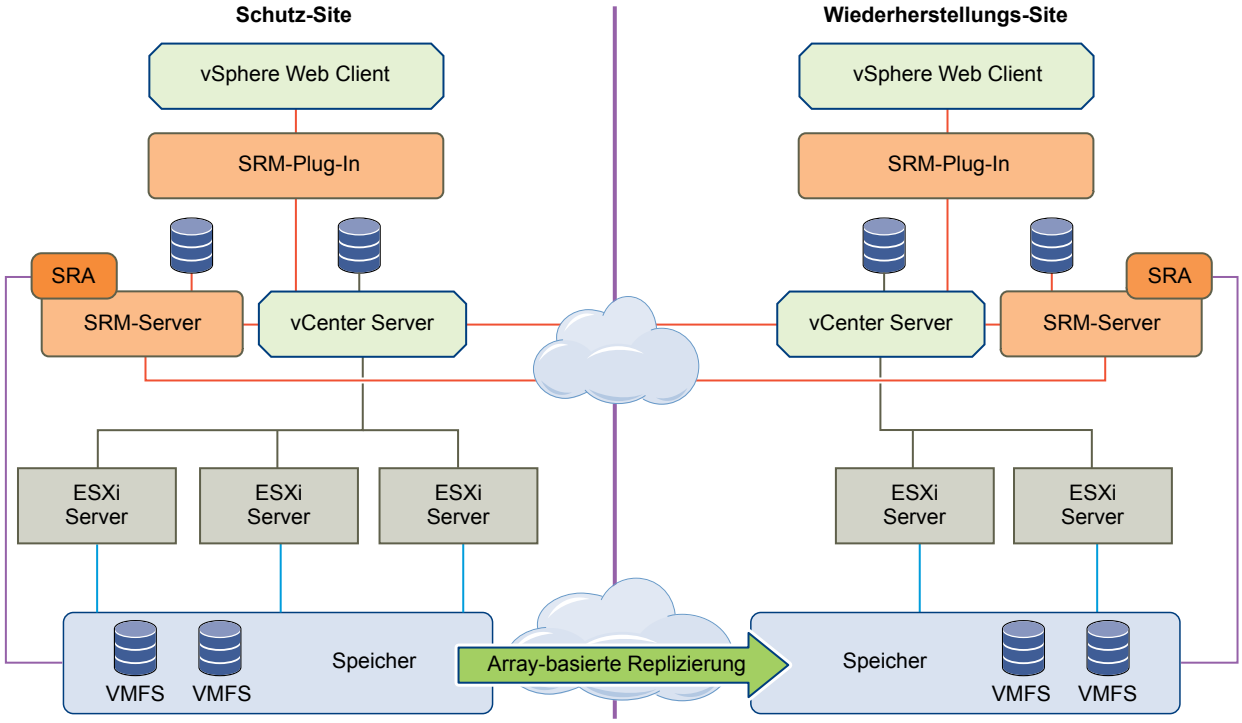
Sie können virtuelle Maschinen schützen, die Festplatten enthalten, die VMware vSphere Flash Read Cache-Speicher verwenden. Da der Host, auf dem eine virtuelle Maschine wiederhergestellt wird, möglicherweise nicht für Flash Read Cache konfiguriert ist, deaktiviert Site Recovery Manager Flash Read Cache auf Festplatten, wenn die virtuellen Maschinen auf der Wiederherstellungs-Site gestartet werden.
Site Recovery Manager legt die Reservierung auf 0 fest. Merken Sie sich die Cachereservierung der virtuellen Maschine von vSphere Web Client, bevor Sie eine Wiederherstellung auf einer virtuellen Maschine

durchführen, die für die Verwendung von vSphere Flash Read Cache konfiguriert ist. Nach der Wiederherstellung können Sie die virtuelle Maschine auf einen Host mit Flash Read Cache-Speicher migrieren und die ursprüngliche Flash Read Cache-Einstellung auf der virtuellen Maschine manuell wiederherstellen.

Speicherreplizierungsadapter

Speicherreplizierungsadapter sind nicht Bestandteil einer Site Recovery Manager-Version. Sie werden von Ihrem Array-Anbieter entwickelt und unterstützt. Sie müssen einen spezifischen Speicherreplizierungsadapter für jedes Array installieren, das Sie mit Site Recovery Manager auf dem Site Recovery Manager Server-Host verwenden. Site Recovery Manager unterstützt die Verwendung mehrerer SRAs.

Abbildung 2-1. Site Recovery Manager -Architektur mit Array-basierter Replizierung



Konfigurieren der Array-basierten Replizierung

Für den Schutz von virtuellen Maschinen, die Sie mithilfe der Array-basierte Replizierung replizieren, müssen Sie auf jeder Site Speicherreplizierungsadapter (SRAs) konfigurieren.

Installieren von SRA (Storage Replication Adapter)

Wenn Sie die Array-basierte Replizierung verwenden, müssen Sie einen jeweils spezifischen Speicherreplizierungsadapter (Storage Replication Adapter, SRA) für jedes Speicher-Array installieren, das Sie mit Site Recovery Manager verwenden. Ein SRA ist ein durch einen Array-Anbieter bereitgestelltes Programm, das Site Recovery Manager in die Lage versetzt, mit einer bestimmten Art von Array zu arbeiten.

Sie müssen einen entsprechenden SRA auf den Site Recovery Manager Server-Hosts für die Schutz- und die Wiederherstellungs-Site installieren. Wenn Sie mehr als einen Speicher-Array-Typ verwenden, müssen Sie auf beiden Site Recovery Manager Server-Hosts SRA für jeden Array-Typ installieren.

Hinweis Sie können Site Recovery Manager zur Verwendung mehrerer Typen von Speicher-Arrays konfigurieren, allerdings können die VM-Festplatten für eine einzelne virtuelle Maschine nicht auf mehreren Arrays verschiedener Anbieter gespeichert werden. Sämtliche Festplatten für eine virtuelle Maschine müssen im gleichen Array gespeichert werden.

SRAs enthalten eigene Installationsanweisungen. Sie müssen die Version eines SRA installieren, die der jeweiligen Site Recovery Manager-Version entspricht. Installieren Sie die gleiche Version des SRAs an beiden Sites. Mischen Sie nicht unterschiedliche SRA-Versionen.

Bei Verwendung von vSphere Replication ist kein SRA erforderlich.

Voraussetzungen

- Überprüfen Sie die Verfügbarkeit eines SRA für Ihren Speichertyp anhand des *VMware-Kompatibilitätshandbuchs* für Site Recovery Manager unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.
- Laden Sie den SRA herunter. Gehen Sie dazu auf https://my.vmware.com/web/vmware/downloads, wählen Sie **VMware vCenter Site Recovery Manager > Produkt herunterladen** aus, und wählen Sie anschließend **Treiber & Tools > Storage Replication Adapters > Zu den Downloads** aus.
- Wenn Sie einen SRA von einer anderen Anbieter-Site beziehen, stellen Sie sicher, dass er für Ihre Site Recovery Manager-Version zertifiziert ist. Überprüfen Sie dazu das *VMware-Kompatibilitätshandbuch* für Site Recovery Manager unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=sra.
- Lesen Sie die Dokumentation Ihres SRA-Anbieters durch. SRAs unterstützen nicht alle Funktionen, die Speicher-Arrays unterstützen. Die Dokumentation Ihres SRA-Anbieters enthält Details zu dem, was der SRA unterstützt und benötigt. Beispielsweise gibt es für HP und EMC detaillierte physische Anforderungen, die erfüllt werden müssen, damit der SRA wie erwartet ausgeführt werden kann.
- Installieren Sie Site Recovery Manager Server, bevor Sie die SRAs installieren.

- Für Ihren SRA ist möglicherweise die Installation anderer Komponenten erforderlich, die vom Anbieter bereitgestellt werden. Möglicherweise müssen Sie einige dieser Komponenten auf dem Site Recovery Manager Server-Host installieren. Andere Komponenten erfordern möglicherweise nur, dass Site Recovery Manager Server auf das Netzwerk zugreifen kann. Neueste Informationen zu diesen Anforderungen finden Sie in den Versionshinweisen und Readme-Dateien der von Ihnen installierten SRAs.
- Aktivieren Sie die Fähigkeit des Speicher-Arrays zur Erstellung von Snapshot-Kopien der replizierten Geräte. Informationen finden Sie in der SRA-Dokumentation.

Vorgehensweise

1. Installieren Sie den SRA auf jedem Site Recovery Manager Server-Host.

   Der SRA wird unter `C:\Programme\VMware\VMware vCenter Site Recovery Manager\storage\sra` installiert.
2. Navigieren Sie im vSphere Web Client zu **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
3. Klicken Sie auf der Registerkarte **Überwachen** auf **SRAs** und klicken Sie dann auf die Schaltfläche **SRAs erneut prüfen**.

   Damit werden die SRA-Informationen aktualisiert, sodass Site Recovery Manager die SRAs erkennen kann.

Konfigurieren von Array-Managern

Nachdem Sie die Schutz-Site und die Wiederherstellungs-Site gekoppelt haben, konfigurieren Sie die jeweiligen Array-Manager, damit Site Recovery Manager replizierte Geräte erkennen, Datenspeichergruppen berechnen und Speichervorgänge initiieren kann.

In der Regel konfigurieren Sie Array-Manager nur einmal, nachdem Sie die Sites verbunden haben. Sie müssen sie nur dann neu konfigurieren, wenn sich die Verbindungsinformationen bzw. Anmeldeinformationen des Array-Managers geändert haben oder Sie einen anderen Array-Satz verwenden möchten.

Voraussetzungen

- Verbinden Sie die Sites wie in Verbinden der Schutz- und der Wiederherstellungs-Site in *Installation und Konfiguration von Site Recovery Manager* beschrieben.
- Installieren Sie SRAs an beiden Sites, wie in Installieren von SRA (Storage Replication Adapter) beschrieben.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Array-basierte Replizierung**.
2. Klicken Sie auf der Registerkarte **Objekte** auf das Symbol, um einen Array-Manager hinzuzufügen.

3 Wählen Sie eine dieser beiden Optionen aus:

   - Hinzufügen eines Array-Manager-Paars
   - Hinzufügen eines einzelnen Array-Managers.

4 Wählen Sie eine Site oder ein Site-Paar für den Array-Manager aus und klicken Sie auf **Weiter**.

5 Wählen Sie den Typ des Array-Managers, den Site Recovery Manager verwenden soll, im Dropdown-Menü **SRA-Typ** aus.

   Falls kein Managertyp angezeigt wird, müssen Sie entweder erneut auf SRAs prüfen oder überprüfen, ob Sie ein SRA auf dem Site Recovery Manager Server-Host installiert haben.

6 Geben Sie im Textfeld **Anzeigename** einen Namen für das Array ein.

   Wählen Sie einen beschreibenden Namen. So können Sie leicht erkennen, welcher Speicher mit diesem Array-Manager verknüpft ist.

7 Geben Sie die erforderlichen Informationen für den Typ des von Ihnen ausgewählten SRAs an.

   Weitere Informationen zum Ausfüllen dieser Textfelder finden Sie in der Dokumentation Ihres SRA-Anbieters. SRAs weisen unterschiedliche Textfelder auf, jedoch haben alle SRAs Textfelder für die IP-Adresse, Protokollinformationen, Zuordnungen zwischen Array-Namen und IP-Adressen, den Benutzernamen und das Kennwort.

8 Klicken Sie auf **Weiter**.

9 Wenn Sie ein Array-Manager-Paar hinzufügen, konfigurieren Sie die Array-Paare und klicken Sie dann auf **Weiter**.

   Sie können außerdem Array-Paare im Einzeloptionsmodus konfigurieren, wenn der Array-Manager auf der Peer-Site schon erstellt ist.

10 Wählen Sie die Array-Paare aus der Liste aus.

11 Überprüfen Sie die Konfiguration und klicken Sie auf **Beenden**.

12 Wiederholen Sie nötigenfalls die Schritte, um einen Array-Manager für die Wiederherstellungs-Site zu konfigurieren.

Erneutes Prüfen von Arrays zur Erkennung von Konfigurationsänderungen

Site Recovery Manager überprüft Arrays standardmäßig alle 24 Stunden auf Änderungen an Gerätekonfigurationen. Sie können jedoch zu jeder beliebigen Zeit eine erneute Prüfung eines Arrays durchführen.

Sie können die Häufigkeit neu konfigurieren, mit der Site Recovery Manager regelmäßige Array-Prüfungen durchführt, indem Sie die Option `storage.minDsGroupComputationInterval` in „Erweiterte Einstellungen“ ändern. Weitere Informationen finden Sie unter Ändern der Speichereinstellungen.

Das Konfigurieren von Array-Managern führt dazu, dass Site Recovery Manager Datenspeichergruppen anhand der Menge der erkannten replizierten Speichergeräte berechnet. Wenn Sie die Konfiguration des Arrays auf einer Site ändern, um Geräte hinzuzufügen oder zu entfernen, muss Site Recovery Manager die Arrays erneut prüfen und die Datenspeichergruppen neu berechnen.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Array-basierte Replizierung**.
2. Wählen Sie ein Array aus.
3. Wählen Sie auf der Registerkarte **Verwalten** die Option **Array-Paare** aus.

   Die Registerkarte **Array-Paare** enthält Informationen zu allen Speichergeräten im Array, einschließlich des lokalen Gerätenamens, des Geräts, an das es gekoppelt ist, der Richtung der Replizierung und der Schutzgruppe, zu der das Gerät gehört, sowie Informationen dazu, ob der Datenspeicher lokal oder remote ist, und zur Konsistenzgruppen-ID für jedes SRA-Gerät.
4. Klicken Sie mit der rechten Maustaste auf ein Array-Paar und wählen Sie **Geräte erkennen** aus, um die Arrays erneut zu durchsuchen und die Datenspeichergruppen erneut zu berechnen.

Bearbeiten von Array-Managern

Verwenden Sie den Assistenten „Array-Manager bearbeiten“, um den Namen eines Array-Managers oder andere Einstellungen, wie z. B. die IP-Adresse oder den Benutzernamen und das Kennwort, zu ändern.

Weitere Informationen zum Ausfüllen der Adapterfelder finden Sie in der Dokumentation Ihres SRA-Anbieters. SRAs weisen unterschiedliche Felder auf, jedoch haben alle SRAs Felder für die IP-Adresse, Protokollinformationen, Zuordnungen zwischen Array-Namen und IP-Adressen, Benutzernamen und Kennwörtern.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Array-basierte Replizierung**.
2. Klicken Sie mit der rechten Maustaste auf ein Array und wählen Sie **Array-Manager bearbeiten**.
3. Ändern Sie den Namen des Arrays im Feld **Anzeigename**.

   Wählen Sie einen beschreibenden Namen. So können Sie leicht erkennen, welcher Speicher mit diesem Array-Manager verknüpft ist. Der Typ des Array-Managers kann nicht geändert werden.
4. Ändern Sie die Adapterinformationen.

   Diese Felder werden vom SRA erstellt.
5. Aktivieren Sie ein Array-Paar und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Beenden**, um die Änderung des Array-Managers abzuschließen.

Festlegen eines nicht replizierten Datenspeichers für Auslagerungsdateien

Alle virtuellen Maschinen benötigen eine Auslagerungsdatei. Standardmäßig erstellt vCenter Server Auslagerungsdateien im selben Datenspeicher wie die anderen Dateien der virtuellen Maschine. Damit Site Recovery Manager Auslagerungsdateien nicht repliziert, können Sie virtuelle Maschinen so konfigurieren, dass diese sie in einem nicht replizierten Datenspeicher erstellen.

Unter normalen Umständen sollten die Auslagerungsdateien in demselben Datenspeicher wie andere Dateien der virtuellen Maschine gespeichert werden. Unter Umständen müssen Sie möglicherweise die Replizierung von Auslagerungsdateien verhindern, um einen übermäßigen Verbrauch der Netzwerkbandbreite zu vermeiden. Einige Speicheranbieter empfehlen, Auslagerungsdateien nicht zu replizieren. Verhindern Sie die Replizierung von Auslagerungsdateien nur dann, wenn es absolut erforderlich ist.

Hinweis Wenn Sie einen nicht replizierten Datenspeicher für Auslagerungsdateien verwenden, müssen Sie einen nicht replizierten Datenspeicher für alle geschützten Hosts und Cluster sowohl auf der Schutz-Site als auch auf der Wiederherstellungs-Site erstellen. Der nicht replizierte Datenspeicher muss für alle Hosts in einem Cluster sichtbar sein, anderenfalls funktioniert vMotion nicht.

Vorgehensweise

1. Wählen Sie im vSphere Web Client einen Host aus und wählen Sie **Verwalten > Einstellungen**.
2. Klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf der Registerkarte **VM-Optionen** auf **Erweiterte Einstellungen**.
4. Wählen Sie als Speicherort der Auslagerungsdatei **Vom Host festgelegter Datenspeicher** aus.

   Die weiteren Optionen sind der Standardspeicherort und das Verzeichnis der virtuellen Maschine.
5. Klicken Sie auf **OK**.
6. Schalten Sie alle virtuellen Maschinen auf dem Host aus und ein.

   Das Zurücksetzen des Gastbetriebssystems reicht nicht aus. Eine Änderung des Speicherorts der Auslagerungsdatei wird wirksam, nachdem Sie die virtuellen Maschinen ausschalten und anschließend wieder einschalten.
7. Durchsuchen Sie den Datenspeicher, den Sie für Auslagerungsdateien ausgewählt haben, und vergewissern Sie sich, dass VSWP-Dateien für die virtuellen Maschinen vorhanden sind.

Verwenden von vSphere Replication mit Site Recovery Manager

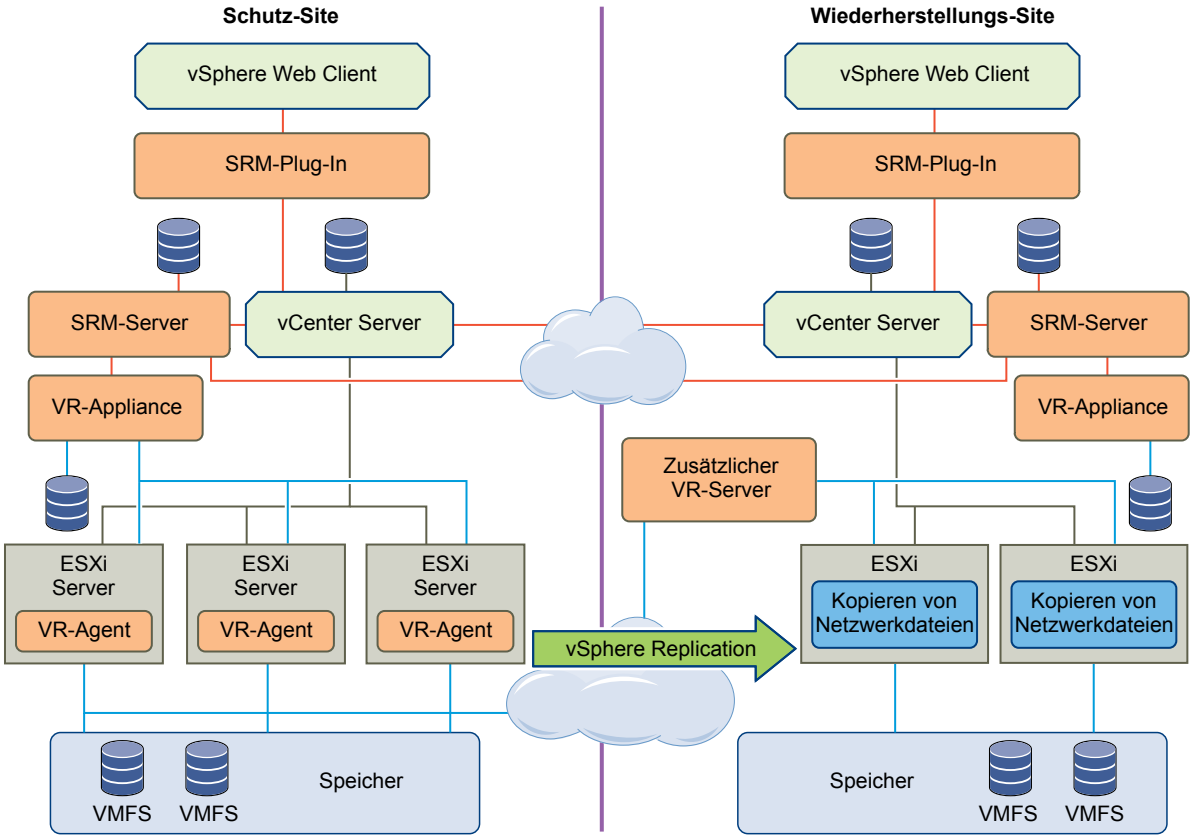
Site Recovery Manager kann vSphere Replication zum Replizieren von Daten auf Server an der Wiederherstellungs-Site verwenden.

Sie stellen die vSphere Replication-Appliance bereit und konfigurieren vSphere Replication auf den virtuellen Maschinen unabhängig von Site Recovery Manager. Informationen zum Bereitstellen und Konfigurieren von vSphere Replication finden Sie in der Dokumentation zu vSphere Replication unter https://www.vmware.com/support/pubs/vsphere-replication-pubs.html.

vSphere Replication erfordert keine Speicher-Arrays. Bei der Speicherreplizierungsquelle und dem Speicherreplizierungsziel von vSphere Replication handelt es sich um ein beliebiges Speichergerät, einschließlich, jedoch nicht beschränkt auf, Speicher-Arrays.

vSphere Replication lässt sich zur regelmäßigen Erstellung und Verwahrung von Snapshots von geschützten virtuellen Maschinen an der Wiederherstellungs-Site konfigurieren. Die Anfertigung mehrerer Point-in-Time-Snapshots (PIT) von virtuellen Maschinen ermöglicht es Ihnen, mehr als ein Replikat einer virtuellen Maschine an der Wiederherstellungs-Site beizubehalten. Jeder Snapshot gibt den Zustand der virtuellen Maschine zu einem bestimmten Zeitpunkt an. Sie können den wiederherzustellenden Snapshot auswählen, wenn Sie mit vSphere Replication eine Wiederherstellung durchführen.

Abbildung 2-2. Site Recovery Manager -Architektur mit vSphere Replication



Replizieren einer virtuellen Maschine und Aktivieren mehrerer Zeitpunktinstanzen

Sie können virtuelle Maschinen zu bestimmten Zeitpunkten wiederherstellen, z. B. dem Zeitpunkt des zuletzt bekannten konsistenten Zustands.

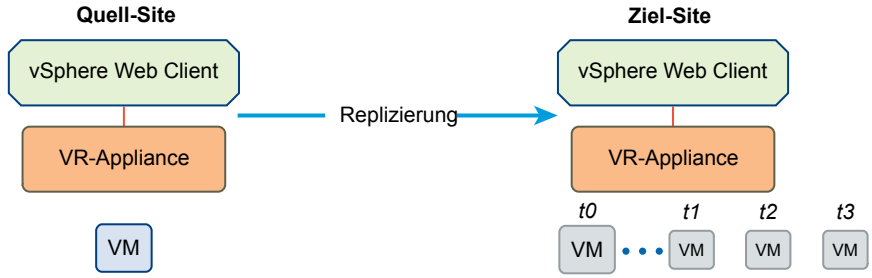
Wenn Sie vSphere Replication auf einer virtuellen Maschine konfigurieren, können Sie die Aufbewahrung mehrerer Zeitpunktinstanzen (PIT) in den Wiederherstellungseinstellungen aktivieren.
vSphere Replication behält eine Reihe von Snapshot-Instanzen der virtuellen Maschine auf der Ziel-Site bei, basierend auf der festgelegten Aufbewahrungsrichtlinie. vSphere Replication unterstützt maximal 24 Snapshot-Instanzen. Nach der Wiederherstellung einer virtuellen Maschine können Sie sie auf einen bestimmten Snapshot wiederherstellen.

Während der Replizierung repliziert vSphere Replication alle Aspekte der virtuellen Maschine auf die Ziel-Site, einschließlich aller potenziellen Viren und beschädigten Anwendungen. Wenn eine virtuelle Maschine mit einem Virus infiziert oder beschädigt ist und Sie vSphere Replication so konfiguriert haben, um Snapshots zu bestimmten Zeitpunkten aufzubewahren, können Sie die virtuelle Maschine wiederherstellen und sie auf einen Snapshot der virtuellen Maschine in ihrem nicht beschädigten Zustand wiederherstellen.

Sie können unter Verwendung der Zeitpunktinstanzen beispielsweise den letzten bekannten guten Zustand einer Datenbank wiederherstellen.

Hinweis vSphere Replication repliziert keine VM-Snapshots.

Abbildung 2-3. Wiederherstellen einer virtuellen Maschine zu bestimmten Zeitpunkten



Bei einer Wiederherstellung stellt Site Recovery Manager nur den neuesten der PIT-Snapshots wieder her. Um ältere Snapshots wiederherstellen zu können, müssen Sie die Option **vrReplication > preserveMpitImagesAsSnapshots** unter **Erweiterte Einstellungen** in der Site Recovery Manager-Benutzeroberfläche aktivieren. Weitere Informationen hierzu finden Sie unter Ändern der vSphere Replication-Einstellungen.

Um eine virtuelle Maschine aus einem älteren PIT-Snapshot wiederherzustellen, müssen Sie die virtuelle Maschine nach der Wiederherstellung manuell auf diesen Snapshot zurücksetzen. Weitere Informationen hierzu finden Sie unter Wiederherstellen eines Point-in-Time-Snapshots einer virtuellen Maschine.

Wenn Sie einen PIT-Snapshot einer virtuellen Maschine wiederherstellen, für die Sie IP-Anpassung konfiguriert haben, übernimmt Site Recovery Manager die Anpassung nur für den neuesten PIT-Snapshot. Wenn Sie einen älteren PIT-Snapshot einer virtuellen Maschine mit IP-Anpassung wiederherstellen, müssen Sie die IP-Einstellungen manuell konfigurieren.

Verwenden von Array-basierter Replizierung und vSphere Replication mit Site Recovery Manager

Sie können in Ihrer Site Recovery Manager-Bereitstellung eine Kombination aus Array-basierter Replizierung und vSphere Replication verwenden.

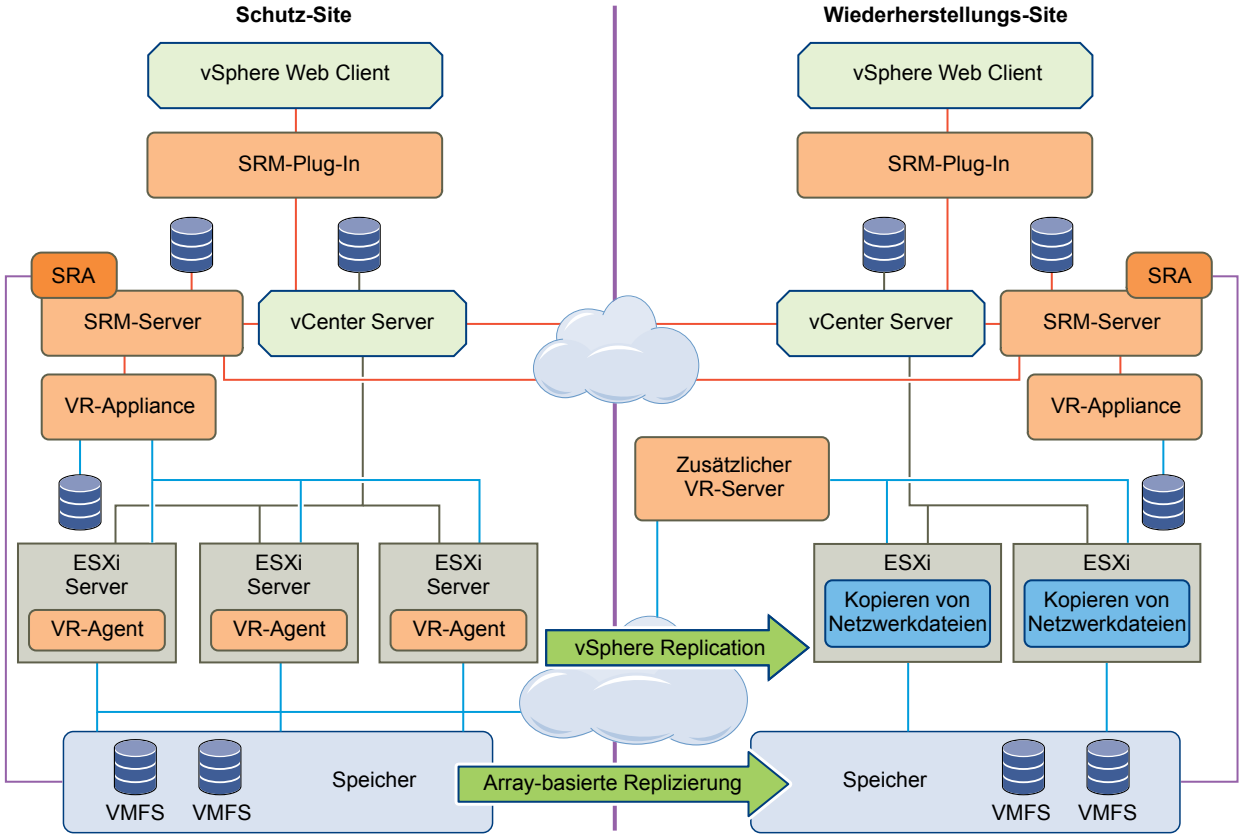
Wenn Sie eine gemischte Site Recovery Manager-Bereitstellung erstellen möchten, die Array-basierte Replizierung und vSphere Replication verwendet, müssen Sie die Schutz- und Wiederherstellungs-Sites für beide Arten der Replizierung konfigurieren.

- Richten Sie die Speicher-Arrays ein, verbinden Sie sie und installieren Sie die geeigneten Speicherreplizierungsadapter (SRA) auf beiden Sites.
- Stellen Sie vSphere Replication-Appliances auf beiden Sites bereit und konfigurieren Sie die Verbindung zwischen den Appliances.
- Konfigurieren Sie virtuelle Maschinen je nach Bedarf so, dass die Replizierung mit Array-basierter Replizierung bzw. vSphere Replication erfolgt.

  Hinweis Versuchen Sie nicht, vSphere Replication auf einer virtuellen Maschine zu konfigurieren, die sich auf einem Datenspeicher befindet, der mit Array-basierter Replizierung repliziert wird.

Sie erstellen Array-basierte Schutzgruppen für virtuelle Maschinen, die Sie mit Array-basierter Replizierung konfigurieren, und vSphere Replication-Schutzgruppen für virtuelle Maschinen, die Sie mit vSphere Replication konfigurieren. Verschiedene Replizierungsarten in einer Schutzgruppe sind unzulässig. Sie können Array-basierte Schutzgruppen und vSphere Replication-Schutzgruppen im selben Wiederherstellungsplan verwenden.

Abbildung 2-4. Site Recovery Manager -Architektur mit Array-basierter Replizierung und vSphere Replication



Erstellen und Verwalten von Schutzgruppen

3

Nachdem Sie eine Replizierungslösung konfiguriert haben, können Sie Schutzgruppen erstellen. Bei einer Schutzgruppe handelt es sich um eine Sammlung von virtuellen Maschinen, die von Site Recovery Manager gemeinsam geschützt werden.

Einem Wiederherstellungsplan können Sie eine oder mehrere Schutzgruppen hinzufügen. Ein Wiederherstellungsplan gibt an, wie Site Recovery Manager die virtuellen Maschinen in den enthaltenen Schutzgruppen wiederherstellt.

Sie konfigurieren virtuelle Maschinen und erstellen Schutzgruppen auf unterschiedlicher Art und Weise, je nachdem, ob Sie die Array-basierte Replizierung oder vSphere Replication verwenden. Sie können keine Schutzgruppen erstellen, die virtuelle Maschinen, für die Sie die Array-basierte Replizierung konfiguriert haben, mit virtuellen Maschinen kombinieren, für die Sie die vSphere Replication konfiguriert haben. Sie können eine Kombination aus Array-basierten Schutzgruppen und vSphere Replication-Schutzgruppen im selben Wiederherstellungsplan verwenden.

Nach der Konfiguration der Replizierung auf virtuellen Maschinen müssen Sie jede virtuelle Maschine einem vorhandenen Ressourcenpool, Ordner und Netzwerk auf der Wiederherstellungs-Site zuweisen. Sie können Standardwerte für die gesamte Site für diese Zuweisungen angeben, indem Sie Bestandslistenzuordnungen auswählen. Wenn Sie keine Bestandslistenzuordnungen angeben, konfigurieren Sie Zuordnungen für jede virtuelle Maschine in der Schutzgruppe einzeln.

Nachdem Sie eine Schutzgruppe erstellt haben, erstellt Site Recovery Manager Platzhalter-VMs auf der Wiederherstellungs-Site und wendet die Bestandslistenzuordnungen auf jede virtuelle Maschine in der Gruppe an. Falls Site Recovery Manager einem Ordner, Netzwerk oder Ressourcenpool auf der Wiederherstellungs-Site keine virtuelle Maschine zuordnen kann, versetzt Site Recovery Manager die virtuelle Maschine in den Status „Zuordnung fehlt“ und erstellt für sie keinen Platzhalter.

Site Recovery Manager kann keine virtuellen Maschinen schützen, auf denen Sie die Replizierung nicht bzw. fehlerhaft konfiguriert haben. Bei der Array-basierten Replizierung gilt dies, selbst wenn sich die virtuellen Maschinen auf einem geschützten Datenspeicher befinden.

- Grundlegendes zu Array-basierten Schutzgruppen und Datenspeichergruppen

  Wenn Sie eine Schutzgruppe für die Array-basierte Replizierung erstellen, geben Sie Array-Informationen an und Site Recovery Manager berechnet anschließend die Gruppe von virtuellen Maschinen in einer Datenspeichergruppe. Die Datenspeichergruppen enthalten alle Dateien der geschützten virtuellen Maschinen.

- vSphere Replication-Schutzgruppen

  Sie können für vSphere Replication konfigurierte virtuelle Maschinen zu vSphere Replication-Schutzgruppen hinzufügen.

- Schutzgruppen erstellen

  Sie erstellen Schutzgruppen, um Site Recovery Manager den Schutz virtueller Maschinen zu ermöglichen.

- Organisieren von Schutzgruppen in Ordnern

  Sie können Ordner erstellen, in denen Sie Schutzgruppen organisieren.

- Hinzufügen oder Entfernen von Datenspeichergruppen oder virtuellen Maschinen zu bzw. aus einer Schutzgruppe

  Sie können Datenspeichergruppen in einer Array-basierten Schutzgruppe hinzufügen bzw. entfernen oder aber virtuelle Maschinen in einer vSphere Replication-Schutzgruppe hinzufügen bzw. entfernen. Darüber hinaus können Sie den Namen und die Beschreibung einer Schutzgruppe ändern.

- Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe

  Wenn eine Schutzgruppe den Status „Nicht konfiguriert“ aufweist, können Sie in einem Schritt den Schutz für alle nicht konfigurierten virtuellen Maschinen mithilfe vorhandener Bestandslistenzuordnungen konfigurieren.

- Konfigurieren von Bestandslistenzuordnungen für eine einzelne virtuelle Maschine in einer Schutzgruppe

  Sie können die Zuordnungen für die virtuellen Maschinen in einer Schutzgruppe einzeln konfigurieren. Auf diese Weise können Sie auf der Wiederherstellungs-Site unterschiedliche Ressourcen für verschiedene virtuelle Maschinen verwenden.

- Ändern der Einstellungen einer geschützten virtuellen Maschine

  Sie können die Einstellungen einer virtuellen Maschine in einer Schutzgruppe ändern. Das Bearbeiten der Einstellungen einer virtuellen Maschine zum Hinzufügen oder Ändern von Speichergeräten, z. B. von Festplatten oder DVD-Laufwerken, kann sich auf den Schutz dieser virtuellen Maschine auswirken.

- Entfernen des Schutzes von einer virtuellen Maschine

  Sie können den Schutz von einer replizierten virtuellen Maschine vorübergehend entfernen, ohne sie aus der Schutzgruppe zu entfernen.

- Status der Schutzgruppe – Referenz

  Sie können den Status einer Schutzgruppe überwachen und den für jeden Status zulässigen Vorgang bestimmen.

- Schutzstatus der virtuellen Maschine – Referenz

  Sie können den Status einer virtuellen Maschine in einer Schutzgruppe überwachen und den für jeden Status zulässigen Vorgang bestimmen.

Grundlegendes zu Array-basierten Schutzgruppen und Datenspeichergruppen

Wenn Sie eine Schutzgruppe für die Array-basierte Replizierung erstellen, geben Sie Array-Informationen an und Site Recovery Manager berechnet anschließend die Gruppe von virtuellen Maschinen in einer Datenspeichergruppe. Die Datenspeichergruppen enthalten alle Dateien der geschützten virtuellen Maschinen.

Zum Hinzufügen virtueller Maschinen zu einer Array-basierten Schutzgruppe platzieren Sie diese in einem Datenspeicher, der zu einer Datenspeichergruppe gehört, die Site Recovery Manager einer Schutzgruppe zuordnet. Site Recovery Manager berechnet die Datenspeichergruppen neu, wenn eine Änderung bei einer geschützten virtuellen Maschine festgestellt wird. Wenn Sie beispielsweise eine Festplatte, die einer anderen LUN angehört, zu einer geschützten virtuellen Maschine hinzufügen, fügt Site Recovery Manager die LUN zur Datenspeichergruppe dieser Schutzgruppe hinzu. Sie müssen den Schutz neu konfigurieren, um die neue LUN zu schützen. Site Recovery Manager berechnet Konsistenzgruppen, wenn Sie ein Array-Paar konfigurieren oder wenn Sie die Geräteliste aktualisieren.

Sie können virtuelle Maschinen auch unter Verwendung von Storage vMotion zur Schutzgruppe hinzufügen, indem Sie die Dateien auf einen der Datenspeicher der Datenspeichergruppe verschieben. Sie können eine virtuelle Maschine aus einer Array-basierten Schutzgruppe entfernen, indem Sie die Dateien der virtuellen Maschine auf einen anderen Datenspeicher verschieben.

Sofern Ihr Speicher-Array Konsistenzgruppen unterstützt, ist Site Recovery Manager mit vSphere Storage DRS und vSphere Storage vMotion kompatibel. Sie können mit Storage DRS und Storage vMotion Dateien von virtuellen Maschinen innerhalb einer von Site Recovery Manager geschützten Konsistenzgruppe verschieben. Falls Ihr Speicher-Array keine Konsistenzgruppen unterstützt, können Sie Storage DRS oder Storage vMotion nicht in Verbindung mit Site Recovery Manager verwenden.

Wie Site Recovery Manager Datenspeichergruppen berechnet

Site Recovery Manager bestimmt die Zusammenstellung einer Datenspeichergruppe durch die virtuellen Maschinen, die über Dateien im Datenspeicher in der Gruppe verfügen, sowie durch die Geräte, auf denen diese Datenspeicher gespeichert sind.

Wenn Sie Array-basierte Replizierung verwenden, unterstützt jedes Speicher-Array mehrere replizierte Datenspeicher. Auf SANs (Storage Area Network), die Verbindungsprotokolle wie Fibre-Channel und iSCSI verwenden, werden diese Datenspeicher LUNs genannt (logische Speichereinheiten) und umfassen einen oder mehrere physische Datenspeicher. Auf NFS-Arrays (Network File System) werden die replizierten Datenspeicher üblicherweise als Volumes bezeichnet. In jedem Paar von replizierten Speichergeräten ist ein Datenspeicher die Replizierungsquelle und der andere ist das Replizierungsziel. Daten, die auf den Quelldatenspeicher geschrieben werden, werden anhand eines Zeitplans an den Zieldatenspeicher repliziert, der von der Replizierungssoftware des Arrays gesteuert wird. Wenn Sie Site Recovery Manager für die Arbeit mit einem Speicherreplizierungsadapter (SRA) konfigurieren, befindet sich die Replizierungsquelle auf der Schutz-Site und das Replizierungsziel auf der Wiederherstellungs-Site.

Ein Datenspeicher bietet Speicher für Dateien von virtuellen Maschinen. Durch das Ausblenden der Details von physischen Speichergeräten vereinfachen Datenspeicher die Zuteilung der Speicherkapazität und bieten ein einheitliches Modell zur Erfüllung der Speicheranforderungen von virtuellen Maschinen. Da jeder Datenspeicher mehrere Geräte umfassen kann, muss Site Recovery Manager sicherstellen, dass alle Geräte, die den Datenspeicher stützen, repliziert werden, bevor es die virtuellen Maschinen schützen kann, die diesen Datenspeicher verwenden. Site Recovery Manager muss sicherstellen, dass alle Datenspeicher, die geschützte Dateien der virtuellen Maschine enthalten, repliziert werden. Während einer Wiederherstellung oder eines Tests muss Site Recovery Manager all diese Datenspeicher gemeinsam abwickeln.

Hierfür fasst Site Recovery Manager Datenspeicher in Datenspeichergruppen zusammen, um virtuelle Maschinen aufzunehmen, die mehrere Datenspeicher umfassen. Site Recovery Manager überprüft und gewährleistet regelmäßig, dass die Datenspeichergruppen alle erforderlichen Datenspeicher enthalten, um einen Schutz für die entsprechenden virtuellen Maschinen zu bieten. Falls erforderlich, berechnet Site Recovery Manager die Datenspeichergruppen neu. Dies ist beispielsweise der Fall, wenn neue Geräte zu einer virtuellen Maschine hinzugefügt und diese Geräte auf einem Datenspeicher gespeichert werden, der zuvor nicht Teil der Datenspeichergruppe war.

Eine Datenspeichergruppe besteht aus der kleinsten Menge von Datenspeichern, die erforderlich sind, damit beim Speichern einer Datei einer virtuellen Maschine auf einem Datenspeicher in der Gruppe alle Dateien der virtuellen Maschine auf Datenspeichern gespeichert werden, die Teil derselben Gruppe sind. Wenn beispielsweise eine virtuelle Maschine über Festplatten auf zwei verschiedenen Datenspeichern verfügt, fasst Site Recovery Manager beide Datenspeicher in einer Datenspeichergruppe zusammen. Site Recovery Manager fasst Geräte nach festgelegten Kriterien in Datenspeichergruppen zusammen.

- Zwei unterschiedliche Datenspeicher enthalten Dateien, die zur selben virtuellen Maschine gehören.
- Datenspeicher, die zu zwei virtuellen Maschinen gehören, teilen ein RDM-Gerät auf einem SAN-Array, wie z B. im Falle eines MSCS-Clusters.
- Zwei Datenspeicher umfassen Erweiterungen, die verschiedenen Partitionen desselben Geräts entsprechen.
- Ein einzelner Datenspeicher umfasst zwei Erweiterungen, die Partitionen auf zwei unterschiedlichen Geräten entsprechen. Die zwei Erweiterungen müssen sich in einer einzelnen Konsistenzgruppe befinden und der SRA muss Informationen zur Konsistenzgruppe vom Array im Geräteerkennungsstadium zur Verfügung stellen. Anderenfalls ist das Erstellen von Schutzgruppen auf Basis dieses Datenspeichers nicht möglich, selbst wenn der SRA meldet, dass die Erweiterungen, die diesen Datenspeicher bilden, repliziert werden.
- Mehrere Datenspeicher gehören zu einer Konsistenzgruppe. Eine Konsistenzgruppe ist eine Sammlung von replizierten Datenspeichern, bei der jeder Status der Ziel-Datenspeichergruppe zu einem bestimmten Zeitpunkt als der Status der Quell-Datenspeichergruppe existiert hat. Informell werden die Datenspeicher zusammen repliziert, sodass bei der Ausführung einer Wiederherstellung mithilfe dieser Datenspeicher die Software, die auf die Ziele zugreift, die Daten nicht in einem Zustand sieht, den die Software nicht handhaben kann.

Schützen von virtuellen Maschinen auf VMFS-Datenspeichern, die sich über mehrere LUNs oder Erweiterungen erstrecken

Nicht alle SRAs stellen Informationen zur Konsistenzgruppe aus dem Speicher-Array bereit, weil nicht alle Speicher-Arrays Konsistenzgruppen unterstützen. Wenn ein SRA nach einem Datenspeicher-Erkennungsbefehl Informationen zur Konsistenzgruppe aus dem Array meldet, müssen sich die LUNs, die einen VMFS-Datenspeicher mit mehreren Erweiterungen bilden, in derselben Konsistenzgruppe des Speicher-Arrays befinden. Wenn das Array keine Konsistenzgruppen unterstützt und der SRA keine Informationen zur Konsistenzgruppe bereitstellt, kann Site Recovery Manager keine virtuellen Maschinen schützen, die sich auf dem aus mehreren Erweiterungen bestehenden Datenspeicher befinden.

vSphere Replication -Schutzgruppen

Sie können für vSphere Replication konfigurierte virtuelle Maschinen zu vSphere Replication-Schutzgruppen hinzufügen.

Beim Erstellen oder Bearbeiten einer vSphere Replication-Schutzgruppe sind die für vSphere Replication konfigurierten virtuellen Maschinen in der vCenter Server-Bestandsliste zur Auswahl verfügbar.

Sie wählen einen Zielspeicherort in einem Datenspeicher auf dem Remotestandort aus, wenn Sie vSphere Replication auf einer virtuellen Maschine konfigurieren. Wenn Sie eine virtuelle Maschine mit vSphere Replication zu einer Schutzgruppe hinzufügen, erstellt Site Recovery Manager eine Platzhalter-VM für die Wiederherstellung. Das Replizierungsziel für vSphere Replication und die von Site Recovery Manager erstellte Platzhalter-VM können sich auf der Wiederherstellungs-Site im selben Datenspeicher befinden, weil sie in unterschiedlichen Datenspeicherordnern erstellt werden. Wenn sich das Replizierungsziel und die Platzhalter-VMs im selben Datenspeicher befinden, erstellt Site Recovery Manager den Namen der Platzhalter-VM unter Verwendung des Namens der Replizierungsziel-VM und des Suffixes `(1)`. Um Verwirrung zu vermeiden, hat es sich bewährt, unterschiedliche Datenspeicher für das vSphere Replication-Replizierungsziel und die Site Recovery Manager-Platzhalter-VMs zu verwenden. Site Recovery Manager wendet die Bestandslistenzuordnungen auf die Platzhalter-VM an der Wiederherstellungs-Site an.

vSphere Replication synchronisiert die Festplattendateien der Replizierungsziel-VM entsprechend dem beim Konfigurieren von vSphere Replication auf der virtuellen Maschine festgelegten RPO (Recovery Point Objective). Wenn Sie eine Wiederherstellung mit Site Recovery Manager durchführen, schaltet Site Recovery Manager die Replizierungsziel-VM ein und registriert sie anstelle der Platzhalter-VM bei vCenter Server an der Wiederherstellungs-Site.

Bei Verwendung von vSphere Replication-Schutzgruppen ist Site Recovery Manager von vSphere Replication abhängig, aber vSphere Replication ist nicht von Site Recovery Manager abhängig. Sie können vSphere Replication unabhängig von Site Recovery Manager verwenden. Sie können vSphere Replication z. B. verwenden, um alle virtuellen Maschinen in der vCenter Server-Bestandsliste

zu replizieren, aber nur eine Teilmenge dieser virtuellen Maschinen zu Schutzgruppen hinzuzufügen. Änderungen, die Sie an der vSphere Replication-Konfiguration vornehmen, können den Site Recovery Manager-Schutz auf den zu Schutzgruppen hinzugefügten virtuellen Maschinen beeinflussen.

- Site Recovery Manager überwacht den vSphere Replication-Status der virtuellen Maschinen in vSphere Replication-Schutzgruppen. Wenn die Replizierung für eine virtuelle Maschine in einer Schutzgruppe nicht funktioniert, kann Site Recovery Manager die virtuelle Maschine nicht wiederherstellen.
- Wenn Sie die Konfiguration von vSphere Replication auf einer virtuellen Maschine aufheben, behält Site Recovery Manager diese virtuelle Maschine weiterhin in den Schutzgruppen, zu denen Sie sie hinzugefügt haben. Site Recovery Manager kann keine Wiederherstellung dieser virtuellen Maschine durchführen, so lange die Replizierung nicht wieder konfiguriert wurde. Wenn Sie die Konfiguration von vSphere Replication auf einer virtuellen Maschine aufheben, können Sie sie manuell aus der Schutzgruppe entfernen.
- Haben Sie vSphere Replication auf einer virtuellen Maschine konfiguriert, die sich in einem von Site Recovery Manager bereits mit Array-basierter Replizierung geschützten Datenspeicher befindet, und versuchen Sie, diese virtuelle Maschine zu einer vSphere Replication-Schutzgruppe hinzuzufügen, meldet Site Recovery Manager einen Fehler.

Wenn Sie eine virtuelle Maschine mit vSphere Replication aus einer Schutzgruppe entfernen, repliziert vSphere Replication diese virtuelle Maschine weiterhin auf die Wiederherstellungs-Site. Die virtuelle Maschine wird nicht zusammen mit den anderen virtuellen Maschinen in der Schutzgruppe wiederhergestellt, wenn Sie einen entsprechenden Wiederherstellungsplan ausführen.

Schutzgruppen erstellen

Sie erstellen Schutzgruppen, um Site Recovery Manager den Schutz virtueller Maschinen zu ermöglichen.

Schutzgruppen können in Ordnern organisiert werden. Verschiedene Ansichten in vSphere Web Client zeigen die Namen der Schutzgruppen an, aber nicht die Namen der Ordner. Wenn Sie zwei Schutzgruppen mit demselben Namen in unterschiedlichen Ordnern abgelegt haben, ist es möglicherweise schwer, sie in einigen Ansichten von vSphere Web Client auseinanderzuhalten. Stellen Sie deshalb sicher, dass die Schutzgruppennamen ordnerübergreifend eindeutig sind. In Umgebungen, in denen nicht alle Benutzer über Ansichtsrechte für alle Ordner verfügen, legen Sie keine Schutzgruppen in Ordnern ab, um sicherzustellen, dass die Namen der Schutzgruppen eindeutig sind.

Warten Sie, wenn Sie Schutzgruppen erstellen, um sicherzugehen, dass die Vorgänge erwartungsgemäß abgeschlossen werden. Vergewissern Sie sich, dass Site Recovery Manager die Schutzgruppe erstellt und die virtuellen Maschinen in der Gruppe ordnungsgemäß geschützt werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie eine der folgenden Aufgaben ausgeführt haben:

- Virtuelle Maschinen in Datenspeichern, für die Sie die Array-basierte Replizierung konfiguriert haben, wurden einbezogen
- vSphere Replication wurde auf virtuellen Maschinen konfiguriert
- Eine Kombination dieser beiden Schritte wurde ausgeführt

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Schutzgruppen**.
2. Klicken Sie auf der Registerkarte **Objekte** auf das Symbol, um eine Schutzgruppe zu erstellen.
3. Geben Sie auf der Seite „Name und Speicherort“ einen Namen und eine Beschreibung für die Schutzgruppe ein, wählen Sie ein Site-Paar oder einen Ordner aus und klicken Sie auf **Weiter**.
4. Wählen Sie auf der Seite „Schutzgruppentyp“ die Schutz-Site und den Replizierungstyp aus und klicken Sie auf **Weiter**.

Option	Aktion
Array-basierte Replizierungsgruppen	Wählen Sie **Array-basierte Replizierung (ABR)** und ein Array-Paar aus.
vSphere Replication-Schutzgruppen	Wählen Sie **vSphere Replication** aus.

5. Wählen Sie Datenspeichergruppen oder virtuelle Maschinen aus, die der Schutzgruppe hinzugefügt werden sollen.

Option	Aktion
Array-basierte Schutzgruppen	Wählen Sie Datenspeichergruppen aus und klicken Sie auf **Weiter**.
vSphere Replication-Schutzgruppen	Wählen Sie virtuelle Maschinen in der Liste aus und klicken Sie auf **Weiter**.

   Beim Erstellen von vSphere Replication-Schutzgruppen werden nur virtuelle Maschinen, die Sie für vSphere Replication konfiguriert haben und die sich nicht bereits in einer Schutzgruppe befinden, in der Liste angezeigt.

6. Überprüfen Sie die gewählten Einstellungen, und klicken Sie auf **Beenden**.

   Den Fortschritt bei der Erstellung der Schutzgruppe können Sie auf der Registerkarte **Objekte** unter **Schutzgruppen** überwachen.

   - Falls Site Recovery Manager Bestandslistenzuordnungen erfolgreich auf die geschützten virtuellen Maschinen angewendet hat, lautet der Status der Schutzgruppe „OK“.
   - Falls Sie keine Bestandslistenzuordnungen konfiguriert haben oder falls Site Recovery Manager die Bestandslistenzuordnungen nicht anwenden konnte, lautet der Status der Schutzgruppe „Nicht konfiguriert“.

Weiter

Wenn die Schutzgruppe den Status „Nicht konfiguriert“ aufweist, wenden Sie Bestandslistenzuordnungen auf die virtuellen Maschinen an:

- Weitere Informationen zum Anwenden von Bestandslistenzuordnungen für die gesamte Site oder zum Überprüfen der Gültigkeit bereits festgelegter Bestandslistenzuordnungen finden Sie unter Auswahl von Bestandslistenzuordnungen in *Installation und Konfiguration von Site Recovery Manager*. Weitere Informationen zum Anwenden dieser Zuordnungen auf alle virtuellen Maschinen finden Sie unter Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe.
- Weitere Informationen zum Anwenden von Bestandslistenzuordnungen auf einzelne virtuelle Maschinen in der Schutzgruppe finden Sie unter Konfigurieren von Bestandslistenzuordnungen für eine einzelne virtuelle Maschine in einer Schutzgruppe.

Organisieren von Schutzgruppen in Ordnern

Sie können Ordner erstellen, in denen Sie Schutzgruppen organisieren.

Das Organisieren von Schutzgruppen in Ordnern ist nützlich, wenn Sie über viele Schutzgruppen verfügen. Sie können den Zugriff auf die Schutzgruppen einschränken, indem Sie sie in Ordner ablegen und den Ordnern unterschiedliche Berechtigungen für unterschiedliche Benutzer oder Gruppen zuweisen. Informationen dazu, wie Sie Ordnern Berechtigungen zuweisen, finden Sie unter Zuweisen von Site Recovery Manager-Rollen und -Berechtigungen.

Vorgehensweise

1. Klicken Sie in der Home-Ansicht des vSphere Web Client auf **Site-Wiederherstellung**.
2. Erweitern Sie **Bestandslistenstrukturen** und klicken Sie auf **Schutzgruppen**.
3. Wählen Sie auf der Registerkarte **Verwandte Objekte** aus und klicken Sie auf **Ordner**.
4. Klicken Sie auf das Symbol **Ordner erstellen**, geben Sie einen Namen für den zu erstellenden Ordner ein, und klicken Sie auf **OK**.
5. Fügen Sie dem Ordner neue oder bereits vorhandene Schutzgruppen hinzu.

Option	Beschreibung
Neue Schutzgruppe erstellen	Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Schutzgruppe erstellen** aus.
Vorhandene Schutzgruppe hinzufügen	Ziehen Sie mit der Maus Schutzgruppen von der Bestandslistenstruktur in den Ordner.

6. (Optional) Zum Umbenennen oder Löschen eines Ordners klicken Sie mit der rechten Maustaste auf den Ordner und wählen **Ordner umbenennen** oder **Ordner löschen** aus.

   Sie können nur leere Ordner löschen.

Hinzufügen oder Entfernen von Datenspeichergruppen oder virtuellen Maschinen zu bzw. aus einer Schutzgruppe

Sie können Datenspeichergruppen in einer Array-basierten Schutzgruppe hinzufügen bzw. entfernen oder aber virtuelle Maschinen in einer vSphere Replication-Schutzgruppe hinzufügen bzw. entfernen. Darüber hinaus können Sie den Namen und die Beschreibung einer Schutzgruppe ändern.

Voraussetzungen

Sie haben eine Schutzgruppe erstellt.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Schutzgruppen**.
2. Klicken Sie mit der rechten Maustaste auf eine Schutzgruppe und wählen Sie **Schutzgruppe bearbeiten** aus.
3. (Optional) Ändern Sie den Namen und die Beschreibung der Schutzgruppe und klicken Sie auf **Weiter**.

   Die Einstellung „Speicherort“ kann nicht geändert werden.
4. Klicken Sie auf **Weiter**.

   Die Einstellungen „Schutz-Site“ und „Replizierungstyp“ können nicht geändert werden. Für Array-basierte Schutzgruppen kann das Array-Paar nicht geändert werden.
5. Ändern Sie die in der Schutzgruppe enthaltenen Datenspeichergruppen oder virtuellen Maschinen.
   - Für Array-basierte Schutzgruppen wählen Sie Datenspeichergruppen aus oder heben die Auswahl von Datenspeichergruppen auf, um sie zur Schutzgruppe hinzuzufügen bzw. aus dieser zu entfernen. Klicken Sie anschließend auf **Weiter**.
   - Für vSphere Replication-Schutzgruppen wählen Sie virtuelle Maschinen aus oder heben die Auswahl von virtuellen Maschinen auf, um sie zur Schutzgruppe hinzuzufügen bzw. aus dieser zu entfernen. Klicken Sie anschließend auf **Weiter**.
6. Überprüfen Sie die Einstellungen und klicken Sie auf **Weiter**, um die Einstellungen zu übernehmen.

   Sie können die Änderungen nicht rückgängig machen oder stornieren, während Site Recovery Manager die Schutzgruppe aktualisiert.
7. Klicken Sie auf **Beenden**, um den Assistenten zu schließen.

Falls Sie Bestandslistenzuordnungen für die gesamte Site konfiguriert haben, wendet Site Recovery Manager die Zuordnungen auf die virtuellen Maschinen an, die Sie zur Schutzgruppe hinzugefügt haben. Wenn der Vorgang erfolgreich ausgeführt wird, lautet der Status für die virtuellen Maschinen „OK“.

Hinweis Wenn Sie Datenspeicher oder virtuelle Maschinen zu einer Schutzgruppe hinzufügen, werden Bestandslistenzuordnungen nur auf die neuen virtuellen Maschinen angewendet. Angenommen, Sie ändern Bestandslistenzuordnungen und fügen dann einen Datenspeicher zu einer Schutzgruppe hinzu, die den Status „OK“ aufweist. In diesem Fall wendet Site Recovery Manager die neuen Zuordnungen auf die neu geschützten virtuellen Maschinen an, die sich im neuen Datenspeicher befinden. Die zuvor geschützten virtuellen Maschinen verwenden weiterhin die alten Zuordnungen.

Falls Sie keine Bestandslistenzuordnungen für die gesamte Site konfiguriert haben, lautet der Status für die Schutzgruppe „Nicht konfiguriert“, und die neuen virtuellen Maschinen weisen den Status „Zuordnung fehlt“ auf.

Weiter

Wenn die Schutzgruppe den Status „Nicht konfiguriert“ aufweist und der Status für die neuen virtuellen Maschinen „Zuordnung fehlt“ lautet, wenden Sie Bestandslistenzuordnungen auf die virtuellen Maschinen an:

- Weitere Informationen zum Anwenden von Bestandslistenzuordnungen für die gesamte Site oder zum Überprüfen der Gültigkeit bereits festgelegter Bestandslistenzuordnungen finden Sie unter Auswahl von Bestandslistenzuordnungen in *Installation und Konfiguration von Site Recovery Manager*. Weitere Informationen zum Anwenden dieser Zuordnungen auf alle virtuellen Maschinen finden Sie unter Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe.
- Weitere Informationen zum Anwenden von Bestandslistenzuordnungen auf einzelne virtuelle Maschinen in der Schutzgruppe finden Sie unter Konfigurieren von Bestandslistenzuordnungen für eine einzelne virtuelle Maschine in einer Schutzgruppe.

Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe

Wenn eine Schutzgruppe den Status „Nicht konfiguriert“ aufweist, können Sie in einem Schritt den Schutz für alle nicht konfigurierten virtuellen Maschinen mithilfe vorhandener Bestandslistenzuordnungen konfigurieren.

Site Recovery Manager wendet Bestandslistenzuordnungen für die gesamte Site auf virtuelle Maschinen an, wenn Sie eine Schutzgruppe erstellen oder wenn Sie virtuelle Maschinen zu einer vorhandenen Schutzgruppe hinzufügen. Falls Sie die Bestandslistenzuordnungen für die gesamte Site ändern, nachdem Sie eine Schutzgruppe erstellt oder ihnen virtuelle Maschinen hinzugefügt haben, werden die virtuellen Maschinen weiterhin mit den ursprünglichen Bestandslistenzuordnungen wiederhergestellt. Um neue Bestandslistenzuordnungen anzuwenden, müssen Sie den Schutz auf den virtuellen Maschinen in der Schutzgruppe neu konfigurieren.

Für den Status „Nicht konfiguriert“ einer Schutzgruppe gibt es mehrere mögliche Gründe:

- Sie haben keine Bestandslistenzuordnungen für die gesamte Site konfiguriert, bevor Sie die Schutzgruppe erstellt haben.
- Sie haben keine Platzhalterdatenspeicherzuordnungen konfiguriert, bevor Sie die Schutzgruppe erstellt haben.
- Sie haben virtuelle Maschinen zu einer Schutzgruppe hinzugefügt, nachdem Sie sie erstellt haben.
- Virtuelle Maschinen haben möglicherweise ihren Schutz verloren, weil Sie sie neu konfiguriert haben, nachdem Sie sie einer Schutzgruppe hinzugefügt haben. Beispielsweise, wenn Sie virtuelle Festplatten oder Geräte hinzugefügt oder entfernt haben.

Voraussetzungen

- Konfigurieren Sie Bestandslistenzuordnungen für die gesamte Site (neu). Weitere Informationen zum Auswählen von Bestandslistenzuordnungen finden Sie unter Auswahl von Bestandslistenzuordnungen in *Installation und Konfiguration von Site Recovery Manager*.
- Konfigurieren Sie Platzhalterdatenspeicherzuordnungen (neu). Weitere Informationen zum Konfigurieren eines Platzhalterdatenspeichers finden Sie unter Konfigurieren eines Platzhalterdatenspeichers in *Installation und Konfiguration von Site Recovery Manager*.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Schutzgruppen**.
2. Wählen Sie eine Schutzgruppe aus und klicken Sie auf der Registerkarte **Verwandte Objekte** auf die Registerkarte **Virtuelle Maschinen**.
3. Klicken Sie auf das Symbol **Alle konfigurieren**.

   Mindestens eine virtuelle Maschine in einer Schutzgruppe muss sich im Status „Nicht konfiguriert“ für die Schaltfläche **Alle konfigurieren** befinden, um aktiviert zu werden.
4. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie Bestandslistenzuordnungen auf alle nicht konfigurierten virtuellen Maschinen anwenden möchten.
   - Falls Site Recovery Manager Bestandslistenzuordnungen erfolgreich auf die virtuellen Maschinen angewendet hat, lautet der Status der Schutzgruppe „OK“.
   - Falls Site Recovery Manager einige oder alle Bestandslistenzuordnungen nicht anwenden konnte, lautet der Status der virtuellen Maschinen „Nicht konfiguriert“ oder „Zuordnung fehlt“.
   - Falls Site Recovery Manager die Bestandslistenzuordnungen angewendet hat, aber keine Platzhalter für virtuelle Maschinen erstellen konnte, lautet der Status der virtuellen Maschinen „Fehler beim Erstellen der Platzhalter-VM“.
5. (Optional) Falls der Status der virtuellen Maschinen „Nicht konfiguriert“ oder „Zuordnung fehlt“ lautet, überprüfen Sie die Bestandslistenzuordnungen und klicken Sie erneut auf **Alle konfigurieren**.

6 (Optional) Falls der Status der virtuellen Maschinen „Fehler beim Erstellen der Platzhalter-VM“ lautet, überprüfen Sie die Zuordnung des Platzhalterdatenspeichers und versuchen Sie, die Platzhalter-VMs neu zu erstellen.

- Um den Platzhalter für eine einzelne virtuelle Maschine neu zu erstellen, klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Platzhalter neu erstellen** aus.
- Um den Platzhalter für mehrere virtuelle Maschinen neu zu erstellen, klicken Sie mit der rechten Maustaste auf die Schutzgruppe und wählen Sie **Platzhalter-VMs wiederherstellen** aus.

Konfigurieren von Bestandslistenzuordnungen für eine einzelne virtuelle Maschine in einer Schutzgruppe

Sie können die Zuordnungen für die virtuellen Maschinen in einer Schutzgruppe einzeln konfigurieren. Auf diese Weise können Sie auf der Wiederherstellungs-Site unterschiedliche Ressourcen für verschiedene virtuelle Maschinen verwenden.

Sie können einzelne Bestandslistenzuordnungen konfigurieren, selbst wenn Sie Bestandslistenzuordnungen für die gesamte Site konfiguriert haben. Falls Sie keine Bestandslistenzuordnungen für die gesamte Site konfiguriert haben, können Sie den Schutz für eine einzelne virtuelle Maschine entfernen und die Ordner- und Ressourcenzuordnungen konfigurieren, um die Zuordnungen für die gesamte Site außer Kraft zu setzen. Sie können die Netzwerkzuordnung für eine einzelne virtuelle Maschine ändern, ohne den Schutz zu entfernen.

Für einzelne virtuelle Maschinen können keine Platzhalterdatenspeicher angegeben werden. Sie müssen Datenspeicher auf der Schutz-Site zu Platzhalterdatenspeichern auf der Wiederherstellungs-Site auf der Site-Ebene zuordnen. Weitere Informationen zum Konfigurieren eines Platzhalterdatenspeichers finden Sie unter Konfigurieren eines Platzhalterdatenspeichers in *Installation und Konfiguration von Site Recovery Manager*.

Voraussetzungen

Sie haben eine Schutzgruppe erstellt.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Schutzgruppen**.

2 Wählen Sie die Schutzgruppe aus, die die zu konfigurierende virtuelle Maschine enthält.

3 Klicken Sie auf der Registerkarte **Verwandte Objekte** auf die Registerkarte **Virtuelle Maschinen**.

4 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Schutz konfigurieren** aus.

5 Konfigurieren Sie Bestandslistenzuordnungen, indem Sie die Ressourcen erweitern, deren Status „Nicht konfiguriert“ lauten, und Ressourcen auf der Wiederherstellungs-Site auswählen.

   Sie können nur die Ordner-, Ressourcenpool- und Netzwerkzuordnungen ändern.

6 (Optional) Um diese Zuordnungen auf alle geschützten virtuellen Maschinen der Site anzuwenden, aktivieren Sie das Kontrollkästchen **Als Bestandslistenzuordnung speichern** für jede Ressource.

   Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die Zuordnung nur auf diese virtuelle Maschine angewendet.

7 Klicken Sie auf **OK**.

   - Falls Site Recovery Manager Bestandslistenzuordnungen erfolgreich auf die virtuelle Maschine angewendet hat, lautet der Status der virtuellen Maschine „OK“.
   - Falls Site Recovery Manager einige oder alle Bestandslistenzuordnungen nicht anwenden konnte, lautet der Status der virtuellen Maschine „Nicht konfiguriert“ oder „Zuordnung fehlt“.
   - Falls Site Recovery Manager die Bestandslistenzuordnungen angewendet hat, aber keine Platzhalter-VM erstellen konnte, lautet der Status der virtuellen Maschine „Fehler beim Erstellen der Platzhalter-VM“.

8 (Optional) Falls der Status der virtuellen Maschine „Nicht konfiguriert“ oder „Zuordnung fehlt“ lautet, wählen Sie **Schutz konfigurieren** erneut aus und überprüfen die Bestandslistenzuordnungen.

9 (Optional) Falls der Status der virtuellen Maschine „Fehler beim Erstellen der Platzhalter-VM“ lautet, überprüfen Sie die Zuordnung des Platzhalterdatenspeichers auf der Site-Ebene, klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Platzhalter neu erstellen** aus.

Ändern der Einstellungen einer geschützten virtuellen Maschine

Sie können die Einstellungen einer virtuellen Maschine in einer Schutzgruppe ändern. Das Bearbeiten der Einstellungen einer virtuellen Maschine zum Hinzufügen oder Ändern von Speichergeräten, z. B. von Festplatten oder DVD-Laufwerken, kann sich auf den Schutz dieser virtuellen Maschine auswirken.

Falls Sie die Array-basierte Replizierung verwenden, wirkt sich das Hinzufügen oder Ändern von Geräten auf einer virtuellen Maschine in Abhängigkeit von der Art und Weise, wie Sie das neue Gerät erstellen, auf den Schutz aus.

- Wenn sich das neue Gerät auf einem replizierten Datenspeicher befindet, der nicht Bestandteil einer Schutzgruppe ist, wechselt die Schutzgruppe, die die virtuelle Maschine enthält, in den Status „Nicht konfiguriert“. Konfigurieren Sie die Schutzgruppe neu, um den Datenspeicher, der das neue Gerät enthält, zur Schutzgruppe hinzuzufügen.
- Wenn sich das neue Gerät auf einem replizierten Datenspeicher befindet, der von einer anderen Schutzgruppe geschützt wird, verliert der Schutz der virtuellen Maschine seine Gültigkeit.
- Wenn sich das neue Gerät auf einem nicht replizierten Datenspeicher befindet, müssen Sie den Datenspeicher replizieren oder den Schutz für das Gerät entfernen.

- Wenn Sie Storage vMotion zum Verschieben einer virtuellen Maschine auf einen nicht replizierten Datenspeicher oder auf einen replizierten Datenspeicher auf einem Array verwenden, für das Site Recovery Manager nicht über einen Speicherreplizierungsadapter (SRA) verfügt, verliert der Schutz der virtuellen Maschine seine Gültigkeit. Sie können Storage vMotion zum Verschieben einer virtuellen Maschine auf einen Datenspeicher verwenden, der Teil einer anderen Schutzgruppe ist.

Wenn Sie ein Gerät zu einer virtuellen Maschine hinzufügen, die Sie mithilfe von vSphere Replication schützen, müssen Sie vSphere Replication auf der virtuellen Maschine neu konfigurieren, um die Replizierungsoptionen für das neue Gerät auszuwählen. Weitere Informationen zur Neukonfiguration der Einstellungen für vSphere Replication finden Sie in der Dokumentation zu vSphere Replication unter https://www.vmware.com/support/pubs/vsphere-replication-pubs.html.

Nachdem Sie virtuelle Maschinen geändert haben, müssen Sie den Schutz für virtuelle Maschinen neu konfigurieren, die den Status „Nicht konfiguriert“, „Gerät nicht gefunden“, „Nicht aufgelöste Geräte“ oder „Zuordnung fehlt“ aufweisen. Siehe Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe und Konfigurieren von Bestandslistenzuordnungen für eine einzelne virtuelle Maschine in einer Schutzgruppe.

Deaktivieren der Replizierung auf einer geschützten virtuellen Maschine

Für alle virtuellen Maschinen in einer Schutzgruppe muss entweder die Array-basierte Replizierung oder vSphere Replication konfiguriert werden. Wenn Sie die Replizierung auf einer virtuellen Maschine deaktivieren, die Bestandteil einer Schutzgruppe ist, kann Site Recovery Manager diese virtuelle Maschine nicht wiederherstellen, und der Status für diese Schutzgruppe lautet „Nicht konfiguriert“.

- Wenn Sie den Schutz für eine virtuelle Maschine entfernen, die Bestandteil einer Array-basierten Schutzgruppe ist, müssen Sie die Dateien dieser virtuellen Maschine auf einen nicht geschützten Datenspeicher verschieben. Wenn Sie die Dateien einer nicht geschützten virtuellen Maschine in einem Datenspeicher belassen, der von Site Recovery Manager zu einer Datenspeichergruppe hinzugefügt wurde, schlägt die Wiederherstellung für die gesamte Datenspeichergruppe fehl.
- Wenn Sie vSphere Replication auf einer virtuellen Maschine deaktivieren, die Sie zu einer Schutzgruppe hinzugefügt haben, schlägt die Wiederherstellung für diese virtuelle Maschine fehl, wird aber für alle ordnungsgemäß konfigurierten virtuellen Maschinen in der Gruppe erfolgreich ausgeführt. Sie müssen die Schutzgruppe bearbeiten, um die virtuelle Maschine zu entfernen. Weitere Informationen hierzu finden Sie unter Hinzufügen oder Entfernen von Datenspeichergruppen oder virtuellen Maschinen zu bzw. aus einer Schutzgruppe.

Entfernen des Schutzes von einer virtuellen Maschine

Sie können den Schutz von einer replizierten virtuellen Maschine vorübergehend entfernen, ohne sie aus der Schutzgruppe zu entfernen.

Durch Entfernen des Schutzes wird die Platzhalter-VM auf der Wiederherstellungs-Site gelöscht. Wenn Sie den Schutz von einer virtuellen Maschine entfernen, wird der Status der virtuellen Maschine und der Schutzgruppe auf „Nicht konfiguriert“ festgelegt. Ein Wiederherstellungsplan, der die Schutzgruppe enthält, wird erfolgreich ausgeführt, aber Site Recovery Manager stellt die virtuellen Maschinen mit dem Status „Nicht konfiguriert“ nicht wieder her.

Für das Entfernen des Schutzes von einer virtuellen Maschine gibt es verschiedene Gründe:

- Sie verwenden vSphere Replication und möchten eine geschützte virtuelle Maschine neu konfigurieren. Sie können den Schutz bei der Neukonfiguration der virtuellen Maschine entfernen, sodass der aktuell ausgeführte Site Recovery Manager-Test oder echte Wiederherstellungen nicht durch die Änderungen betroffen sind. Wenn Sie beispielsweise Geräte zu einer virtuellen Maschine hinzufügen und eine Wiederherstellung ausführen, bevor Sie vSphere Replication auf den neuen Geräten konfigurieren, werden für die Wiederherstellung Fehler angezeigt, falls Sie nicht den Schutz von der virtuellen Maschine entfernen.
- Sie verwenden die Array-basierte Replizierung und jemand verschiebt eine virtuelle Maschine, die Sie nicht schützen möchten, in einen replizierten Datenspeicher. Wenn Sie den Schutz von der virtuellen Maschine entfernen, wird für die Schutzgruppe weiterhin der Status „Nicht konfiguriert“ angezeigt, aber die Testwiederherstellung und die echte Wiederherstellung werden weiterhin erfolgreich ausgeführt.
- Sie verwenden die Array-basierte Replizierung und eine virtuelle Maschine weist Geräte auf, die auf einem nicht replizierten Datenspeicher gespeichert sind. Sie können den Schutz von der virtuellen Maschine entfernen, damit Wiederherstellungen für alle anderen virtuellen Maschinen in der Gruppe erfolgreich ausgeführt werden, während Sie die Gerätedateien verlagern.
- Bei einer Array-basierten Replizierung gibt es einen Unterschied zwischen dem Site Recovery Manager-Schutz einer virtuellen Maschine und der Site Recovery Manager-Speicherverwaltung für diese virtuelle Maschine. Wenn Sie den Schutz von einer virtuellen Maschine entfernen, wird die Maschine von Site Recovery Manager nicht mehr wiederhergestellt, aber der Speicher der VM-Dateien wird weiterhin überwacht und verwaltet.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Schutzgruppen**.
2. Wählen Sie eine Schutzgruppe aus und wählen Sie **Verwandte Objekte > Virtuelle Maschinen**.
3. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Schutz entfernen**.
4. Klicken Sie auf **Ja**, um das Entfernen des Schutzes von der virtuellen Maschine zu bestätigen.

Status der Schutzgruppe – Referenz

Sie können den Status einer Schutzgruppe überwachen und den für jeden Status zulässigen Vorgang bestimmen.

Tabelle 3-1. Status der Schutzgruppe

Zustand	Beschreibung
Wird geladen...	Erscheint kurz beim Laden der Schnittstelle, bis der Status der Schutzgruppe angezeigt wird.
OK	Die Gruppe befindet sich im Leerlauf. Alle virtuellen Maschinen weisen den Status „OK“ auf. Sie können die Gruppe bearbeiten.
Nicht konfiguriert	Die Gruppe befindet sich im Leerlauf. Manche virtuellen Maschinen weisen möglicherweise nicht den Status „OK“ auf. Sie können die Gruppe bearbeiten.
Testen	Die Gruppe wird in einem Plan verwendet, der einen Test ausführt. Sie können die Gruppe nicht bearbeiten.
Test abgeschlossen	Die Gruppe wird in einem Plan verwendet, der einen Test ausführt. Sie können die Gruppe nicht bearbeiten. Für die Gruppe wird wieder der Status „OK“ oder „Nicht konfiguriert“ angezeigt, wenn die Bereinigung erfolgreich ausgeführt wurde.
Bereinigen	Die Gruppe wird in einem Plan verwendet, der nach einem Test bereinigt wird. Sie können die Gruppe nicht bearbeiten. Für die Gruppe wird wieder der Status „OK“ oder „Nicht konfiguriert“ angezeigt, wenn die Bereinigung erfolgreich ausgeführt wurde. Falls die Bereinigung fehlschlägt, wechselt die Gruppe in den Status „Testen“.
Wiederherstellen	Die Gruppe wird in einem Plan verwendet, der eine Wiederherstellung ausführt. Sie können die Gruppe nicht bearbeiten. Falls die Wiederherstellung erfolgreich ausgeführt wird, wechselt die Gruppe in den Status „Wiederhergestellt“. Falls die Wiederherstellung fehlschlägt, wechselt die Gruppe in den Status „Teilweise wiederhergestellt“.
Teilweise wiederhergestellt	Die Gruppe wird in einem Plan verwendet, für den eine Wiederherstellung durchgeführt wurde, aber die Wiederherstellung ist für manche virtuelle Maschinen fehlgeschlagen. Sie können virtuelle Maschinen entfernen, aber nicht konfigurieren oder wiederherstellen.
Wiederhergestellt	Die Gruppe wird in einem Plan verwendet, der eine Wiederherstellung erfolgreich ausgeführt hat. Sie können virtuelle Maschinen entfernen, aber nicht konfigurieren oder wiederherstellen.
Neu schützen	Die Gruppe wird in einem Plan verwendet, der einen Vorgang zum erneuten Schützen ausführt. Sie können die Gruppe nicht bearbeiten. Für die Gruppe wird wieder der Status „OK“ oder „Nicht konfiguriert“ angezeigt, wenn der Vorgang zum erneuten Schützen erfolgreich ausgeführt wurde. Falls der Vorgang zum erneuten Schützen fehlschlägt, wechselt die Gruppe in den Status „Teilweise neu geschützt“.

Tabelle 3-1. Status der Schutzgruppe (Fortsetzung)

Zustand	Beschreibung
Teilweise neu geschützt	Die Gruppe wird in einem Plan verwendet, für den ein Vorgang zum erneuten Schützen fehlgeschlagen ist. Sie können virtuelle Maschinen entfernen, aber nicht konfigurieren oder wiederherstellen.
Schutz wird konfiguriert	Schutzvorgänge werden auf virtuellen Maschinen in der Gruppe ausgeführt.
Schutz wird entfernt	Das Entfernen des Schutzes für virtuelle Maschinen in der Gruppe wird ausgeführt.
Platzhalter werden wiederhergestellt	Das Erstellen von Platzhaltern für virtuelle Maschinen in der Gruppe wird ausgeführt.
Vorgänge laufen	Eine Kombination aus mindestens einem Vorgang „Schutz konfigurieren“ und einem Vorgang „Schutz entfernen“ wird in der Gruppe ausgeführt.

Schutzstatus der virtuellen Maschine – Referenz

Sie können den Status einer virtuellen Maschine in einer Schutzgruppe überwachen und den für jeden Status zulässigen Vorgang bestimmen.

Tabelle 3-2. Schutzstatus der virtuellen Maschine

Zustand	Beschreibung
Platzhalter-VM nicht gefunden	Sie haben die Platzhalter-VM gelöscht. Das Symbol „Platzhalter-VM wiederherstellen“ ist aktiviert.
Ursprüngliche geschützte VM wurde nicht gefunden	Sie haben die ursprüngliche Produktions-VM nach dem Failover und vor dem erneuten Schützen gelöscht. Das Symbol „Platzhalter-VM wiederherstellen“ ist aktiviert.
Der von der VM verwendete Datenspeicher *Name* fehlt in der Gruppe	Die virtuelle Maschine benötigt einen Datenspeicher, der nicht in der Schutzgruppe vorhanden ist. Bearbeiten Sie die Schutzgruppe, um den Datenspeicher hinzuzufügen.
Der von der VM verwendete Datenspeicher *Name* ist in einer anderen Gruppe geschützt	Die virtuelle Maschine benötigt einen Datenspeicher, der in einer anderen Schutzgruppe vorhanden ist. Entfernen Sie den Datenspeicher aus der anderen Schutzgruppe und bearbeiten Sie die aktuelle Schutzgruppe, um den Datenspeicher hinzuzufügen. Ein Datenspeicher kann nicht in zwei Schutzgruppen gleichzeitig vorhanden sein.
Gerät nicht gefunden: *Gerätename*	Sie haben einer geschützten virtuellen Maschine eine nicht replizierte Festplatte oder ein Gerät hinzugefügt. Sie müssen die Replizierung der virtuellen Maschine bearbeiten, um den Schutz für das Gerät zu aktivieren oder zu deaktivieren.
Zuordnung fehlt: Ordner *Name*; Netzwerk *Name*; Ressourcenpool *Name*	Für diese virtuelle Maschine sind keine Ordner-, Ressourcenpool- oder Netzwerkzuordnungen konfiguriert. Korrigieren Sie die Bestandslistenzuordnungen für die Site oder konfigurieren Sie die virtuelle Maschine manuell.

Tabelle 3-2. Schutzstatus der virtuellen Maschine (Fortsetzung)

Zustand	Beschreibung
Fehler beim Erstellen der Platzhalter-VM: *Fehlerzeichenfolge vom Server*	Fehler beim Erstellen der Platzhalter-VM.
OK	Die geschützte virtuelle Maschine ist vorhanden und sowohl der Anbieter- als auch der Platzhalterstatus lauten „Bereinigen“.
Ungültig: *Fehler*	Die virtuelle Maschine ist nicht gültig, da der Home-Datenspeicher nicht repliziert wurde oder die virtuelle Maschine gelöscht wurde. Die Fehlerzeichenfolge vom Server enthält die Details. Entfernen Sie den Schutz für die virtuelle Maschine manuell.
Nicht konfiguriert	Sie haben nach dem Erstellen der Schutzgruppe eine neue virtuelle Maschine hinzugefügt. Verwenden Sie „Alle konfigurieren“, um den Schutz für die virtuelle Maschine zu konfigurieren.
Fehler: *Fehler*	Folgende Fehler sind möglich: ■ Der Ressourcenpool, der Ordner oder das Netzwerk der Wiederherstellungs-Site befinden sich nicht im selben Datencenter. ■ Der Platzhalterdatenspeicher wurde nicht gefunden. ■ Ein beliebiger vCenter Server-Fehler, der beim Erstellen des Platzhalters aufgetreten ist, wie z. B. Verbindungs- oder Berechtigungsprobleme.
Schutz wird konfiguriert	Ein VM-Vorgang.
Schutz wird entfernt	Ein VM-Vorgang.
Platzhalter wird wiederhergestellt	Ein VM-Vorgang.
Wird geladen...	Erscheint kurz beim Laden der Schnittstelle, bis der Status der virtuellen Maschine angezeigt wird.
Zuordnungskonflikt	Site Recovery Manager Server hat einen Bestandslistenkonflikt gemeldet. Der Ressourcenpool und der Ordner der virtuellen Maschine befinden sich in unterschiedlichen Datencentern.
Replizierungsfehler	vSphere Replication meldet einen Fehler im Zusammenhang mit der virtuellen Maschine.
Replizierungswarnung	vSphere Replication meldet eine Warnung im Zusammenhang mit der virtuellen Maschine.

Erstellen, Testen und Ausführen von Wiederherstellungsplänen

4

Sobald Sie Site Recovery Manager auf der Schutz- und der Wiederherstellungs-Site konfiguriert haben, können Sie einen Wiederherstellungsplan erstellen, testen und ausführen.

Ein Wiederherstellungsplan ist wie ein automatisiertes Ausführungsskript. Er steuert jeden Schritt des Wiederherstellungsvorgangs, einschließlich der Reihenfolge, in der Site Recovery Manager virtuelle Maschinen aus- oder einschaltet, der Netzwerkadressen, die die virtuellen Maschinen verwenden, usw. Wiederherstellungspläne sind flexibel und benutzerdefinierbar.

Ein Wiederherstellungsplan enthält eine oder mehrere Schutzgruppen. Eine Schutzgruppe kann in mehr als einen Wiederherstellungsplan aufgenommen werden. Sie können beispielsweise einen Wiederherstellungsplan erstellen, um eine geplante Migration von Diensten von der geschützten auf die Wiederherstellungs-Site durchzuführen, und einen anderen Wiederherstellungsplan erstellen, um ein nicht geplantes Ereignis abzuwickeln, wie z. B. einen Stromausfall oder eine Naturkatastrophe. In diesem Beispiel können Sie anhand dieser verschiedenen, auf eine Schutzgruppe verweisenden Wiederherstellungspläne entscheiden, wie Sie die Wiederherstellung durchführen. Informationen zum Erstellen einer Schutzgruppe finden Sie unter Schutzgruppen erstellen.

Sie können zum Wiederherstellen einer bestimmten Schutzgruppe nur einen Wiederherstellungsplan gleichzeitig ausführen. Wenn Sie mehrere Wiederherstellungspläne, die dieselbe Schutzgruppe angeben, gleichzeitig testen oder ausführen, kann nur ein Wiederherstellungsplan für die Schutzgruppe durchgeführt werden. Sonstige ausgeführte Wiederherstellungspläne, die dieselbe Schutzgruppe angeben, geben Warnmeldungen für diese Schutzgruppe und die virtuellen Maschinen, die sie enthält, aus. Die Warnungen melden, dass die virtuellen Maschinen wiederhergestellt wurden, melden jedoch keine weiteren Schutzgruppen, die andere Wiederherstellungspläne abdecken.

- Testen eines Wiederherstellungsplans

  Wenn Sie einen Wiederherstellungsplan erstellen oder ändern, sollte Sie ihn testen, bevor Sie ihn für eine geplante Migration oder eine Notfallwiederherstellung einsetzen.

- Durchführen einer geplanten Migration oder einer Notfallwiederherstellung durch Ausführung eines Wiederherstellungsplans

  Sie können einen Wiederherstellungsplan zu einem geplanten Zeitpunkt ausführen, um virtuelle Maschinen von der Schutz-Site auf die Wiederherstellungs-Site zu migrieren. Darüber hinaus können Sie einen Wiederherstellungsplan auch ungeplant durchführen, falls auf der Schutz-Site ein unvorhergesehenes Ereignis eintritt, bei dem Daten verloren gehen könnten.

- Unterschiede zwischen dem Test und der Ausführung eines Wiederherstellungsplans

  Das Testen eines Wiederherstellungsplans hat keine nachhaltigen Auswirkungen auf die Schutz- oder Wiederherstellungs-Site, das Ausführen eines Wiederherstellungsplans hat jedoch erhebliche Auswirkungen auf beide Sites.

- Durchführen einer Testwiederherstellung von virtuellen Maschinen über mehrere Hosts an der Wiederherstellungs-Site hinweg

  Sie können Wiederherstellungspläne erstellen, anhand derer virtuelle Maschinen auf mehreren Wiederherstellungs-Site-Hosts in einem Quarantäne-Testnetzwerk wiederhergestellt werden können.

- Erstellen, Testen und Ausführen eines Wiederherstellungsplans

  Sie führen mehrere Aufgaben durch, um einen Wiederherstellungsplan zu erstellen, zu testen und auszuführen.

- Schritte zum Exportieren des Wiederherstellungsplans

  Sie können die Schritte eines Wiederherstellungsplans in verschiedenen Formaten zur späteren Verwendung oder zum Aufbewahren einer Sicherungskopie Ihrer Pläne exportieren.

- Anzeigen und Exportieren des Verlaufs eines Wiederherstellungsplans

  Sie können Berichte über jede Durchführung von Wiederherstellungsplänen, Überprüfung von Wiederherstellungsplänen oder Testbereinigungen anzeigen und exportieren.

- Löschen eines Wiederherstellungsplans

  Falls Sie einen Wiederherstellungsplan nicht mehr benötigen, können Sie ihn löschen.

- Status des Wiederherstellungsplans – Referenz

  Sie können den Status eines Wiederherstellungsplans überwachen und den für jeden Status zulässigen Vorgang bestimmen. Der Status eines Wiederherstellungsplans wird durch die Status der Schutzgruppen innerhalb des Wiederherstellungsplans bestimmt.

Testen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan erstellen oder ändern, sollte Sie ihn testen, bevor Sie ihn für eine geplante Migration oder eine Notfallwiederherstellung einsetzen.

Indem Sie einen Wiederherstellungsplan testen, stellen Sie sicher, dass die virtuellen Maschinen, die vom Plan geschützt werden, korrekt auf der Wiederherstellungs-Site wiederhergestellt werden. Wenn Sie Wiederherstellungspläne nicht testen, werden bei einer tatsächlichen Notfallwiederherstellung möglicherweise nicht alle virtuellen Maschinen wiederhergestellt. Dies führt zu Datenverlusten.

Beim Testen eines Wiederherstellungsplans werden fast alle Aspekte des Wiederherstellungsplans überprüft, obwohl Site Recovery Manager einige Zugeständnisse macht, damit laufende Vorgänge auf der Schutz- und Wiederherstellungs-Site nicht unterbrochen werden. Dagegen beeinträchtigen Wiederherstellungspläne, die lokale virtuelle Maschinen anhalten, Tests und aktuelle Wiederherstellungen. Von dieser Ausnahme abgesehen unterbricht die Ausführung einer Testwiederherstellung nicht die Replizierung oder laufende Aktivitäten auf beiden Sites.

Falls Sie vSphere Replication verwenden, wenn Sie einen Wiederherstellungsplan testen, kann sich die virtuelle Maschine auf der Schutz-Site weiterhin mit den replizierten Festplattendateien virtueller Maschinen auf der Wiederherstellungs-Site synchronisieren. Der vSphere Replication-Server erstellt Redo-Protokolle auf den Festplattendateien virtueller Maschinen auf der Wiederherstellungs-Site, sodass die Synchronisierung normal weiterlaufen kann. Wenn Sie nach der Durchführung eines Tests eine Bereinigung ausführen, entfernt der vSphere Replication-Server die Redo-Protokolle aus den Festplattendateien auf der Wiederherstellungs-Site und hält die akkumulierten Änderungen in den Protokollen auf VM-Festplatten fest.

Falls Sie Array-basierte Replizierung verwenden, werden beim Testen eines Wiederherstellungsplans die virtuellen Maschinen auf der Schutz-Site weiterhin in die Festplattendateien der VM-Repliken auf der Wiederherstellungs-Site repliziert. Während der Testwiederherstellung erstellt das Array auf der Wiederherstellungs-Site einen Snapshot der Volumes, die die Festplattendateien der virtuellen Maschinen hosten. Die Array-Replizierung wird während des laufenden Tests normal fortgesetzt. Wenn Sie nach der Durchführung eines Tests eine Bereinigung ausführen, entfernt das Array die zuvor im Rahmen des Testwiederherstellungs-Workflows erstellten Snapshots.

Sie können Testwiederherstellungen so oft wie nötig ausführen. Sie können den Test eines Wiederherstellungsplans jederzeit abbrechen.

Vor dem Starten eines Failovers oder eines weiteren Tests müssen Sie einen Bereinigungsvorgang ausführen und erfolgreich abschließen. Weitere Informationen hierzu finden Sie unter Bereinigen nach dem Testen eines Wiederherstellungsplans.

Die Berechtigung zum Testen eines Wiederherstellungsplans umfasst nicht die Berechtigung zur Ausführung eines Wiederherstellungsplans. Die Berechtigung zum Ausführen eines Wiederherstellungsplans umfasst nicht die Berechtigung zum Testen eines Wiederherstellungsplans. Sie müssen jede Berechtigung separat zuweisen. Weitere Informationen hierzu finden Sie unter Zuweisen von Site Recovery Manager-Rollen und -Berechtigungen.

Test- und Datencenter-Netzwerke

Wenn Sie einen Wiederherstellungsplan testen, kann Site Recovery Manager ein Testnetzwerk erstellen, das verwendet wird, um wiederhergestellte virtuelle Maschinen zu verbinden. Wenn Sie ein Testnetzwerk erstellen, können Sie den Test durchführen, ohne potenzielle Unterbrechungen der virtuellen Maschinen in der Produktionsumgebung zu riskieren.

Das Testnetzwerk wird durch seinen eigenen virtuellen Switch verwaltet und in den meisten Fällen können wiederhergestellte virtuelle Maschinen dieses Netzwerk verwenden, ohne die Netzwerkeigenschaften, wie IP-Adresse, Gateway usw., ändern zu müssen. Um das Testnetzwerk zu verwenden, wählen Sie **Auto** aus, wenn Sie die Einstellungen für das Testnetzwerk beim Erstellen eines Wiederherstellungsplans konfigurieren. Ein Testnetzwerk ist nicht über mehrere Hosts verteilt. Sie müssen für jedes Netzwerk, das bei der Wiederherstellung von einem Wiederherstellungsplan verwendet wird, ein Testnetzwerk konfigurieren.

Sie müssen alle virtuellen Maschinen wiederherstellen, die im selben Testnetzwerk miteinander interagieren müssen. Wenn beispielsweise ein Webserver auf Informationen einer Datenbank zugreift, sollten die virtuellen Maschinen für diesen Webserver und die Datenbank zusammen auf demselben Netzwerk wiederhergestellt werden.

Ein Datencenter-Netzwerk ist ein Netzwerk, das in der Regel vorhandene virtuelle Maschinen auf der Wiederherstellungs-Site unterstützt. Sie können ein Datencenternetzwerk als Testnetzwerk auswählen. Um es einzusetzen, müssen wiederhergestellte virtuelle Maschinen seine Regeln hinsichtlich der Verfügbarkeit der Netzwerkadressen einhalten. Diese virtuellen Maschinen müssen eine Netzwerkadresse verwenden, die vom Switch des Netzwerks bedient und geroutet werden kann, und sie müssen das richtige Gateway und den richtigen DNS-Host usw. verwenden. Wiederhergestellte virtuelle Maschinen, die DHCP verwenden, können ohne zusätzliche Anpassung eine Verbindung zu diesem Netzwerk herstellen. Für andere virtuelle Maschinen ist eine IP-Anpassung und sind zusätzliche Schritte im Wiederherstellungsplan erforderlich, um die Anpassung zu übernehmen.

Durchführen einer geplanten Migration oder einer Notfallwiederherstellung durch Ausführung eines Wiederherstellungsplans

Sie können einen Wiederherstellungsplan zu einem geplanten Zeitpunkt ausführen, um virtuelle Maschinen von der Schutz-Site auf die Wiederherstellungs-Site zu migrieren. Darüber hinaus können Sie einen Wiederherstellungsplan auch ungeplant durchführen, falls auf der Schutz-Site ein unvorhergesehenes Ereignis eintritt, bei dem Daten verloren gehen könnten.

Bei einer geplanten Migration synchronisiert Site Recovery Manager die virtuelle Maschine auf der Wiederherstellungs-Site mit den virtuellen Maschinen auf der Schutz-Site. Site Recovery Manager versucht, die geschützten Maschinen ordnungsgemäß herunterzufahren, und nimmt eine abschließende Synchronisierung vor, um Datenverlust zu verhindern. Anschließend werden die virtuellen Maschinen auf der Wiederherstellungs-Site eingeschaltet. Falls bei der Durchführung der geplanten Migration Fehler auftreten, wird der Plan gestoppt. Beheben Sie die Fehler und führen Sie dann den Plan erneut aus. Nach der Wiederherstellung können Sie die virtuellen Maschinen neu schützen.

Bei Notfallwiederherstellungen versucht Site Recovery Manager, zunächst eine Speichersynchronisierung durchzuführen. Wenn dieser Vorgang erfolgreich ist, verwendet Site Recovery Manager den synchronisierten Speicherstatus, um virtuelle Maschinen auf der Wiederherstellungs-Site mit dem zuletzt verfügbaren Status entsprechend des Recovery Point Objective (RPO), den Sie bei der Konfiguration Ihrer Replizierungstechnologie festgelegt haben, wiederherzustellen. Wenn Sie einen Wiederherstellungsplan zur Notfallwiederherstellung durchführen, versucht Site Recovery Manager, die virtuellen Maschinen auf der Schutz-Site herunterzufahren. Falls Site Recovery Manager die virtuellen Maschinen nicht herunterfahren kann, startet Site Recovery Manager dennoch die Kopien auf der Wiederherstellungs-Site. Für den Fall, dass die Schutz-Site nach der Notfallwiederherstellung wieder online geschaltet wird, weist der Wiederherstellungsplan einen inkonsistenten Status auf, in dem virtuelle Maschinen des Produktionssystems auf beiden Sites ausgeführt werden. Dies wird als Split-Brain-Szenario bezeichnet.

Site Recovery Manager erkennt diesen Status und ermöglicht die erneute Ausführung des Wiederherstellungsplans, um die virtuellen Maschinen auf der Schutz-Site auszuschalten. Anschließend wechselt der Wiederherstellungsplan wieder in den inkonsistenten Status und Sie können die Funktion „Neu schützen“ ausführen.

Wenn Site Recovery Manager erkennt, dass sich ein Datenspeicher auf der Schutz-Site im Status „Keine Pfade verfügbar“ befindet, und verhindert, dass eine virtuelle Maschine heruntergefahren wird, wartet Site Recovery Manager, bevor erneut versucht wird, die virtuelle Maschine herunterzufahren. Der Status „Keine Pfade verfügbar“ ist in der Regel vorübergehend. Also wartet Site Recovery Manager, bis ein Datenspeicher mit dem Status „Keine Pfade verfügbar“ wieder online ist, um die geschützten virtuellen Maschinen auf diesem Datenspeicher ordnungsgemäß herunterzufahren.

Site Recovery Manager erkennt anhand des Taktsignalstatus von VMware Tools, wenn eine virtuelle Maschine auf der Wiederherstellungs-Site ausgeführt wird. Auf diese Weise kann Site Recovery Manager sicherstellen, dass alle virtuellen Maschinen auf der Wiederherstellungs-Site ausgeführt werden. Aus diesem Grund wird empfohlen, VMware Tools auf geschützten virtuellen Maschinen zu installieren. Wenn Sie VMware Tools auf geschützten virtuellen Maschinen nicht installieren oder nicht installieren können, müssen Sie Site Recovery Manager so konfigurieren, dass nicht auf den Start von VMware Tools in den wiederhergestellten virtuellen Maschinen gewartet wird und die Schritte zum Herunterfahren des Gastbetriebssystems übersprungen werden. Weitere Informationen hierzu finden Sie unter Ändern von Wiederherstellungseinstellungen.

Nachdem Site Recovery Manager die abschließende Replizierung beendet hat, nimmt Site Recovery Manager Änderungen an beiden Sites vor, deren Rücknahme viel Zeit und Aufwand in Anspruch nimmt. Daher müssen Sie das Recht zum Testen eines Wiederherstellungsplans und das Recht zum Ausführen eines Wiederherstellungsplans separat zuweisen.

Ausführen einer Wiederherstellung mit erzwungener Wiederherstellung

Wenn die Schutz-Site offline ist und Site Recovery Manager die regulären Aufgaben nicht zeitnah ausführen kann und dadurch der RTO (Recovery Time Objective) auf einen inakzeptablen Wert ansteigt, können Sie die Wiederherstellung mit der Option „Erzwungene Wiederherstellung“ ausführen. Die erzwungene Wiederherstellung startet die virtuellen Maschinen auf der Wiederherstellungs-Site, ohne dass Vorgänge auf der Schutz-Site durchgeführt werden.

Vorsicht Verwenden Sie die erzwungene Wiederherstellung nur dann, wenn Recovery-Time-Objective (RTO) durch eine mangelhafte Konnektivität zur Schutz-Site erheblich beeinträchtigt wird.

Die erzwungene Wiederherstellung soll verwendet werden, wenn Infrastruktur der Schutz-Site ausfällt und infolgedessen geschützte virtuelle Maschinen nicht mehr verwaltet und heruntergefahren bzw. ausgeschaltet werden können bzw. deren Registrierung nicht aufgehoben werden kann. In solch einem Fall kann der Systemzustand für einen längeren Zeitraum nicht geändert werden. Um das Problem zu beheben, können Sie eine Wiederherstellung erzwingen. Das Erzwingen einer Wiederherstellung schließt den Vorgang des Herunterfahrens der virtuellen Maschinen an der Schutz-Site nicht ab. Dies führt zu einem Split-Brain-Szenario, aber die Wiederherstellung wird möglicherweise schnell abgeschlossen.

Wird die Notfallwiederherstellung mit Array-basierter Replizierung ausgeführt, während das Speicher-Array an der Schutz-Site offline oder nicht verfügbar ist, kann dies die Spiegelung zwischen dem Speicher-Array für den Schutz und dem Speicher-Array für die Wiederherstellung beeinträchtigen. Nachdem Sie die erzwungene Wiederherstellung ausgeführt haben, müssen Sie überprüfen, ob die Spiegelung zwischen dem geschützten Array und dem Wiederherstellungs-Array ordnungsgemäß eingerichtet ist, bevor Sie weitere Replizierungsvorgänge durchführen können. Wurde das Spiegeln nicht ordnungsgemäß eingerichtet, müssen Sie es unter Verwendung der Speicher-Array-Software reparieren.

Bei Ausführung der Notfallwiederherstellung mithilfe von vSphere Replication bereitet Site Recovery Manager vSphere Replication-Speicher für den erneuten Schutz vor. Sie müssen die Spiegelung nicht wie bei der Array-basierten Replizierung überprüfen.

Wenn Sie die erzwungene Wiederherstellung aktivieren, während der Speicher der Schutz-Site noch verfügbar ist, werden alle ausstehenden Änderungen an der Schutz-Site erst dann auf die Wiederherstellungs-Site repliziert, wenn die Sequenz startet. Die Replizierung der Änderungen wird entsprechend des Zeitraums für das Recovery Point Objective (RPO) des Speicher-Arrays durchgeführt. Wird eine neue virtuelle Maschine oder Vorlage auf der Schutz-Site hinzugefügt und eine Wiederherstellung vor Ablauf des Speicher-RPO-Zeitraums initiiert, wird die neue virtuelle Maschine oder Vorlage nicht auf dem replizierten Datenspeicher angezeigt und geht verloren. Um zu vermeiden, dass die neue virtuelle Maschine oder Vorlage verloren geht, warten Sie bis zum Ende des RPO-Zeitraums, bevor Sie den Wiederherstellungsplan mit erzwungener Wiederherstellung ausführen.

Um bei der Ausführung der Notfallwiederherstellung die erzwungene Wiederherstellung auszuwählen, müssen Sie die Option `recovery.forceRecovery` in „Erweiterte Einstellungen“ auf dem Site Recovery Manager-Server auf der Wiederherstellungs-Site aktivieren. Im Assistenten „Wiederherstellungsplan ausführen“ können Sie die Option für die erzwungene Wiederherstellung nur im Notfallwiederherstellungsmodus ausführen. Für die geplante Migration ist sie nicht verfügbar.

Nach Abschluss der erzwungenen Wiederherstellung und nachdem Sie die Spiegelung der Speicher-Arrays verifiziert haben, können Sie das Problem beheben, das zur erzwungenen Wiederherstellung führte. Wenn das zugrunde liegende Problem behoben wurde, führen Sie die geplante Migration oder den Wiederherstellungsplan erneut aus und beheben Sie alle Probleme, die auftreten. Führen Sie den Plan so lange erneut aus, bis er erfolgreich abgeschlossen wird. Das erneute Ausführen des Wiederherstellungsplans wirkt sich nicht auf die wiederhergestellten virtuellen Maschinen an der Wiederherstellungs-Site aus.

Hinweis Wenn Sie die geplante Migration ausführen, nachdem Sie eine erzwungene Wiederherstellung ausgeführt haben, fahren virtuelle Maschinen auf der Schutz-Site möglicherweise nicht herunter, sofern die zugrunde liegenden Datenspeicher schreibgeschütztnur ausgelesen werden oder nicht verfügbar sind. Melden Sie sich in diesem Fall bei vCenter Server auf der Schutz-Site an und schalten Sie die virtuellen Maschinen manuell aus. Nachdem Sie die virtuellen Maschinen ausgeschaltet haben, führen Sie die geplante Migration erneut aus.

Unterschiede zwischen dem Test und der Ausführung eines Wiederherstellungsplans

Das Testen eines Wiederherstellungsplans hat keine nachhaltigen Auswirkungen auf die Schutz- oder Wiederherstellungs-Site, das Ausführen eines Wiederherstellungsplans hat jedoch erhebliche Auswirkungen auf beide Sites.

Sie benötigen unterschiedliche Rechte für das Testen und das Ausführen eines Wiederherstellungsplans.

Tabelle 4-1. So unterscheidet sich das Testen eines Wiederherstellungsplans vom Ausführen eines Wiederherstellungsplans

Unterschiede	Testen eines Wiederherstellungsplans	Ausführen eines Wiederherstellungsplans
Erforderliche Berechtigungen	Erfordert die Berechtigung **Site Recovery Manager.Wiederherstellungspläne.Testen**.	Erfordert die Berechtigung **Site Recovery Manager.Wiederherstellungspläne.Wiederherstellen**.
Auswirkungen auf virtuelle Maschinen an der Schutz-Site	Keine	Site Recovery Manager schaltet virtuelle Maschinen in umgekehrter Reihenfolge der Priorität aus und stellt alle auf der Schutz-Site angehaltenen virtuellen Maschinen wieder her.
Auswirkungen auf virtuelle Maschinen an der Wiederherstellungs-Site	Site Recovery Manager hält lokale virtuelle Maschinen an, falls dies im Wiederherstellungsplan vorgesehen ist. Site Recovery Manager startet nach Bereinigung des Tests angehaltene virtuelle Maschinen neu.	Site Recovery Manager hält lokale virtuelle Maschinen an, falls dies im Wiederherstellungsplan vorgesehen ist.
Auswirkungen auf die Replizierung	Site Recovery Manager erstellt temporäre Snapshots des replizierten Speichers an der Wiederherstellungs-Site. Bei der Array-basierten Replizierung prüft Site Recovery Manager die Arrays erneut, damit sie ermittelt werden.	Bei einer geplanten Migration synchronisiert Site Recovery Manager replizierte Datenspeicher. Anschließend wird die Replizierung gestoppt und die Zielgeräte werden auf der Wiederherstellungs-Site beschreibbar gemacht. Während einer Notfallwiederherstellung versucht Site Recovery Manager, die gleichen Schritte durchzuführen. Falls diese jedoch nicht zum gewünschten Ergebnis führen, ignoriert Site Recovery Manager die Fehler auf der Schutz-Site.
Netzwerk	Wenn Sie Testnetzwerke explizit zuweisen, verbindet Site Recovery Manager wiederhergestellte virtuelle Maschinen mit einem Testnetzwerk. Wenn die Netzwerkzuweisung für die virtuelle Maschine **Auto** lautet, weist Site Recovery Manager virtuelle Maschinen temporären Netzwerken zu, die mit keinem physischen Netzwerk verbunden sind.	Site Recovery Manager verbindet wiederhergestellte virtuelle Maschinen mit dem benutzerspezifischen Datencenter-Netzwerk.
Unterbrechung eines Wiederherstellungsplans	Sie können einen Test jederzeit abbrechen.	Sie können die Wiederherstellung jederzeit abbrechen.

Durchführen einer Testwiederherstellung von virtuellen Maschinen über mehrere Hosts an der Wiederherstellungs-Site hinweg

Sie können Wiederherstellungspläne erstellen, anhand derer virtuelle Maschinen auf mehreren Wiederherstellungs-Site-Hosts in einem Quarantäne-Testnetzwerk wiederhergestellt werden können.

Mit Site Recovery Manager können die vSwitches DVS-basiert sein und sich über mehrere Hosts verteilen. Wenn Sie das Standard-Testnetzwerk akzeptieren, das mit der Bezeichnung „Auto“ konfiguriert ist, werden virtuelle Maschinen, die über mehrere Hosts wiederhergestellt werden, während Tests von Wiederherstellungsplänen in ihr eigenes Testnetzwerk gestellt. Jeder Test-Switch ist zwischen den Hosts isoliert. Folglich sind virtuelle Maschinen, die sich in demselben Wiederherstellungsplan befinden, isoliert, wenn die Testwiederherstellung beendet ist. Um den virtuellen Maschinen die Kommunikation zu ermöglichen, richten Sie DVS-Switches oder VLANs ein und wählen Sie diese aus. Durch ein isoliertes VLAN, das alle Hosts miteinander verbindet, aber keine Verbindung zu einem Produktionsnetzwerk herstellt, können Sie eine Wiederherstellung realistischer testen. Um alle Wiederherstellungs-Hosts miteinander zu verbinden, aber vom Produktionsnetzwerk isoliert zu bleiben, halten Sie sich an die folgenden Empfehlungen:

- Erstellen Sie DVS-Switches, die mit einem isolierten privaten VLAN verbunden sind. Ein solches VLAN ermöglicht, dass Hosts und virtuelle Maschinen verbunden, jedoch von Produktions-VMs isoliert sind. Verwenden Sie eine Namenskonvention, aus der ersichtlich wird, dass der DVS zum Testen bestimmt ist, und wählen Sie diesen DVS in der Spalte für das Testnetzwerk des Wiederherstellungsplans im Wiederherstellungsplan-Editor aus.
- Erstellen Sie Test-VLANs auf einem physischen Netzwerk, die keine Route zurück zur Schutz-Site bieten. Führen Sie für VLANs Trunk-Tests zu vSphere-Clustern der Wiederherstellungs-Site durch und erstellen Sie virtuelle Switches für Test-VLAN-IDs. Achten Sie dabei auf eine klare Namenskonvention, aus der deutlich wird, dass diese Switches zu Testzwecken genutzt werden. Wählen Sie diese Switches aus der Spalte für das Testnetzwerk zur Wiederherstellung im Wiederherstellungsplan-Editor aus.

Erstellen, Testen und Ausführen eines Wiederherstellungsplans

Sie führen mehrere Aufgaben durch, um einen Wiederherstellungsplan zu erstellen, zu testen und auszuführen.

Vorgehensweise

1 Erstellen eines Wiederherstellungsplans

   Sie erstellen einen Wiederherstellungsplan, um festzulegen, wie Site Recovery Manager virtuelle Maschinen wiederherstellt.

2 Organisieren von Wiederherstellungsplänen in Ordnern

   Sie können Ordner erstellen, in denen Sie Wiederherstellungspläne organisieren.

3 Bearbeiten eines Wiederherstellungsplans

Sie können einen Wiederherstellungsplan bearbeiten, um die Eigenschaften, die Sie bei der Erstellung angegeben haben, zu ändern. Sie können Wiederherstellungspläne entweder von der Schutz-Site oder der Wiederherstellungs-Site aus bearbeiten.

4 Testen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan testen, führt Site Recovery Manager die virtuellen Maschinen des Wiederherstellungsplans in einem Testnetzwerk aus und erstellt einen temporären Snapshot der replizierten Daten an der Wiederherstellungs-Site. Site Recovery Manager unterbricht keine Vorgänge an der Schutz-Site.

5 Bereinigen nach dem Testen eines Wiederherstellungsplans

Nach dem Testen eines Wiederherstellungsplans können Sie den Wiederherstellungsplan wieder in den Status 'Bereit' versetzen, indem Sie einen Bereinigungsvorgang durchführen. Sie müssen den Bereinigungsvorgang abschließen, bevor Sie ein Failover oder einen anderen Test ausführen können.

6 Ausführen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan ausführen, migriert Site Recovery Manager alle virtuellen Maschinen im Wiederherstellungsplan auf die Wiederherstellungs-Site. Site Recovery Manager versucht, die entsprechenden virtuellen Maschinen auf der Schutz-Site herunterzufahren.

7 Wiederherstellen eines Point-in-Time-Snapshots einer virtuellen Maschine

Mit vSphere Replication können Sie Point-in-Time-Snapshots von virtuellen Maschinen beibehalten. Sie können Site Recovery Manager so konfigurieren, dass mehrere Point-in-Time-Snapshots (PIT) einer virtuellen Maschine wiederhergestellt werden, wenn Sie einen Wiederherstellungsplan ausführen.

8 Abbrechen eines Tests oder einer Wiederherstellung

Sie können den Test eines Wiederherstellungsplans abbrechen, wenn er den Status „Test läuft“ oder „Failover wird durchgeführt“ aufweist.

Erstellen eines Wiederherstellungsplans

Sie erstellen einen Wiederherstellungsplan, um festzulegen, wie Site Recovery Manager virtuelle Maschinen wiederherstellt.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne**.

2 Klicken Sie auf der Registerkarte **Objekte** auf das Symbol zum Erstellen eines Wiederherstellungsplans.

3 Geben Sie einen Namen und eine Beschreibung für den Plan ein, wählen Sie einen Ordner aus und klicken Sie anschließend auf **Weiter**.

4 Wählen Sie die Wiederherstellungs-Site aus und klicken Sie auf **Weiter**.

5 Wählen Sie eine oder mehrere Schutzgruppen für den Plan aus, der wiederhergestellt werden soll, und klicken Sie auf **Weiter**.

6 Klicken Sie auf den Wert **Testnetzwerk**, wählen Sie ein während der Testwiederherstellung zu verwendendes Netzwerk aus, und klicken Sie auf **Weiter**.

   Die Standardoption ist die automatische Erstellung eines isolierten Netzwerks.

7 Überprüfung Sie die Zusammenfassung der Angaben und klicken Sie auf **Beenden**, um den Wiederherstellungsplan zu erstellen.

Organisieren von Wiederherstellungsplänen in Ordnern

Sie können Ordner erstellen, in denen Sie Wiederherstellungspläne organisieren.

Das Organisieren von Wiederherstellungsplänen in Ordnern ist nützlich, wenn Sie über viele Wiederherstellungspläne verfügen. Sie können den Zugriff auf die Wiederherstellungspläne einschränken, indem Sie sie in Ordner ablegen und den Ordnern unterschiedliche Berechtigungen für unterschiedliche Benutzer oder Gruppen zuweisen. Informationen dazu, wie Sie Ordnern Berechtigungen zuweisen, finden Sie unter Zuweisen von Site Recovery Manager-Rollen und -Berechtigungen.

Vorgehensweise

1 Klicken Sie in der Home-Ansicht des vSphere Web Client auf **Site-Wiederherstellung**.

2 Erweitern Sie **Bestandslistenstrukturen** und klicken Sie auf **Wiederherstellungspläne**.

3 Wählen Sie auf der Registerkarte **Verwandte Objekte** aus und klicken Sie auf **Ordner**.

4 Klicken Sie auf das Symbol **Ordner erstellen**, geben Sie einen Namen für den zu erstellenden Ordner ein, und klicken Sie auf **OK**.

5 Fügen Sie dem Ordner neue oder bereits vorhandene Wiederherstellungspläne hinzu.

Option	Beschreibung
Neuen Wiederherstellungsplan erstellen	Klicken Sie mit der rechten Maustaste auf den Ordner und wählen Sie **Wiederherstellungsplan erstellen** aus.
Vorhandenen Wiederherstellungsplan hinzufügen	Ziehen Sie mit der Maus Wiederherstellungspläne von der Bestandslistenstruktur in den Ordner.

6 (Optional) Zum Umbenennen oder Löschen eines Ordners klicken Sie mit der rechten Maustaste auf den Ordner und wählen **Ordner umbenennen** oder **Ordner löschen** aus.

   Sie können nur leere Ordner löschen.

Bearbeiten eines Wiederherstellungsplans

Sie können einen Wiederherstellungsplan bearbeiten, um die Eigenschaften, die Sie bei der Erstellung angegeben haben, zu ändern. Sie können Wiederherstellungspläne entweder von der Schutz-Site oder der Wiederherstellungs-Site aus bearbeiten.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne**.
2. Klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan und wählen Sie **Plan bearbeiten** aus.

   Sie können einen Wiederherstellungsplan auch bearbeiten, indem Sie auf das Symbol **Wiederherstellungsplan bearbeiten** klicken, das sich in der Ansicht **Wiederherstellungsschritte** auf der Registerkarte **Überwachen** befindet.
3. (Optional) Ändern Sie im Textfeld **Name des Wiederherstellungsplans** den Namen oder die Beschreibung des Plans und klicken Sie auf **Weiter**.
4. Klicken Sie auf der Seite „Wiederherstellungs-Site“ auf **Weiter**.

   Sie können die Wiederherstellungs-Site nicht ändern.
5. (Optional) Wählen Sie eine oder mehrere Schutzgruppen aus bzw. heben Sie die Auswahl einer oder mehrerer Schutzgruppen auf, um sie zum Wiederherstellungsplan hinzuzufügen bzw. aus diesem zu entfernen. Klicken Sie anschließend auf **Weiter**.
6. (Optional) Klicken Sie auf das Testnetzwerk, um ein anderes Testnetzwerk auf der Wiederherstellungs-Site auszuwählen, und klicken Sie anschließend auf **Weiter**.
7. Überprüfen Sie die zusammengefassten Informationen und klicken Sie auf **Beenden**, um die Änderungen in den Wiederherstellungsplan zu übernehmen.

   Sie können in der Ansicht „Kürzlich bearbeitete Aufgaben“ das Aktualisieren des Plans verfolgen.

Testen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan testen, führt Site Recovery Manager die virtuellen Maschinen des Wiederherstellungsplans in einem Testnetzwerk aus und erstellt einen temporären Snapshot der replizierten Daten an der Wiederherstellungs-Site. Site Recovery Manager unterbricht keine Vorgänge an der Schutz-Site.

Beim Testen eines Wiederherstellungsplans werden alle Schritte des Plans ausgeführt, abgesehen vom Herunterfahren der virtuellen Maschinen an der Schutz-Site und abgesehen davon, dass Geräte an der Wiederherstellungs-Site zwingend davon ausgehen, Master der replizierten Daten zu sein. Wenn der Plan das Anhalten von lokalen virtuellen Maschinen an der Wiederherstellungs-Site vorsieht, hält Site Recovery Manager diese virtuellen Maschinen während des Tests an. Durch das Testen eines Wiederherstellungsplans werden keine Änderungen an der Produktionsumgebung beider Sites vorgenommen.

Beim Testen des Wiederherstellungsplans wird auf der Wiederherstellungs-Site ein Snapshot aller Festplattendateien der virtuellen Maschinen im Wiederherstellungsplan erstellt. Das Erstellen der Snapshots erhöht die E/A-Latenz auf dem Speicher. Wenn Sie beim Testen der Wiederherstellungspläne langsamere Antwortzeiten bemerken und Sie den VMware Virtual SAN-Speicher verwenden, überwachen Sie die E/A-Latenz unter Verwendung des Überwachungs-Tools in der Virtual SAN-Schnittstelle.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Testen** aus.

   Sie können einen Test auch ausführen, indem Sie auf das Symbol **Wiederherstellungsplan testen** klicken, das sich in der Ansicht **Wiederherstellungsschritte** auf der Registerkarte **Überwachen** befindet.
3. (Optional) Wählen Sie **Neueste Änderungen an der Wiederherstellungs-Site replizieren**.

   Durch die Auswahl dieser Option wird sichergestellt, dass die Wiederherstellungs-Site über die neueste Kopie der geschützten virtuellen Maschinen verfügt. Jedoch kann die Synchronisierung länger dauern.
4. Klicken Sie auf **Weiter**.
5. Überprüfen Sie die Testinformationen und klicken Sie auf **Beenden**.
6. Klicken Sie auf der Registerkarte **Überwachen** auf **Wiederherstellungsschritte**, um den Testfortschritt zu überwachen und auf Meldungen zu reagieren.

   Auf der Registerkarte **Wiederherstellungsschritte** wird der Fortschritt der einzelnen Schritte angezeigt. Mit der Aufgabe „Testen“ in „Kürzlich bearbeitete Aufgaben“ wird der Gesamtfortschritt nachverfolgt.

   Hinweis Site Recovery Manager führt die Wiederherstellungsschritte in der vorgeschriebenen Reihenfolge aus. Es wird jedoch nicht darauf gewartet, bis der Schritt zum Vorbereiten des Speichers für alle Schutzgruppen beendet ist, bevor mit den nächsten Schritten fortgefahren wird.

Weiter

Führen Sie nach Abschluss des Tests des Wiederherstellungsplans eine Bereinigung durch, um den Wiederherstellungsplan auf den ursprünglichen Zustand vor dem Test zurückzusetzen.

Bereinigen nach dem Testen eines Wiederherstellungsplans

Nach dem Testen eines Wiederherstellungsplans können Sie den Wiederherstellungsplan wieder in den Status 'Bereit' versetzen, indem Sie einen Bereinigungsvorgang durchführen. Sie müssen den Bereinigungsvorgang abschließen, bevor Sie ein Failover oder einen anderen Test ausführen können.

Site Recovery Manager führt nach einem Test mehrere Bereinigungsvorgänge durch.

- Ausschalten der wiederhergestellten virtuellen Maschinen.

- Ersetzen der wiederhergestellten virtuellen Maschinen durch Platzhalter-VMs, wobei ihre Identität und Konfigurationsinformationen beibehalten werden.
- Bereinigen der replizierten Speicher-Snapshots, die von den wiederhergestellten virtuellen Maschinen während des Tests verwendet wurden.

Voraussetzungen

Vergewissern Sie sich, dass Sie einen Wiederherstellungsplan getestet haben.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Bereinigen** aus.

   Sie können die Bereinigung auch ausführen, indem Sie auf das Bereinigungssymbol klicken, das sich in der Ansicht **Wiederherstellungsschritte** auf der Registerkarte **Überwachen** befindet.
3. Überprüfen Sie die Bereinigungsinformationen und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Beenden**.
5. Falls nach Abschluss der Bereinigung Fehler gemeldet werden, führen Sie den Bereinigungsvorgang erneut aus, indem Sie die Option **Bereinigung erzwingen** wählen.

   Die Option **Bereinigung erzwingen** erzwingt das Entfernen von virtuellen Maschinen und ignoriert dabei alle Fehlermeldungen, um den Plan in den Zustand „Bereit“ zurückzusetzen. Führen Sie bei Bedarf die Bereinigung mit der Option **Bereinigung erzwingen** mehrfach aus, bis die Bereinigung erfolgreich verläuft.

Ausführen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan ausführen, migriert Site Recovery Manager alle virtuellen Maschinen im Wiederherstellungsplan auf die Wiederherstellungs-Site. Site Recovery Manager versucht, die entsprechenden virtuellen Maschinen auf der Schutz-Site herunterzufahren.

Vorsicht Ein Wiederherstellungsplan nimmt erhebliche Änderungen an den Konfigurationen der Schutz-Site und der Wiederherstellungs-Site vor und stoppt die Replizierung. Führen Sie keinen Wiederherstellungsplan aus, den Sie nicht getestet haben. Eine Rücknahme dieser Änderungen nimmt möglicherweise viel Zeit und Aufwand in Anspruch und kann zu längeren Dienstausfallzeiten führen.

Voraussetzungen

Um die erzwungene Wiederherstellung verwenden zu können, müssen Sie zuerst diese Funktion aktivieren. Sie aktivieren die erzwungene Wiederherstellung, indem Sie die Einstellung **recovery.forceRecovery** aktivieren, wie in Ändern von Wiederherstellungseinstellungen beschrieben.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.

2 Klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Ausführen** aus.

3 Überprüfen Sie die Informationen der Bestätigungseingabeaufforderung und wählen Sie **Mir ist bewusst, dass dieser Prozess die virtuellen Maschinen und die Infrastruktur sowohl des geschützten als auch des Wiederherstellungs-Datencenters dauerhaft verändert**.

4 Wählen Sie den Typ der Wiederherstellung aus, der ausgeführt werden soll.

Option	Beschreibung
Geplante Migration	Stellt virtuelle Maschinen auf der Wiederherstellungs-Site wieder her, wenn beide Sites ausgeführt werden. Wenn Fehler auf der Schutz-Site während einer geplanten Migration auftreten, schlägt der geplante Migrationsvorgang fehl.
Notfallwiederherstellung	Stellt virtuelle Maschinen auf der Wiederherstellungs-Site wieder her, wenn auf der Schutz-Site ein Problem aufgetreten ist. Falls während einer Notfallwiederherstellung Fehler auf der Schutz-Site auftreten, wird die Notfallwiederherstellung fortgesetzt und schlägt nicht fehl.

5 (Optional) Aktivieren Sie das Kontrollkästchen **Erzwungene Wiederherstellung – nur Vorgänge der Wiederherstellungs-Site**.

Diese Option ist verfügbar, wenn Sie die Funktion für die erzwungene Wiederherstellung aktiviert und **Notfallwiederherstellung** ausgewählt haben.

6 Klicken Sie auf **Weiter**.

7 Überprüfen Sie die Wiederherstellungsinformationen und klicken Sie auf **Beenden**.

8 Klicken Sie auf die Registerkarte **Überwachen** und auf **Wiederherstellungsschritte**.

Auf der Registerkarte **Wiederherstellungsschritte** wird der Fortschritt der einzelnen Schritte angezeigt. Im Bereich „Kürzlich bearbeitete Aufgaben“ wird der Gesamtfortschritt des Plans angezeigt.

Wiederherstellen eines Point-in-Time-Snapshots einer virtuellen Maschine

Mit vSphere Replication können Sie Point-in-Time-Snapshots von virtuellen Maschinen beibehalten. Sie können Site Recovery Manager so konfigurieren, dass mehrere Point-in-Time-Snapshots (PIT) einer virtuellen Maschine wiederhergestellt werden, wenn Sie einen Wiederherstellungsplan ausführen.

Sie konfigurieren die Beibehaltung von PIT-Snapshots bei der Konfiguration von vSphere Replication auf einer virtuellen Maschine. Weitere Informationen zu PIT-Snapshots finden Sie unter Replizieren einer virtuellen Maschine und Aktivieren mehrerer Zeitpunktinstanzen.

Um PIT-Snapshots zu aktivieren, konfigurieren Sie Replizierungen einer virtuellen Maschine über die vSphere Replication-Schnittstelle in vSphere Web Client.

Bei einer Wiederherstellung stellt Site Recovery Manager nur den neuesten der PIT-Snapshots wieder her. Um ältere Snapshots wiederherstellen zu können, müssen Sie die Option `vrReplication > preserveMpitImagesAsSnapshots` in „Erweiterte Einstellungen“ der Site Recovery Manager-Schnittstelle aktivieren. Wenn Sie einen PIT-Snapshot einer virtuellen Maschine wiederherstellen, für die Sie IP-Anpassung konfiguriert haben, übernimmt Site Recovery Manager die Anpassung nur für den neuesten PIT-Snapshot. Wenn Sie einen älteren PIT-Snapshot einer virtuellen Maschine mit IP-Anpassung wiederherstellen, müssen Sie die IP-Einstellungen manuell konfigurieren.

Point-in-Time-Wiederherstellung ist mit Array-basierter Replizierung nicht verfügbar.

Vorgehensweise

1. Konfigurieren Sie Site Recovery Manager, um ältere PIT-Snapshots beizubehalten, indem Sie die Option **vrReplication > preserveMpitImagesAsSnapshots** festlegen.
2. Verwenden Sie die vSphere Replication-Schnittstelle zum Konfigurieren der Replizierung einer virtuellen Maschine, indem Sie die Option zur Beibehaltung mehrerer PIT-Snapshots auswählen.
3. Fügen Sie auf der Site Recovery Manager-Schnittstelle die virtuelle Maschine zu einer vSphere Replication-Schutzgruppe hinzu.
4. Schließen Sie die vSphere Replication-Schutzgruppe in einen Wiederherstellungsplan ein.
5. Führen Sie den Wiederherstellungsplan aus.

   Wenn der Wiederherstellungsplan fertig gestellt ist, wird die virtuelle Maschine mit der Anzahl der PIT-Snapshots, die Sie konfiguriert haben, auf der Wiederherstellungs-Site wiederhergestellt.
6. Klicken Sie in der Ansicht **VMs und Vorlagen** mit der rechten Maustaste auf die wiederhergestellte virtuelle Maschine und wählen Sie **Snapshot > Snapshot-Manager**.
7. Wählen Sie einen PIT-Snapshot dieser virtuellen Maschine aus und klicken Sie auf **Wechseln zu**.

   Die wiederhergestellte virtuelle Maschine stellt den PIT-Snapshot wieder her, den Sie ausgewählt haben.
8. (Optional) Wenn Sie die virtuelle Maschine für IP-Anpassung konfiguriert haben und nicht den aktuellen, sondern einen älteren PIT-Snapshot auswählen, konfigurieren Sie die IP-Einstellungen auf der wiederhergestellten virtuellen Maschine manuell.

Abbrechen eines Tests oder einer Wiederherstellung

Sie können den Test eines Wiederherstellungsplans abbrechen, wenn er den Status „Test läuft“ oder „Failover wird durchgeführt“ aufweist.

Wenn Sie einen Test oder eine Wiederherstellung abbrechen, startet Site Recovery Manager keine neuen Prozesse. Prozesse, die bereits ausgeführt werden, werden unter Einhaltung bestimmter Regeln angehalten. Zum Abbrechen eines Failovers müssen Sie das Failover erneut ausführen.

- Prozesse, die nicht gestoppt werden können, wie z. B. das Einschalten oder das Warten auf ein Taktsignal, werden vollständig ausgeführt, bevor der ganze Vorgang abgebrochen wird.

- Prozesse, die dafür sorgen, dass Speichergeräte hinzugefügt oder entfernt werden, werden durch Bereinigungsvorgänge rückgängig gemacht, bevor der ganze Vorgang abgebrochen wird.

Wie lange es dauert, um einen Test oder eine Wiederherstellung abzubrechen, hängt von der Art und Anzahl der Prozesse ab, die derzeit ausgeführt werden.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Abbrechen** aus. Sie können den Plan auch über die Registerkarte „Wiederherstellungsschritte“ abbrechen.

Weiter

Führen Sie nach dem Abbrechen eines Tests eine Bereinigung aus.

Schritte zum Exportieren des Wiederherstellungsplans

Sie können die Schritte eines Wiederherstellungsplans in verschiedenen Formaten zur späteren Verwendung oder zum Aufbewahren einer Sicherungskopie Ihrer Pläne exportieren.

Während der Ausführung einer Testwiederherstellung bzw. echten Wiederherstellung können Sie die Schritte eines Wiederherstellungsplans nicht exportieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie über einen Wiederherstellungsplan verfügen.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Überwachen** auf **Wiederherstellungsschritte**.
3. Klicken Sie auf das Symbol **Schritte zum Exportieren des Wiederherstellungsplans**.

   Sie können die Schritte eines Wiederherstellungsplans als HTML-, XML-, CSV-, Microsoft Excel oder Microsoft Word-Dokument speichern.
4. Klicken Sie auf **Bericht erzeugen**.
5. Klicken Sie auf **Bericht herunterladen** und schließen Sie das Fenster.

Anzeigen und Exportieren des Verlaufs eines Wiederherstellungsplans

Sie können Berichte über jede Durchführung von Wiederherstellungsplänen, Überprüfung von Wiederherstellungsplänen oder Testbereinigungen anzeigen und exportieren.

Verläufe des Wiederherstellungsplans geben Informationen über jede Durchführung, jeden Test oder jede Bereinigung eines Wiederherstellungsplans an. Der Verlauf enthält Informationen über das Ergebnis, Start- und Endzeiten des gesamten Plans, sowie Informationen über jeden Schritt innerhalb des Plans. Sie können den Verlauf jederzeit exportieren, aber er enthält immer nur Einträge für abgeschlossene Vorgänge. Ist ein Vorgang noch in Bearbeitung, wird der Verlauf nach Abschluss des Vorgangs angezeigt.

SRM speichert den Verlauf für gelöschte Wiederherstellungspläne. Sie können Verlaufsberichte für vorhandene und gelöschte Pläne über **Site-Wiederherstellung > Sites** exportieren. Wählen Sie eine Site aus und klicken Sie auf die Registerkarte **Verlauf der Wiederherstellungspläne**.

Voraussetzungen

Sie haben einen Wiederherstellungsplan durchgeführt, überprüft oder eine Bereinigung nach einem Test durchgeführt.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Überwachen** auf **Verlauf**.
3. (Optional) Klicken Sie auf das Symbol „Exportieren“, um den Wiederherstellungsplanverlauf für einen bestimmten Zeitraum bzw. einen bestimmten Ausführ-, Test- oder Bereinigungsvorgang anzuzeigen.

   Sie können den Verlauf eines Wiederherstellungsplans als HTML-, XML-, CSV-, Microsoft Excel oder Microsoft Word-Dokument speichern.

Löschen eines Wiederherstellungsplans

Falls Sie einen Wiederherstellungsplan nicht mehr benötigen, können Sie ihn löschen.

Der Wiederherstellungsplan muss sich in einem konsistenten Zustand befinden, bevor Sie ihn löschen können.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. (Optional) Klicken Sie auf der Registerkarte **Überwachen** auf **Verlauf** und dann auf **Verlaufsbericht exportieren**, um den Verlauf des Plans herunterzuladen.

   Den Verlauf für gelöschte Pläne können Sie unter **Verlauf** anzeigen.

3 Klicken Sie mit der rechten Maustaste auf den zu löschenden Wiederherstellungsplan und wählen Sie **Wiederherstellungsplan löschen** aus.

Status des Wiederherstellungsplans – Referenz

Sie können den Status eines Wiederherstellungsplans überwachen und den für jeden Status zulässigen Vorgang bestimmen. Der Status eines Wiederherstellungsplans wird durch die Status der Schutzgruppen innerhalb des Wiederherstellungsplans bestimmt.

Tabelle 4-2. Wiederherstellungsstatus

Zustand	Beschreibung
Bereit	Wiederherstellungsschritte können ausgeführt werden.
Test läuft	Durch Abbrechen eines Tests wechselt der Plan in den Status „Abbruchvorgang läuft“.
Test abgeschlossen	Der Test wurde mit Fehlern oder ohne Fehler abgeschlossen.
Test unterbrochen	Der Server ist beim Ausführen eines Tests fehlgeschlagen.
Bereinigungsvorgang läuft	Nach der erfolgreichen Bereinigung wechselt der Wiederherstellungsplan in den Status „Bereit“. Wenn die Bereinigung unvollständig ist, wird in den Status „Bereinigung unvollständig“ gewechselt. Falls Sie die Option „Bereinigung erzwingen“ festlegen, wird nach einem Fehler in den Status „Bereit“ gewechselt. Falls bei der Bereinigung ein Fehler auftritt, wird in den Status „Bereinigung unvollständig“ gewechselt.
Bereinigung unvollständig	Bei der Bereinigung sind Fehler aufgetreten. Sie können die Bereinigung erneut ausführen. Wenn Sie die Bereinigung in diesem Status ausführen, zeigt der Bereinigungsassistent eine Option zum Ignorieren der Fehler an.
Bereinigung unterbrochen	Site Recovery Manager ist bei der Bereinigung fehlgeschlagen. Wiederherstellungsoptionen können nicht geändert werden.
Wiederherstellungsvorgang läuft	Wenn Sie die Wiederherstellung abbrechen, wird in den Status „Abbruchvorgang läuft“ gewechselt.
Notfallwiederherstellung abgeschlossen	Während der Wiederherstellung an der Schutz-Site sind beim Herunterfahren der VM Fehler aufgetreten. Dies ist möglicherweise darauf zurückzuführen, dass die Sites nicht verbunden waren (der Schritt vor Split-Brain). Eine Eingabeaufforderung des Systems warnt vor Split-Brain und fordert zum erneuten Ausführen der Wiederherstellung auf, wenn die Sites wieder verbunden sind. Wenn die Sites verbunden sind, wird in den Status „Wiederherstellung erforderlich“ (Split-Brain) gewechselt.

Tabelle 4-2. Wiederherstellungsstatus (Fortsetzung)

Zustand	Beschreibung
Wiederherstellung gestartet	Eine Wiederherstellung wurde auf der Peer-Site gestartet, aber wenn die Sites nicht verbunden sind, ist der genaue Status unbekannt. Melden Sie sich bei der Wiederherstellungs-Site an oder verbinden Sie die Sites erneut, um den aktuellen Status abzurufen.
Wiederherstellung erforderlich (Split-Brain)	Die Sites waren während der Wiederherstellung getrennt. Ein Split-Brain-Szenario wurde beim erneuten Verbinden der Sites festgestellt. Sie werden vom System aufgefordert, die Wiederherstellung erneut auszuführen, um die Sites zu synchronisieren.
Wiederherstellung abgeschlossen	Alle VMs wurden wiederhergestellt, jedoch mit Fehlern. Die Fehler werden durch die erneute Ausführung der Wiederherstellung nicht behoben. Der Wiederherstellungsplan wechselt in diesen Status, nachdem die Split-Brain-Wiederherstellung behoben wurde. Sie können die Wiederherstellungsschritte des letzten Wiederherstellungszyklus anzeigen.
Unvollständige Wiederherstellung	Die Wiederherstellung wurde abgebrochen oder es liegt ein Datenspeicherfehler vor. Führen Sie die Wiederherstellung erneut aus. Sie müssen entweder die Fehler beheben und die Wiederherstellung erneut ausführen oder aber den Schutz für fehlerhafte VMs entfernen. Der Wiederherstellungsplan erkennt die Behebung von Fehlern für beide Vorgehensweisen und aktualisiert den Status auf „Wiederherstellung abgeschlossen“.
Teilweise Wiederherstellung	Einige, aber nicht alle Schutzgruppen werden durch einen überlappenden Wiederherstellungsplan wiederhergestellt.
Wiederherstellung unterbrochen	Aufgrund eines Fehlers bei der Wiederherstellung wird die Wiederherstellung unterbrochen. Klicken Sie auf **Wiederherstellen**, um den Vorgang fortzusetzen. Wiederherstellungsoptionen können nicht geändert werden.
Abbruchvorgang läuft	Durch das Abbrechen eines Tests ergibt sich der Status „Test abgeschlossen“, wobei das letzte Ergebnis storniert wird. Durch das Abbrechen einer Wiederherstellung ergibt sich der Status „Unvollständige Wiederherstellung“, wobei das letzte Ergebnis storniert wird.
Neuer Schutz läuft	Falls der Server in diesem Status fehlschlägt, wird in den Status „Neuer Schutz unterbrochen“ gewechselt.
Teilweise neu geschützt	Der überlappende Wiederherstellungsplan wurde neu geschützt. Die bereits neu geschützten Gruppen wechseln in den Status „Bereit“, aber dies ist zulässig, da die anderen Gruppen den Status „Wiederhergestellt“ aufweisen.
Neuer Schutz unvollständig	Für das erneute Schützen wurden die Speichervorgänge nicht abgeschlossen. Die Sites müssen verbunden sein, damit das erneute Schützen erfolgreich ist.

Tabelle 4-2. Wiederherstellungsstatus (Fortsetzung)

Zustand	Beschreibung
Neuer Schutz unterbrochen	Falls Site Recovery Manager Server beim erneuten Schützen fehlschlägt, führen Sie die Funktion zum erneuten Schützen erneut aus, um den Vorgang fortzusetzen und den Status ordnungsgemäß zu bereinigen.
Auf Benutzereingabe warten während des Tests	Der Test wird unterbrochen. Schließen Sie die Eingabeaufforderung, um den Test fortzusetzen.
Auf Benutzereingabe warten während der Wiederherstellung	Die Wiederherstellung wird unterbrochen. Schließen Sie die Eingabeaufforderung, um die Wiederherstellung fortzusetzen.
Verwendete Schutzgruppen	Der Plan enthält Gruppen, die zu Testzwecken von einem anderen Plan verwendet werden. Dieser Status wird auch angezeigt, wenn der andere Wiederherstellungsplan einen Testvorgang für die Gruppen ausgeführt hat, aber die Bereinigung nicht ausgeführt hat. Warten Sie, bis der andere Plan den Test durchgeführt hat, oder bereinigen bzw. bearbeiten Sie den Plan, um die Gruppen zu entfernen.
Richtungsfehler	Die Gruppen weisen einen gemischten Status auf, was einem ungültigen Status entspricht. Einige Gruppen weisen den Status „Bereit“ in beide Richtungen auf: eine Site ist geschützt, und eine Site wird innerhalb einer bestimmte Gruppe wiederhergestellt. Entfernen Sie einige Schutzgruppen. Dieser Fehler ist darauf zurückzuführen, dass überlappende Wiederherstellungspläne ausgeführt wurden und alle Gruppen im Wiederherstellungsplan bereits erneut geschützt wurden.
Plan nicht synchronisiert	Dieser Status kann in folgenden Situationen auftreten: ■ Zwischen einer erfolgreichen Testwiederherstellung und einem Bereinigungsvorgang. Der Wiederherstellungsplan kann in diesem Status nicht bearbeitet werden. Führen Sie die Bereinigung aus, um den Wiederherstellungsplan wieder auf den Status „Bereit“ zurückzusetzen. Bearbeiten Sie den Wiederherstellungsplan, falls er im Status „Plan nicht synchronisiert“ verbleibt. ■ Sie können den Wiederherstellungsplan im regulären Betrieb bearbeiten. Durch das Öffnen des Wiederherstellungsplans zur Bearbeitung erzwingt Site Recovery Manager die Synchronisierung interner Daten von Site Recovery Manager zum Wiederherstellungsplan zwischen den Schutz- und Wiederherstellungsservern von Site Recovery Manager. Dadurch wird der Status „Plan nicht synchronisiert“ entfernt.

Tabelle 4-2. Wiederherstellungsstatus (Fortsetzung)

Zustand	Beschreibung
Keine Schutzgruppen	Der Wiederherstellungsplan enthält keine Schutzgruppen und kann nicht ausgeführt werden. Sie können leere Wiederherstellungspläne über die API oder durch Löschen der Schutzgruppen erstellen.
Interner Fehler	Eine Schutzgruppe mit einem unbekannten Status ist im Wiederherstellungsplan vorhanden, oder ein anderer unerwarteter Fehler ist aufgetreten. Sie können den Wiederherstellungsplan nicht ausführen, aber löschen.

Konfigurieren eines Wiederherstellungsplans

5

Sie können einen Wiederherstellungsplan so konfigurieren, dass er Befehle auf dem Site Recovery Manager Server oder auf einer virtuellen Maschine ausführt, Meldungen anzeigt, auf die reagiert werden muss, wenn der Plan ausgeführt wird, nicht unbedingt erforderliche virtuelle Maschinen während der Wiederherstellung anhält, Abhängigkeiten zwischen virtuellen Maschinen konfiguriert, VM-Netzwerkeinstellungen anpasst und die Wiederherstellungspriorität geschützter virtueller Maschinen ändert.

Ein einfacher Wiederherstellungsplan, bei dem nur ein Testnetzwerk, mit dem die wiederhergestellten virtuellen Maschinen eine Verbindung herstellen, und Zeitüberschreitungswerte für das Warten auf das Einschalten und die Anpassung der virtuellen Maschinen angegeben werden, bietet eine effektive Möglichkeit, eine Site Recovery Manager-Konfiguration zu testen. Die meisten Wiederherstellungspläne müssen für den Einsatz in Produktionsumgebungen konfiguriert werden. Ein Wiederherstellungsplan für einen Notfall auf der Schutz-Site unterscheidet sich möglicherweise von einem Wiederherstellungsplan für die geplante Migration von Diensten von einer auf eine andere Site.

Hinweis Ein Wiederherstellungsplan spiegelt immer den aktuellen Zustand der Schutzgruppen wider, die er wiederherstellt. Wenn eines der Mitglieder einer Schutzgruppe einen anderen Status als „OK“ aufweist, müssen Sie die Probleme beheben, bevor Sie Änderungen am Wiederherstellungsplan vornehmen können.

- Schritte für den Wiederherstellungsplan

  Ein Wiederherstellungsplan führt mehrere Schritte aus, die für einen bestimmten Workflow, z. B. eine geplante Migration oder einen Vorgang zum erneuten Schützen, in einer bestimmten Reihenfolge ausgeführt werden müssen. Sie können die Reihenfolge oder den Zweck der Schritte nicht ändern, aber Sie können Ihre eigenen Schritte einfügen, mit denen Meldungen angezeigt und Befehle ausgeführt werden können.

- Erstellen von benutzerdefinierten Wiederherstellungsschritten

  Sie können benutzerdefinierte Wiederherstellungsschritte erstellen, die Befehle ausführen oder während einer Wiederherstellung Meldungen für den Benutzer ausgeben.

- Anhalten virtueller Maschinen, wenn ein Wiederherstellungsplan ausgeführt wird

  Site Recovery Manager kann während einer Wiederherstellung und einer Testwiederherstellung virtuelle Maschinen auf der Wiederherstellungs-Site anhalten.

- Festlegen der Wiederherstellungspriorität einer virtuellen Maschine

  Standardmäßig legt Site Recovery Manager für alle virtuellen Maschinen in einem neuen Wiederherstellungsplan für die Wiederherstellung die Prioritätsstufe 3 fest. Sie können die Wiederherstellungspriorität einer virtuellen Maschine erhöhen oder herabsetzen. Die Wiederherstellungspriorität gibt die Reihenfolge des Herunterfahrens und des Einschaltens von virtuellen Maschinen vor.

- Konfigurieren der Abhängigkeiten virtueller Maschinen

  Wenn eine virtuelle Maschine auf Dienste angewiesen ist, die auf einer anderen virtuellen Maschine in derselben Schutzgruppe ausgeführt werden, können Sie eine Abhängigkeit zwischen den virtuellen Maschinen konfigurieren. Durch die Konfiguration einer Abhängigkeit können Sie sicherstellen, dass die virtuellen Maschinen in der richtigen Reihenfolge auf der Recovery-Site gestartet werden. Abhängigkeiten sind nur dann gültig, wenn die virtuellen Maschinen die gleiche Priorität haben.

- Konfigurieren der Optionen zum Starten und Herunterfahren von virtuellen Maschinen

  Sie können konfigurieren, wie während einer Wiederherstellung eine virtuelle Maschine auf der Wiederherstellungs-Site gestartet und heruntergefahren wird.

- Einschränkungen beim Schutz und der Wiederherstellung von virtuellen Maschinen

  Der Schutz und die Wiederherstellung von virtuellen Maschinen durch Site Recovery Manager unterliegt Beschränkungen.

Schritte für den Wiederherstellungsplan

Ein Wiederherstellungsplan führt mehrere Schritte aus, die für einen bestimmten Workflow, z. B. eine geplante Migration oder einen Vorgang zum erneuten Schützen, in einer bestimmten Reihenfolge ausgeführt werden müssen. Sie können die Reihenfolge oder den Zweck der Schritte nicht ändern, aber Sie können Ihre eigenen Schritte einfügen, mit denen Meldungen angezeigt und Befehle ausgeführt werden können.

Site Recovery Manager führt verschiedene Schritte im Wiederherstellungsplan auf unterschiedliche Art aus.

- Einige Schritte werden während aller Wiederherstellungen ausgeführt.
- Einige Schritte werden nur während Testwiederherstellungen ausgeführt.
- Einige Schritte werden während Testwiederherstellungen immer übersprungen.

Es ist wichtig, die Wiederherstellungsschritte, ihre Reihenfolge und den Kontext, in dem sie ausgeführt werden, zu verstehen, wenn Sie Anpassungen an einem Wiederherstellungsplan vornehmen.

Reihenfolge der Wiederherstellung

Wenn Sie einen Wiederherstellungsplan ausführen, beginnt er damit, die virtuellen Maschinen der Schutz-Site auszuschalten. Site Recovery Manager schaltet virtuelle Maschinen entsprechend der von Ihnen festgelegten Priorität aus, wobei die Maschinen mit hoher Priorität zuletzt ausgeschaltet werden. Site Recovery Manager lässt diesen Schritt aus, wenn Sie einen Wiederherstellungsplan testen.

Site Recovery Manager schaltet Gruppen von virtuellen Maschinen auf der Wiederherstellungs-Site entsprechend der von Ihnen festgelegten Priorität ein. Bevor eine Prioritätsgruppe startet, müssen alle virtuellen Maschinen der nächst höheren Prioritätsgruppe wiederhergestellt werden oder ihre Wiederherstellung muss fehlschlagen. Falls es Abhängigkeiten zwischen den virtuellen Maschinen in derselben Prioritätsgruppe gibt, schaltet, Site Recovery Manager zuerst die virtuellen Maschinen ein, von denen andere virtuelle Maschinen abhängen. Falls Site Recovery Manager die Abhängigkeiten virtueller Maschinen erfüllt, versucht Site Recovery Manager, so viele virtuelle Maschinen parallel einzuschalten, wie dies von vCenter Server unterstützt wird.

Zeitüberschreitung und Pausen des Wiederherstellungsplans

Während der Ausführung der Schritte eines Wiederherstellungsplans können verschiedene Arten von Zeitüberschreitungen auftreten. Zeitüberschreitungen führen zu einer Unterbrechung des Plans für ein festgelegtes Zeitintervall, um den Abschluss eines Schrittes abzuwarten.

Meldungsschritte sorgen dafür, dass der Plan so lange unterbrochen wird, bis der Benutzer die Meldung bestätigt hat. Bevor Sie einen Meldungsschritt zu einem Wiederherstellungsplan hinzufügen, sollten Sie sicherstellen, dass er wirklich erforderlich ist. Bevor Sie einen Wiederherstellungsplan testen oder ausführen, der Meldungsschritte enthält, stellen Sie sicher, dass ein Benutzer den Fortschritt des Plans überwachen und bei Bedarf auf Meldungen antworten kann.

Erstellen von benutzerdefinierten Wiederherstellungsschritten

Sie können benutzerdefinierte Wiederherstellungsschritte erstellen, die Befehle ausführen oder während einer Wiederherstellung Meldungen für den Benutzer ausgeben.

Site Recovery Manager kann benutzerdefinierte Schritte entweder auf dem
Site Recovery Manager Server oder in einer virtuellen Maschine ausführen, die Teil des Wiederherstellungsplans ist. Sie können keine benutzerdefinierten Schritte auf virtuellen Maschinen ausführen, die angehalten werden sollen.

Während des erneuten Schützens behält Site Recovery Manager alle benutzerdefinierten Wiederherstellungsschritte im Wiederherstellungsplan bei. Wenn Sie nach dem erneuten Schützen eine Wiederherstellung oder einen Test durchführen, werden benutzerdefinierte Wiederherstellungsschritte auf der neuen Wiederherstellungs-Site (der ursprünglichen Schutz-Site) ausgeführt.

Nach dem erneuten Schützen können Sie in der Regel benutzerdefinierte Wiederherstellungsschritte verwenden, die Meldungen ohne Änderungen direkt anzeigen. Nach dem erneuten Schützen müssen Sie möglicherweise einige benutzerdefinierte Wiederherstellungsschritte ändern, wenn diese Schritte Befehle ausführen, die Site-spezifische Informationen enthalten, wie z. B. Netzwerkkonfigurationen.

- Typen von benutzerdefinierten Wiederherstellungsschritten

  Sie können verschiedene Typen von benutzerdefinierten Wiederherstellungsschritten erstellen, um sie in Wiederherstellungspläne aufzunehmen.

- Wie Site Recovery Manager mit Fehlschlägen bei benutzerdefinierten Wiederherstellungsschritten umgeht

  Je nach Art des Wiederherstellungsschritts behandelt Site Recovery Manager Fehlschläge bei benutzerdefinierten Wiederherstellungsschritten unterschiedlich.

- Erstellen von Meldungsaufforderungen oder Befehlsschritten der obersten Ebene

  Sie können Wiederherstellungsschritte der obersten Ebene überall im Wiederherstellungsplan hinzufügen. Bei Befehlsschritten der obersten Ebene handelt es sich um Befehle oder Skripts, die Sie während einer Wiederherstellung auf Site Recovery Manager Server ausführen. Sie können auch Schritte zum Anzeigen von Meldungsaufforderungen hinzufügen, die ein Benutzer während einer Wiederherstellung bestätigen muss.

- Erstellen von Meldungsaufforderungen oder Befehlsschritten für einzelne virtuelle Maschinen

  Sie können benutzerdefinierte Wiederherstellungsschritte erstellen, um Benutzer aufzufordern, Aufgaben durchzuführen, oder dafür zu sorgen, dass Site Recovery Manager Aufgaben für eine virtuelle Maschine vor und nach dem Einschalten durch Site Recovery Manager durchführt.

- Richtlinien zum Schreiben von Befehlsschritten

  Alle Stapeldateien oder -befehle für benutzerdefinierte Wiederherstellungsschritte, die Sie zu einem Wiederherstellungsplan hinzufügen, müssen bestimmte Anforderungen erfüllen.

- Umgebungsvariablen für Befehlsschritte

  Site Recovery Manager stellt Umgebungsvariablen zur Verfügung, die Sie in Befehlen für benutzerdefinierte Wiederherstellungsschritte verwenden können.

Typen von benutzerdefinierten Wiederherstellungsschritten

Sie können verschiedene Typen von benutzerdefinierten Wiederherstellungsschritten erstellen, um sie in Wiederherstellungspläne aufzunehmen.

Benutzerdefinierte Wiederherstellungsschritte sind entweder Befehls-Wiederherstellungsschritte oder Meldungsaufforderungsschritte.

Befehls-Wiederherstellungsschritte

Befehls-Wiederherstellungsschritte enthalten entweder Befehle der obersten Ebene oder Befehle pro virtueller Maschine.

Befehle der obersten Ebene	Diese werden auf dem Site Recovery Manager Server ausgeführt. Sie können beispielsweise diese Befehle zum Einschalten physischer Geräte oder zum Umleiten des Netzwerkdatenverkehrs verwenden.
Befehle pro virtueller Maschine	Site Recovery Manager verknüpft Befehle pro virtueller Maschine mit den neu wiederhergestellten virtuellen Maschinen während des Wiederherstellungsvorgangs. Sie können diese Befehle verwenden, um nach dem Einschalten einer virtuellen Maschine Konfigurationsaufgaben durchzuführen. Sie können diese Befehle entweder vor oder nach dem Einschalten einer virtuellen Maschine ausführen. Befehle, die Sie so konfigurieren, dass sie

nach dem Einschalten der virtuellen Maschine ausgeführt werden, können entweder auf dem Site Recovery Manager Server oder in der neu wiederhergestellten virtuellen Maschine ausgeführt werden. Befehle, die auf der neu wiederhergestellten virtuellen Maschine ausgeführt werden, werden im Kontext des Benutzerkontos ausgeführt, das VMware Tools für die wiederhergestellte virtuelle Maschine verwendet. Je nach Funktion des Befehls, den Sie schreiben, müssen Sie möglicherweise das Benutzerkonto, das von VMware Tools auf der wiederhergestellten virtuellen Maschine verwendet wird, ändern.

Wiederherstellungsschritte mit Eingabeaufforderungen

Zeigen Sie während der Wiederherstellung eine Meldung auf der Site Recovery Manager-Benutzeroberfläche an. Sie können diese Meldung verwenden, um die Wiederherstellung zu unterbrechen und dem Benutzer, der den Wiederherstellungsplan ausführt, Informationen zur Verfügung zu stellen. Die Meldung kann beispielsweise die Benutzer anweisen, eine manuelle Wiederherstellungsaufgabe durchzuführen oder Schritte zu überprüfen. Die einzige Aktion, die Benutzer als direkte Reaktion auf eine Aufforderung unternehmen können, ist, die Meldung auszublenden. Dies ermöglicht ein Fortsetzen der Wiederherstellung.

Wie Site Recovery Manager mit Fehlschlägen bei benutzerdefinierten Wiederherstellungsschritten umgeht

Je nach Art des Wiederherstellungsschritts behandelt Site Recovery Manager Fehlschläge bei benutzerdefinierten Wiederherstellungsschritten unterschiedlich.

Site Recovery Manager versucht, alle benutzerdefinierten Wiederherstellungsschritte durchzuführen, aber manche Befehls-Wiederherstellungsschritte werden möglicherweise nicht beendet.

Befehls-Wiederherstellungsschritte

Standardmäßig wartet Site Recovery Manager 5 Minuten auf den Abschluss von Befehls-Wiederherstellungsschritten. Sie können den Zeitüberschreitungswert für jeden Befehl konfigurieren. Wenn ein Befehl innerhalb dieses Zeitlimits abgeschlossen wurde, wird der nächste Wiederherstellungsschritt im Wiederherstellungsplan ausgeführt. Wie Site Recovery Manager Fehlschläge bei benutzerdefinierten Befehlen handhabt, hängt vom Befehlstyp ab.

Befehlstyp	Beschreibung
Befehle der obersten Ebene	Falls ein Wiederherstellungsschritt fehlschlägt, protokolliert Site Recovery Manager den Fehler und zeigt eine Warnung auf der Registerkarte **Wiederherstellungsschritte** an. Die nachfolgenden benutzerdefinierten Wiederherstellungsschritte werden weiterhin ausgeführt.
Befehle pro virtueller Maschine	Diese werden stapelweise entweder vor oder nach dem Einschalten einer virtuellen Maschine ausgeführt. Falls ein Befehl fehlschlägt, werden die verbleibenden, im Stapel befindlichen Befehle pro virtueller Maschine nicht ausgeführt. Wenn Sie beispielsweise fünf Befehle hinzufügen, die vor dem Einschalten der virtuellen Maschine ausgeführt werden sollen, und fünf weitere Befehle, die nach dem Einschalten der virtuellen Maschine ausgeführt werden sollen, und der dritte Befehl des Stapels, der vor dem Einschalten ausgeführt werden soll, fehlschlägt, werden die verbleibenden zwei Befehle, die vor dem Einschalten ausgeführt werden sollen, nicht ausgeführt. Site Recovery Manager schaltet die virtuelle Maschine nicht ein und kann daher keine Befehle nach dem Einschalten ausführen.

Wiederherstellungsschritte mit Eingabeaufforderungen

Benutzerdefinierte Wiederherstellungsschritte mit Eingabeaufforderungen können nicht fehlschlagen. Der Wiederherstellungsplan wird so lange angehalten, bis der Benutzer die Eingabeaufforderung durch Klicken auf „OK“ ausblendet.

Erstellen von Meldungsaufforderungen oder Befehlsschritten der obersten Ebene

Sie können Wiederherstellungsschritte der obersten Ebene überall im Wiederherstellungsplan hinzufügen. Bei Befehlsschritten der obersten Ebene handelt es sich um Befehle oder Skripts, die Sie während einer Wiederherstellung auf Site Recovery Manager Server ausführen. Sie können auch Schritte zum Anzeigen von Meldungsaufforderungen hinzufügen, die ein Benutzer während einer Wiederherstellung bestätigen muss.

Voraussetzungen

- Sie haben einen Wiederherstellungsplan, dem benutzerdefinierte Schritte hinzugefügt werden sollen.
- Weitere Informationen über das Schreiben von Befehlen, die zu Befehlsschritten hinzugefügt werden, finden Sie unter Richtlinien zum Schreiben von Befehlsschritten und Umgebungsvariablen für Befehlsschritte.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Überwachen** auf **Wiederherstellungsschritte**.

3 Verwenden Sie das Dropdown-Menü **Anzeigen**, um den Typ des Wiederherstellungsplans auszuwählen, dem Sie einen Schritt hinzufügen möchten.

Option	Beschreibung
Testschritte	Fügt einen auszuführenden Schritt für das Testen eines Wiederherstellungsplans hinzu.
Wiederherstellungsschritte	Fügt einen auszuführenden Schritt für die Durchführung einer geplanten Migration oder einer Notfallwiederherstellung hinzu.

Sie können in den Bereinigungsvorgängen oder den Vorgängen zum erneuten Schützen keine Schritte hinzufügen.

4 Klicken Sie mit der rechten Maustaste auf einen Schritt davor oder danach, um einen benutzerdefinierten Schritt hinzuzufügen, und wählen Sie **Schritt hinzufügen**.

5 Wählen Sie **Befehl auf SRM-Server** oder **Eingabeaufforderung**.

6 Geben Sie im Textfeld **Name** einen Namen für den Schritt ein.

Der Name des Schritts erscheint in der Liste der Schritte in der Ansicht **Schritte wiederherstellen**.

7 Geben Sie in das Textfeld **Inhalt** die Befehle ein, die bei diesem Schritt ausgeführt werden sollen.

- Wenn Sie **Befehl auf SRM-Server** ausgewählt haben, geben Sie den auszuführenden Befehl bzw. das auszuführende Skript ein.
- Wenn Sie **Eingabeaufforderung** ausgewählt haben, geben Sie den Text der Meldung ein, die während der Ausführung des Wiederherstellungsplans angezeigt werden soll.

8 (Optional) Passen Sie die Einstellung der **Zeitüberschreitung** für den Befehl an, der auf Site Recovery Manager Server ausgeführt werden soll.

Diese Option ist nicht verfügbar, wenn Sie einen Eingabeaufforderungsschritt erstellen.

9 Wählen Sie, wo in der Schrittfolge der neue Schritt eingefügt werden soll.

- **Vor ausgewähltem Schritt**
- **Nach ausgewähltem Schritt**

10 Klicken Sie auf **OK**, um den Schritt zum Wiederherstellungsplan hinzuzufügen.

Erstellen von Meldungsaufforderungen oder Befehlsschritten für einzelne virtuelle Maschinen

Sie können benutzerdefinierte Wiederherstellungsschritte erstellen, um Benutzer aufzufordern, Aufgaben durchzuführen, oder dafür zu sorgen, dass Site Recovery Manager Aufgaben für eine virtuelle Maschine vor und nach dem Einschalten durch Site Recovery Manager durchführt.

Site Recovery Manager ordnet einer geschützten oder wiederhergestellten virtuellen Maschine Befehlsschritte in der gleichen Art und Weise wie Anpassungsinformationen zu. Wenn mehrere Wiederherstellungspläne dieselbe virtuelle Maschine enthalten, nimmt Site Recovery Manager die Befehle und Eingabeaufforderungen in alle Wiederherstellungspläne auf.

Voraussetzungen

- Sie haben einen Wiederherstellungsplan, dem benutzerdefinierte Schritte hinzugefügt werden sollen.
- Weitere Informationen über das Schreiben von Befehlen, die zu Befehlsschritten hinzugefügt werden, finden Sie unter Richtlinien zum Schreiben von Befehlsschritten und Umgebungsvariablen für Befehlsschritte.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
3. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und klicken Sie auf **Wiederherstellung konfigurieren**.
4. Klicken Sie auf der Registerkarte **Eigenschaften für die Wiederherstellung** auf **Pre-Power-On-Schritte** bzw. **Post-Power-On-Schritte**.
5. Klicken Sie auf das Pluszeichen, um einen Schritt hinzuzufügen.
6. Wählen Sie den Typ des zu erstellenden Schritts aus.

Option	Beschreibung
Eingabeaufforderung	Fordert den Benutzer auf, eine Aufgabe durchzuführen oder Informationen anzugeben, die er bestätigen muss, bevor der Plan den nächsten Schritt ausführt. Diese Option ist verfügbar sowohl für Pre-Power-On-Schritte als auch für Post-Power-On-Schritte.
Befehl auf SRM-Server	Führt einen Befehl auf Site Recovery Manager Server aus. Diese Option ist verfügbar sowohl für Pre-Power-On-Schritte als auch für Post-Power-On-Schritte.
Befehl auf wiederhergestellter VM	Führt einen Befehl auf der wiederhergestellten virtuellen Maschine aus. Diese Option steht nur für Post-Power-On-Schritte zur Verfügung.

7. Geben Sie im Textfeld **Name** einen Namen für den Schritt ein.

   Der Name des Schritts erscheint in der Liste der Schritte in der Ansicht **Schritte wiederherstellen**.
8. Geben Sie in das Textfeld **Inhalt** die Befehle ein, die bei diesem Schritt ausgeführt werden sollen.
   - Wenn Sie **Befehl auf SRM-Server** oder **Befehl auf wiederhergestellter VM** gewählt haben, geben Sie den auszuführenden Befehl bzw. das auszuführende Skript an.
   - Wenn Sie **Eingabeaufforderung** ausgewählt haben, geben Sie den Text der Meldung ein, die während der Ausführung des Wiederherstellungsplans angezeigt werden soll.
9. (Optional) Passen Sie die Einstellung der **Zeitüberschreitung** für den Befehl an, der auf Site Recovery Manager Server ausgeführt werden soll.

   Diese Option ist nicht verfügbar, wenn Sie einen Eingabeaufforderungsschritt erstellen.
10. Klicken Sie auf **OK**, um den Schritt zum Wiederherstellungsplan hinzuzufügen.

11 Klicken Sie auf **OK**, um die virtuelle Maschine so neu zu konfigurieren, dass der Befehl vor oder nach dem Einschalten der virtuellen Maschine ausgeführt wird.

Richtlinien zum Schreiben von Befehlsschritten

Alle Stapeldateien oder -befehle für benutzerdefinierte Wiederherstellungsschritte, die Sie zu einem Wiederherstellungsplan hinzufügen, müssen bestimmte Anforderungen erfüllen.

Wenn Sie einen Befehlsschritt erstellen, um ihn zu einem Wiederherstellungsplan hinzuzufügen, stellen Sie sicher, dass er die Umgebung berücksichtigt, in der er ausgeführt werden muss. Fehler in einem Befehlsschritt beeinträchtigen die Integrität eines Wiederherstellungsplans. Testen Sie den Befehl auf dem Site Recovery Manager Server der Wiederherstellungs-Site, bevor Sie ihn zum Plan hinzufügen.

- Sie müssen die Windows-Befehlsshell mit dem vollständigen Pfad auf dem lokalen Host starten. Verwenden Sie z. B. zur Ausführung eines Skripts, das sich in `c:\alarmscript.bat` befindet, die folgende Befehlszeile:

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

- Sie müssen Stapeldateien und Befehle auf dem Site Recovery Manager Server der Wiederherstellungs-Site installieren.
- Stapeldateien und -befehle müssen innerhalb von 300 Sekunden abgeschlossen werden. Anderenfalls wird der Wiederherstellungsplan mit einem Fehler beendet. Zur Änderung dieses Grenzwerts lesen Sie Ändern von Wiederherstellungseinstellungen.
- Stapeldateien oder -befehle, die Ausgaben generieren, die Zeichen mit ASCII-Werten größer als 127 enthalten, müssen die UTF-8-Codierung verwenden. Site Recovery Manager zeichnet nur die letzten 4 KB der Skriptausgabe in Protokolldateien und im Wiederherstellungsverlauf auf. Skripts, die mehr Ausgabe generieren, sollten die Ausgabe in eine Datei umleiten, anstatt sie zur Protokollierung an die Standardausgabe zu senden.

Umgebungsvariablen für Befehlsschritte

Site Recovery Manager stellt Umgebungsvariablen zur Verfügung, die Sie in Befehlen für benutzerdefinierte Wiederherstellungsschritte verwenden können.

Befehlsschritte werden unter der Identität des Kontos „LocalSystem“ auf dem
Site Recovery Manager Server-Host der Wiederherstellungs-Site ausgeführt. Wenn ein Befehlsschritt ausgeführt wird, stellt Site Recovery Manager Umgebungsvariablen zur Verfügung, die bei dem Schritt verwendet werden können.

Tabelle 5-1. Umgebungsvariablen, die allen Befehlsschritten zur Verfügung stehen

Name	Wert	Beispiel
VMware_RecoveryName	Name des Wiederherstellungsplans, der gerade ausgeführt wird.	Plan A
VMware_RecoveryMode	Wiederherstellungsmodus	Test oder Wiederherstellung

Tabelle 5-1. Umgebungsvariablen, die allen Befehlsschritten zur Verfügung stehen (Fortsetzung)

Name	Wert	Beispiel
VMware_VC_Host	Hostname von vCenter Server auf der Wiederherstellungs-Site.	vc_hostname.example.com
VMware_VC_Port	Netzwerkport, der zum Kontaktieren von vCenter Server verwendet wird.	443

Site Recovery Manager stellt zusätzliche Umgebungsvariablen für Befehlsschritte pro virtueller Maschine zur Verfügung, die entweder auf dem Site Recovery Manager Server oder auf der wiederhergestellten virtuellen Maschine ausgeführt werden.

Tabelle 5-2. Umgebungsvariablen, die Befehlsschritten pro virtueller Maschine zur Verfügung stehen

Name	Wert	Beispiel
VMware_VM_Uuid	Von vCenter verwendete UUID zur eindeutigen Identifizierung dieser virtuellen Maschine.	4212145a-eeae-a02c-e525-ebba70b0d4f3
VMware_VM_Name	Name dieser virtuellen Maschine, wie auf der Schutz-Site festgelegt.	Meine neue virtuelle Maschine
VMware_VM_Ref	ID des verwalteten Objekts der virtuellen Maschine.	vm-1199
*VMware_VM-Gast*Name	Name des Gastbetriebssystems, wie von der VIM-API festgelegt.	andererGast
*VMware_VM-Gast*Ip	IP-Adresse der virtuellen Maschine, falls bekannt.	192.168.0.103
VMware_VM-Pfad	Pfad der VMDK-Datei dieser virtuellen Maschine.	`[datastore-123] jquser-vm2/jquser-vm2.vmdk`

Anhalten virtueller Maschinen, wenn ein Wiederherstellungsplan ausgeführt wird

Site Recovery Manager kann während einer Wiederherstellung und einer Testwiederherstellung virtuelle Maschinen auf der Wiederherstellungs-Site anhalten.

Das Anhalten virtueller Maschinen an der Wiederherstellungs-Site ist nützlich in aktiv/aktiv-Datencenterumgebungen sowie dort, wo nicht kritische Arbeitslasten auf Wiederherstellungs-Sites ausgeführt werden. Durch das Anhalten von virtuellen Maschinen, die nicht kritische Arbeitslasten an der Wiederherstellungs-Site hosten, gibt Site Recovery Manager Kapazitäten für die wiederhergestellten virtuellen Maschinen frei. Site Recovery Manager setzt die Ausführung von virtuellen Maschinen fort, die während eines Failover-Vorgangs angehalten wurden, wenn das Failover in die umgekehrte Richtung ausgeführt wird.

Sie können nur virtuelle Maschinen hinzufügen, die an der Wiederherstellungs-Site angehalten werden sollen.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Überwachen** auf **Wiederherstellungsschritte**.
3. Klicken Sie mit der rechten Maustaste auf **Nicht kritische VMs auf der Wiederherstellungs-Site anhalten** und wählen Sie **Nicht kritische VM hinzufügen**.
4. Wählen Sie die virtuellen Maschinen auf der Wiederherstellungs-Site aus, die während einer Wiederherstellung angehalten werden sollen.
5. Klicken Sie auf **OK**.

Site Recovery Manager hält die virtuellen Maschinen auf der Wiederherstellungs-Site an, wenn der Wiederherstellungsplan ausgeführt wird.

Festlegen der Wiederherstellungspriorität einer virtuellen Maschine

Standardmäßig legt Site Recovery Manager für alle virtuellen Maschinen in einem neuen Wiederherstellungsplan für die Wiederherstellung die Prioritätsstufe 3 fest. Sie können die Wiederherstellungspriorität einer virtuellen Maschine erhöhen oder herabsetzen. Die Wiederherstellungspriorität gibt die Reihenfolge des Herunterfahrens und des Einschaltens von virtuellen Maschinen vor.

Wenn Sie die Priorität einer virtuellen Maschine ändern, wendet Site Recovery Manager die neue Priorität auf alle Wiederherstellungspläne an, in denen diese virtuelle Maschine enthalten ist.

Site Recovery Manager startet virtuelle Maschinen auf der Wiederherstellungs-Site entsprechend der Priorität, die Sie festgelegt haben. Site Recovery Manager startet zuerst virtuelle Maschinen mit Priorität 1, dann virtuelle Maschinen mit Priorität 2 usw. Site Recovery Manager erkennt anhand des Taktsignalstatus von VMware Tools, wenn eine virtuelle Maschine auf der Wiederherstellungs-Site ausgeführt wird. Auf diese Weise kann Site Recovery Manager sicherstellen, dass alle virtuellen Maschinen einer bestimmten Priorität ausgeführt werden, bevor die virtuellen Maschinen der nächsten Priorität gestartet werden. Aus diesem Grund müssen Sie VMware Tools auf geschützten virtuellen Maschinen installieren.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
3. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Alle Prioritätsaktionen** aus.
4. Wählen Sie eine neue Priorität für die virtuelle Maschine aus.

   Die höchste Priorität ist 1. Die niedrigste Priorität ist 5.
5. Klicken Sie auf **Ja** und bestätigen Sie die Änderung der Priorität.

Konfigurieren der Abhängigkeiten virtueller Maschinen

Wenn eine virtuelle Maschine auf Dienste angewiesen ist, die auf einer anderen virtuellen Maschine in derselben Schutzgruppe ausgeführt werden, können Sie eine Abhängigkeit zwischen den virtuellen Maschinen konfigurieren. Durch die Konfiguration einer Abhängigkeit können Sie sicherstellen, dass die virtuellen Maschinen in der richtigen Reihenfolge auf der Recovery-Site gestartet werden. Abhängigkeiten sind nur dann gültig, wenn die virtuellen Maschinen die gleiche Priorität haben.

Wenn ein Wiederherstellungsplan ausgeführt wird, startet Site Recovery Manager die virtuellen Maschinen, auf die andere virtuelle Maschinen angewiesen sind, bevor er die virtuellen Maschinen mit den Abhängigkeiten startet. Falls Site Recovery Manager eine virtuelle Maschine nicht starten kann, auf die eine andere virtuelle Maschine angewiesen ist, wird der Wiederherstellungsplan weiterhin ausgeführt und eine Warnmeldung generiert. Sie können Abhängigkeiten nur zwischen virtuellen Maschinen konfigurieren, die sich in derselben Wiederherstellungsprioritätsgruppe befinden. Wenn Sie eine virtuelle Maschine so konfigurieren, dass sie auf eine virtuellen Maschine in einer niedrigeren Prioritätsgruppe angewiesen ist, überschreibt Site Recovery Manager die Abhängigkeit und startet zuerst die virtuelle Maschine in der höheren Prioritätsgruppe.

Wenn Sie eine Schutzgruppe, die die abhängige virtuelle Maschine enthält, aus dem Wiederherstellungsplan entfernen, wird der Status der Schutzgruppe in den Abhängigkeiten für die virtuelle Maschine mit der Abhängigkeit auf `Nicht in diesem Plan` gesetzt. Wenn die konfigurierte virtuelle Maschine eine andere Priorität als die virtuelle Maschine hat, auf die sie angewiesen ist, wird der Status der abhängigen virtuellen Maschine auf „Niedrigere Priorität“ oder „Höhere Priorität“ gesetzt.

Voraussetzungen

- Stellen Sie sicher, dass sich die virtuelle Maschine mit der Abhängigkeit und die virtuelle Maschine, auf die sie angewiesen ist, in demselben Wiederherstellungsplan befinden.
- Stellen Sie sicher, dass sich die virtuelle Maschine mit der Abhängigkeit und die virtuellen Maschin, auf die sie angewiesen ist, in derselben Wiederherstellungsprioritätsgruppe befinden.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
3. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine, die auf eine oder mehrere andere virtuelle Maschinen angewiesen ist, und wählen Sie **Wiederherstellung konfigurieren**.
4. Erweitern Sie **VM-Abhängigkeiten**.
5. Stellen Sie sicher, dass die virtuellen Maschinen, auf die diese virtuelle Maschine angewiesen ist, eingeschaltet sind und der Status der Abhängigkeiten „OK“ ist.
6. (Optional) Um eine Abhängigkeit zu entfernen, wählen Sie eine virtuelle Maschine aus der Liste der virtuellen Maschinen aus, auf die diese virtuelle Maschine angewiesen ist, und klicken Sie auf **Entfernen**.

7 Klicken Sie auf **OK**.

Konfigurieren der Optionen zum Starten und Herunterfahren von virtuellen Maschinen

Sie können konfigurieren, wie während einer Wiederherstellung eine virtuelle Maschine auf der Wiederherstellungs-Site gestartet und heruntergefahren wird.

Sie können konfigurieren, ob das Gastbetriebssystem einer virtuellen Maschine heruntergefahren wird, bevor sie auf der Wiederherstellungs-Site ausgeschaltet wird. Sie können konfigurieren, ob eine virtuelle Maschine auf der Wiederherstellungs-Site eingeschaltet wird. Sie können auch Verzögerungen nach dem Einschalten einer virtuellen Maschine konfigurieren, um VMware Tools oder anderen Anwendungen zu ermöglichen, auf der wiederhergestellten virtuellen Maschine zu starten, bevor der Wiederherstellungsplan weiter ausgeführt wird.

Voraussetzungen

Sie haben einen Wiederherstellungsplan erstellt.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.

2 Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.

3 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Wiederherstellung konfigurieren**.

4 Erweitern Sie **Aktion beim Herunterfahren** und wählen Sie für diese virtuelle Maschine die Methode zum Herunterfahren.

Option	Beschreibung
Gastbetriebssystem vor dem Ausschalten herunterfahren	Fährt die virtuelle Maschine ordnungsgemäß herunter, bevor sie ausgeschaltet wird. Sie können einen Zeitüberschreitungswert für das Herunterfahren festlegen. Das Setzen des Zeitüberschreitungswerts auf 0 ist gleichbedeutend mit der Option „Ausschalten“. Diese Option setzt voraus, dass auf der virtuellen Maschine VMware Tools ausgeführt wird. **Hinweis** Die virtuelle Maschine wird nach Ablauf der Zeitüberschreitung ausgeschaltet. Wenn das Betriebssystem der virtuellen Maschine die Aufgaben für das Herunterfahren zum Zeitpunkt der Zeitüberschreitung nicht abgeschlossen hat, gehen möglicherweise Daten verloren. Stellen Sie für eine große virtuelle Maschine, die für das ordnungsgemäße Herunterfahren viel Zeit beansprucht, eine Zeitüberschreitung bis zum Ausschalten von angemessener Länge ein.
Ausschalten	Schaltet die virtuelle Maschine aus, ohne das Gastbetriebssystem herunterzufahren.

5 Erweitern Sie **Startaktion** und wählen Sie, ob nach einer Wiederherstellung die virtuelle Maschine eingeschaltet werden soll.

Option	Beschreibung
Einschalten	Schaltet die virtuelle Maschine auf der Wiederherstellungs-Site ein.
Nicht einschalten	Stellt die virtuelle Maschine wieder her, schaltet sie jedoch nicht ein.

6 (Optional) Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Auf VMware Tools warten**.

Diese Option ist nur dann verfügbar, wenn Sie **Einschalten** in Schritt 5 ausgewählt haben.

Wenn Sie **Auf VMware Tools warten** auswählen, wartet Site Recovery Manager, bis nach dem Einschalten der virtuellen Maschine VMware Tools gestartet wurde, bevor der Wiederherstellungsplan zum nächsten Schritt geht. Sie können ein Zeitlimit für das Starten von VMware Tools festlegen.

7 (Optional) Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Zusätzliche Verzögerung, bevor die Post-Power-On-Schritte ausgeführt und abhängige VMs gestartet werden** und geben Sie die Dauer der zusätzlichen Verzögerung an.

Diese Option ist nur dann verfügbar, wenn Sie **Einschalten** in Schritt 5 ausgewählt haben.

Sie könnten beispielsweise eine zusätzliche Verzögerung für die Zeit nach dem Einschalten einer virtuellen Maschine angeben, damit Anwendungen, auf die eine andere virtuelle Maschine angewiesen ist, gestartet werden können.

Einschränkungen beim Schutz und der Wiederherstellung von virtuellen Maschinen

Der Schutz und die Wiederherstellung von virtuellen Maschinen durch Site Recovery Manager unterliegt Beschränkungen.

Schutz und Wiederherstellung von angehaltenen virtuellen Maschinen

Wenn Sie eine virtuelle Maschine anhalten, erstellt vSphere deren Arbeitsspeicherzustand und speichert diesen. Wenn die virtuelle Maschine wieder fortgesetzt wird, stellt vSphere den gespeicherten Arbeitsspeicherzustand wieder her, damit die virtuelle Maschine fortgesetzt werden kann, ohne dass die Anwendungen und Gastbetriebssysteme, die auf der virtuellen Maschine ausgeführt werden, unterbrochen werden.

Schutz und Wiederherstellung von virtuellen Maschinen mit Snapshots

Die Array-basierte Replizierung unterstützt den Schutz und die Wiederherstellung von virtuellen Maschinen mit Snapshots. Hierbei gibt es jedoch Einschränkungen.

Sie können über den Parameter `workingDir` in den VMX-Dateien einen benutzerdefinierten Speicherort zum Speichern der Snapshot-Delta-Dateien angeben. Site Recovery Manager unterstützt nicht die Verwendung des Parameters `workingDir`.

Einschränkungen gelten zudem, wenn Sie Versionen von ESX oder ESXi Server ausführen, die älter als Version 4.1 sind.

- Wenn die virtuelle Maschine über mehrere VMDK-Festplattendateien verfügt, müssen alle Festplattendateien in demselben Ordner wie die VMX-Datei selbst enthalten sein.
- Wenn eine virtuelle Maschine an ein Raw Disk Mapping-Festplattengerät (RDM-Festplattengerät) angehängt wird, müssen Sie die Zuordnungsdatei in demselben Ordner wie die VMX-Datei speichern. RDM-Snapshots sind nur dann verfügbar, wenn Sie die RDM-Zuordnung unter Verwendung des virtuellen Kompatibilitätsmodus erstellen.

Wenn Sie einen ESX oder ESXi Server 4.1 oder höher ausführen, gelten diese Einschränkungen nicht.

vSphere Replication unterstützt den Schutz von virtuellen Maschinen mit Snapshots, Sie können jedoch nur den neuesten Snapshot wiederherstellen. vSphere Replication löscht die Snapshot-Informationen der wiederhergestellten virtuellen Maschine. Als Folge davon stehen die Snapshots nach der Wiederherstellung nicht mehr zur Verfügung, es sei denn, Sie konfigurieren vSphere Replication so, dass mehrere Point-in-Time-Snapshots aufbewahrt werden. Weitere Informationen über das Wiederherstellen von älteren Snapshots durch die Verwendung mehrerer Point-in-Time-Snapshots mit vSphere Replication finden Sie unter Replizieren einer virtuellen Maschine und Aktivieren mehrerer Zeitpunktinstanzen.

Schutz und Wiederherstellung von virtuellen Maschinen mit Arbeitsspeicherzustands-Snapshots

Beim Schützen von virtuellen Maschinen mit Arbeitsspeicherzustands-Snapshots müssen die ESXi-Hosts der Schutz- und der Wiederherstellungs-Site über kompatible CPUs verfügen, wie dies in den VMware-Knowledgebase-Artikeln vMotion CPU-Kompatibilitätsanforderungen für Intel-Prozessoren und vMotion CPU-Kompatibilitätsanforderungen für AMD-Prozessoren definiert ist. Auf den Hosts müssen außerdem dieselben BIOS-Funktionen aktiviert sein. Wenn die BIOS-Konfigurationen der Server nicht übereinstimmen, wird eine Kompatibilitätsfehlermeldung angezeigt, auch wenn sie ansonsten identisch sind. Die beiden häufigsten Funktionen, die überprüft werden sollten, sind „Non-Execute Memory Protection“ (NX/XD) und „Virtualization Technology“ (VT/AMD-V).

Schutz und Wiederherstellung von virtuellen Linked Clone-Maschinen

vSphere Replication unterstützt nicht den Schutz und die Wiederherstellung von virtuellen Maschinen, bei denen es sich um verknüpfte Klone handelt.

Die Array-basierte Replizierung unterstützt den Schutz und die Wiederherstellung von virtuellen Maschinen, bei denen es sich um verknüpfte Klone handelt, wenn alle Knoten in der Snapshot-Baumstruktur repliziert werden.

Schutz und Wiederherstellung von virtuellen Maschinen mit Reservierungen, Affinitätsregeln oder Grenzwerten

Wenn Site Recovery Manager eine virtuelle Maschine auf der Wiederherstellungs-Site wiederherstellt, werden weder Reservierungen, Affinitätsregeln noch Grenzwerte beibehalten, die Sie für die virtuelle Maschine festgelegt haben. Site Recovery Manager behält weder Reservierungen, Affinitätsregeln noch Grenzwerte auf der Wiederherstellungs-Site bei, da die Wiederherstellungs-Site möglicherweise andere Ressourcenanforderungen als die Schutz-Site hat.

Sie können Reservierungen, Affinitätsregeln und Grenzwerte für wiederhergestellte virtuelle Maschinen festlegen, indem Sie Reservierungen und Grenzwerte auf den Ressourcenpools der Wiederherstellungs-Site konfigurieren und die Zuordnungen des Ressourcenpools entsprechend festlegen. Alternativ können Sie Reservierungen, Affinitätsregeln oder Grenzwerte manuell auf den Platzhalter-VMs der Wiederherstellungs-Site festlegen.

Schutz und Wiederherstellung von virtuellen Maschinen mit Komponenten auf mehreren Arrays

Die Array-basierte Replizierung in Site Recovery Manager hängt vom Konzept eines Array-Paars ab. Site Recovery Manager definiert Gruppen von Datenspeichern, die es in Form von Einheiten wiederherstellt. Folglich gelten Einschränkungen für das Speichern der Komponenten von virtuellen Maschinen, die Sie mithilfe der Array-basierten Replizierung schützen.

- Site Recovery Manager unterstützt nicht das Speichern von Komponenten virtueller Maschinen auf mehreren Arrays auf der Schutz-Site, die in ein einzelnes Array auf der Wiederherstellungs-Site repliziert werden.
- Site Recovery Manager unterstützt nicht das Speichern von Komponenten virtueller Maschinen auf mehreren Arrays auf der Schutz-Site, die in mehrere Arrays auf der Wiederherstellungs-Site repliziert werden, wenn sich die Komponenten virtueller Maschinen über beide Arrays erstrecken.

Wenn Sie Komponenten virtueller Maschinen von mehreren Arrays in ein einzelnes Array oder in einen Bereich von Arrays auf der Wiederherstellungs-Site replizieren, stimmen die VMX-Konfigurationen der UUID der Datenspeicher auf der Schutz-Site nicht mit den Konfigurationen auf der Wiederherstellungs-Site überein.

Der Speicherort der VMX-Datei einer virtuellen Maschine bestimmt das Array-Paar, zu dem eine virtuelle Maschine gehört. Eine virtuelle Maschine kann nicht zu zwei Array-Paaren gehören. Wenn sie also über mehr als eine Festplatte verfügt und sich eine der Festplatten in einem Array befindet, das nicht Teil des Array-Paars ist, zu dem die virtuelle Maschine gehört, kann Site Recovery Manager nicht die ganze virtuelle Maschine schützen. Site Recovery Manager behandelt die Festplatte, die sich nicht in demselben Array-Paar wie die virtuelle Maschine befindet, als ein nicht repliziertes Gerät.

Folglich sollten Sie alle virtuellen Festplatten, Auslagerungsdateien, RDM-Geräte und das Arbeitsverzeichnis der virtuellen Maschine auf LUNs in demselben Array speichern, sodass Site Recovery Manager alle Komponenten der virtuellen Maschine schützen kann.

Anpassen der IP-Eigenschaften für virtuelle Maschinen

6

Sie können die IP-Einstellungen für virtuelle Maschinen für die Schutz- und die Wiederherstellungs-Site anpassen. Die Standard-IP-Einstellungen einer virtuellen Maschine werden durch die angepassten IP-Eigenschaften überschrieben, wenn auf der Ziel-Site die wiederhergestellte virtuelle Maschine gestartet wird.

Wenn Sie die IP-Eigenschaften einer virtuellen Maschine nicht anpassen, verwendet Site Recovery Manager während einer Wiederherstellung oder eines Tests von der Schutz-Site auf die Wiederherstellungs-Site die IP-Einstellungen für die Wiederherstellungs-Site. Site Recovery Manager verwendet die IP-Einstellungen für die Schutz-Site nach dem erneuten Schützen während der Wiederherstellung oder des Tests von der ursprünglichen Wiederherstellungs-Site auf die ursprüngliche Schutz-Site.

Site Recovery Manager unterstützt verschiedene Typen der IP-Anpassung.

- Das Verwenden von IPv4- und IPv6-Adressen.
- Das Konfigurieren unterschiedlicher IP-Anpassungen für jede Site.
- Das Verwenden von DHCP, statischen IPv4- oder statischen IPv6-Adressen.
- Das Anpassen der Adressen von virtuellen Windows- und Linux-Maschinen.
- Das Anpassen von mehreren Netzwerkkarten für jede virtuelle Maschine.

Eine Liste der Gastbetriebssysteme, für die Site Recovery Manager die IP-Anpassung unterstützt, finden Sie in den *Kompatibilitätstabellen für vCenter Site Recovery Manager 6.0* unter https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.

Sie ordnen geschützten virtuellen Maschinen Anpassungseinstellungen zu. Folglich greifen alle Wiederherstellungspläne auf eine einzige Kopie der benutzerdefinierten Einstellungen zurück, wenn dieselbe geschützte virtuelle Maschine Bestandteil von mehreren Wiederherstellungsplänen ist. Sie konfigurieren die IP-Anpassung als Teil des Vorgangs der Konfiguration der Wiederherstellungseigenschaften einer virtuellen Maschine.

Wenn Sie keine Netzwerkkarte auf der Wiederherstellungs-Site anpassen, verwendet die Netzwerkkarte weiterhin die IP-Einstellungen der Schutz-Site und umgekehrt und Site Recovery Manager übernimmt während der Wiederherstellung keine IP-Anpassungen für die virtuelle Maschine.

Sie können IP-Anpassungen auf einzelne oder mehrere virtuelle Maschinen anwenden.

Wenn Sie die IP-Anpassung auf virtuellen Maschinen konfigurieren, fügt Site Recovery Manager diesen virtuellen Maschinen Wiederherstellungsschritte hinzu.

Starten des Gastbetriebssystems	Der Vorgang zum Starten des Gastbetriebssystems erfolgt parallel für alle virtuellen Maschinen, für die Sie die IP-Anpassung konfigurieren.
IP anpassen	Site Recovery Manager überträgt die IP-Anpassungen an die virtuelle Maschine.
Herunterfahren des Gastbetriebssystems	Site Recovery Manager fährt die virtuelle Maschine herunter und startet sie neu, um sicherzugehen, dass die Änderungen wirksam werden und von den Diensten des Gastbetriebssystems angewendet werden, wenn die virtuelle Maschine neu gestartet wird.

Nach Abschluss des IP-Anpassungsvorgangs werden virtuelle Maschinen entsprechend den Prioritätsgruppen und den von Ihnen festgelegten Abhängigkeiten eingeschaltet. Der Einschaltvorgang erfolgt für jede virtuelle Maschine unmittelbar vor dem Prozess „Auf VMware Tools warten“.

Hinweis Sie müssen zum Anpassen der IP-Eigenschaften einer virtuellen Maschine VMware Tools oder die VMware Operating System Specific Packages (OSPs) auf der virtuellen Maschine installieren. Siehe http://www.vmware.com/download/packages.html.

- Manuelles Anpassen der IP-Eigenschaften für eine einzelne virtuelle Maschine

  Sie können die IP-Einstellungen einer einzelnen virtuellen Maschine sowohl für die Schutz-Site als auch für die Wiederherstellungs-Site manuell anpassen.

- Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen

  Sie können die IP-Eigenschaften mehrerer virtueller Maschinen auf der Schutz- und Wiederherstellungs-Site anpassen, indem Sie das Tool „DR IP Customizer“ verwenden und IP-Zuordnungsregeln auf Subnetzebene definieren.

Manuelles Anpassen der IP-Eigenschaften für eine einzelne virtuelle Maschine

Sie können die IP-Einstellungen einer einzelnen virtuellen Maschine sowohl für die Schutz-Site als auch für die Wiederherstellungs-Site manuell anpassen.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne** und wählen Sie einen Wiederherstellungsplan aus.
2. Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.
3. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und klicken Sie auf **Wiederherstellung konfigurieren**.
4. Klicken Sie auf die Registerkarte **IP-Anpassung** und wählen Sie **Manuelle IP-Anpassung** aus.
5. Wählen Sie die Netzwerkkarte aus, für die Sie IP-Einstellungen ändern möchten.

6 Klicken Sie je nachdem, ob Sie IP-Einstellungen auf der Schutz-Site oder auf der Wiederherstellungs-Site konfigurieren möchten, auf **Schutz konfigurieren** oder **Wiederherstellung konfigurieren**.

7 Klicken Sie auf die Registerkarte **IPv4**, um IPv4-Einstellungen zu konfigurieren, und wählen Sie DHCP aus, oder geben Sie im Falle von statischen Adressen eine IP-Adresse, die Subnetzinformationen und die Gateway-Server-Adressen an.

   Wenn die virtuelle Maschine eingeschaltet ist und VMware Tools darauf installiert ist, können Sie alternativ auf **Abrufen** klicken, um die aktuellen Einstellungen, die auf der virtuellen Maschine konfiguriert sind, zu importieren.

8 Klicken Sie auf die Registerkarte **IPv6**, um IPv6-Einstellungen zu konfigurieren.

   a Wenn Sie IPv6 nicht verwenden möchten, wählen Sie **Keine Anpassung** aus.

   b Wählen Sie, um IPv6-Einstellungen zu konfigurieren, DHCP aus, oder geben Sie im Falle von statischen Adressen eine IP-Adresse, die Subnetzinformationen und die Gateway-Server-Adressen an.

      Wenn die virtuelle Maschine eingeschaltet ist und VMware Tools darauf installiert ist, können Sie alternativ auf **Abrufen** klicken, um die aktuellen Einstellungen, die auf der virtuellen Maschine konfiguriert sind, zu importieren.

9 Klicken Sie auf die Registerkarte **DNS**, um DNS-Einstellungen zu konfigurieren.

   a Wählen Sie die Art und Weise, wie DNS-Server ermittelt werden.

      Sie können DHCP zum Auffinden von DNS-Servern verwenden oder Sie können primäre und alternative DNS-Server angeben.

   b Geben Sie ein DNS-Suffix ein und klicken Sie auf **Hinzufügen** oder wählen Sie ein vorhandenes DNS-Suffix aus und klicken Sie auf **Entfernen**, **Nach oben verschieben** oder **Nach unten verschieben**.

      Wenn die virtuelle Maschine eingeschaltet ist und VMware Tools darauf installiert ist, können Sie alternativ auf **Abrufen** klicken, um die aktuellen Einstellungen, die auf der virtuellen Maschine konfiguriert sind, zu importieren.

10 Klicken Sie auf die Registerkarte **WINS**, um die primäre und die sekundäre WINS-Adresse einzugeben.

   Die Registerkarte WINS ist nur verfügbar, wenn Sie DHCP oder IPv4-Adressen für virtuelle Windows-Maschinen konfigurieren.

11 Wiederholen Sie die Schritte Schritt 6 bis Schritt 9, um Einstellungen der Wiederherstellungs-Site oder Schutz-Site zu konfigurieren, falls erforderlich.

   Wenn Sie beispielsweise IP-Einstellungen für die Schutz-Site konfiguriert haben, können Sie die Einstellungen für die Wiederherstellungs-Site konfigurieren.

12 Wiederholen Sie bei Bedarf den Konfigurationsvorgang für andere Netzwerkkarten.

Hinweis Virtuelle Maschinen mit manuell definierter IP-Anpassung sind während der Wiederherstellung nicht von der Evaluierung der IP-Zuordnungsregel betroffen. Manuell festgelegte IP-Konfiguration hat Vorrang vor IP-Zuordnungsregeln.

Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen

Sie können die IP-Eigenschaften mehrerer virtueller Maschinen auf der Schutz- und Wiederherstellungs-Site anpassen, indem Sie das Tool „DR IP Customizer“ verwenden und IP-Zuordnungsregeln auf Subnetzebene definieren.

In vorherigen Versionen von Site Recovery Manager haben Sie mithilfe des Tools „DR IP Customizer“ IP-Eigenschaften für mehrere virtuelle Maschinen angepasst. Zusätzlich zum Tool „DR IP Customizer“ können Sie IP-Eigenschaften für mehrere virtuelle Maschinen anpassen, indem Sie auf Subnetzebene IP-Anpassungsregeln definieren.

Sie können in Kombination mit dem Tool „DR IP Customizer“ IP-Anpassungsregeln auf Subnetzebene verwenden.

- Die Nutzung des Tools „DR IP Customizer“ ist eine schnelle Möglichkeit, mithilfe einer CSV-Datei explizite IP-Anpassungseinstellungen für mehrere virtuelle Maschinen zu definieren.
- Sie wenden mit dem vSphere Web Client IP-Anpassungsregeln auf Subnetzebene auf virtuelle Maschinen an.

Virtuelle Maschinen, die Sie mithilfe des Tools „DR IP Customizer“ konfigurieren, unterliegen nicht den IP-Anpassungsregeln auf Subnetzebene. Sie können entweder mithilfe des Tools „DR IP Customizer“ oder mit IP-Subnetzregeln dieselben IP-Anpassungsergebnisse erzielen.

Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen unter Verwendung des Tools „DR IP Customizer“

Mithilfe des Tools „DR IP Customizer“ können Sie explizite IP-Anpassungseinstellungen für mehrere geschützte virtuelle Maschinen auf der Schutz- und der Wiederherstellungs-Site definieren.

Neben dem Definieren von IP-Zuordnungsregeln auf Subnetzebene können Sie das Tool „DR IP Customizer“ verwenden, um maßgeschneiderte Netzwerkeinstellungen auf virtuelle Maschinen anzuwenden, wenn sie auf der Recovery-Site gestartet werden. Sie übergeben dem Tool „DR IP Customizer“ die benutzerdefinierten IP-Einstellungen in Form einer kommagetrennten Datei (CSV-Datei).

Anstatt eine CSV-Datei manuell zu erstellen, können Sie das Tool „DR IP Customizer“ verwenden, um eine CSV-Datei zu exportieren, die Informationen über die Netzwerkkonfigurationen der geschützten virtuellen Maschinen enthält. Sie können diese Datei als Vorlage für die CSV-Datei verwenden, die auf die Wiederherstellungs-Site angewendet werden soll, indem Sie die Werte in der Datei anpassen.

1 Führen Sie das Tool „DR IP Customizer“ aus, um eine CSV-Datei zu generieren, die die Netzwerkinformationen für die geschützten virtuellen Maschinen enthält.

2 Passen Sie die generierte CSV-Datei mit den Netzwerkinformationen an, die für die Wiederherstellungs-Site relevant sind.

3 Führen Sie das Tool „DR IP Customizer“ erneut aus, um die CSV-Datei mit den angepassten Netzwerkkonfigurationen anzuwenden, die anzuwenden sind, wenn die virtuellen Maschinen auf der Wiederherstellungs-Site gestartet werden.

Sie können das Tool „DR IP Customizer“ auf der Schutz-Site oder auf der Wiederherstellungs-Site ausführen. Geschützte virtuelle Maschinen haben auf den verschiedenen Sites unterschiedliche IDs. Wenn Sie die Einstellungen anwenden möchten, müssen Sie daher das DR IP Customizer-Tool auf derselben Site ausführen, auf der Sie die CSV-Datei generiert haben.

Sie können die IP-Einstellungen für die Schutz- und die Wiederherstellungs-Site anpassen, sodass Site Recovery Manager während Vorgängen zum erneuten Schützen die richtigen Konfigurationen verwendet.

Eine Liste der Gastbetriebssysteme, für die Site Recovery Manager die IP-Anpassung unterstützt, finden Sie in den *Kompatibilitätstabellen für vCenter Site Recovery Manager 6.0* unter https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.

- Melden von IP-Adresszuordnungen für Wiederherstellungspläne

  Das Modul für die Meldung von IP-Adresszuordnungen generiert ein XML-Dokument, das die IP-Eigenschaften von geschützten virtuellen Maschinen sowie ihre Platzhalter, gruppiert nach Site und Wiederherstellungsplan, beschreibt. Diese Informationen können Ihnen dabei helfen, die Netzwerkanforderungen eines Wiederherstellungsplans zu verstehen.

- Syntax des Tools „DR IP Customizer“

  Das Tool „DR IP Customizer“ enthält Optionen, die Sie zum Erfassen der Netzwerkinformationen über die virtuellen Maschinen verwenden können, die Site Recovery Manager schützt. Zudem können Sie die Optionen zum Anwenden von Anpassungen auf virtuelle Maschinen verwenden, wenn sie auf der Wiederherstellungs-Site gestartet werden.

- Struktur der DR IP Customizer-CSV-Datei

  Die Datei mit kommagetrennten Einträgen (CSV-Datei) für DR IP Customizer enthält eine Kopfzeile, die die Bedeutung der einzelnen Spalten in der Datei definiert, sowie eine oder mehrere Zeilen für jede Platzhalter-VM in einem Wiederherstellungsplan.

- Ändern der CSV-Datei für DR IP Customizer

  Sie ändern die CSV-Datei für DR IP Customizer, wenn auf virtuelle Maschinen bei deren Start auf der Wiederherstellungs-Site angepasste Netzwerkeinstellungen angewendet werden sollen.

- Ausführen von DR IP Customizer, um die IP-Eigenschaften für mehrere virtuelle Maschinen anzupassen

  Sie können das Tool „DR IP Customizer“ verwenden, um die IP-Eigenschaften für mehrere virtuelle Maschinen anzupassen, die von Site Recovery Manager geschützt werden.

Melden von IP-Adresszuordnungen für Wiederherstellungspläne

Das Modul für die Meldung von IP-Adresszuordnungen generiert ein XML-Dokument, das die IP-Eigenschaften von geschützten virtuellen Maschinen sowie ihre Platzhalter, gruppiert nach Site und Wiederherstellungsplan, beschreibt. Diese Informationen können Ihnen dabei helfen, die Netzwerkanforderungen eines Wiederherstellungsplans zu verstehen.

Da das Modul für die Meldung von IP-Adresszuordnungen eine Verbindung zu beiden Sites herstellen muss, können Sie den Befehl beliebig auf einer der beiden Sites ausführen. Wenn der Befehl ausgeführt wird, werden Sie aufgefordert, die vCenter-Anmeldeinformationen für jede Site anzugeben.

Vorgehensweise

1. Starten Sie eine Befehlsshell auf dem Site Recovery Manager Server-Host auf der Schutz- oder der Wiederherstellungs-Site.
2. Wechseln Sie zum Verzeichnis `C:\Programme\VMware\VMware vCenter Site Recovery Manager\bin`.
3. Führen Sie den Befehl `dr-ip-reporter.exe` aus.
   - Wenn Sie einen Platform Services Controller haben, der eine einzige vCenter Server-Instanz enthält, führen Sie den folgenden Befehl aus:

     ```
     dr-ip-reporter.exe --cfg ..\config\vmware-dr.xml
     --out Pfad_zur_Berichtsdatei.xml
     --uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
     ```

     Dieses Beispiel verweist `dr-ip-reporter.exe` auf die Datei `vmware-dr.xml` von Site Recovery Manager Server und generiert die Berichtsdatei für die vCenter Server-Instanz, die dem Platform Services Controller unter https://*Platform_Services_Controller-Adresse* zugeordnet ist.
   - Wenn Sie einen Platform Services Controller haben, der mehrere vCenter Server-Instanzen enthält, müssen Sie die vCenter Server-ID im `--vcid`-Parameter angeben.

     ```
     dr-ip-reporter.exe --cfg ..\config\vmware-dr.xml
     --out Pfad_zur_Berichtsdatei.xml
     --uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
     --vcid vCenter_Server-ID
     ```

Dieses Beispiel verweist `dr-ip-reporter.exe` auf die Datei `vmware-dr.xml` von Site Recovery Manager Server und generiert die Berichtsdatei für die vCenter Server-Instanz mit der ID *vCenter_Server-ID*.

Hinweis Die vCenter Server-ID ist nicht die gleiche wie der vCenter Server-Name.

- Um die Liste der Netzwerke auf die von einem bestimmten Wiederherstellungsplan benötigten Netzwerke einzuschränken, fügen Sie die Option `-plan` in die Befehlszeile ein:

```
dr-ip-reporter.exe --cfg ..\config\vmware-dr.xml
--out Pfad_zur_Berichtsdatei.xml
--uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
--plan Name_des_Wiederherstellungsplans
```

Syntax des Tools „DR IP Customizer“

Das Tool „DR IP Customizer“ enthält Optionen, die Sie zum Erfassen der Netzwerkinformationen über die virtuellen Maschinen verwenden können, die Site Recovery Manager schützt. Zudem können Sie die Optionen zum Anwenden von Anpassungen auf virtuelle Maschinen verwenden, wenn sie auf der Wiederherstellungs-Site gestartet werden.

Hinweis Diese Version von Site Recovery Manager ermöglicht Ihnen das Definieren von IP-Zuordnungsregeln auf Subnetzebene, um IP-Einstellungen auf virtuellen Maschinen anzupassen, wozu auch das Tool „DR IP Customizer“ geeignet ist. Sie können IP-Zuordnungsregeln auf Subnetzebene in Verbindung mit dem Tool „DR IP Customizer“ verwenden. Informationen dazu, wie Sie IP-Zuordnungsregeln auf Subnetzebene und das Tool „DR IP Customizer“ zusammen verwenden können, finden Sie unter Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen.

Die Programmdatei `dr-ip-customizer.exe` steht im Ordner `C:\Programme\VMware\VMware vCenter Site Recovery Manager\bin` auf der Site Recovery Manager Server-Hostmaschine. Wenn Sie `dr-ip-customizer.exe` ausführen, müssen Sie abhängig davon, ob Sie eine kommagetrennte Datei (CSV-Datei) generieren oder anwenden möchten, verschiedene Optionen angeben.

```
dr-ip-customizer.exe
--cfg XML-Datei der SRM-Server-Konfiguration
--cmd apply/drop/generate
[--csv Name der vorhandenen CSV-Datei]
[--out Name der neu zu generierenden CSV-Datei]
--uri https://host[:port]/lookupservice/sdk
--vcid UUID
[--ignore-thumbprint]
[--extra-dns-columns]
[--verbose]
```

Sie können das Tool „DR IP Customizer“ auf der Schutz-Site oder auf der Wiederherstellungs-Site ausführen. Geschützte virtuelle Maschinen haben auf den verschiedenen Sites unterschiedliche IDs. Wenn Sie die Einstellungen anwenden möchten, müssen Sie daher das DR IP Customizer-Tool auf derselben Site ausführen, auf der Sie die CSV-Datei generiert haben.

Manche Optionen des Tools „DR IP Customizer“ sind obligatorisch, andere sind wiederum optional.

Tabelle 6-1. DR IP Customizer-Optionen

Option	Beschreibung	Obligatorisch
`-h [ --help ]`	Zeigt Nutzungsinformationen zu `dr-ip-customizer.exe` an.	Nein
`--cfg arg`	Pfad zur Anwendungs-XML-Konfigurationsdatei, `vmware-dr.xml`.	Ja
`--cmd arg`	Sie verwenden verschieden Befehle, um DR IP Customizer in verschiedenen Modi auszuführen. ■ Der Befehl `apply` wendet die Netzwerkanpassungseinstellungen aus einer vorhandenen CSV-Datei auf die Wiederherstellungspläne auf den Site Recovery Manager Server-Instanzen an. ■ Der Befehl `generate` generiert eine Basis-CSV-Datei für alle virtuellen Maschinen, die Site Recovery Manager für eine vCenter Server-Instanz schützt. ■ Der Befehl `drop` entfernt die Wiederherstellungseinstellungen von den in der Eingabe-CSV-Datei angegebenen virtuellen Maschinen. Geben Sie stets dieselbe vCenter Server-Instanz für die Befehle `apply` und `drop` an, die Sie zum Generieren der CSV-Datei verwendet haben.	Ja
`--csv arg`	Pfad zur CSV-Datei.	Ja, wenn die Befehle `apply` und `drop` ausgeführt werden.
`-o [ --out ] arg`	Name der neuen CSV-Ausgabedatei, die mit dem Befehl `generate` erstellt werden soll. Wenn Sie den Namen einer vorhandenen CSV-Datei angeben, überschreibt der Befehl `generate` den aktuellen Inhalt.	Ja, wenn Sie den Befehl `generate` ausführen.
`--uri arg`	Lookup Service-URL auf dem Platform Service Controller mit dem Formular `https://host[:port]/lookupservice/sdk`. Geben Sie den Port an, wenn dieser nicht 443 ist. Die Site Recovery Manager-Instanz ordnet diese Adresse dem infra-Knoten der primären Site zu. Verwenden Sie dieselbe vCenter Server-Instanz für die Befehle `apply` und `drop`, die Sie zum Generieren der CSV-Datei verwendet haben.	Ja

Tabelle 6-1. DR IP Customizer-Optionen (Fortsetzung)

Option	Beschreibung	Obligatorisch
`--vcid arg`	Die UUID für die vCenter Server-Instanz der primären Site.	Optional, es sei denn, die Infrastruktur der primären Site enthält mehr als eine vCenter Server-Instanz.
`-i [ --ignore-thumbprint ]`	Ignoriert die Eingabeaufforderung der vCenter Server-Fingerabdruckbestätigung.	Nein
`-e [ --extra-dns-columns ]`	Muss angegeben werden, wenn die Eingabe-CSV-Datei zusätzliche Spalten für DNS-Informationen enthält.	Nein
`-v [ --verbose ]`	Aktiviert die ausführliche Ausgabe. Sie können die Option `--verbose` in der Befehlszeile für `dr-ip-customizer.exe` angeben, um zusätzliche Diagnosemeldungen zu protokollieren.	Nein

Das Tool kann die UUID in den Lookup Service drucken, wenn der `--vcid`-Wert wie in diesem Beispiel nicht angegeben ist:

```
dr-ip-customizer.exe --cfg testConfig.xml -i --cmd generate -o c: \tmp\x.csv --uri
https://service.company.com:443/lookupservice/sdk --vcid ?
```

```
FEHLER: VC-Instanz konnte nicht gefunden werden. Verwenden Sie eine der folgenden
bekannten VC-Instanzen: e07c907e-cd41-4fe7-b38a-f4c0e677a18c vc.company.com
```

Das Ergebnis ist die UUID der vCenter Server-Instanz, gefolgt von dem vCenter Server-DNS-Hostnamen für jeden beim Lookup Service registrierten vCenter Server.

Struktur der DR IP Customizer-CSV-Datei

Die Datei mit kommagetrennten Einträgen (CSV-Datei) für DR IP Customizer enthält eine Kopfzeile, die die Bedeutung der einzelnen Spalten in der Datei definiert, sowie eine oder mehrere Zeilen für jede Platzhalter-VM in einem Wiederherstellungsplan.

Hinweis Diese Version von Site Recovery Manager ermöglicht Ihnen das Definieren von IP-Zuordnungsregeln auf Subnetzebene, um IP-Einstellungen auf virtuellen Maschinen anzupassen, wozu auch das Tool „DR IP Customizer“ geeignet ist. Sie können IP-Zuordnungsregeln auf Subnetzebene in Verbindung mit dem Tool „DR IP Customizer“ verwenden. Informationen dazu, wie Sie IP-Zuordnungsregeln auf Subnetzebene und das Tool „DR IP Customizer“ zusammen verwenden können, finden Sie unter Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen.

Die Konfiguration von IP-Einstellungen für beide Sites ist optional. Sie können die Einstellungen nur für die Schutz-Site, nur für die Wiederherstellungs-Site und für beide Sites vornehmen. Sie können alle Sites so konfigurieren, dass sie jeweils andere Sätze an Netzwerkadaptern und diese auf völlig andere Weise verwenden.

Bestimmte Felder in der CSV-Datei müssen in jeder Zeile ausgefüllt werden. Andere Felder können frei bleiben, sofern keine benutzerdefinierte Einstellung erforderlich ist.

Tabelle 6-2. Spalten der DR IP Customizer-CSV-Datei

Spalte	Beschreibung	Anpassungsregeln
VM-ID	Ein eindeutiger Bezeichner, den DR IP Customizer dazu verwendet, Informationen aus mehreren Zeilen zu erfassen, um sie auf eine einzele virtuelle Maschine anzuwenden. Bei dieser ID handelt es sich um eine interne DR IP Customizer-ID, die nicht der ID der virtuellen Maschine entspricht, die vCenter Server verwendet.	Nicht anpassbar. Darf nicht leer sein.
VM-Name	Der lesbare Name der virtuellen Maschine, wie er in der Bestandsliste von vCenter Server angezeigt wird.	Nicht anpassbar. Darf nicht leer sein.
vCenter Server	Adresse einer vCenter Server-Instanz, entweder auf der Schutz-Site oder auf der Wiederherstellungs-Site. Sie definieren die IP-Einstellungen für eine virtuelle Maschine auf jeder Site in der Spalte vCenter Server.	Nicht anpassbar. Darf nicht leer sein. Diese Spalte kann beide vCenter Server-Instanzen enthalten. Für jede vCenter Server-Instanz wird eine eigene Zeile benötigt. Sie können einen Satz von IP-Einstellungen für die Verwendung auf einer Site konfigurieren und einen anderen zur Verwendung auf der anderen Site. Sie können auch IP-Einstellungen zur Verfügung stellen, die für Vorgänge zum erneuten Schützen beiden Sites verwendet werden.

Tabelle 6-2. Spalten der DR IP Customizer-CSV-Datei (Fortsetzung)

Spalte	Beschreibung	Anpassungsregeln
Adapter-ID	Die ID des Adapters, der angepasst werden soll. Die Adapter-ID 0 definiert globale Einstellungen für alle Adapter einer virtuellen Maschine. Mit der Vergabe von Werten für die Adapter-ID 1, 2, 3 usw. werden die Einstellungen für bestimmte Netzwerkkarten auf einer virtuellen Maschine definiert.	Anpassbar. Darf nicht leer sein. Die einzigen Felder, die Sie in einer Zeile für die Adapter-ID 0 ändern können, sind DNS-Server und DNS-Suffix(e). Diese Werte, falls angegeben, werden von allen anderen Adaptern geerbt, die von dieser VM-ID verwendet werden. Sie können in der CSV-Datei mehrere DNS-Server auf mehreren Zeilen einfügen. Wenn Sie beispielsweise zwei globale DNS-Hosts benötigen, können Sie zwei Zeilen für die Adapter-ID 0 einfügen. ■ Eine Zeile, die alle Informationen zur virtuellen Maschine und einen DNS-Host enthält. ■ Eine Zeile, die nur den zweiten DNS-Host enthält. Wenn Sie einem bestimmten Adapter einen anderen DNS-Server hinzufügen möchten, fügen Sie den DNS-Server der entsprechenden Adapterzeile hinzu. Fügen Sie z. B. den DNS-Server der Adapter-ID 1 hinzu.
DNS-Domäne	DNS-Domäne für diesen Adapter.	Anpassbar. Darf leer bleiben. Wenn Sie einen Wert eingeben, müssen Sie das Format **`beispiel.firma.com`** verwenden.
Net BIOS	Wählen Sie, ob auf diesem Adapter NetBIOS aktiviert werden soll.	Anpassbar. Darf leer bleiben. Wenn die Spalte nicht leer bleibt, muss sie eine der folgenden Zeichenfolgen enthalten: `disableNetBIOS`, `enableNetBIOS` oder `enableNetBIOSViaDhcp`.
Primärer WINS	DR IP Customizer validiert, ob WINS-Einstellungen nur auf virtuelle Windows-Maschinen angewendet werden, er validiert jedoch nicht die NetBIOS-Einstellungen.	Anpassbar. Darf leer bleiben.
Sekundärer WINS	DR IP Customizer validiert, ob WINS-Einstellungen nur auf virtuelle Windows-Maschinen angewendet werden, er validiert jedoch nicht die NetBIOS-Einstellungen.	Anpassbar. Darf leer bleiben.

Tabelle 6-2. Spalten der DR IP Customizer-CSV-Datei (Fortsetzung)

Spalte	Beschreibung	Anpassungsregeln
IP-Adresse	IPv4-Adresse für diese virtuelle Maschine.	Anpassbar. Darf nicht leer sein. Virtuelle Maschinen können über mehrere virtuelle Netzwerkadapter verfügen. Sie können jeden virtuellen Netzwerkadapter mit einer statischen IPv4-Adresse konfigurieren. Wenn das Feld nicht auf eine bestimmte statische Adresse festgelegt ist, müssen Sie es auf DHCP stellen.
Subnetzmaske	Subnetzmaske für diese virtuelle Maschine.	Anpassbar. Darf leer bleiben.
Gateway(s)	IPv4-Gateway oder -Gateways für diese virtuelle Maschine.	Anpassbar. Darf leer bleiben.
IPv6-Adresse	IPv6-Adresse für diese virtuelle Maschine.	Anpassbar. Kann leer gelassen werden, wenn Sie IPv6 nicht benutzen. Virtuelle Maschinen können über mehrere virtuelle Netzwerkadapter verfügen. Sie können jeden virtuellen Netzwerkadapter mit einer statischen IPv6-Adresse konfigurieren. Wenn das Feld nicht auf eine bestimmte statische Adresse festgelegt ist, müssen Sie es auf DHCP stellen. Wenn Sie Site Recovery Manager Server auf Windows Server 2003 ausführen und IPv6-Adressen für eine virtuelle Maschine anpassen, müssen Sie IPv6 auf den Site Recovery Manager Server-Instanzen aktivieren. Site Recovery Manager führt während der Anpassung eine Validierung der IP-Adressen durch. Dafür muss IPv6 auf dem Site Recovery Manager Server aktiviert sein, wenn Sie IPv6-Adressen anpassen. Spätere Versionen von Windows Server haben IPv6 standardmäßig aktiviert.
Länge des IPv6-Subnetzpräfixes	Zu verwendende Länge des IPv6-Subnetzpräfixes.	Anpassbar. Darf leer bleiben.
IPv6-Gateway(s)	IPv4-Gateway oder -Gateways für diesen Adapter.	Anpassbar. Darf leer bleiben.

Tabelle 6-2. Spalten der DR IP Customizer-CSV-Datei (Fortsetzung)

Spalte	Beschreibung	Anpassungsregeln
DNS-Server	Adresse des DNS-Servers bzw. der DNS-Server.	Anpassbar. Darf leer bleiben. Wenn Sie diese Einstellung in einer Zeile für die Adapter-ID 0 eingeben, wird sie als globale Einstellung behandelt. Auf virtuellen Windows-Maschinen gilt diese Einstellung für jeden Adapter, wenn Sie sie in anderen Adapter-ID-Zeilen als solchen für die Adapter-ID 0 angeben. Auf virtuellen Linux-Maschinen ist dies immer eine globale Einstellung für alle Adapter. Diese Spalte kann einen oder mehrere IPv4- bzw. IPv6-DNS-Server für jede Netzwerkkarte enthalten.
DNS-Suffix(e)	Suffix bzw. Suffixe für DNS-Server.	Anpassbar. Darf leer bleiben. Dies sind globale Einstellungen für alle Adapter auf virtuellen Windows- und Linux-Maschinen.

Ändern der CSV-Datei für DR IP Customizer

Sie ändern die CSV-Datei für DR IP Customizer, wenn auf virtuelle Maschinen bei deren Start auf der Wiederherstellungs-Site angepasste Netzwerkeinstellungen angewendet werden sollen.

Hinweis Diese Version von Site Recovery Manager ermöglicht Ihnen das Definieren von IP-Zuordnungsregeln auf Subnetzebene, um IP-Einstellungen auf virtuellen Maschinen anzupassen, wozu auch das Tool „DR IP Customizer“ geeignet ist. Sie können IP-Zuordnungsregeln auf Subnetzebene in Verbindung mit dem Tool „DR IP Customizer“ verwenden. Informationen dazu, wie Sie IP-Zuordnungsregeln auf Subnetzebene und das Tool „DR IP Customizer“ zusammen verwenden können, finden Sie unter Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen.

Eine Herausforderung bei der Darstellung von VM-Netzwerkkonfigurationen in einer CSV-Datei besteht darin, dass Konfigurationen virtueller Maschinen hierarchische Informationen enthalten. Beispielsweise kann eine einzelne virtuelle Maschine mehrere Adapter enthalten und jeder Adapter kann über mehrere Listen von Elementen, z. B. Gateways, verfügen. Das CSV-Format bietet keine Möglichkeit, Informationen hierarchisch darzustellen. Folglich kann jede Zeile der CSV-Datei, die von DR IP Customizer generiert wird, einen Teil oder alle Informationen für eine bestimmte virtuelle Maschine enthalten.

Bei einer virtuellen Maschine mit einer einfachen Netzwerkkonfiguration finden alle Informationen in einer einzelnen Zeile Platz. Im Falle einer etwas komplexeren virtuellen Maschine werden möglicherweise mehrere Zeilen benötigt. Für virtuelle Maschinen mit mehreren Netzwerkkarten oder mehreren Gateways sind mehrere Zeilen erforderlich. Jede Zeile in der CSV-Datei enthält Identifikationsdaten, die beschreiben, auf welche virtuelle Maschine und welchen Adapter sich die Informationen beziehen. Die Informationen werden zusammengefasst und auf die entsprechende virtuelle Maschine angewendet.

Befolgen Sie diese Richtlinien, wenn Sie die CSV-Datei für DR IP Customizer ändern.

- Lassen Sie Werte für nicht erforderliche Einstellungen weg.
- Verwenden Sie für jeden Adapter die geringstmögliche Anzahl an Zeilen.
- Verwenden Sie in keinem Feld Kommas.
- Geben Sie bei Bedarf die Adapter-ID Einstellungen an. DR IP Customizer wendet die Einstellungen, die Sie für Adapter-ID 0 angeben, auf alle Netzwerkkarten an. Sollen Einstellungen für einzelne Netzwerkkarten gelten, geben Sie die Werte in den Feldern für die Adapter-ID 1, 2, ..., *n* an.
- Wenn Sie mehr als einen Wert für eine Spalte angeben möchten, erstellen Sie eine zusätzliche Zeile für diesen Adapter und geben Sie den Wert in der Spalte dieser Zeile ein. Um sicherzustellen, dass die zusätzliche Zeile der dafür vorgesehenen virtuellen Maschine zugewiesen wird, kopieren Sie die Werte der VM-ID, des VM-Namens, von vCenter Server und der Adapter-ID.
- Wenn Sie eine IP-Adresse für einen Netzwerkadapter auf jeder der Schutz- und Wiederherstellungs-Sites oder wenn Sie mehrere DNS-Server-Adressen angeben möchten, fügen Sie für jede Adresse eine neue Zeile hinzu. Kopieren Sie die Werte für die VM-ID, den VM-Namen und die Adapter-ID für jede Zeile.

Beispiele für DR IP Customizer-CSV-Dateien

Sie erhalten eine CSV-Datei, die die Netzwerkinformationen für die geschützten virtuellen Maschinen auf dem vCenter Server enthält, indem Sie `dr-ip-customizer.exe` mit dem Befehl `--cmd generate` ausführen. Sie bearbeiten die CSV-Datei zum Anpassen der IP-Einstellungen der geschützten virtuellen Maschinen.

Sie können ein Paket der Beispiel-CSV-Dateien herunterladen, die in diesem Abschnitt beschrieben werden.

Hinweis Diese Version von Site Recovery Manager ermöglicht Ihnen das Definieren von IP-Zuordnungsregeln auf Subnetzebene, um IP-Einstellungen auf virtuellen Maschinen anzupassen, wozu auch das Tool „DR IP Customizer“ geeignet ist. Sie können IP-Zuordnungsregeln auf Subnetzebene in Verbindung mit dem Tool „DR IP Customizer“ verwenden. Informationen dazu, wie Sie IP-Zuordnungsregeln auf Subnetzebene und das Tool „DR IP Customizer“ zusammen verwenden können, finden Sie unter Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen.

Beispiel: Eine generierte DR IP Customizer-CSV-Datei

Für ein einfaches Setup mit nur zwei geschützten virtuellen Maschinen enthält die generierte CSV-Datei möglicherweise nur die ID der virtuellen Maschine, den Namen der virtuellen Maschine, die Namen der vCenter Server-Instanzen auf beiden Sites und einen einzelnen Adapter.

```
VM ID,VM Name,vCenter Server,Adapter ID,DNS Domain,Net BIOS,
Primary WINS,Secondary WINS,IP Address,Subnet Mask,Gateway(s),
IPv6 Address,IPv6 Subnet Prefix length,IPv6 Gateway(s),
DNS Server(s),DNS Suffix(es)
```

```
protected-vm-10301,vm-3-win,vcenter-server-site-B,0,,,,,,,,,,
protected-vm-10301,vm-3-win,vcenter-server-site-A,0,,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-B,0,,,,,,,,,,
protected-vm-20175,vm-1-linux,vcenter-server-site-A,0,,,,,,,,,,
```

Diese generierte CSV-Datei enthält zwei virtuelle Maschinen: vm-3-win und vm-1-linux. Die virtuellen Maschinen sind auf der Schutz- und der Wiederherstellungs-Site, vcenter-server-site-B und vcenter-server-site-A, vorhanden. DR IP Customizer generiert einen Eintrag für jede virtuelle Maschine und jede Site mit Adapter-ID 0. Sie können zum Anpassen der Netzwerkkarten zusätzliche Zeilen hinzufügen, sobald Sie wissen, wie viele Netzwerkkarten sich auf jeder virtuellen Maschine befinden.

Beispiel: Festlegen statischer IPv4-Adressen

Sie können die generierte CSV-Datei ändern, um einer der virtuellen Maschinen (vm-3-win) zwei Netzwerkadapter mit statischen IPv4-Adressen auf der Schutz- und der Wiederherstellungs-Site zuzuweisen.

Aus Gründen der Lesbarkeit werden in der folgenden Tabelle die leeren Spalten der Beispiel-CSV-Datei ausgeblendet. Die Spalten DNS-Domäne, NetBIOS, IPv6-Adresse, Länge des IPv6-Subnetzpräfixes und IPv6-Gateway(s) werden weggelassen.

Tabelle 6-3. Festlegen statischer IPv4-Adressen in einer geänderten CSV-Datei

VM-ID	VM-Name	vCenter Server	Adapter-ID	Primärer WINS	Sekundärer WINS	IP-Adresse	Subnetzmaske	Gateway(s)	DNS-Server	DNS-Suffix(e)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com

Tabelle 6-3. Festlegen statischer IPv4-Adressen in einer geänderten CSV-Datei (Fortsetzung)

VM-ID	VM-Name	vCenter Server	Adapter-ID	Primärer WINS	Sekundärer WINS	IP-Adresse	Subnetzmaske	Gateway(s)	DNS-Server	DNS-Suffix(e)
protected-vm-10301		vcenter-server-site-A	1			192.168.0.21	255.255.255.0	192.168.0.1		
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

Die in dieser CSV-Datei enthaltenen unterschiedlichen statischen IPv4-Einstellungen werden auf vm-3-win auf der Schutz- und der Wiederherstellungs-Site angewendet.

- Auf der Site vcenter-server-site-B:
  - Legt für alle Netzwerkkarten dieser virtuellen Maschine die DNS-Suffixe example.com und eng.example.com fest.
  - Fügt eine Netzwerkkarte, Adapter-ID 1, mit dem primären und dem sekundären WINS-Server 2.2.3.4 und 2.2.3.5, die statische IPv4-Adresse 192.168.1.21 und DNS-Server 1.1.1.1 hinzu.
  - Fügt eine Netzwerkkarte, Adapter-ID 2, mit dem primären und dem sekundären WINS-Server 2.2.3.4 und 2.2.3.5, die statische IPv4-Adresse 192.168.1.22 und DNS-Server 1.1.1.2 hinzu.
- Auf der Site vcenter-server-site-A:
  - Legt für alle Netzwerkkarten dieser virtuellen Maschine die DNS-Suffixe example.com und eng.example.com fest.
  - Legt die DNS-Server 1.1.0.1 und 1.1.0.2 für alle Netzwerkkarten dieser virtuellen Maschine fest.
  - Fügt eine Netzwerkkarte, Adapter-ID 1, mit einer statischen IPv4-Adresse 192.168.0.21 hinzu.
  - Fügt eine Netzwerkkarte, Adapter-ID 2, mit dem primären und dem sekundären WINS-Server 1.2.3.4 und 1.2.3.5 sowie die statische IPv4-Adresse 192.168.0.22 hinzu.

Beispiel: Festlegen von statischen und DHCP IPv4-Adressen

Sie können die generierte CSV-Datei ändern, um einer der virtuellen Maschinen (vm-3-win) mehrere Netzwerkkarten zuzuweisen, die eine Kombination aus statischen und DHCP IPv4-Adressen verwenden. Die Einstellungen können sich auf der Schutz- und der Wiederherstellungs-Site unterscheiden.

Aus Gründen der Lesbarkeit werden in der folgenden Tabelle die leeren Spalten der Beispiel-CSV-Datei ausgeblendet. Die Spalten DNS-Domäne, NetBIOS, IPv6-Adresse, Länge des IPv6-Subnetzpräfixes und IPv6-Gateway(s) werden weggelassen.

Tabelle 6-4. Festlegen statischer und DHCP IPv4-Adressen in einer geänderten CSV-Datei

VM-ID	VM-Name	vCenter Server	Adapter-ID	Primärer WINS	Sekundärer WINS	IP-Adresse	Subnetzmaske	Gateway(s)	DNS-Server	DNS-Suffix(e)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0							eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	dhcp			1.1.1.1	
protected-vm-10301		vcenter-server-site-B	2	2.2.3.4	2.2.3.5	192.168.1.22	255.255.255.0	192.168.1.1	1.1.1.2	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.1	example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0						1.1.0.2	eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp				
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1		

In dieser CSV-Datei werden unterschiedliche statische und dynamische IPv4-Einstellungen auf vm-3-win auf der Schutz- und der Wiederherstellungs-Site angewendet.

- Auf der Site vcenter-server-site-B:
  - Legt für alle Netzwerkkarten dieser virtuellen Maschine die DNS-Suffixe example.com und eng.example.com fest.
  - Fügt eine Netzwerkkarte, Adapter-ID 1, mit dem primären und dem sekundären WINS-Server 2.2.3.4 und 2.2.3.5 hinzu, die DHCP zum Beziehen einer IP-Adresse verwendet, und legt den statischen DNS-Server 1.1.1.1 fest.

- Fügt eine Netzwerkkarte, Adapter-ID 2, mit dem primären und dem sekundären WINS-Server 2.2.3.4 und 2.2.3.5, die statische IPv4-Adresse 192.168.1.22 und DNS-Server 1.1.1.2 hinzu.

- Auf der Site vcenter-server-site-A:
  - Legt für alle Netzwerkkarten dieser virtuellen Maschine die DNS-Suffixe auf example.com und eng.example.com fest.
  - Legt die DNS-Server 1.1.0.1 und 1.1.0.2 für alle Netzwerkkarten dieser virtuellen Maschine fest.
  - Fügt eine Netzwerkkarte, Adapter-ID 1, hinzu, die DHCP zum Beziehen einer IPv4-Adresse und der global zugewiesenen DNS-Server-Informationen verwendet.
  - Fügt eine Netzwerkkarte, Adapter-ID 2, mit dem primären und dem sekundären WINS-Server 1.2.3.4 und 1.2.3.5, sowie die statische IPv4-Adresse 192.168.0.22 hinzu.

Beispiel: Festlegen statischer und DHCP IPv4- und IPv6-Adressen

Sie können die generierte CSV-Datei ändern, um einer der virtuellen Maschinen (vm-3-win) mehrere Netzwerkkarten zuzuweisen. Die Netzwerkkarten können eine Kombination aus statischen und DHCP IPv4- und IPv6-Adressen verwenden. Die Einstellungen können sich auf der Schutz- und der Wiederherstellungs-Site unterscheiden.

Aus Gründen der Lesbarkeit werden in der folgenden Tabelle die leeren Spalten der Beispiel-CSV-Datei ausgeblendet. Die Spalten DNS-Domäne und NetBIOS werden weggelassen.

Tabelle 6-5. Festlegen statischer und DHCP IPv4- und IPv6-Adressen in einer geänderten CSV-Datei

VM-ID	VM-Name	vCenter Server	Adapter-ID	Primärer WINS	Sekundärer WINS	IP-Adresse	Subnetzmaske	Gateway(s)	IPv6-Adresse	Länge des IPv6-Subnetzpräfixes	IPv6-Gateway(s)	DNS-Server	DNS-Suffix(e)
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-B	0										eng.example.com
protected-vm-10301		vcenter-server-site-B	1	2.2.3.4	2.2.3.5	192.168.1.21	255.255.255.0	192.168.1.1	dhcp			1.1.1.1	

Tabelle 6-5. Festlegen statischer und DHCP IPv4- und IPv6-Adressen in einer geänderten CSV-Datei (Fortsetzung)

VM-ID	VM-Name	vCenter Server	Adapter-ID	Primärer WINS	Sekundärer WINS	IP-Adresse	Subnetzmaske	Gateway(s)	IPv6-Adresse	Länge des IPv6-Subnetzpräfixes	IPv6-Gateway(s)	DNS-Server	DNS-Suffix(e)
protected-vm-10301		vcenter-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	
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										example.com
protected-vm-10301	vm-3-win	vcenter-server-site-A	0										eng.example.com
protected-vm-10301		vcenter-server-site-A	1			dhcp			::ffff:192.168.0.22	32	::ffff:192.168.0.1	::ffff:192.168.0.250	
protected-vm-10301		vcenter-server-site-A	1									::ffff:192.168.0.251	
protected-vm-10301		vcenter-server-site-A	2	1.2.3.4	1.2.3.5	192.168.0.22	255.255.255.0	192.168.0.1				1.1.1.1	

In dieser CSV-Datei werden unterschiedliche IP-Einstellungen auf vm-3-win auf der Schutz- und der Wiederherstellungs-Site angewendet.

- Auf der Site vcenter-server-site-B:
  - Legt für alle Netzwerkkarten dieser virtuellen Maschine die DNS-Suffixe example.com und eng.example.com fest.
  - Fügt eine Netzwerkkarte, Adapter-ID 1, mit dem primären und dem sekundären WINS-Server 2.2.3.4 und 2.2.3.5 hinzu, die die statische IPv4-Adresse 192.168.1.21 festlegt, DHCP zum Beziehen einer IPv6-Adresse und DNS-Server 1.1.1.1 verwendet.

- Fügt eine Netzwerkkarte, Adapter-ID 2, mit dem primären und dem sekundären WINS-Server 2.2.3.4 und 2.2.3.5 hinzu, die DHCP zum Beziehen einer IPv4-Adresse verwendet, die statische IPv6-Adresse ::ffff:192.168.1.22 festlegt und DNS-Server 1.1.1.2 verwendet.

- Auf der Site vcenter-server-site-A:
  - Legt für alle Netzwerkkarten dieser virtuellen Maschine die DNS-Suffixe auf example.com und eng.example.com fest.
  - Fügt eine Netzwerkkarte, Adapter-ID 1, hinzu, die DHCP zum Beziehen einer IPv4-Adresse verwendet und die statische IPv6-Adresse ::ffff:192.168.1.22 festlegt. Adapter-ID 1 verwendet die statischen IPv6-DNS-Server ::ffff:192.168.0.250 und ::ffff:192.168.0.251.
  - Fügt eine Netzwerkkarte, Adapter-ID 2, mit dem primären und dem sekundären WINS-Server 1.2.3.4 und 1.2.3.5, die statische IPv4-Adresse 192.168.0.22 und DNS-Server 1.1.1.1 hinzu. Wenn die IPv6-Spalte leer gelassen wird, verwendet Adapter-ID 2 DHCP für IPv6-Adressen.

Ausführen von DR IP Customizer, um die IP-Eigenschaften für mehrere virtuelle Maschinen anzupassen

Sie können das Tool „DR IP Customizer“ verwenden, um die IP-Eigenschaften für mehrere virtuelle Maschinen anzupassen, die von Site Recovery Manager geschützt werden.

Hinweis Diese Version von Site Recovery Manager ermöglicht Ihnen das Definieren von IP-Zuordnungsregeln auf Subnetzebene, um IP-Einstellungen auf virtuellen Maschinen anzupassen, wozu auch das Tool „DR IP Customizer“ geeignet ist. Sie können IP-Zuordnungsregeln auf Subnetzebene in Verbindung mit dem Tool „DR IP Customizer“ verwenden. Informationen dazu, wie Sie IP-Zuordnungsregeln auf Subnetzebene und das Tool „DR IP Customizer“ zusammen verwenden können, finden Sie unter Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen.

Voraussetzungen

- Verwenden Sie das Tool „DR IP Customizer“ auf einem Computer, der auf die vCenter Server-Instanzen in Ihrer Umgebung zugreifen kann.
- Das Benutzerkonto, das Sie zum Ausführen des Tools „DR IP Customizer“ verwenden, erfordert mindestens die Rolle des Administrators für die Site Recovery Manager-Wiederherstellungspläne.

Vorgehensweise

1. Öffnen Sie eine Befehlsshell auf dem Site Recovery Manager Server-Host.
2. Wechseln Sie zum Verzeichnis `C:\Programme\VMware\VMware vCenter Site Recovery Manager\bin`.

3 Führen Sie den Befehl `dr-ip-customizer.exe` aus, um eine Datei mit kommagetrennten Werten zu generieren (CSV-Datei), die Informationen über die geschützten virtuellen Maschinen enthält.

   - Wenn Sie einen Platform Services Controller haben, der eine einzige vCenter Server-Instanz enthält, führen Sie den folgenden Befehl aus:

     ```
     dr-ip-customizer.exe --cfg SRM-Installationsverzeichnis\config\vmware-dr.xml
     --cmd generate --out "Pfad_zur_CSV-Datei.csv"
     --uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
     ```

     Dieses Beispiel verweist `dr-ip-customizer.exe` auf die Datei `vmware-dr.xml` von Site Recovery Manager Server und generiert die CSV-Datei für die vCenter Server-Instanz, die dem Platform Services Controller unter https://*Platform_Services_Controller-Adresse* zugeordnet ist.

   - Wenn Sie einen Platform Services Controller haben, der mehrere vCenter Server-Instanzen enthält, müssen Sie die vCenter Server-ID im `--vcid`-Parameter angeben. Wenn Sie `--vcid` nicht angeben oder wenn Sie eine falsche ID angeben, listet das Tool alle verfügbaren vCenter Server-Instanzen.

     ```
     dr-ip-customizer.exe --cfg SRM-Installationsverzeichnis\config\vmware-dr.xml
     --cmd generate --out "Pfad_zur_CSV-Datei.csv"
     --uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
     --vcid vCenter_Server-ID
     ```

     Dieses Beispiel verweist `dr-ip-customizer.exe` auf die Datei `vmware-dr.xml` von Site Recovery Manager Server und generiert die -CSV-Datei für die vCenter Server-Instanz mit der ID *vCenter_Server-ID*.

     Hinweis Die vCenter Server-ID ist nicht die gleiche wie der vCenter Server-Name.

4 (Optional) Überprüfen Sie den vCenter Server-Fingerabdruck und geben Sie **y** ein, um zu bestätigen, dass Sie dieser vCenter Server-Instanz vertrauen.

   Wenn Sie die Option `--ignore-thumbprint` angegeben haben, werden Sie nicht aufgefordert, den Fingerabdruck zu überprüfen.

5 Geben Sie die Anmeldedaten für die vCenter Server-Instanz ein.

   Sie werden möglicherweise erneut aufgefordert, zu bestätigen, dass Sie dieser vCenter Server-Instanz vertrauen.

6 Bearbeiten Sie die generierte CSV-Datei, um die IP-Eigenschaften für die virtuellen Maschinen im Wiederherstellungsplan anzupassen.

   Sie können die CSV-Datei mit einem Tabellenkalkulationsprogramm bearbeiten. Speichern Sie die geänderte CSV-Datei unter einem neuen Namen.

7 Führen Sie `dr-ip-customizer.exe` aus, um die angepassten IP-Eigenschaften aus der geänderten CSV-Datei anzuwenden.

Sie können das Tool „DR IP Customizer“ auf der Schutz-Site oder auf der Wiederherstellungs-Site ausführen. Geschützte virtuelle Maschinen haben auf den verschiedenen Sites unterschiedliche IDs. Wenn Sie die Einstellungen anwenden möchten, müssen Sie daher das DR IP Customizer-Tool auf derselben Site ausführen, auf der Sie die CSV-Datei generiert haben.

- Wenn Sie einen Platform Services Controller haben, der eine einzige vCenter Server-Instanz enthält, führen Sie den folgenden Befehl aus:

```
dr-ip-customizer.exe --cfg SRM-Installationsverzeichnis\config\vmware-dr.xml
--cmd apply --csv "Pfad_zur_CSV-Datei.csv"
--uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
```

Dieses Beispiel verweist `dr-ip-customizer.exe` auf die Datei `vmware-dr.xml` von Site Recovery Manager Server und wendet die Anpassungen in der CSV-Datei auf den vCenter Server an, der Platform Services Controller unter https://*Platform_Services_Controller-Adresse* zugeordnet ist.

- Wenn Sie einen Platform Services Controller haben, der mehrere vCenter Server-Instanzen enthält, müssen Sie die vCenter Server-ID im `--vcid`-Parameter angeben.

```
dr-ip-customizer.exe --cfg SRM-Installationsverzeichnis\config\vmware-dr.xml
--cmd apply --csv "Pfad_zur_CSV-Datei.csv"
--uri https://Platform_Services_Controller-Adresse[:Port]/lookupservice/sdk
--vcid vCenter_Server-ID
```

Dieses Beispiel verweist `dr-ip-customizer.exe` auf die Datei `vmware-dr.xml` von Site Recovery Manager Server und wendet die Anpassungen in der CSV-Datei auf die vCenter Server-Instanz mit der ID *vCenter_Server-ID* an.

Die angegebenen Anpassungen werden während einer Wiederherstellung auf alle virtuellen Maschinen angewendet, die in der CSV-Datei genannt sind. Es ist nicht erforderlich, IP-Einstellungen für diese Maschinen manuell zu konfigurieren, wenn Sie deren Wiederherstellungsplan-Eigenschaften bearbeiten.

Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen durch Definieren der IP-Anpassungsregeln

Sie können eine einzelne IP-Zuordnungsregel auf Subnetzebene für eine ausgewählte konfigurierte Zuordnung eines virtuellen Netzwerks auf den Schutz- und den Wiederherstellungs-Sites angeben.

Mit Zuordnungen auf Subnetzebene entfällt die Notwendigkeit, genaue IP-Zuordnungen auf Adapterebene zu definieren. Stattdessen geben Sie eine IP-Anpassungsregel an, die Site Recovery Manager auf alle relevanten Adapter anwendet. Die IP-Anpassungsregel wird für Test- und Wiederherstellungs-Workflows verwendet. Sie können zwischen verschiedenen Netzwerkzuordnungen keine IP-Anpassungsregeln wiederverwenden.

Wichtig IP-Subnetz-Zuordnungsregeln unterstützen nur IPv4. Die regelbasierte IPv6-Anpassung wird nicht von Site Recovery Manager unterstützt. Wenn Sie IP-Subnetz-Zuordnungsregeln für eine virtuelle Maschine mit aktiviertem IPv6 anwenden, bleiben die IPv6-Einstellungen, DHCP oder statisch, nach der Wiederherstellung unberührt. Site Recovery Manager wertet keine IP-Zuordnungsregeln für virtuelle Maschinen aus, die für die Verwendung der manuellen IP-Anpassung konfiguriert sind.

Die IP-Anpassungsregel gilt für virtuelle Maschinen, bei denen ein Failover von dem IPv4-Subnetz einer Schutz-Site auf das IPv4-Subnetz einer Wiederherstellungs-Site durchgeführt wird, z. B. von 10.17.23.0/24 auf 10.18.22.0/24. Die IP-Anpassungsregel besagt, dass während einer Wiederherstellung Site Recovery Manager die vorhandene IP-Konfiguration der Netzwerkkarten der wiederhergestellten virtuellen Maschine auswertet und auf dem Subnetz 10.17.23.0/24 erkannte Netzwerkkarten für das Subnetz 10.18.22.0/24 neu konfiguriert.

Trifft die Regel zu, leitet Site Recovery Manager die neue statische IPv4-Adresse aus der alten Adresse ab, indem er die Host-Bits der ursprünglichen IPv4-Adresse beibehält und sie in das Zielsubnetz einsetzt. Beispiel: Die ursprüngliche Adresse der Schutz-Site lautet 10.17.23.55/24 und die neue Adresse ist 10.18.22.55/24.

Wenn das Textfeld für das Standard-Gateway leer ist, leitet Site Recovery Manager den neuen Gateway-Parameter vom ursprünglichen Parameter ab, indem die Host-Bits der ursprünglichen IPv4-Adresse beibehalten und in das Zielsubnetz eingesetzt werden. Beispiel: Das ursprüngliche Gateway der Schutz-Site lautet 10.17.23.1 und das neue Gateway ist 10.18.22.1. Wenn Sie explizit einen Gateway-Parameter angeben, überprüft Site Recovery Manager die Syntax der IPv4-Adresse und wendet sie genau an.

Site Recovery Manager wendet das DNS und weitere Parameter wie angegeben an. DHCP-aktivierte Netzwerkkarten unterliegen nicht der Anpassung, da während der Wiederherstellung ihre Netzwerkkonfiguration unverändert bleibt.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Wählen Sie auf der Registerkarte **Verwalten** die Option **Netzwerkzuordnungen** aus.
3. Wählen Sie eine Netzwerkzuordnung aus, für die eine Anpassungsregel definiert werden soll.

4 Klicken Sie zum Definieren einer Regel auf **IP-Anpassungsregel hinzufügen**.

5 Geben Sie den Namen für die Regel ein.

6 Geben Sie Subnetz-IP-Bereiche an, die der Schutz- und der Wiederherstellungs-Site zugeordnet werden sollen.

7 Geben Sie die Netzwerkeinstellungen für das Wiederherstellungs-Site-Netzwerk an.

8 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Übernehmen der IP-Anpassungsregeln für eine virtuelle Maschine

Sie können eine IP-Anpassungsregel auf die Wiederherstellungseinstellungen einer geschützten virtuellen Maschine übernehmen.

Wenn Sie eine IP-Anpassungsregel übernehmen, geben Sie für jede Netzwerkzuordnung eine Subnetz-IP-Zuordnungsregel an.

Wenn Sie die Option `recovery.useIpMapperAutomatically` der erweiterten Einstellungen auf „True“ festlegen und die IP-Zuordnungsregel für virtuelle Netzwerke konfigurieren, wertet Site Recovery Manager die Subnetz-IP-Zuordnungsregel während der Wiederherstellung aus, um die virtuellen Maschinen anzupassen. Wenn Sie diese Option auf „False“ festlegen, wertet Site Recovery Manager die IP-Zuordnungsregeln während der Wiederherstellung nicht aus. Sie können die Auswirkung dieser Option für jede virtuelle Maschine überschreiben, indem Sie die Option **IP-Anpassung** verwenden.

Die Standardeinstellung für `recovery.useIpMapperAutomatically` ist „True“. Wenn Sie sie auf „Auto“ festlegen, passt Site Recovery Manager die virtuelle Maschine mithilfe der IP-Anpassungsregel an.

Voraussetzungen

Eine Liste der Gastbetriebssysteme, für die Site Recovery Manager die IP-Anpassung unterstützt, finden Sie in den *Kompatibilitätstabellen für vCenter Site Recovery Manager 6.0* unter https://www.vmware.com/support/srm/srm-compat-matrix-6-0.html.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne**.

2 Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.

3 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und klicken Sie auf **Wiederherstellung konfigurieren**.

4 Klicken Sie auf **IP-Anpassung**.

5 Wählen Sie in der Liste für den IP-Anpassungsmodus die Option **IP-Anpassungsregeln ggf. verwenden** und klicken Sie auf **OK**.

Erneuter Schutz virtueller Maschinen nach einer Wiederherstellung

7

Nach einer Wiederherstellung wird die Wiederherstellungs-Site zur neuen Schutz-Site, ist aber noch nicht geschützt. Wenn die ursprüngliche Schutz-Site betriebsbereit ist, können Sie die Richtung des Schutzes umkehren, um die ursprüngliche Schutz-Site als neue Wiederherstellungs-Site zu verwenden, damit die neue Schutz-Site geschützt wird.

Den erneuten Schutz manuell in der umgekehrten Richtung einzurichten, indem alle Schutzgruppen und Wiederherstellungspläne neu erstellt werden, ist zeitaufwändig und fehleranfällig. Site Recovery Manager bietet die Funktion zum erneuten Schutz, die eine automatisierte Möglichkeit darstellt, den Schutz umzukehren.

Nachdem Site Recovery Manager eine Wiederherstellung durchgeführt hat, werden die geschützten virtuellen Maschinen auf der Wiederherstellungs-Site gestartet. Da die vorherige Schutz-Site offline sein könnte, sind diese virtuellen Maschinen nicht geschützt. Durch den erneuten Schutz wird die Replizierungsrichtung umgekehrt, wenn die Schutz-Site wieder online ist, um die wiederhergestellten virtuellen Maschinen der Wiederherstellungs-Site an der ursprünglichen Schutz-Site zu schützen.

Der erneute Schutz nutzt die Schutzinformationen, die vor einer Wiederherstellung festgehalten wurden, um die Richtung des Schutzes umzukehren. Sie können den Vorgang des erneuten Schutzes nur starten, nachdem die Wiederherstellung ohne Fehler beendet wurde. Falls die Wiederherstellung mit Fehlern durchgeführt wurde, müssen Sie alle Fehler beheben und die Wiederherstellung so lange erneut ausführen, bis keine Fehler mehr auftreten.

Sie können nach der Einrichtung eines erneuten Schutzes Tests durchführen, um sicherzugehen, dass die neue Konfiguration der Schutz- bzw. Wiederherstellungs-Site gültig ist.

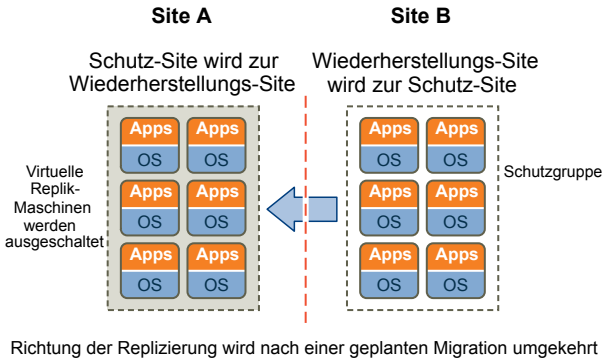
Sie können Schutzgruppen, die virtuellen Maschinen enthalten, die sowohl für die Array-basierte Replizierung als auch für vSphere Replication konfiguriert sind, erneut schützen.

Beispiel: Durchführen eines Vorgangs des erneuten Schutzes

Site A ist die Schutz-Site und Site B ist die Wiederherstellungs-Site. Wenn Site A offline geht, führen Sie den Notfallwiederherstellungs-Workflow des Wiederherstellungsplans aus, um die virtuellen Maschinen auf Site B online zu schalten. Nach der Wiederherstellung werden die geschützten virtuellen Maschinen von Site A auf Site B ohne Schutz gestartet.

Wenn Site A wieder online ist, schließen Sie die Wiederherstellung mittels einer geplanten Migration ab, da Sie die virtuellen Maschinen und Datenspeicher der Site A herunterfahren und unmounten müssen, bevor Sie den Schutz umkehren. Starten Sie dann einen Vorgang des erneuten Schutzes, um die wiederhergestellten virtuellen Maschinen auf Site B zu schützen. Site B wird zur Schutz-Site und Site A wird zur Wiederherstellungs-Site. Site Recovery Manager kehrt die Replizierungsrichtung von Site B nach Site A um.

Abbildung 7-1. Site Recovery Manager -Vorgang des erneuten Schutzes



- Erneuter Schutz von virtuellen Maschinen mithilfe der Array-basierten Replizierung durch Site Recovery Manager

  Beim Vorgang des erneuten Schutzes mithilfe der Array-basierten Replizierung kehrt Site Recovery Manager die Richtung des Schutzes um und erzwingt anschließend die Synchronisierung des Speichers von der neuen Schutz-Site auf die neue Wiederherstellungs-Site.

- Erneuter Schutz von virtuellen Maschinen mithilfe von vSphere Replication durch Site Recovery Manager

  Beim Vorgang des erneuten Schutzes mithilfe von vSphere Replication kehrt Site Recovery Manager die Richtung des Schutzes um und erzwingt anschließend die Synchronisierung des Speichers von der neuen Schutz-Site auf die neue Wiederherstellungs-Site.

- Vorbedingungen zum Durchführen des erneuten Schutzes

  Sie können den erneuten Schutz nur dann durchführen, wenn bestimmte Vorbedingungen erfüllt sind.

- Erneutes Schützen virtueller Maschinen

  Der erneute Schutz führt bei Site Recovery Manager-Schutzgruppen und Wiederherstellungsplänen zu einer Neukonfigurierung, um die Arbeitsrichtung umzukehren. Nach dem erneuten Schützen können Sie virtuelle Maschinen mithilfe eines geplanten Migrations-Workflows auf der ursprünglichen Site wiederherstellen.

- Zustände beim erneuten Schutz

  Der Vorgang zum erneuten Schutz durchläuft mehrere Zustände, die Sie im Wiederherstellungsplan des Site Recovery Manager-Plug-Ins im vSphere-Client beobachten können.

Erneuter Schutz von virtuellen Maschinen mithilfe der Array-basierten Replizierung durch Site Recovery Manager

Beim Vorgang des erneuten Schutzes mithilfe der Array-basierten Replizierung kehrt Site Recovery Manager die Richtung des Schutzes um und erzwingt anschließend die Synchronisierung des Speichers von der neuen Schutz-Site auf die neue Wiederherstellungs-Site.

Wenn Sie den Vorgang zum erneuten Schützen initiieren, weist Site Recovery Manager die zugrunde liegenden Speicher-Arrays an, die Richtung der Replizierung umzukehren. Sobald die Replizierung umgekehrt wurde, erstellt Site Recovery Manager Platzhalter-VMs auf der neuen Wiederherstellungs-Site (der ursprünglichen Schutz-Site).

Bei der Erstellung von Platzhalter-VMs auf der neuen Schutz-Site verwendet Site Recovery Manager den Speicherort der ursprünglich geschützten virtuellen Maschine, um festzulegen, wo die Platzhalter-VM erstellt werden soll. Site Recovery Manager verwendet die Identität der ursprünglich geschützten virtuellen Maschine zum Erstellen des Platzhalters. Wenn die ursprünglich geschützten virtuellen Maschinen nicht mehr verfügbar sind, verwendet Site Recovery Manager die Bestandslistenzuordnungen von der ursprünglichen Wiederherstellungs-Site zur ursprünglichen Schutz-Site, um die Ressourcenpools und -ordner für die Platzhalter-VMs festzulegen. Vor dem Durchführen des erneuten Schutzes müssen Sie Bestandslistenzuordnungen auf beiden Sites konfigurieren. Andernfalls schlägt der erneute Schutz möglicherweise fehl.

Beim erneuten Schützen von virtuellen Maschinen mit der Array-basierten Replizierung speichert Site Recovery Manager die Dateien für die Platzhalter-VMs im Platzhalterdatenspeicher der ursprünglichen Schutz-Site und nicht in dem Datenspeicher, in dem sich die ursprünglich geschützten virtuellen Maschinen befanden.

Die Erzwingung der Synchronisierung von Daten von der neuen Schutz-Site zur neuen Wiederherstellungs-Site stellt sicher, dass die Wiederherstellungs-Site über eine aktuelle Kopie der geschützten virtuellen Maschinen, die auf der Schutz-Site ausgeführt werden, verfügt. Die Erzwingung dieser Synchronisierung stellt sicher, dass eine sofortige Wiederherstellung möglich ist, sobald der Vorgang des erneuten Schutzes abgeschlossen ist.

Weitere Informationen zum erneuten Schutz von virtuellen Maschinen mithilfe von vSphere Replication durch Site Recovery Manager finden Sie unter Erneuter Schutz von virtuellen Maschinen mithilfe von vSphere Replication durch Site Recovery Manager.

Erneuter Schutz von virtuellen Maschinen mithilfe von vSphere Replication durch Site Recovery Manager

Beim Vorgang des erneuten Schutzes mithilfe von vSphere Replication kehrt Site Recovery Manager die Richtung des Schutzes um und erzwingt anschließend die Synchronisierung des Speichers von der neuen Schutz-Site auf die neue Wiederherstellungs-Site.

Beim Durchführen des Vorgangs zum erneuten Schützen mit vSphere Replication verwendet Site Recovery Manager die ursprünglichen VMDK-Dateien als anfängliche Kopien während der Synchronisierung. Die vollständige Synchronisierung, die in den Wiederherstellungsschritten erscheint, führt meistens Prüfsummenausgaben aus. Nur ein kleiner Teil der Daten wird über das Netzwerk übertragen.

Die Erzwingung der Synchronisierung von Daten von der neuen Schutz-Site zur neuen Wiederherstellungs-Site stellt sicher, dass die Wiederherstellungs-Site über eine aktuelle Kopie der geschützten virtuellen Maschinen, die auf der Schutz-Site ausgeführt werden, verfügt. Die Erzwingung dieser Synchronisierung stellt sicher, dass eine sofortige Wiederherstellung möglich ist, sobald der Vorgang des erneuten Schutzes abgeschlossen ist.

Vorbedingungen zum Durchführen des erneuten Schutzes

Sie können den erneuten Schutz nur dann durchführen, wenn bestimmte Vorbedingungen erfüllt sind.

Sie können Schutzgruppen, die virtuellen Maschinen enthalten, die sowohl für die Array-basierte Replizierung als auch für vSphere Replication konfiguriert sind, erneut schützen.

Bevor Sie den erneuten Schutz ausführen können, müssen Sie die Vorbedingungen erfüllen.

1. Führen Sie eine geplante Migration aus und stellen Sie sicher, dass alle Schritte des Wiederherstellungsplans erfolgreich beendet wurden. Wenn bei der Wiederherstellung Fehler auftreten, beheben Sie die Probleme, die die Fehler verursacht haben, und führen Sie die Wiederherstellung erneut aus. Wenn Sie eine Wiederherstellung erneut ausführen, werden Vorgänge, die zuvor erfolgreich ausgeführt wurden, übersprungen. Beispielsweise werden erfolgreich wiederhergestellte virtuelle Maschinen nicht erneut wiederhergestellt und ohne Unterbrechung weiter ausgeführt.
2. Die ursprüngliche Schutz-Site muss verfügbar sein. Die vCenter Server-Instanzen, ESXi Server, Site Recovery Manager Server-Instanzen und die entsprechenden Datenbanken müssen alle wiederherstellbar sein.
3. Wenn Sie eine Notfallwiederherstellung durchgeführt haben, müssen Sie eine geplante Migration durchführen, wenn beide Sites wieder betriebsbereit sind. Falls bei der Durchführung der geplanten Migration Fehler auftreten, müssen diese zunächst behoben und die geplante Migration erneut durchgeführt werden, bis sie erfolgreich abgeschlossen ist.

Der erneute Schutz ist unter bestimmten Umständen nicht verfügbar.

- Wiederherstellungspläne können ohne Fehler nicht beendet werden. Damit der erneute Schutz verfügbar ist, müssen alle Schritte des Wiederherstellungsplans erfolgreich abgeschlossen werden.

- Sie können die ursprüngliche Site nicht wiederherstellen, wenn beispielsweise ein physischer Notfall die ursprüngliche Site zerstört. Um die Verbindungen zwischen der Schutz-Site und der Wiederherstellungs-Site aufzuheben und sie wiederherzustellen, müssen beide Sites verfügbar sein. Wenn Sie die ursprüngliche Schutz-Site nicht wiederherstellen können, müssen Sie Site Recovery Manager sowohl auf der Schutz-Site als auch auf der Wiederherstellungs-Site neu installieren.

Erneutes Schützen virtueller Maschinen

Der erneute Schutz führt bei Site Recovery Manager-Schutzgruppen und Wiederherstellungsplänen zu einer Neukonfigurierung, um die Arbeitsrichtung umzukehren. Nach dem erneuten Schützen können Sie virtuelle Maschinen mithilfe eines geplanten Migrations-Workflows auf der ursprünglichen Site wiederherstellen.

Voraussetzungen

Weitere Informationen hierzu finden Sie unter Vorbedingungen zum Durchführen des erneuten Schutzes.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne**.
2. Klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan und wählen Sie **Neu schützen** aus.
3. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Ihnen bewusst ist, dass das erneute Schützen nicht rückgängig gemacht werden kann.
4. (Optional) Aktivieren Sie das Kontrollkästchen **Bereinigung erzwingen**, um Fehler während des Bereinigungsvorgangs auf der Wiederherstellungs-Site zu ignorieren, und klicken Sie dann auf **Weiter**.

   Die Option **Bereinigung erzwingen** ist nur verfügbar, nachdem Sie einen anfänglichen Vorgang zum erneuten Schützen ausgeführt haben, bei dem Fehler aufgetreten sind.
5. Überprüfen Sie die Informationen für den erneuten Schutz und klicken Sie auf **Beenden**.
6. Wählen Sie den Wiederherstellungsplan aus und klicken Sie auf der Registerkarte **Überwachen > Wiederherstellungsschritte**, um den Fortschritt des Vorgangs zum erneuten Schützen zu überwachen.
7. Wenn der Vorgang zum erneuten Schützen abgeschlossen ist, wählen Sie den Wiederherstellungsplan aus, klicken Sie auf der Registerkarte **Überwachen > Verlauf** und klicken Sie dann auf die Schaltfläche **Exportieren Sie den Bericht für ein ausgewähltes Verlaufselement**.

   Der Wiederherstellungsplan kann wieder in den Zustand „Bereit“ versetzt werden, auch wenn während des Vorgangs zum erneuten Schützen Fehler aufgetreten sind. Suchen Sie im Verlaufsbericht den Vorgang zum erneuten Schützen, und vergewissern Sie sich, dass keine Fehler aufgetreten sind. Wenn während des Vorgangs zum erneuten Schützen Fehler aufgetreten sind, versuchen Sie, diese zu beheben, und führen Sie eine Testwiederherstellung aus, um sicherzustellen, dass keine Fehler

mehr vorliegen. Werden die während des erneuten Schützens aufgetretenen Fehler nicht behoben und versuchen Sie anschließend, eine geplante Migration oder einer Notfallwiederherstellung ohne vorheriges Beseitigen der Fehler auszuführen, werden einige virtuelle Maschinen möglicherweise nicht wiederhergestellt.

Site Recovery Manager tauscht die Wiederherstellungs-Site und die Schutz-Site aus.
Site Recovery Manager erstellt an der neuen Wiederherstellungs-Site Platzhalterkopien der virtuellen Maschinen von der neuen Schutz-Site.

Zustände beim erneuten Schutz

Der Vorgang zum erneuten Schutz durchläuft mehrere Zustände, die Sie im Wiederherstellungsplan des Site Recovery Manager-Plug-Ins im vSphere-Client beobachten können.

Falls der erneute Schutz fehlschlägt oder nur zum Teil erfolgreich verläuft, können Sie Maßnahmen zur Abhilfe ergreifen, um den erneuten Schutz vollständig abzuschließen.

Tabelle 7-1. Zustände beim erneuten Schutz

Zustand	Beschreibung	Maßnahmen zur Abhilfe
Neuer Schutz läuft	Site Recovery Manager führt den erneuten Schutz aus.	Keine
Teilweise neu geschützt	Dieser Status tritt auf, wenn mehrere Wiederherstellungspläne auf dieselben Schutzgruppen zugreifen und der erneute Schutz für einige Gruppen in einigen Plänen erfolgreich verläuft, für andere jedoch nicht.	Führen Sie den erneuten Schutz für die teilweise neu geschützten Pläne nochmals aus.
Neuer Schutz unvollständig	Tritt aufgrund von Fehlern beim erneuten Schützen auf. Dieser Zustand kann beispielsweise aufgrund eines Fehlers bei der Synchronisierung des Speichers oder aufgrund eines Fehlers bei der Erstellung der Platzhalter-VMs auftreten.	■ Wenn während des Vorgangs zum erneuten Schutz die Synchronisierung des Speichers fehlschlägt, stellen Sie sicher, dass die Sites verbunden sind, überprüfen Sie den Fortschritt beim erneuten Schützen im vSphere-Client und starten Sie die Aufgabe zum erneuten Schutz noch einmal. Fall der erneute Schutz immer noch nicht abgeschlossen wird, führen Sie die Aufgabe zum erneuten Schutz mit der Option **Bereinigung erzwingen** aus. ■ Falls das Erstellen von Platzhalter-VMs durch Site Recovery Manager fehlschlägt, ist die Wiederherstellung dennoch möglich. Überprüfen Sie die Schritte zum erneuten Schutz im vSphere-Client, beheben Sie offene Probleme und starten Sie die Aufgabe zum erneuten Schutz erneut.
Neuer Schutz unterbrochen	Tritt auf, wenn eine der Site Recovery Manager-Instanzen während des Vorgangs zum erneuten Schutz unerwartet beendet wird.	Stellen Sie sicher, dass beide Site Recovery Manager-Instanzen ausgeführt werden, und starten Sie die Aufgabe zum erneuten Schutz erneut.

Wiederherstellen der ursprünglichen Konfiguration der Wiederherstellungs-Site durch Failback

8

Wenn Sie nach einer Wiederherstellung die ursprüngliche Konfiguration der Schutz- und der Wiederherstellungs-Site wiederherstellen möchten, können Sie eine Folge optionaler Vorgänge durchführen, die unter dem Begriff Failback zusammengefasst werden.

Nach einer geplanten Migration oder einer Notfallwiederherstellung wird die ehemalige Wiederherstellungs-Site zur Schutz-Site. Sofort nach der Wiederherstellung hat die neue Schutz-Site keine Wiederherstellungs-Site, auf der sie wiederhergestellt werden könnte. Wenn Sie den erneuten Schutz ausführen, wird die neue Schutz-Site durch die ursprüngliche Schutz-Site geschützt. Dabei wird die ursprüngliche Schutzrichtung umgekehrt. Weitere Informationen über das erneute Schützen finden Sie unter Kapitel 7 Erneuter Schutz virtueller Maschinen nach einer Wiederherstellung.

Wenn Sie die anfängliche Konfiguration (die Konfiguration vor der Wiederherstellung) der Schutz- und der Wiederherstellungs-Site wiederherstellen möchten, führen Sie ein Failback aus.

Bei der Ausführung von Failback führen Sie eine Folge von Vorgängen zum erneuten Schutz und für die geplante Migration aus.

1. Durchführen eines erneuten Schutzes. Die Wiederherstellungs-Site wird zur Schutz-Site. Die vorherige Schutz-Site wird zur Wiederherstellungs-Site.
2. Führen Sie eine geplante Migration durch, um die virtuellen Maschinen an der Schutz-Site herunterzufahren und die virtuellen Maschinen an der Wiederherstellungs-Site zu starten. Sie können einen Test durchführen, bevor Sie die geplante Migration starten, um Unterbrechungen bei der Verfügbarkeit der virtuellen Maschinen zu vermeiden. Wenn der Test Fehler erkennt, können Sie sie beheben, bevor Sie die geplante Migration durchführen.
3. Führen Sie einen zweiten Vorgang zum erneuten Schützen durch, um vor der Wiederherstellung die jeweils ursprüngliche Konfiguration der Schutz- und der Wiederherstellungs-Site zurückzusetzen.

Sie können ein Failback konfigurieren und ausführen, wenn Sie bereit sind, die Dienste auf der ursprünglichen Schutz-Site wiederherzustellen, nachdem die Site nach einem Vorfall wieder online ist.

Beispiel: Durchführen eines Failback-Vorgangs

Site A ist die Schutz-Site und Site B ist die Wiederherstellungs-Site. Eine Wiederherstellung wird durchgeführt, bei der die virtuellen Maschinen von Site A nach Site B migriert werden. Sie führen ein Failback durch, um Site A als die Schutz-Site wiederherzustellen.

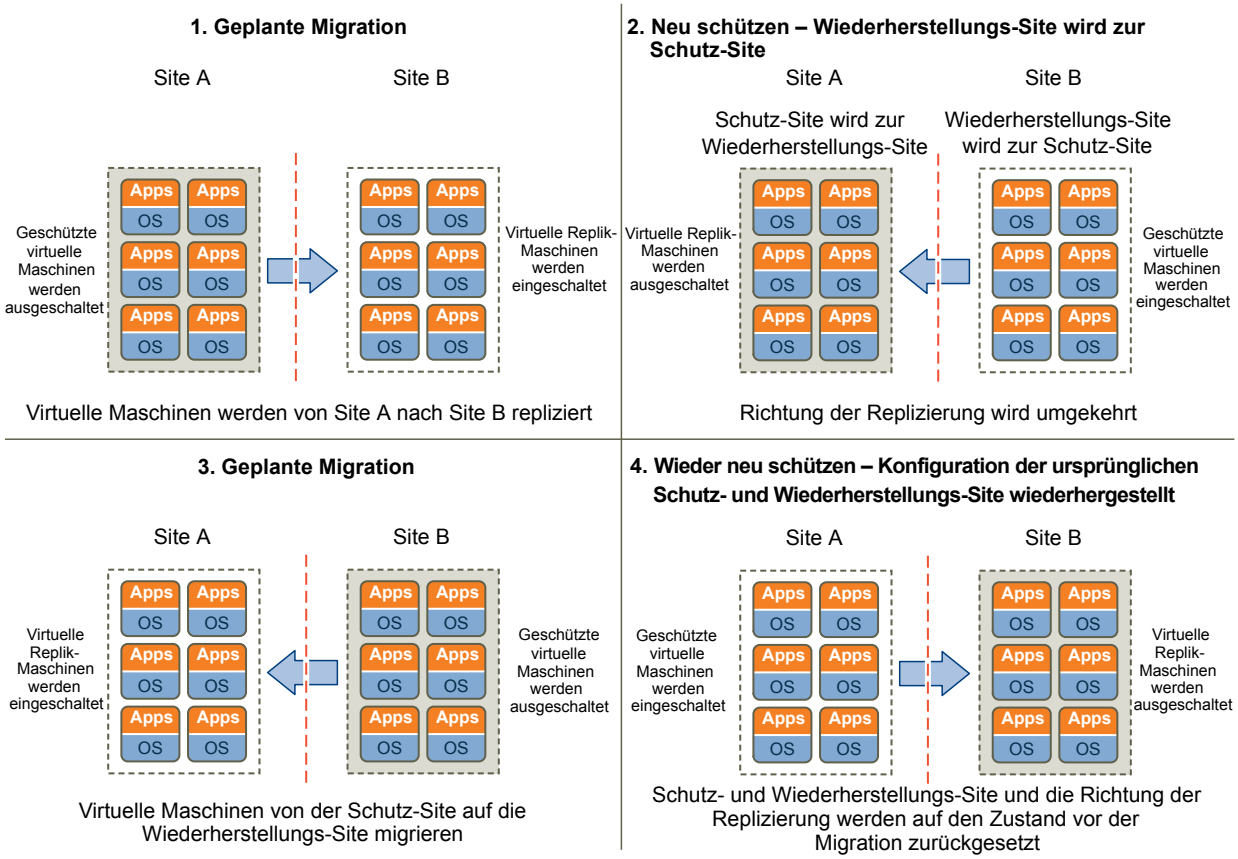
1. Virtuelle Maschinen werden von Site A nach Site B repliziert.

2 Durchführen eines erneuten Schutzes. Site B, die vorherige Schutz-Site, wird zur Wiederherstellungs-Site. Site Recovery Manager verwendet die Schutzinformationen, um den Schutz von Site B herzustellen. Site A wird zur Wiederherstellungs-Site.

3 Führen Sie eine geplante Migration durch, um die geschützten virtuellen Maschinen von Site B an Site A wiederherzustellen.

4 Führen Sie einen zweiten Vorgang zum erneuten Schutz neu aus. Site A wird zur Schutz-Site und Site B wird zur Wiederherstellungs-Site.

Abbildung 8-1. Site Recovery Manager -Failback-Vorgang



Durchführen eines Failbacks

Nachdem Site Recovery Manager eine Wiederherstellung durchgeführt hat, können Sie ein Failback durchführen, um die ursprüngliche Konfiguration der Schutz- und der Wiederherstellungs-Site wiederherzustellen.

Zum besseren Verständnis: Site A ist die ursprüngliche Schutz-Site vor der Wiederherstellung. Site B ist die ursprüngliche Wiederherstellungs-Site. Nach der Wiederherstellung von Site A auf Site B werden die wiederhergestellten virtuellen Maschinen auf Site B ohne Schutz ausgeführt.

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

- Sie haben eine Wiederherstellung im Rahmen einer geplanten Migration oder einer Notfallwiederherstellung durchgeführt.
- Die ursprüngliche Schutz-Site, Site A, wird ausgeführt.
- Wenn Sie eine Notfallwiederherstellung durchgeführt haben, müssen Sie eine geplante Migrationswiederherstellung ausführen, sobald die Hosts und Datenspeicher auf der ursprünglichen Schutz-Site, Site A, wieder ausgeführt werden.
- Nach der Wiederherstellung haben Sie den erneuten Schutz nicht durchgeführt.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Wiederherstellungspläne**.
2. Klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan und wählen Sie **Neu schützen** aus.
3. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Ihnen bewusst ist, dass das erneute Schützen nicht rückgängig gemacht werden kann, und klicken Sie auf **Weiter**.
4. Legen Sie fest, ob **Bereinigung erzwingen** aktiviert werden soll, und klicken Sie auf **Weiter**.

   Diese Option ist nur verfügbar, nachdem Sie „Neu schützen“ einmal ausgeführt haben und Fehler aufgetreten sind. Durch die Aktivierung dieser Option werden das Entfernen von virtuellen Maschinen, Ignorieren von Fehlern und Zurücksetzen des Wiederherstellungsplans auf den Status „Bereit“ erzwungen.
5. Überprüfen Sie die Informationen für den erneuten Schutz und klicken Sie auf **Beenden**.
6. Klicken Sie auf der Registerkarte **Überwachen** auf **Wiederherstellungsschritte**, um den Vorgang zum erneuten Schützen bis zum Abschluss zu überwachen.
7. (Optional) Führen Sie, falls nötig, das erneute Schützen erneut aus, bis keine Fehler mehr auftreten.

   Wenn das erneute Schützen abgeschlossen ist, hat Site Recovery Manager die Replizierung umgekehrt. Site B, die ursprüngliche Wiederherstellungs-Site, ist jetzt die Schutz-Site.
8. (Optional) Nach Abschluss des Tests klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Bereinigen** aus, um den Wiederherstellungsplan zu bereinigen.
9. Klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Wiederherstellung** aus, um den Wiederherstellungsplan als eine geplante Migration auszuführen.

10 Klicken Sie auf der Registerkarte **Überwachen** auf **Wiederherstellungsschritte**, um die geplante Migration bis zum Abschluss zu überwachen.

   Bei der geplanten Migration werden die virtuellen Maschinen auf der neuen Schutz-Site, Site B, heruntergefahren. Die virtuellen Maschinen werden auf Site A, der neuen Wiederherstellungs-Site, gestartet. Führen Sie, falls nötig, die geplante Migration erneut aus, bis sie ohne Fehler abgeschlossen wird.

   Nach Abschluss der geplanten Migration werden die virtuellen Maschinen auf der ursprünglichen Schutz-Site, Site A, ausgeführt. Die virtuellen Maschinen sind jedoch nicht geschützt. Die virtuellen Maschinen der ursprünglichen Wiederherstellungs-Site, Site B, sind ausgeschaltet.

11 Klicken Sie mit der rechten Maustaste auf den Wiederherstellungsplan und wählen Sie **Neu schützen** aus. Folgen Sie dann den Anweisungen des Assistenten, um einen zweiten Vorgang zum erneuten Schützen durchzuführen.

   Hierdurch wird die ursprüngliche Schutzrichtung, wie sie vor der Wiederherstellung bestand, wiederhergestellt.

Sie haben die jeweils ursprüngliche Konfiguration der Schutz- und Wiederherstellungs-Site vor der Wiederherstellung wiederhergestellt. Die Schutz-Site ist Site A und die Wiederherstellungs-Site ist Site B.

Interoperabilität von Site Recovery Manager mit anderer Software

9

Site Recovery Manager Server dient als Erweiterung von vCenter Server an einer Site. Site Recovery Manager ist mit anderen VMware-Lösungen und mit Drittanbieter-Software kompatibel.

Sie können andere VMware-Lösungen, wie z. B. vCenter Update Manager, vCenter Server Heartbeat, VMware Fault Tolerance, vSphere Storage vMotion, vSphere Storage DRS, und vCenter CapacityIQ , in Bereitstellungen ausführen, die Sie mit Site Recovery Manager schützen. Geben Sie allerdings mit Bedacht vor, wenn Sie andere VMware-Lösungen mit der vCenter Server-Instanz verbinden, mit der der Site Recovery Manager Server verbunden ist. Das Verbinden anderer VMware-Lösungen mit derselben vCenter Server-Instanz, mit der Site Recovery Manager verbunden ist, führt möglicherweise zu Problemen, wenn Sie ein Upgrade von Site Recovery Manager oder vSphere durchführen. Überprüfen Sie die Kompatibilität und Interoperabilität der Versionen dieser Lösungen mit Ihrer Version von Site Recovery Manager anhand der *VMware-Produktinteroperabilitätstabellen*.

Dieses Kapitel behandelt die folgenden Themen:

Site Recovery Manager und vCenter Server

Site Recovery Manager nutzt vCenter Server-Dienste, wie beispielsweise Speicherverwaltung, Authentifizierung, Autorisierung und Gastanpassung. Site Recovery Manager verwendet auch den Standardsatz der vSphere-Verwaltungstools zur Verwaltung dieser Dienste.

Da der Site Recovery Manager Server für einige Dienste von vCenter Server abhängig ist, müssen Sie vCenter Server auf einer Site installieren und konfigurieren, bevor Sie Site Recovery Manager installieren.

Sie können Site Recovery Manager und vSphere Replication mit der vCenter Server Appliance oder mit einer standardmäßigen vCenter Server-Installation verwenden. Die vCenter Server Appliance kann auch an einer Site und eine standardmäßige vCenter Server-Installation an einer anderen Site vorliegen.

Wie Änderungen an der vCenter Server -Bestandsliste Site Recovery Manager beeinflussen

Da sich Site Recovery Manager-Schutzgruppen auf eine Teilmenge der vCenter Server-Bestandsliste beziehen, können durch vCenter Server-Administratoren und -Benutzer vorgenommene Änderungen an der geschützten Bestandsliste Auswirkungen auf die Integrität des Schutzes und der Wiederherstellung von Site Recovery Manager haben. Site Recovery Manager ist von der Verfügbarkeit bestimmter Objekte, z. B. von virtuellen Maschinen, Ordnern, Ressourcenpools und Netzwerken, in der vCenter Server-Bestandsliste auf der Schutz-Site und der Wiederherstellungs-Site abhängig. Durch das Löschen von Ressourcen, z. B. von Ordnern oder Netzwerken, die von Wiederherstellungsplänen referenziert werden, kann der Plan ungültig werden. Das Umbenennen oder Verschieben von Objekten in der vCenter Server-Bestandsliste hat keine Auswirkungen auf Site Recovery Manager, sofern bei Test- oder Wiederherstellungsvorgängen alle Ressourcen zugänglich sind.

Site Recovery Manager kann bestimmte Änderungen an der Schutz-Site ohne Betriebsunterbrechungen tolerieren.

- Entfernen von geschützten virtuellen Maschinen.
- Entfernen eines Objekts, für das eine Bestandslistenzuordnung existiert.

Site Recovery Manager kann bestimmte Änderungen an der Wiederherstellungs-Site ohne Betriebsunterbrechungen tolerieren.

- Verschieben von Platzhalter-VMs in einen anderen Ordner oder Ressourcenpool.
- Entfernen eines Objekts, für das eine Bestandslistenzuordnung existiert.

Site Recovery Manager und die vCenter Server -Datenbank

Initialisieren Sie bei einem Update der vCenter Server-Installation, die Site Recovery Manager erweitert, nicht die vCenter Server-Datenbank neu. Site Recovery Manager speichert Identifikationsdaten zu allen vCenter Server-Objekten in der Site Recovery Manager-Datenbank. Wenn Sie die vCenter Server-Datenbank erneut initialisieren, stimmen die von Site Recovery Manager gespeicherten Identifikationsdaten nicht mehr mit den Identifikationsdaten in der neuen vCenter Server-Instanz überein, was dazu führt, dass Objekte nicht mehr gefunden werden.

Verwenden von Site Recovery Manager und vSphere Replication mit VMware Virtual SAN-Speicher

Sie können den VMware Virtual SAN-Speicher mit vSphere Replication und Site Recovery Manager verwenden.

Site Recovery Manager 6.0 unterstützt vSphere Replication 6.0 mit VMware Virtual SAN 6.0.

So interagiert Site Recovery Manager während der Wiederherstellung mit DPM und DRS

Distributed Power Management (DPM) und Distributed Resource Scheduler (DRS) sind nicht obligatorisch, aber Site Recovery Manager unterstützt beide Dienste, und dies bietet bei der Verwendung von Site Recovery Manager gewisse Vorteile.

DPM ist eine VMware-Funktion, die den Energieverbrauch von ESX-Hosts verwaltet. DRS ist eine VMware-Komponente, die die Zuweisung von virtuellen Maschinen zu ESX-Hosts verwaltet.

Site Recovery Manager deaktiviert DPM vorübergehend für den Cluster auf der Wiederherstellungs-Site und stellt sicher, dass alle Hosts im Cluster eingeschaltet sind, wenn die Wiederherstellung bzw. die Testwiederherstellung beginnt. Dies ermöglicht bei der Wiederherstellung von virtuellen Maschinen eine ausreichende Hostkapazität. Nach Abschluss der Wiederherstellung bzw. des Tests stellt
Site Recovery Manager die DPM-Einstellungen auf dem Cluster der Wiederherstellungs-Site auf ihre ursprünglichen Werte zurück.

Im Falle von geplanten Migrationen und Vorgängen zum erneuten Schützen deaktiviert
Site Recovery Manager DPM auch auf den betroffenen Clustern der Schutz-Site und stellt sicher, dass alle Hosts im Cluster eingeschaltet sind. Dies ermöglicht Site Recovery Manager, Vorgänge auf Hostebene abzuschließen, z. B. das Unmounten von Datenspeichern oder das Bereinigen von Speicher nach einem Vorgang zum erneuten Schützen. Nach Abschluss der geplanten Migration bzw. des Vorgangs zum erneuten Schützen stellt Site Recovery Manager die DPM-Einstellungen auf dem Cluster der Schutz-Site auf die ursprünglichen Werte zurück.

Die Hosts im Cluster bleiben im Zustand „Wird ausgeführt“, sodass DPM sie bei Bedarf ausschalten kann. Site Recovery Manager registriert virtuelle Maschinen auf allen verfügbaren ESX-Hosts in Round-Robin-Reihenfolge, um die potenzielle Last so gleichmäßig wie möglich zu verteilen. Site Recovery Manager verwendet immer die DRS-Platzierung, um die Last intelligent auf die Hosts zu verteilen, bevor er wiederhergestellte virtuelle Maschinen auf der Wiederherstellungs-Site einschaltet, selbst wenn DRS auf dem Cluster deaktiviert ist.

Falls DRS aktiviert ist und sich im vollautomatischen Modus befindet, verschiebt DRS möglicherweise andere virtuelle Maschinen, um die Last noch besser auf die Cluster zu verteilen, während Site Recovery Manager die wiederhergestellten virtuellen Maschinen einschaltet. DRS verteilt alle virtuellen Maschinen auch weiter auf die Cluster, nachdem Site Recovery Manager die wiederhergestellten virtuellen Maschinen eingeschaltet hat.

So interagiert Site Recovery Manager mit Storage DRS oder Storage vMotion

Sie können Site Recovery Manager beim Schutz virtueller Maschinen auf Sites verwenden, die für Storage DRS oder Storage vMotion konfiguriert sind, wenn Sie bestimmte Richtlinien einhalten.

Das Verhalten von Storage DRS oder Storage vMotion hängt davon ab, ob Sie Site Recovery Manager mit Array-basierter Replizierung oder mit vSphere Replication verwenden.

Informationen dazu, wie Site Recovery Manager Datenspeicher-Tagging für Storage DRS verarbeitet, finden Sie unter http://kb.vmware.com/kb/2108196.

Verwenden von Site Recovery Manager mit Array-basierter Replizierung auf Sites mit Storage DRS oder Storage vMotion

Folgen Sie den Richtlinien, wenn Sie Array-basierte Replizierung verwenden, um virtuelle Maschinen auf Sites mit Storage DRS oder Storage vMotion zu schützen.

- Während der Berechnung der Platzierungsempfehlungen für die Durchführung einer automatischen oder manuellen Migration berücksichtigt Storage DRS den Schutz und den Replikationsstatus von Datenspeichern. Storage DRS überprüft, ob der Datenspeicher repliziert wird oder nicht, Teil einer Konsistenzgruppe oder Schutzgruppe ist, und führt das Tagging des Datenspeichers entsprechend durch. Weitere Informationen darüber, wie Site Recovery Manager das Tagging von Datenspeichern handhabt, finden Sie unter http://kb.vmware.com/kb/2108196.
- Site Recovery Manager unterstützt Storage DRS-Cluster, die Datenspeicher aus unterschiedlichen Konsistenzgruppen enthalten. Wenn Sie eine virtuelle Maschine auf einen Datenspeicher migrieren, der nicht Teil einer der Schutzgruppe ist, müssen Sie die Schutzgruppe neu konfigurieren, um diesen Datenspeicher aufzunehmen.
- Site Recovery Manager unterstützt Storage vMotion ohne Einschränkungen zwischen nicht replizierten Datenspeichern und zwischen replizierten Datenspeichern in der gleichen Konsistenzgruppe. In diesen Fällen kann Storage DRS automatisch Storage vMotion in Clustern im automatischen Modus durchführen, oder Empfehlungen für Storage vMotion in Clustern im manuellen Modus ausgeben.

- Besondere Beachtung gilt für Storage vMotion zwischen replizierten und nicht replizierten Datenspeichern, oder zwischen replizierten Datenspeichern in unterschiedlichen Konsistenzgruppen. In diesen Fällen initiiert oder empfiehlt Storage DRS nicht automatisch Storage vMotion. Eine manuelle Initiierung von Storage vMotion führt zu einer Warnung mit Details zu den möglichen Auswirkungen.
- Verwenden Sie Storage DRS oder Storage vMotion nicht, um virtuelle Maschinen regelmäßig zu verschieben. Akzeptieren Sie keine Empfehlungen, virtuelle Maschinen regelmäßig manuell zu verschieben. Sie können virtuelle Maschinen gelegentlich verschieben, aber übermäßiges Verschieben von virtuellen Maschinen kann zu Problemen führen. Beim Verschieben virtueller Maschinen muss das Array die virtuellen Maschinen über das Netzwerk replizieren und dies ist zeitaufwendig und verbraucht Bandbreite. Wenn virtuelle Maschinen durch Storage DRS oder Storage vMotion verschoben werden, können während einer Wiederherstellung Probleme auftreten:
  - Wenn eine virtuelle Maschine durch Storage DRS oder Storage vMotion in eine andere Konsistenzgruppe innerhalb derselben Schutzgruppe verschoben wird, vergeht etwas Zeit zwischen der Weitergabe des neuen Speicherorts der virtuellen Maschine durch Site Recovery Manager an die Wiederherstellungs-Site und der Replizierung der Änderungen durch das Array auf die Wiederherstellungs-Site. Außerdem vergeht Zeit, in der die Arrays die Quell- und Ziel-Konsistenzgruppen replizieren, bis ein konsistenter Zustand auf der Wiederherstellungs-Site erreicht ist. Während das Array alle Änderungen an die Wiederherstellungs-Site weitergibt, kann eine Notfallwiederherstellung dieser virtuellen Maschine fehlschlagen.
  - Wenn Storage DRS oder Storage vMotion eine virtuelle Maschine in eine andere Schutzgruppe verschiebt, generiert Site Recovery Manager einen Schutzfehler für diese virtuelle Maschine. Sie müssen die Konfiguration des Schutzes der virtuellen Maschine in der alten Schutzgruppe aufheben und Schutz für die virtuelle Maschine in der neuen Schutzgruppe konfigurieren. Bis zur Konfiguration des Schutzes in der neuen Schutzgruppe schlagen geplante Migrationen oder Notfallwiederherstellungen dieser virtuellen Maschine fehl.
- Das Hinzufügen einer Festplatte zu einer geschützten virtuellen Maschine führt zu den gleichen Problemen wie das Verschieben einer kompletten virtuellen Maschine. Site Recovery Manager hindert Sie nicht daran, diese Aktion auszuführen, aber wenn eine virtuelle Maschine eine nicht replizierte Festplatte enthält und Sie diese nicht vom Schutz ausschließen, kommt es nach der Verschiebung beim Einschalten der virtuellen Maschine zu einem Fehler.

Verwenden von Site Recovery Manager mit vSphere Replication auf Sites mit Storage DRS oder Storage vMotion

Folgen Sie den Richtlinien, wenn Sie vSphere Replication verwenden, um virtuelle Maschinen auf Sites mit Storage DRS oder Storage vMotion zu schützen oder wiederherzustellen.

- vSphere Replication ist zumit vSphere Storage vMotion und vSphere Storage DRS sowohl an Schutz-Sites als auch an Wiederherstellungs-Sites kompatibel. Sie können Storage vMotion und Storage DRS zum Verschieben der Dateien der replizierten Festplatte einer von vSphere Replication geschützten virtuellen Maschine verwenden, ohne dass dies Auswirkungen auf die Replizierung hat. Site Recovery Manager erkennt die Änderungen und Fehler über die virtuelle Maschine erfolgreich.

- Site Recovery Manager unterstützt Storage DRS-Cluster an der Wiederherstellungs-Site mit Datenspeichern, die die replizierten Festplatten von vSphere Replication enthalten.
- vSphere Replication ist mit Storage vMotion kompatibel und speichert den Status einer Festplatte oder virtuellen Maschine, wenn das Basisverzeichnis der Festplatte oder virtuellen Maschine verschoben wird. Die Replizierung der Festplatte oder virtuellen Maschine wird nach der Verschiebung normal fortgesetzt.
- Storage vMotion wird von Storage DRS bei einer vollständigen Synchronisierung nur dann ausgelöst, wenn eine sehr aggressive Einstellung für die Storage DRS-Regeln ausgewählt wurde oder wenn für eine große Zahl von virtuellen Maschinen gleichzeitig eine vollständige Synchronisierung durchgeführt wird. Der E/A-Latenz-Schwellenwert für Storage DRS beträgt standardmäßig 15 ms. Standardmäßig führt Storage DRS alle 8 Stunden Lastausgleichsvorgänge durch. Storage DRS wartet zudem, bis ausreichende Statistiken zur E/A-Last erfasst wurden, bevor Storage vMotion-Empfehlungen generiert werden. Folglich beeinträchtigt eine vollständige Synchronisierung die Storage DRS-Empfehlungen nur, wenn sie lange dauert und wenn die während dieser Zeit durch die vollständige Synchronisierung verursachten zusätzlichen Eingaben/Ausgaben dazu führen, dass der E/A-Latenz-Schwellenwert überschritten wird.
- Wenn Sie Storage DRS im manuellen Modus auf Datenspeichern einer geschützten virtuellen Maschine verwenden, bestehen nach einem Failover möglicherweise veraltete Empfehlungen. Wenn Sie diese veralteten Storage DRS-Empfehlungen anwenden, wird nach dem erneuten Schützen der Failover-VMs zur ursprünglichen Site die Site Recovery Manager-Platzhalter-VM beschädigt, was dazu führt, dass eine weitere Wiederherstellung zur ursprünglichen Site für die VMs fehlschlägt, für die die Storage DRS-Empfehlungen angewendet wurden. Wenn Sie veraltete Updates anwenden, entfernen Sie die Registrierung der Platzhalter-VM und verwenden Sie den Site Recovery Manager-Reparaturvorgang, um einen gültigen Platzhalter neu zu erstellen. Um dieses Problem zu vermeiden, deaktivieren Sie alle veralteten Empfehlungen von einem vorangegangenen Failover von dieser Site, indem Sie für das betroffene Storage DRS-Speichercluster erneut Storage DRS-Empfehlungen generieren, nachdem das erneute Schützen erfolgreich abgeschlossen ist.

Wie Site Recovery Manager mit vSphere High Availability interagiert

Sie können Site Recovery Manager zum Schützen von virtuellen Maschinen verwenden, auf denen vSphere High Availability (HA) aktiviert ist.

HA schützt virtuelle Maschinen vor ESXi-Hostausfällen, indem virtuelle Maschinen von Hosts, die ausfallen, auf neuen Hosts innerhalb derselben Site neu gestartet werden. Site Recovery Manager schützt virtuelle Maschinen vor Site-Ausfällen, indem die virtuellen Maschinen auf der Wiederherstellungs-Site neu gestartet werden. Der wesentliche Unterschied zwischen HA und Site Recovery Manager besteht darin, dass HA auf einzelnen virtuellen Maschinen arbeitet und die virtuelle Maschinen automatisch neu startet. Site Recovery Manager arbeitet auf Wiederherstellungsplanebene und erfordert, dass ein Benutzer die Wiederherstellung manuell initiiert.

Um die HA-Einstellungen für eine virtuelle Maschine auf die Wiederherstellungs-Site zu übertragen, müssen Sie nach dem Konfigurieren des Schutzes der virtuellen Maschine die HA-Einstellungen auf der Platzhalter-VM festlegen, bevor Sie die Wiederherstellung durchführen.

Sie können HA-VMs mit der Array-basierten Replizierung oder mit vSphere Replication replizieren. Wenn HA eine geschützte virtuelle Maschine auf einem anderen Host auf der Schutz-Site neu startet, führt vSphere Replication eine vollständige Synchronisierung durch, nachdem die virtuelle Maschine neu gestartet wurde.

Site Recovery Manager erfordert HA als Voraussetzung für den Schutz von virtuellen Maschinen nicht. Ebenso erfordert HA Site Recovery Manager nicht.

Site Recovery Manager und vSphere PowerCLI

VMware vSphere PowerCLI bietet eine Windows PowerShell-Schnittstelle für den Zugriff auf Site Recovery Manager-Aufgaben mittels Befehlszeile.

vSphere PowerCLI legt die Site Recovery Manager-APIs frei. Sie können vSphere PowerCLI verwenden, um Site Recovery Manager zu verwalten oder Skripts zu erstellen, die Site Recovery Manager-Aufgaben automatisieren.

Weitere Informationen darüber, wie Site Recovery Manager durch die Verwendung von vSphere PowerCLI verwaltet wird, finden Sie in der vSphere PowerCLI-Dokumentation unter https://www.vmware.com/support/developer/PowerCLI/.

Site Recovery Manager und vRealize Orchestrator

Mit dem vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager können Sie bestimmte Site Recovery Manager-Vorgänge automatisieren, indem Sie sie in vRealize Orchestrator-Workflows einbeziehen.

Das vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager stellt Aktionen und Workflows bereit, mit denen Site Recovery Manager-Vorgänge ausgeführt werden. Als vRealize Orchestrator-Administrator können Sie Workflows erstellen, die die Aktionen und Workflows aus dem Site Recovery Manager-Plug-In einschließen. Durch das Einschließen von Site Recovery Manager-Aktionen und -Workflows in vRealize Orchestrator-Workflows können Sie Site Recovery Manager-Vorgänge mit den automatisierten Vorgängen anderer vRealize Orchestrator-Plug-Ins kombinieren.

Beispielsweise können Sie einen Workflow erstellen, der mithilfe der Aktionen und Workflows des vRealize Orchestrator-Plug-Ins für vCenter Server virtuelle Maschinen erstellt und konfiguriert und sie für vCenter Server registriert. Im selben Workflow können Sie mithilfe der Aktionen und Workflows aus dem Site Recovery Manager-Plug-In Schutzgruppen erstellen und die virtuellen Maschinen schützen, sobald sie erstellt wurden. Darüber hinaus können Sie mit den Site Recovery Manager-Aktionen und -Workflows einige der Wiederherstellungseinstellungen für die geschützten virtuellen Maschinen konfigurieren. Durch die Kombination der Aktionen und Workflows von vCenter Server und Site Recovery Manager in einem vRealize Orchestrator-Workflow können Sie demnach den Vorgang zum Erstellen und Schützen virtueller Maschinen automatisieren.

Das vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager können Sie in einer Konfiguration mit gemeinsam genutzter Wiederherstellungs-Site verwenden, bei der Sie mehrere Site Recovery Manager-Instanzen mit einer einzelnen vCenter Server-Instanz verbinden. Darüber hinaus können Sie das vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager mit mehreren Site Recovery Manager-Instanzen in mehreren vCenter Server-Instanzen verwenden, die mit demselben vCenter Single Sign-On-Server verbunden sind.

Weitere Informationen zum Erstellen von Workflows mithilfe von vRealize Orchestrator finden Sie in der Dokumentation zu vRealize Orchestrator.

Weitere Informationen zur Verwendung des vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager finden Sie in der Dokumentation zu den vRealize Orchestrator-Plug-Ins.

Automatisierte Vorgänge des vRealize Orchestrator -Plug-Ins für Site Recovery Manager

Mit dem vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager können Sie das Erstellen Ihrer Site Recovery Manager-Infrastruktur automatisieren, um virtuelle Maschinen zu Schutzgruppen hinzuzufügen und um die Wiederherstellungseinstellungen von virtuellen Maschinen zu konfigurieren.

Mit dem vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager können Sie virtuelle Maschinen schützen, indem Sie sie zur Array-basierten Replizierung oder zu vSphere Replication-Schutzgruppen hinzufügen. Die Konfiguration von vSphere Replication auf virtuellen Maschinen wird mit diesem Plug-In nicht automatisiert. Sie können das vRealize Orchestrator-Plug-In für vSphere Replication verwenden, um vSphere Replication auf virtuellen Maschinen zu konfigurieren, oder konfigurieren Sie vSphere Replication manuell. Informationen zum vRealize Orchestrator-Plug-In für vSphere Replication finden Sie in den Versionshinweisen zu vRealize Orchestrator-Plug-In für vSphere Replication 6.0.

Aufgrund der massiven Auswirkungen einer Wiederherstellung auf die Schutz- und Wiederherstellungs-Sites können Sie Testwiederherstellungen, geplante Migrationen oder Notfallwiederherstellungen nicht mit dem vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager automatisieren. Die Automatisierung von Wiederherstellungen wäre zu kompliziert und würde in jedem Fall das Eingreifen des Benutzers erfordern.

Das vRealize Orchestrator-Plug-In für vCenter Site Recovery Manager enthält vRealize Orchestrator-Aktionen, Workflows, Richtlinienvorlagen zum Auslösen von Aktionen beim Auftreten bestimmter Ereignisse sowie Skriptobjekte, um ausgewählte Elemente der Site Recovery Manager-API für Workflows verfügbar zu machen.

- Dieses Plug-In stellt Aktionen und Workflows bereit, mit denen eine Site Recovery Manager-Infrastruktur erstellt wird:
  - Erstellen von Array-basierten Schutzgruppen und vSphere Replication-Schutzgruppen
  - Erstellen von Bestandslistenzuordnungen zwischen übereinstimmenden Objekten
  - Hinzufügen von Schutzgruppen zu vorhandenen Wiederherstellungsplänen
- Dieses Plug-In stellt Aktionen und Workflows bereit, mit denen virtuelle Maschinen geschützt werden:
  - Schützen einer virtuellen Maschine mithilfe einer vorhandenen Array-basierten Schutzgruppe

    - Schützen einer virtuellen Maschine mithilfe einer vorhandenen vSphere Replication-Schutzgruppe
- Dieses Plug-In stellt Aktionen und Workflows bereit, mit denen Wiederherstellungseinstellungen auf virtuellen Maschinen konfiguriert werden:
    - Festlegen der Wiederherstellungspriorität
    - Erstellen von Wiederherstellungsschritten pro virtueller Maschine
    - Festlegen des abschließenden Betriebszustands einer wiederhergestellten virtuellen Maschine
- Dieses Plug-In stellt Aktionen und Workflows bereit, mit denen Informationen von Site Recovery Manager Server abgerufen werden:
    - Geschützte Datenspeicher auflisten
    - Auflisten von Schutzgruppen und Wiederherstellungsplänen
    - Suchen nach Array-basierten Schutzgruppen anhand des Datenspeichers
    - Abrufen von nicht zugewiesenen Replizierungsdatenspeichern und Wiederherstellungsplanstatus

Schützen von Microsoft Cluster Server und fehlertoleranten virtuellen Maschinen

Sie können Site Recovery Manager zum Schützen von Microsoft Cluster Server (MSCS) und fehlertoleranten virtuellen Maschinen verwenden. Hierbei gibt es jedoch Einschränkungen.

Um Site Recovery Manager zum Schutz von MSCS und fehlertoleranten virtuellen Maschinen zu verwenden, müssen Sie möglicherweise Ihre Umgebung ändern.

Allgemeine Einschränkungen beim Schutz von MSCS und fehlertoleranten virtuellen Maschinen

Für das Schützen von MSCS und fehlertoleranten virtuellen Maschinen gelten die folgenden Einschränkungen:

- Sie können die Array-basierte Replizierung nur verwenden, um virtuelle MSCS-Maschinen zu schützen. Das Schützen von virtuellen MSCS-Maschinen mit vSphere Replication wird nicht unterstützt.
- Für den erneuten Schutz von MSCS bzw. fehlertoleranten virtuellen Maschinen ist VMware High Availability (HA) und VMware Distributed Resource Scheduler (DRS) erforderlich. Wenn Sie während des erneuten Schutzes die virtuellen MSCS-Maschinen und die fehlertoleranten virtuellen Maschinen über deren primäre und sekundäre Sites hinweg verschieben, müssen Sie HA und DRS aktivieren und dabei die Affinitäts- und die Anti-Affinitätsregeln entsprechend festlegen. Weitere Informationen hierzu finden Sie unter DRS-Anforderungen zum Schutz von virtuellen MSCS-Maschinen.
- Site Recovery Manager unterstützt keine virtuellen Maschinen mit Fault Tolerance, die mit mehreren vCPUs bestückt sind (SMP-FT).

Anforderungen für ESXi -Hosts zum Schutz von virtuellen MSCS-Maschinen

Um MSCS oder fehlertolerante virtuelle Maschinen zu schützen, müssen ESXi-Hostmaschinen, auf denen die virtuellen Maschinen ausgeführt werden, bestimmte Kriterien erfüllen.

- Sie müssen eine fehlertolerante virtuelle Maschine und ihren Schatten auf zwei unterschiedlichen ESXi-Server-Instanzen ausführen.
- Sie können einen Cluster von virtuellen MSCS-Maschinen bei den folgenden möglichen Konfigurationen ausführen.

Cluster-in-a-box	Die virtuellen MSCS-Maschinen im Cluster werden auf einem einzelnen ESXi Server ausgeführt. Es darf maximal fünf MSCS-Knoten auf einem ESXi-Server geben.
Systemübergreifende Cluster	Sie können den MSCS-Cluster über maximal zwei ESXi-Server-Instanzen verteilen. Sie können nur einen VM-Knoten eines MSCS-Clusters auf einer einzelnen ESXi Server-Instanz schützen. Es können mehrere MSCS-Knoten-VMs auf einem ESXi-Host ausgeführt werden, sofern sie sich nicht in demselben MSCS-Cluster befinden. Diese Konfiguration benötigt für die Quorum-Festplatte gemeinsam genutzten Speicher auf einem Fibre-Channel-SAN.

DRS-Anforderungen zum Schutz von virtuellen MSCS-Maschinen

Um DRS auf Sites zu verwenden, die virtuelle MSCS-Maschinen enthalten, müssen Sie die DRS-Regeln konfigurieren, um Site Recovery Manager den Schutz der virtuellen Maschinen zu erlauben. Durch die Befolgung der Richtlinien können Sie virtuelle MSCS-Maschinen auf Sites schützen, die DRS ausführen, wenn die Platzhalter-VMs sich entweder in einer MSCS-Bereitstellung des systemübergreifenden Clusters oder in einer MSCS-Bereitstellung des systeminternen Clusters befinden.

- Legen Sie die DRS-Regeln auf den virtuellen Maschinen auf der Schutz-Site fest, bevor Sie MSCS im Gastbetriebssystem konfigurieren. Legen Sie die DRS-Regeln sofort nach dem Bereitstellen, Konfigurieren oder Einschalten der virtuellen Maschinen fest.
- Legen Sie die DRS-Regeln auf den virtuellen Maschinen auf der Wiederherstellungs-Site sofort nach dem Erstellen einer Schutzgruppe von MSCS-Knoten fest, sobald die Platzhalter-VMs auf der Wiederherstellungs-Site angezeigt werden.
- DRS-Regeln, die Sie auf der Schutz-Site festgelegt haben, werden nach der Wiederherstellung nicht auf die Wiederherstellungs-Site übertragen. Aus diesem Grund müssen Sie die DRS-Regeln auf den Platzhalter-VMs auf der Wiederherstellungs-Site festlegen.
- Führen Sie eine Testwiederherstellung oder eine echte Wiederherstellung aus, bevor Sie die DRS-Regeln auf der Wiederherstellungs-Site festlegen.

Wenn Sie die Richtlinien entweder auf der Schutz-Site oder auf der Wiederherstellungs-Site nicht befolgen, verschiebt vSphere vMotion möglicherweise virtuelle MSCS-Maschinen auf eine Konfiguration, die Site Recovery Manager nicht unterstützt.

- In einer systeminternen Cluster-Bereitstellung entweder auf der Schutz-Site oder der Wiederherstellungs-Site verschiebt vSphere vMotion möglicherweise virtuelle MSCS-Maschinen auf unterschiedliche ESXi-Hosts.
- In einer systeminternen Cluster-Bereitstellung entweder auf der Schutz-Site oder der Wiederherstellungs-Site verschiebt vSphere vMotion möglicherweise einige oder alle virtuelle MSCS-Maschinen auf einen einzelnen ESXi-Host.

Verwenden von Site Recovery Manager mit SIOC-Datenspeichern

Storage I/O Control (SIOC) wird von Site Recovery Manager unterstützt.

Geplante Migration von virtuellen Maschinen auf Datenspeichern, die SIOC verwenden

In vorherigen Versionen von Site Recovery Manager mussten Sie vor der Ausführung einer geplanten Migration Storage I/O Control (SIOC) auf Datenspeichern, die Sie in einen Wiederherstellungsplan aufgenommen haben, deaktivieren. Diese Version von Site Recovery Manager unterstützt SIOC vollständig. Vor der Ausführung einer geplanten Migration müssen Sie SIOC also nicht reaktivieren.

Notfallwiederherstellung und neuer Schutz von virtuellen Maschinen auf Datenspeichern, die SIOC verwenden

In vorherigen Versionen von Site Recovery Manager wurde die Wiederherstellung mit Fehlern durchgeführt, wenn Sie einen Wiederherstellungsvorgang mit aktivierter SIOC durchgeführt haben. Nach der Wiederherstellung mussten Sie SIOC auf der Schutz-Site manuell deaktivieren und erneut eine geplante Migrationswiederherstellung durchführen. Sie konnten den Vorgang zum erneuten Schützen erst dann durchführen, wenn Sie eine geplante Migration erfolgreich durchgeführt hatten. Diese Version von Site Recovery Manager unterstützt SIOC vollständig. Die Wiederherstellung gelingt ohne Fehler und Sie können nach einer Notfallwiederherstellung eine geplante Migration und den Vorgang zum erneuten Schützen ausführen, ohne SIOC zu deaktivieren.

Verwenden von Site Recovery Manager mit Zugangssteuerungs-Clustern

Sie können die Zugangssteuerung auf einem Cluster verwenden, um Ressourcen auf der Wiederherstellungs-Site zu reservieren.

Das Verwenden der Zugangssteuerung kann allerdings die Notfallwiederherstellung beeinträchtigen, indem Site Recovery Manager bei der Ausführung eines Wiederherstellungsplans das Einschalten virtueller Maschinen verhindert. Die Zugangssteuerung kann verhindern, dass virtuelle Maschinen eingeschaltet werden, wenn ein Einschalten die relevanten Zugangssteuerungs-Einschränkungen verletzt.

Sie können einen Befehlsschritt zu einem Wiederherstellungs-Plan hinzufügen, um ein PowerCLI-Skript auszuführen, das die Zugangssteuerung während der Wiederherstellung deaktiviert. Weitere Informationen über das Erstellen von Befehlsschritten finden Sie unter Erstellen von benutzerdefinierten Wiederherstellungsschritten.

1 Erstellen Sie einen Befehlsschritt vor dem Einschalten in dem Wiederherstellungsplan, der ein PowerCLI-Skript ausführt, um die Zugangssteuerung zu deaktivieren.

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$false
```

2 Erstellen Sie einen Befehlsschritt nach dem Einschalten in dem Wiederherstellungsplan, um die Zugangssteuerung nach dem Einschalten der virtuellen Maschine neu zu aktivieren.

```
Get-Cluster cluster_name | Set-Cluster -HAAdmissionControlEnabled:$true
```

Wenn Sie die Zugangssteuerung während der Wiederherstellung deaktivieren, müssen Sie die Zugangssteuerung manuell neu aktivieren, nachdem Sie eine Bereinigung nach einer Testwiederherstellung durchgeführt haben. Das Deaktivieren der Zugangssteuerung beeinträchtigt möglicherweise die Hochverfügbarkeit zum Neustarten von virtuellen Maschinen auf der Wiederherstellungs-Site. Deaktivieren Sie die Zugangssteuerung nicht über einen längeren Zeitraum.

Site Recovery Manager und mit RDM-Festplattengeräten verbundene virtuelle Maschinen

Schutz und Wiederherstellung von mit einem RDM-Festplattengerät verbundenen virtuellen Maschinen werden unterschiedlich unterstützt, je nachdem, ob Sie die Array-basierte Replizierung oder vSphere Replication einsetzen.

- Die Array-basierte Replizierung unterstützt RDM-Geräte im physischen und im virtuellen Kompatibilitätsmodus. Wenn Sie Site Recovery Manager mit der Array-basierten Replizierung verwenden, können Sie virtuelle Maschinen, die RDM verwenden, entweder im physischen oder im virtuellen Kompatibilitätsmodus schützen und wiederherstellen.
- vSphere Replication unterstützt RDM-Geräte nur im virtuellen Modus sowohl für das Quell- als auch für das Zielgerät. Wenn Sie vSphere Replication verwenden, können Sie virtuelle Maschinen, die RDM verwenden, nicht im physischen Kompatibilitätsmodus schützen und wiederherstellen.
- Wenn Sie sowohl die Array-basierte Replizierung als auch vSphere Replication verwenden, können Sie nur durch Verwendung der Array-basierten Replizierung virtuelle Maschinen, die RDM verwenden, im physischen Kompatibilitätsmodus schützen und wiederherstellen. Sie können virtuelle Maschinen, die RDM verwenden, entweder durch die Verwendung der Array-basierten Replizierung oder von vSphere Replication im virtuellen Kompatibilitätsmodus schützen und wiederherstellen.

Site Recovery Manager und Active Directory-Domänencontroller

Active Directory bietet eine eigene Replizierungstechnologie und einen eigenen Wiederherstellungsmodus.

Verwenden Sie Site Recovery Manager nicht, um Active Directory-Domänencontroller zu schützen. Verwenden Sie die Active Directory-Replizierungstechnologie und Wiederherstellungmodus-Technologien, um Notfallwiederherstellungssituationen zu bewältigen.

Erweiterte Site Recovery Manager - Konfiguration

10

In der Standardkonfiguration ermöglicht Site Recovery Manager mehrere einfache Wiederherstellungsszenarios. Fortgeschrittene Benutzer können Site Recovery Manager so anpassen, dass ein größerer Bereich von Site Recovery-Anforderungen unterstützt wird.

Dieses Kapitel behandelt die folgenden Themen:

- Neukonfigurieren der Site Recovery Manager-Einstellungen
- Ändern der Einstellungen, um große Site Recovery Manager-Umgebungen auszuführen

Neukonfigurieren der Site Recovery Manager - Einstellungen

Das Dialogfeld **Erweiterte Einstellungen** ermöglicht Ihnen, viele benutzerdefinierte Einstellungen für den Site Recovery Manager-Dienst anzuzeigen und zu ändern. Erweiterte Einstellungen bieten eine Möglichkeit, dass Benutzer mit den entsprechenden Rechten die Standardwerte ändern können, die den Ablauf mehrerer Site Recovery Manager-Funktionen beeinflussen.

Wichtig Wenn Sie ein Upgrade von Site Recovery Manager durchführen, werden keine Ihrer erweiterten Einstellungen, die Sie in der vorherigen Installation konfiguriert haben, aufbewahrt. Dies ist beabsichtigt. Aufgrund von Änderungen bei den Standardwerten oder Verbesserungen der Leistung sind erweiterte Einstellungen, die Sie in einer vorherigen Version von Site Recovery Manager festgelegt haben, möglicherweise für die neue Version nicht erforderlich oder nicht mit ihr kompatibel. Ebenso werden erweiterte Einstellungen nicht aufbewahrt, wenn Sie die gleiche Version von Site Recovery Manager deinstallieren und anschließend erneut installieren und dabei die Datenbank aus der vorherigen Installation verwenden.

Verbindungseinstellungen ändern

Site Recovery Manager kommuniziert mit anderen Diensten.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.
3. Klicken Sie auf **Verbindungen**.

4 Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.

Option	Aktion
Ändern der Anzahl an fehlgeschlagenen Ping-Befehlen, die ein Ereignis des Typs „Site ausgefallen“ auslöst. Der Standardwert ist 5.	Geben Sie einen neuen Wert im Textfeld **connections.hmsPanicDelay** ein.
Ändern Sie die Anzahl der Statusprüfungen (Ping-Befehle), die ausgeführt werden, bevor die Prüfung als fehlgeschlagen betrachtet wird. Der Standardwert ist 2.	Geben Sie einen neuen Wert im Textfeld **connections.hmsPingFailedDelay** ein.
Ändern der Anzahl an fehlgeschlagenen Ping-Befehlen, die ein Ereignis des Typs „Site ausgefallen“ auslöst. Der Standardwert ist 5.	Geben Sie einen neuen Wert im Textfeld **connections.qsPanicDelay** ein.
Ändern Sie die Anzahl der Statusprüfungen (Ping-Befehle), die ausgeführt werden, bevor die Prüfung als fehlgeschlagen betrachtet wird. Der Standardwert ist 2.	Geben Sie einen neuen Wert im Textfeld **connections.qsPingFailedDelay** ein.
Ändern Sie den Zeitüberschreitungswert für die VIX-Service-Verbindung mit der virtuellen Maschine. Die Standardeinstellung beträgt 120 Sekunden.	Geben Sie einen neuen Wert im Textfeld **connections.vixOpenVmTimeout** ein.
Ändern Sie den Zeitüberschreitungswert für das Warten auf Aktualisierungen von Servern. Die Standardeinstellung beträgt 900 Sekunden.	Geben Sie einen neuen Wert im Textfeld **connections.waitForUpdatesTimeout** ein.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Einstellung für die Erfassung von Site Recovery Manager -Verlaufsberichten

Site Recovery Manager-Verlaufsberichte sind hilfreich für die Diagnose des Verhaltens von Site Recovery Manager Server vor und nach dem Auftreten eines Fehlers. Die Anzahl der exportierten Verlaufsberichte können Sie ändern.

Wenn Sie Failover-, Test- und Bereinigungsvorgänge sowie Vorgänge zum erneuten Schutz mit Site A als Schutz-Site und Site B als Wiederherstellungs-Site ausführen, können Sie für diese Vorgänge bei der Erfassung eines Support-Pakets für Site B (die Wiederherstellungs-Site) Verlaufsberichte exportieren. Der aktuellste Verlauf wird direkt aus der Site Recovery Manager-Datenbank abgerufen.

Nachdem der erneute Schutz ausgeführt wurde, ist Site A die neue Wiederherstellungs-Site und Site B ist die Schutz-Site. Wenn Sie Failover-, Test- und Bereinigungsvorgänge sowie Vorgänge zum erneuten Schutz ausführen, können Sie bei der Erfassung eines Support-Pakets für Site A (die Wiederherstellungs-Site) Verlaufsberichte exportieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldedaten verfügen.
- Site Recovery Manager muss mit einer Site Recovery Manager-Datenbank verbunden sein, auf die Sie mit gültigen Datenbankanmeldedaten zugreifen können.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.
3. Wählen Sie **Verlauf exportieren** aus und klicken Sie auf **Bearbeiten**.
4. Ändern Sie ggf. den Wert für **exportHistory.numReports**.

   Sie können einen Wert zwischen 0 und 50 eingeben. Der Standardwert ist 5.
5. Ändern Sie den Wert in Null (0), um keine Berichte zu exportieren.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Einstellungen der lokalen Site

Site Recovery Manager überwacht den Verbrauch der Ressourcen auf dem Site Recovery Manager Server-Host und löst einen Alarm aus, wenn der Schwellenwert für eine Ressource erreicht ist. Sie können die Schwellenwerte und die Art und Weise ändern, in der Site Recovery Manager Alarme auslöst.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.
3. Klicken Sie auf **Status der lokalen Site**.
4. Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.

Option	Aktion
Ändern der Zeitdifferenz, in der Site Recovery Manager die CPU-Nutzung, den Festplattenspeicher und den freien Arbeitsspeicher auf der lokalen Site prüft. Die Standardeinstellung beträgt 60 Sekunden.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.checkInterval** ein.
Ändern des Namens der lokalen Site.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.displayName** ein.

Option	Aktion
Ändern des Zeitlimits, das Site Recovery Manager abwartet, um Alarme zur CPU-Nutzung, zum Festplattenspeicher und zum freien Arbeitsspeicher auf der lokalen Site auszulösen. Die Standardeinstellung beträgt 600 Sekunden.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.eventFrequency** ein.
Ändern der maximal zulässigen Zeitdifferenz zwischen Serveruhren. Die Standardeinstellung ist 20 Sekunden.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.maxClockSkew** ein. Wenn die erkannte Server-Uhrzeit um mehr als die festgelegte Anzahl von Sekunden von der Site Recovery Manager Server-Uhr abweicht, löst Site Recovery Manager ein Ereignis aus.
Ändern des Prozentsatzes der CPU-Nutzung, der dazu führt, dass Site Recovery Manager ein Ereignis des Typs „Hohe CPU-Nutzung“ auslöst. Der Standardwert ist 70.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.maxCpuUsage** ein.
Ändern der Anzahl der Tage vor dem Ablauf des Site Recovery Manager Zertifikats, bis ein Ereignis des Typs „Zertifikat läuft ab“ ausgelöst werden soll. Die Standardeinstellung beträgt 30 Tage.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus. minCertRemainingTime** ein.
Ändern des Prozentsatzes des freien Festplattenspeichers, der dazu führt, dass Site Recovery Manager ein Ereignis des Typs „Wenig Speicherplatz“ auslöst. Die Standardeinstellung beträgt 100 Prozent.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.minDiskSpace** ein.
Ändern der Menge an freiem Arbeitsspeicher, der dazu führt, dass Site Recovery Manager ein Ereignis des Typs „Wenig Arbeitsspeicher“ auslöst. Der Standardwert ist 32 MB.	Geben Sie einen neuen Wert im Textfeld **localSiteStatus.minMemory** ein.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Protokollierungseinstellungen

Sie können die Protokollierungsebenen ändern, die Site Recovery Manager für die Site Recovery Manager Server-Komponenten bereitstellt.

Bei Site Recovery Manager Server finden Protokollaustäusche statt. Wenn Sie Site Recovery Manager Server neu starten oder wenn eine Protokolldatei sehr groß wird, erstellt Site Recovery Manager Server eine neue Protokolldatei und nimmt nachfolgende Protokollmeldungen in die neue Protokolldatei auf. Wenn Site Recovery Manager Server neue Protokolldateien erstellt, werden die alten Protokolldateien aus Speicherplatzgründen komprimiert.

Sie können die Protokollierungsebenen für einige Site Recovery Manager Server-Komponenten reduzieren, da Protokolldateien sehr schnell sehr groß werden. Sie können die Protokollierungsebenen für einige Komponenten erhöhen, um die Problemdiagnose zu verbessern. Die Liste der verfügbaren Protokollierungsebenen ist für alle Site Recovery Manager Server-Komponenten identisch.

keine	Schaltet die Protokollierung aus.
Still	Zeichnet minimale Protokolleinträge auf.
Notfallalarm	Zeichnet ausschließlich Protokolleinträge zu Notfällen auf. Notfallmeldungen werden bei Totalversagen ausgegeben.
Fehler	Zeichnet nur Protokolleinträge für Notfälle und Fehler auf. Fehlermeldungen werden bei Problemen ausgegeben, die zu einem Versagen führen könnten.
Warnung	Zeichnet Protokolleinträge für Notfälle, Fehler und Warnungen auf. Warnungsmeldungen werden bei unerwünschtem Verhalten ausgegeben, das jedoch mit dem Normalbetrieb verbunden sein kann.
Info	Zeichnet Protokolleinträge für Notfälle, Fehler, Warnungen und Informationen auf. Informationsmeldungen stellen Angaben zum Normalbetrieb bereit.
Ausführlich	Zeichnet Protokolleinträge für Notfälle, Fehler, Warnungen, Informationen und ausführliche Meldungen auf. Ausführliche Meldungen stellen detailliertere Angaben als Informationsmeldungen bereit.
Ausführlich (erweitert)	Zeichnet Protokolleinträge für Notfälle, Fehler, Warnungen, Informationen sowie ausführliche und erweiterte ausführliche Meldungen auf. Erweiterte ausführliche Meldungen stellen alle verfügbaren Angaben bereit. Diese Protokollierungsebene ist für das Debugging hilfreich, sie kann jedoch mit einem erheblichen Datenaufkommen einhergehen, das zu Leistungseinbußen führen könnte. **Hinweis** Wählen Sie diese Protokollierungsebene nur auf Anweisung durch den VMware Support aus, um ein Problem zu beheben.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.
3. Klicken Sie auf **Protokoll-Manager**.

4 Klicken Sie auf **Bearbeiten**, um die Protokollierungseinstellungen zu ändern.

Standardmäßig zeichnen alle Komponenten ausführliche Protokolle auf, sofern dies nicht anderweitig in der Beschreibung der Protokollierungsebene angegeben ist.

Option	Beschreibung
Protokollierungsebene für alle Komponenten einstellen, für die kein Eintrag in logManager vorhanden ist. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.Default** aus.
Protokollierungsebene für das externe API-Modul einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.ExternalAPI** aus.
Protokollierungsebene für vSphere Replication einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.HbrProvider** aus.
Protokollierungsebene für das IP-Anpassungstool einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.IPCustomizer** aus.
Protokollierungsebene für die Bestandslistenzuordnung einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.InventoryMapper** aus.
Protokollierungsebene für Lizenzierungsprobleme einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.Licensing** aus.
Protokollierungsebene für Persistenzprobleme einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.Persistence** aus.
Protokollierungsebene für Wiederherstellungsvorgänge einstellen. Der Standardwert ist „Ausführlich (erweitert)“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.Recovery** aus. Standardmäßig ist die Wiederherstellungsprotokollierung auf **Ausführlich (erweitert)** gesetzt.
Protokollierungsebene für Wiederherstellungskonfigurationsvorgänge einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.RecoveryConfig** aus.
Protokollierungsebene für Array-basierte Replizierungsvorgänge einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.Replication** aus.
Protokollierungsebene für Autorisierungsprobleme zwischen Site Recovery Manager Server und vCenter Server einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.ServerAuthorization** aus.
Protokollierungsebene für die Sitzungsverwaltung einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.SessionManager** aus.

Option	Beschreibung
Protokollierungsebene für den SOAP-Web Services-Adapter einstellen. Die Standardeinstellung ist „Info“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.SoapAdapter** aus. Aufgrund des vom SOAP-Adapter erzeugten Datenaufkommens kann die Einstellung der Protokollierungsebene auf **Ausführlich (erweitert)** zu Leistungseinbußen führen. Standardmäßig ist die SOAP-Adapterprotokollierung auf **Info** eingestellt.
Protokollierungsebene für Speicherprobleme einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.Storage** aus.
Protokollierungsebene für Meldungen aus dem Array-basierten Speicheranbieter einstellen. Die Standardeinstellung ist „Ausführlich“.	Wählen Sie eine Protokollierungsebene im Dropdown-Menü **logManager.StorageProvider** aus.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Die neuen Protokollierungsebenen werden nach Klicken auf **OK** gültig. Es ist kein Neustart des Site Recovery Manager-Dienstes erforderlich. Beim Neustart von Site Recovery Manager Server bleiben die von Ihnen vorgenommenen Einstellungen für die Protokollierungsebenen erhalten.

Ändern von Wiederherstellungseinstellungen

Sie können die Standardwerte für Zeitüberschreitungen ändern, die eintreten, wenn Sie einen Wiederherstellungsplan testen oder ausführen. Dies können Sie tun, wenn Aufgaben aufgrund von Zeitüberschreitungen nicht abgeschlossen wurden.

Es können mehrere Arten von Zeitüberschreitungen eintreten, wenn die Schritte eines Wiederherstellungsplans ausgeführt werden. Diese Zeitüberschreitungen führen zu einer Unterbrechung des Plans für ein festgelegtes Zeitintervall, um den Abschluss eines Schrittes abzuwarten.

Site Recovery Manager wendet einige erweiterte Einstellungen auf eine virtuelle Maschine an, sobald Sie den Schutz auf dieser virtuellen Maschine konfigurieren.

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

Site Recovery Manager speichert eine Kopie der Wiederherstellungseinstellungen der virtuellen Maschine auf jeder Site Recovery Manager-Site. Wenn sich die erweiterten Wiederherstellungseinstellungen auf der Schutz- und der Wiederherstellungs-Site unterscheiden, initialisiert Site Recovery Manager die Wiederherstellungseinstellungen einer virtuellen Maschine auf jeder Site mit unterschiedlichen Werten. Wenn Site Recovery Manager dann die virtuelle Maschine von Site A auf Site B wiederherstellt, übernimmt er die lokalen Wiederherstellungseinstellungen für Site B. Bei einer Wiederherstellung von Site B auf Site A

übernimmt Site Recovery Manager die lokalen Wiederherstellungseinstellungen für Site A. Dieser Zustand besteht so lange, bis Sie die Wiederherstellungseinstellungen der einzelnen virtuellen Maschinen auf der Registerkarte „Virtuelle Maschinen“ des Wiederherstellungsplans explizit bearbeiten und speichern. Die Wiederherstellungseinstellungen der betroffenen virtuellen Maschinen werden synchronisiert und auf beiden Site Recovery Manager-Sites identisch.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.
3. Klicken Sie auf **Wiederherstellen**.
4. Klicken Sie auf **Bearbeiten**, um die Einstellungen der Wiederherstellungs-Site zu ändern.

Option	Aktion
Ändern der Zeitüberschreitung für das Ausschalten der virtuellen Maschine in der IP-Anpassung. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen neuen Wert im Textfeld **recovery.customizationShutdownTimeout** ein. Dieser Wert ist der minimale Zeitüberschreitungswert in Sekunden für das Ausschalten der virtuellen Maschine und wird nur in IP-Anpassungs-Workflows verwendet. Wenn Sie die Zeitüberschreitung für das Ausschalten in Wiederherstellungseinstellungen für virtuelle Maschinen angeben, hat der größere der beiden Werte Vorrang.
Ändern der Zeitüberschreitung für die IP-Anpassung. Die Standardeinstellung beträgt 600 Sekunden.	Geben Sie einen neuen Wert im Textfeld **recovery.customizationTimeout** ein. Dieser Wert ist die Zeitüberschreitung, die bei der Vorbereitung von IP-Anpassungsskripts auf dem Site Recovery Manager Server verwendet wird. Diese Einstellung muss nur selten geändert werden.
Ändern der Standardpriorität für das Wiederherstellen einer virtuellen Maschine. Der Standardwert ist 3.	Geben Sie einen neuen Wert im Textfeld **recovery.defaultPriority** ein.
Aktivieren oder Deaktivieren der erzwungenen Wiederherstellung. Der Standardwert lautet „false“.	Aktivieren Sie das Kontrollkästchen **recovery.forceRecovery** bzw. heben Sie die Aktivierung auf. Aktivieren Sie die erzwungene Wiederherstellung in Fällen, in denen RTO durch eine mangelhafte Konnektivität zur Schutz-Site erheblich beeinträchtigt wird. Diese Einstellung entfernt nur die Einschränkung der Auswahl der erzwungenen Wiederherstellung beim Ausführen eines Wiederherstellungsplans. Um die erzwungene Wiederherstellung tatsächlich zu aktivieren, wählen Sie sie beim Ausführen eines Plans aus.
Ändern der Zeitüberschreitung für das Einschalten von Hosts in einem Cluster. Die Standardeinstellung beträgt 1200 Sekunden.	Geben Sie einen neuen Wert im Textfeld **recovery.hostPowerOnTimeout** ein.

Option	Aktion
Ändern der Zeitüberschreitung für das Ausschalten des Gastbetriebssystems. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen neuen Wert im Textfeld **recovery.powerOffTimeout** ein. Der neue Wert für Zeitüberschreitungen gilt für alle Ausschaltungsaufgaben für virtuelle Maschinen an der geschützten Site. **Hinweis** Die virtuelle Maschine wird nach Ablauf der Zeitüberschreitung ausgeschaltet. Wenn das Betriebssystem der virtuellen Maschine die Aufgaben für das Herunterfahren zum Zeitpunkt der Zeitüberschreitung nicht abgeschlossen hat, gehen möglicherweise Daten verloren. Stellen Sie für eine große virtuelle Maschine, die für das ordnungsgemäße Herunterfahren mehr Zeit beansprucht, die Zeitüberschreitung bis zum Ausschalten individuell für diese virtuelle Maschine ein. Informationen zum Einstellen der Zeitüberschreitung bis zum Ausschalten für eine individuelle virtuelle Maschine finden Ssie unter Konfigurieren der Optionen zum Starten und Herunterfahren von virtuellen Maschinen.
Ändern der Verzögerung beim Starten von abhängigen Aufgaben nach dem Einschalten einer virtuellen Maschine. Der Standardwert ist 0.	Geben Sie einen neuen Wert im Textfeld **recovery.powerOnDelay** ein. Der neue Wert gilt für Aufgaben im Zusammenhang mit dem Einschalten der virtuellen Maschinen auf der Wiederherstellungs-Site.
Ändern des Zeitlimits, das VMware Tools beim Einschalten von virtuellen Maschinen warten soll Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen neuen Wert im Textfeld **recovery.powerOnTimeout** ein. Der neue Wert gilt für Aufgaben im Zusammenhang mit dem Einschalten der virtuellen Maschinen auf der Wiederherstellungs-Site. Wenn auf geschützten virtuellen Maschinen VMware Tools nicht installiert ist, setzen Sie diesen Wert auf „0“.
Aktivieren oder Deaktivieren des Überspringens des Herunterfahrens des Gastbetriebssystems. Der Standardwert lautet „false“.	Aktivieren Sie das Kontrollkästchen **recovery.skipGuestShutdown** bzw. heben Sie die Aktivierung auf. Wenn Sie die Option auswählen, hat „recovery.powerOffTimeout“ keine Auswirkungen. Wenn VMware Tools nicht auf der VM installiert ist, aktivieren Sie die Option zum automatischen Deaktivieren von „recovery.powerOffTimeout“, fahren Sie SRM unter Umgehung des Gasts herunter und schalten Sie die VMs direkt und ohne Zeitüberschreitung beim Herunterfahren aus.
Aktivieren bzw. Deaktivieren der automatischen VM-IP-Anpassung während der Wiederherstellung. Der Standardwert lautet „true“.	Aktivieren bzw. Aufheben der Aktivierung des Kontrollkästchens **recovery.uselpMapperAutomatically**. Wenn Sie die Option auswählen und IP-Zuordnungsregeln für virtuelle Netzwerke konfiguriert sind, wertet Site Recovery Manager diese Regeln während der Wiederherstellung aus, um die VMs anzupassen. Wenn Sie die Auswahl der Option aufheben, werden die IP-Zuordnungsregeln während der Wiederherstellung nicht ausgewertet. Sie können die Option für jede VM in „VM-Wiederherstellungseinstellungen/IP-Anpassungsmodus“ überschreiben.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Wenn Sie einzelne dieser erweiterten Einstellungen ändern, nachdem Sie den Schutz auf einer virtuellen Maschine konfiguriert haben, gelten die neuen Einstellungen nicht für diese virtuelle Maschine. Änderungen an diesen erweiterten Einstellungen gelten nur für virtuelle Maschinen, die Sie nach dem Ändern der Einstellungen schützen. Dies ist beabsichtigt, da im Falle einer Übernahme geänderter erweiterter Einstellungen seitens Site Recovery Manager auf virtuelle Maschinen, auf denen Sie bereits den Schutz konfiguriert haben, unerwünschte Änderungen am Schutz dieser virtuellen Maschinen vorgenommen werden könnten.

Weiter

Um in den erweiterten Einstellungen vorgenommene Änderungen auf zuvor geschützte virtuelle Maschinen anzuwenden, müssen Sie diese virtuellen Maschinen einzeln neu konfigurieren. Wenn Sie z.˚B. die Einstellung `defaultPriority` neu konfigurieren, können Sie die Priorität der zuvor geschützten virtuellen Maschine manuell so neu konfigurieren, dass sie der neuen `defaultPriority`-Einstellung entspricht.

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Schutzgruppen** und wählen Sie die Schutzgruppe aus, zu der die virtuelle Maschine gehört.

2 Klicken Sie auf der Registerkarte **Verwandte Objekte** auf **Virtuelle Maschinen**.

3 Wählen Sie die virtuelle Maschine aus und klicken Sie auf **Schutz entfernen**.

   Der Status der virtuellen Maschine ändert sich in „Nicht konfiguriert“.

4 Klicken Sie auf **Alle konfigurieren**, um alle virtuellen Maschinen in der Schutzgruppe neu zu konfigurieren, oder wählen Sie eine virtuelle Maschine aus und klicken Sie auf **Schutz konfigurieren**, um nur diese virtuelle Maschine zu konfigurieren.

   Site Recovery Manager übernimmt die neueren erweiterten Einstellungen auf die virtuelle Maschine.

Ändern der Remote-Manager-Einstellungen

Wenn Sie Aufgaben ausführen, die sehr viel Zeit in Anspruch nehmen, kann es vorkommen, dass das Standard-Zeitlimit auf der Remote-Site überschritten wird, bevor die Aufgabe abgeschlossen ist. Sie können zusätzliche Zeitlimits konfigurieren, um den Abschluss von Aufgaben mit langer Ausführungsdauer zu ermöglichen.

Eine Aufgabe mit langer Ausführungsdauer wäre z. B. die Testwiederherstellung oder Bereinigung einer umfangreichen virtuellen Maschine. Wenn eine virtuelle Maschine über große Festplatten verfügt, kann eine Testwiederherstellung oder eine vollständige Wiederherstellung lange dauern. Beim Standard-Zeitlimit werden die Verbindungen zwischen Sites überwacht, sodass Zeitüberschreitungen entstehen können, wenn eine Aufgabe mehr Zeit als das Standard-Zeitlimit benötigt und während ihrer Ausführung keine Benachrichtigungen an die andere Site sendet. In einem solchen Fall können Sie die Remote-Manager-Einstellungen so ändern, dass Site Recovery Manager das Zeitlimit nicht überschreitet, bevor eine Aufgabe mit langer Ausführungsdauer abgeschlossen ist.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Remote-Manager**.

4 Klicken Sie auf **Bearbeiten**, um die Remote-Manager-Einstellungen zu ändern.

Option	Aktion
Konfigurieren des maximalen Zeitraums, in dem darauf gewartet wird, dass ein Remote-Vorgang abgeschlossen wird. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen Wert für **remoteManager.defaultTimeout** ein.
Markieren einer virtuellen Maschine als durch Site Recovery Manager geschützt. Der Standardwert lautet „true“.	Aktivieren Sie das Kontrollkästchen, um den Wert **remoteManager.enableCustomFields** zu aktivieren.
Festlegen einen Zeitraums, während dem auf Aggregationsanforderungen auf der Remote-Site gewartet wird. Die Standardeinstellung beträgt 2000 Sekunden.	Geben Sie einen Wert für **remoteManager.powerOnAggregationInterval** ein.
Konfigurieren des maximalen Zeitraums, in dem auf das Beenden abgebrochener Aufgaben gewartet wird. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen Wert für **remoteManager.taskCancelDefaultTimeout** ein.
Konfigurieren eines zusätzlichen Zeitlimits für das Abschließen von Aufgaben auf der Remote-Site. Die Standardeinstellung beträgt 900 Sekunden.	Geben Sie einen Wert für **remoteManager.taskDefaultTimeout** ein.
Konfigurieren der Anzahl der Sekunden, bevor eine Aufgabe, bei der eine Zeitüberschreitung eingetreten ist, eine Fortschrittsmeldung ausgibt. Die Standardeinstellung beträgt 180 Sekunden.	Geben Sie einen Wert für **remoteManager.taskProgressDefaultTimeout** ein. Der Aufgabe wird mehr Zeit für den Abschluss gewährt, wenn die Fortschrittsmeldung innerhalb dieses Zeitraums eingeht.

Ändern der Einstellungen für Remote-Sites

Sie können die Standardwerte ändern, die Site Recovery Manager Server auf der Schutz-Site verwendet, um festzustellen, ob Site Recovery Manager Server auf der Remote-Site zur Verfügung steht.

Site Recovery Manager überwacht die Verbindung zwischen der Schutz-Site und der Wiederherstellungs-Site und löst Alarme aus, falls die Verbindung ausfällt. Sie können die Kriterien ändern, die dafür sorgen, dass Site Recovery Manager ein Verbindungsereignis auslöst, und die Art und Weise, in der Site Recovery Manager Alarme auslöst.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Status der Remote-Site**.

4 Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.

Option	Aktion
Ändern der Anzahl an fehlgeschlagenen Ping-Befehlen, die ein Ereignis des Typs „Site ausgefallen“ auslöst. Der Standardwert ist 5.	Geben Sie einen neuen Wert im Textfeld **remoteSiteStatus.panicDelay** ein.
Ändern der Anzahl an Statusprüfungen von Remote-Sites (Ping-Befehle), die ausgeführt werden, bevor die Prüfung als fehlgeschlagen betrachtet wird. Der Standardwert ist 2.	Geben Sie einen neuen Wert im Textfeld **remoteSiteStatus.pingFailedDelay** ein.
Ändern der Einstellung dafür, in welchem Intervall Site Recovery Manager prüft, ob Site Recovery Manager Server auf der Remote-Site zur Verfügung steht. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen neuen Wert im Textfeld **remoteSiteStatus.pingInterval** ein. Wenn Sie einen Wert für **remoteSiteStatus.pingInterval** angeben, der kleiner als der konfigurierte Wert für `connections.drPingInterval` ist, setzt Site Recovery Manager den konfigurierten Wert zurück. Sie können den `connections.drPingInterval`-Wert in der Datei „vmware-dr.xml“ bearbeiten. Wenn der für **remoteSiteStatus.pingInterval** festgelegte Wert außerhalb des Wertebereichs liegt, wird eine Fehlermeldung angezeigt: `Einstellung für 'remoteSiteStatus.pingInterval' ist außerhalb des Bereichs`.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Replizierungseinstellungen

Sie können die Replizierungseinstellungen anpassen, um zu ändern, wie lange Site Recovery Manager darauf wartet, dass die Erstellung von Platzhalter-VMs abgeschlossen ist.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Replikation**.

4 Klicken Sie auf **Bearbeiten**, um die Einstellung **replication.placeholderVmCreationTimeout** und damit die Wartezeit (in Sekunden) beim Erstellen einer Platzhalter-VM zu ändern.

   Der Standardwert ist 300.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

SSO-Einstellung ändern

Sie können die Single Sign On-Einstellung für Site Recovery Manager ändern, um SSO-Token zu verlängern.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **SSO**.

4 Klicken Sie auf **Bearbeiten**, um die Einstellung **sso.sts.tokenLifetime** zu ändern und damit die Anzahl der Sekunden anzugeben, die SSO-Token verwendet werden, bevor sie verlängert werden.

   Der Standardwert beträgt 28800 Sekunden (8 Stunden).

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Speichereinstellungen

Sie können die Speichereinstellungen anpassen, um festzulegen, wie Site Recovery Manager und vCenter Server mit dem Speicherreplizierungsadapter (SRA) kommunizieren.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Speicher**.

4 Klicken Sie auf **Bearbeiten**, um die Speichereinstellungen zu ändern.

Option	Aktion
Ändern der Zeitüberschreitung in Sekunden für die Ausführung eines SRA-Befehls. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storage.commandTimeout** ein.
Site Recovery Manager das automatische Erstellen von Tag-Kategorien und des „Replicated“-Tags, das die Storage DRS-Kompatibilität erfordert, ermöglichen. Der Standardwert lautet „true“.	Aktivieren Sie das Kontrollkästchen **storage.enableSdrsStandardTagCategoryCreation**.
Site Recovery Manager das automatische Erstellen oder die Anfügung von Tags an replizierte oder gesicherte Datenspeicher für die Storage DRS-Kompatibilität ermöglichen. Der Standardwert lautet „true“.	Aktivieren Sie das Kontrollkästchen **storage.enableSdrsTagging**. Wenn Sie das Kontrollkästchen deaktivieren, löscht Site Recovery Manager alle Tags und Tag-Kategorien. Dies und hat zur Folge, dass die Kompatibilität mit Storage DRS nicht mehr gegeben ist.
Site Recovery Manager das Reparieren fehlender oder fehlerhafter Tags auf replizierten oder gesicherten Datenspeichern für die Storage DRS-Kompatibilität ermöglichen. Der Standardwert lautet „true“.	Aktivieren Sie das Kontrollkästchen **storage.enableSdrsTaggingRepair**.
Ändern der maximalen Anzahl gleichzeitiger SRA-Vorgänge. Der Standardwert ist 5.	Geben Sie einen neuen Wert im Textfeld **storage.maxConcurrentCommandCnt** ein.

Option	Aktion
Ändern des Mindestabstands (in Sekunden) zwischen Datenspeichergruppen-Berechnungen. Der Standardwert ist 0.	Geben Sie einen neuen Wert im Textfeld **storage.minDsGroupComputationInterval** ein.
Ändern des Zeitintervalls zwischen Status-Updates für laufende Datensynchronisierungsvorgänge. Die Standardeinstellung beträgt 30 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storage.querySyncStatusPollingInterval** ein.
Ändern des Zeitintervalls zwischen Vorgängen des Storage DRS-Tagging. Die Standardeinstellung beträgt 50 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storage.sdrsTaggingPollInterval** ein.
Ändern des Zeitintervalls zwischen Erkennungsprüfungen von Speicher-Arrays. Der Standardwert beträgt 86400 Sekunden (24 Stunden).	Geben Sie einen neuen Wert im Textfeld **storage.storagePingInterval** ein.
Ändern der maximal zulässigen Dauer für Datensynchronisierungsvorgänge. Der Standardwert beträgt 86400 Sekunden (24 Stunden).	Geben Sie einen neuen Wert im Textfeld **storage.syncTimeout** ein.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Speicheranbietereinstellungen

Bei der Array-basierten Replizierung ist der SAN-Anbieter die Schnittstelle zwischen Site Recovery Manager und Ihrem Speicherreplizierungsadapter (SRA). Für einige SRAs müssen Sie Standardwerte für SAN-Anbieter ändern. Sie können die Standardwerte für die Zeitüberschreitung und andere Verhaltensweisen des Site Recovery Manager-SAN-Anbieters ändern.

Sie können die Einstellungen für die Neusignierung, das Beheben von Problemen bei Datenspeichernamen, die Anzahl der erneuten Hostprüfungen und Zeitüberschreitungen in Sekunden ändern. Weitere Informationen zu diesen Werten finden Sie in der SRA-Dokumentation Ihres Array-Anbieters.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **Speicheranbieter**.

4 Klicken Sie auf **Bearbeiten**, um die Speicheranbietereinstellungen zu ändern.

Option	Aktion
Site Recovery Manager zwingen, Verbindungen von LUNs mit doppelten Volumes zu trennen und neu zu verbinden Der Standardwert lautet „true“.	Aktivieren Sie das Kontrollkästchen **storageProvider.autoDetachLUNsWithDuplicateVolume**.
Festlegen des Flags `LVM.EnableResignature` auf ESXi-Hosts während des Testens und der Wiederherstellung. Der Standardwert ist 0.	Geben Sie im Textfeld **storageProvider.autoResignatureMode** den Wert `0` zum Deaktivieren, den Wert `1` zum Aktivieren oder den Wert `2` zum Ignorieren des Flags ein. Die Standardeinstellung ist 0. Wenn dieses Flag auf 1 eingestellt wird, signiert Site Recovery Manager alle bekannten VMFS-Snapshot-Volumes neu, einschließlich der Volumes, die nicht von Site Recovery Manager verwaltet werden. Wird für dieses Flag die Einstellung 0 beibehalten, signiert Site Recovery Manager nur die von ihm verwalteten VMFS-Snapshot-Volumes neu.
Ändern des Zeitüberschreitungswerts (in Sekunden), um festzulegen, wie lange auf den Abschluss des LUN-Batch-Anhängevorgangs auf den einzelnen ESXi-Hosts gewartet wird. Die Standardeinstellung beträgt 3600 Sekunden.	Geben Sie einen Wert im Textfeld **storageProvider.batchAttachTimeoutSec** ein.
Ändern des Zeitüberschreitungswerts (in Sekunden), um festzulegen, wie lange auf den Abschluss des LUN-Batch-Trennvorgangs auf den einzelnen ESXi-Hosts gewartet wird. Die Standardeinstellung beträgt 3600 Sekunden.	Geben Sie einen Wert im Textfeld **storageProvider.batchDetachTimeoutSec** ein.
Ändern der Zeitspanne, wie lange Site Recovery Manager auf das Mounten von VMFS-Volumes wartet. Die Standardeinstellung beträgt 3600 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storageProvider.batchMountTimeoutSec** ein. Ändern Sie diesen Wert, wenn Zeitüberschreitungen auftreten, die dadurch verursacht werden, dass Site Recovery Manager VMFS-Volumes überprüft, bei denen das Mounten viel Zeit in Anspruch nimmt. Diese Einstellung ist in Site Recovery Manager 5.5.1 und höheren Versionen verfügbar.
Ändern der Zeitspanne, wie lange Site Recovery Manager auf das Unmounten von VMFS-Volumes wartet. Die Standardeinstellung beträgt 3600 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storageProvider.batchUnmountTimeoutSec** ein. Ändern Sie diesen Wert, wenn Zeitüberschreitungen auftreten, die dadurch verursacht werden, dass Site Recovery Manager VMFS-Volumes überprüft, bei denen das Unmounten viel Zeit in Anspruch nimmt. Diese Einstellung ist in Site Recovery Manager 5.5.1 und höheren Versionen verfügbar.
Festlegen der Anzahl von Wiederholungen für Batch-Unmount-Vorgänge der VMFS/NFS-Volumes. Die Standardeinstellung beträgt 3 Versuche.	Geben Sie einen neuen Wert im Textfeld **storageProvider.datastoreUnmountRetryCount** ein.
Ändern der Zeitspanne, wie lange Site Recovery Manager bis zum Versuch, den Datenspeicher auszuhängenzu Unmounten, wartet. Die Standardeinstellung beträgt 1 Sekunde.	Geben Sie einen neuen Wert im Textfeld **storageProvider.datastoreUnmountRetryDelaySec** ein.

Option	Aktion
Entfernen des *snap–xx*-Präfixes, das den Namen von wiederhergestellten Datenspeichern vorangestellt wird, nach einer ordnungsgemäßen Wiederherstellung erzwingen. Der Standardwert lautet „false“.	Aktivieren Sie das Kontrollkästchen **storageProvider.fixRecoveredDatastoreNames**.
Ändern der Zeit, die Site Recovery Manager vor dem Entfernen des *snap–xx*-Präfixes, das den Namen von wiederhergestellten Datenspeichern vorangestellt wird, wartet. Die Standardeinstellung beträgt 0 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storageProvider.fixRecoveredDatastoreNamesDelaySec** ein.
Hostprüfungen während des Testens und der Wiederherstellung verzögern. Die Standardeinstellung beträgt 0 Sekunden.	SRAs können Antworten an Site Recovery Manager senden, bevor ein heraufgestuftes Speichergerät auf der Wiederherstellungs-Site für die ESXi-Hosts verfügbar ist. Wenn Site Recovery Manager eine Antwort von einem SRA empfängt, wird eine erneute Prüfung der Speichergeräte durchgeführt. Wenn die Speichergeräte noch nicht vollständig verfügbar sind, erkennt der ESXi-Server sie nicht, und Site Recovery Manager findet die replizierten Geräte beim Durchführen der erneuten Prüfungen nicht. Datenspeicher werden nicht erstellt und wiederhergestellte virtuelle Maschinen können nicht gefunden werden. Um den Start von erneuten Speicherprüfungen zu verzögern, bis sie auf den ESXi-Hosts verfügbar werden, geben Sie einen neuen Wert in das Textfeld **storageProvider.hostRescanDelaySec** ein. Ändern Sie diesen Wert nur, wenn Probleme auftreten, weil Datenspeicher nicht verfügbar sind.
Hostprüfungen während des Testens und der Wiederherstellung wiederholen. Der Standardwert ist 1.	Geben Sie einen neuen Wert im Textfeld **storageProvider.hostRescanRepeatCnt** ein. Einige Speicher-Arrays benötigen mehr als eine erneute Prüfung, beispielsweise um Snapshots von LUNs zu erkennen, für die ein Failover durchgeführt wurde. In früheren Versionen haben Sie möglicherweise den Parameter **storageProvider.hostRescanRepeatCnt** verwendet, um eine Verzögerung bei Wiederherstellungen festzulegen. Verwenden Sie stattdessen den Parameter **storageProvider.hostRescanDelaySec**.
Ändern der Zeitspanne, wie lange Site Recovery Manager auf den Abschluss der erneuten HBA-Prüfung wartet. Die Standardeinstellung beträgt 300 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storageProvider.hostRescanTimeoutSec** ein.
Festlegen der Anzahl der Versuche von Site Recovery Manager, ein VMFS-Volume neu zu signieren. Der Standardwert ist 1.	Geben Sie einen neuen Wert im Textfeld **storageProvider.resignatureFailureRetryCount** ein.
Zeitüberschreitung für Neusignierung eines VMFS-Volumes einstellen. Die Standardeinstellung beträgt 900 Sekunden.	Geben Sie einen neuen Wert im Textfeld **storageProvider.resignatureTimeoutSec** ein. Wenn Sie die Einstellung für **storageProvider.hostRescanTimeoutSec** ändern, erhöhen Sie die Einstellung für **storageProvider.resignatureTimeoutSec** auf den gleichen Zeitüberschreitungswert, der für **storageProvider.hostRescanTimeoutSec** verwendet wird.

Option	Aktion
Festlegen der VMX-Dateipfade, die Site Recovery Manager nach einem Storage vMotion-Vorgang nicht als mögliche VMX-Kandidatendateien berücksichtigen soll. Der Standardwert ist „.snapshot“.	Einige Arrays erstellen VMX-Dateipfade, die vom `storageProvider.storageVmotionVmxSearch`-Suchalgorithmus ignoriert werden sollen. Geben Sie eine kommagetrennte Liste von Zeichenfolgen in das Textfeld **storageProvider.storageVmotionVmxFilePathsToSkip** ein, um die VMX-Dateipfade festzulegen, die nach einem Storage vMotion-Vorgang ignoriert werden sollen. Site Recovery Manager berücksichtigt VMX-Dateipfade, die mindestens eine dieser Zeichenfolgen enthalten, nach einem Storage vMotion-Vorgang nicht als mögliche VMX-Kandidatendateien.
Nach VMX-Dateien in wiederhergestellten Datenspeichern suchen, um virtuelle Maschinen zu identifizieren, die von Storage vMotion vor oder während eines Tests oder einer Wiederherstellung verschoben wurden. Der Standardwert lautet „true“.	Diese Option ist standardmäßig ausgewählt. Deaktivieren Sie das Kontrollkästchen **storageProvider.storageVmotionVmxSearch**, um diese Option zu deaktivieren.
Angeben des Zeitüberschreitungswerts (in Sekunden), um festzulegen, wie lange auf die Verfügbarkeit neu erkannter Datenspeicher gewartet wird. Die Standardeinstellung beträgt 60 Sekunden.	Geben Sie den neuen Wert im Textfeld **storageProvider.waitForAccessibleDatastoreTimeoutSec** ein.
Aktivieren Sie Site Recovery Manager, um nach der Wiederherstellung auf das Erkennen von Datenspeichern zu warten.	Aktivieren Sie das Kontrollkästchen **storageProvider.waitForDeviceRediscovery**.
Angeben eines Zeitüberschreitungswerts, um festzulegen, wie lange auf die Meldung neu erkannter Datenspeicher durch Virtual Center gewartet wird. Die Standardeinstellung beträgt 30 Sekunden.	Geben Sie den neuen Wert im Textfeld **storageProvider.waitForRecoveredDatastoreTimeoutSec** ein.
Festlegen der Zeitspanne (in Sekunden), wie lange Site Recovery Manager auf das Mounten von VMFS-Volumes wartet. Die Standardeinstellung beträgt 30 Sekunden.	Geben Sie den neuen Wert im Textfeld **storageProvider.waitForVmfsVolumesMountedStateTimeoutSec** ein.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der vSphere Replication -Einstellungen

Sie können die globalen Einstellungen anpassen, um die Art der Interaktion von Site Recovery Manager mit vSphere Replication zu ändern.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Erweiterte Einstellungen**.

3 Klicken Sie auf **vSphere Replication**.

4 Klicken Sie auf **Bearbeiten**, um die vSphere Replication-Einstellungen zu ändern.

Option	Beschreibung
Erlaubt Site Recovery Manager die Wiederherstellung von virtuellen Maschinen, die von anderen Lösungen verwaltet werden. Der Standardwert lautet „false“.	vSphere Replication lässt zu, dass andere Lösungen die Replizierung von virtuellen Maschinen verwalten. Standardmäßig stellt Site Recovery Manager nur die von ihm selbst verwalteten virtuellen Maschinen wieder her. Damit Site Recovery Manager virtuelle Maschinen wiederherstellen kann, deren Replizierungen von anderen Lösungen verwaltet werden, aktivieren Sie das Kontrollkästchen **allowOtherSolutionTagInRecovery**.
Mehrfache ältere PIT-Snapshots (Point-in-Time) während Wiederherstellungen beibehalten. Der Standardwert lautet „true“.	Bei der Konfiguration von vSphere Replication zur Erstellung von PIT-Snapshots von geschützten virtuellen Maschinen stellt Site Recovery Manager lediglich den letzten Snapshot wieder her, wenn Sie eine Wiederherstellung durchführen. Um während einer Wiederherstellung ältere PIT-Snapshots wiederherzustellen, aktivieren Sie das Kontrollkästchen **preserveMpitImagesAsSnapshots**.
Zeitüberschreitungsperiode für vSphere Replication-Synchronisierungsvorgänge ändern. Der Standardwert beträgt 7200.	Geben Sie im Textfeld **synchronizationTimeout** einen neuen Wert ein. Der Wert, den Sie eingeben, muss die Hälfte des Werts für die Zeitüberschreitung sein, die Sie festlegen möchten. Der Standardwert ist 7200 und entspricht einer Zeitüberschreitungsperiode für Synchronisierungsvorgänge von 14400 Sekunden. Ändern Sie diesen Wert, falls Zeitüberschreitungsfehler auftreten, wenn vSphere Replication virtuelle Maschinen an der Wiederherstellungs-Site synchronisiert.
Standard-RPO-Einstellungen für Replizierungen ändern. Der Standardwert beträgt 240.	Geben Sie einen neuen Wert im Textfeld **vrReplication.timeDefault** ein. Der Standardwert beträgt 240 Minuten (4 Stunden). Dieser Wert wird bei der Konfiguration von Replizierungen ausgewählt, Sie können jedoch eine andere RPO-Einstellung im Assistenten **Replizierung konfigurieren** vornehmen, wenn Sie die Replizierung für eine einzelne virtuelle Maschine oder für eine Gruppe virtueller Maschinen konfigurieren.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Einstellungen, um große Site Recovery Manager -Umgebungen auszuführen

Wenn Sie Site Recovery Manager zum Testen oder Wiederherstellen einer großen Anzahl an virtuellen Maschinen verwenden, müssen Sie möglicherweise die standardmäßigen Site Recovery Manager-Einstellungen ändern, um die bestmöglichen Wiederherstellungszeiten in Ihrer Umgebung zu erzielen oder um Zeitüberschreitungen zu vermeiden.

In großen Umgebungen ist es möglich, dass Site Recovery Manager sehr viele virtuelle Maschinen gleichzeitig ein- oder ausschaltet. Das gleichzeitige Ein- oder Ausschalten von sehr vielen virtuellen Maschinen kann die virtuelle Infrastruktur schwer belasten, was möglicherweise zu Zeitüberschreitungen führt. Sie können bestimmte Site Recovery Manager-Einstellungen ändern, um Zeitüberschreitungen zu vermeiden, indem Sie entweder die Anzahl der Ein- und Ausschaltvorgänge, die Site Recovery Manager gleichzeitig durchführt, beschränken oder die Zeitlimits erhöhen.

Die Beschränkungen, die Sie für Ein- und Ausschaltvorgänge festlegen, hängen von der Anzahl der gleichzeitigen Ein- und Ausschaltvorgänge ab, die Ihre Infrastruktur verkraften kann.

Sie können in den Menüs der **Erweiterten Einstellungen** im vSphere Web Client oder im Client-Plug-In von Site Recovery Manager gewisse Optionen ändern. Zum Ändern anderer Einstellungen bearbeiten Sie die Konfigurationsdatei `vmware-dr.xml` auf dem Site Recovery Manager Server. Verwenden Sie zum Ändern der Einstellungen immer die Client-Menüs, wenn es Optionen gibt. Wenn Sie die Einstellungen ändern, müssen Sie dieselben Änderungen auf den Instanzen von Site Recovery Manager Server und vCenter Server auf der Schutz- und der Wiederherstellungs-Site vornehmen.

Die Einstellungen, die Sie ändern können, werden unter Einstellungen für große Site Recovery Manager-Umgebungen beschrieben.

Vorgehensweise

1. Wählen Sie im vSphere Web Client einen Cluster aus.
2. Wählen Sie auf der Registerkarte **Verwalten** die Option **Einstellungen > vSphere DRS** aus.
3. Klicken Sie auf **Bearbeiten**.
4. Legen Sie in **Erweiterte Optionen** die Einstellung `srmMaxBootShutdownOps` fest.

Option	Beschreibung
Textfeld Option	Geben Sie `srmMaxBootShutdownOps` ein.
Textfeld Wert	Geben Sie die maximale Anzahl der Ein- und Ausschaltvorgänge ein, z. B. 32. Wenn Sie den Wert auf 32 festlegen, beginnt der nächste Gast mit dem Ein- oder Ausschalten, sobald einer des ersten von 32 Batches abgeschlossen wurde, d. h. die VMs 1 bis 32 starten zusammen. Anschließend startet VM 33, sobald einer des ersten Batches abgeschlossen wurde, VM 34 startet, sobald der zweite des ersten Batches abgeschlossen wurde usw.

5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
6. Melden Sie sich beim Site Recovery Manager Server-Host an.
7. Öffnen Sie die Datei `vmware-dr.xml` in einem Texteditor.

   Sie finden die Datei `vmware-dr.xml` im Ordner `C:\Programme\VMware\VMware vCenter Site Recovery Manager\config`.
8. Ändern Sie die Einstellungen für `defaultMaxBootAndShutdownOpsPerCluster` und `defaultMaxBootAndShutdownOpsPerHost` in der Datei `vmware-dr.xml`:

```
<config>
...
   <defaultMaxBootAndShutdownOpsPerCluster>24</defaultMaxBootAndShutdownOpsPerCluster>
   <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
...
</config>
```

Wenn diese Elemente noch nicht in der Datei `vmware-dr.xml` vorhanden sind, können Sie diese überall im Abschnitt `<config>` hinzufügen. Wenn Sie den `<defaultMaxBootAndShutdownOpsPerCluster>`-Wert auf 24 festlegen, beginnt der nächste Gast mit dem Ein- oder Ausschalten, sobald einer des ersten von 24 Batches abgeschlossen wurde, d. h. die VMs 1 bis 24 starten zusammen. Anschließend startet VM 25, sobald einer des ersten Batches abgeschlossen wurde, VM 26 startet, sobald der zweite des ersten Batches abgeschlossen wurde usw.

9 Starten Sie den Site Recovery Manager Server neu, damit die neuen Einstellungen wirksam werden.

10 Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.

11 Wählen Sie **Erweiterte Einstellungen > vSphere Replication** und erhöhen Sie die `vrReplication.synchronizationTimeout`-Einstellung.

Der Standardwert ist 7200 und entspricht einer Zeitüberschreitungsperiode für Synchronisierungsvorgänge von 14400 Sekunden.

12 Wählen Sie **Erweiterte Einstellungen > Speicher** und erhöhen Sie die `storage.commandTimeout`-Einstellung.

Die Standardeinstellung beträgt 300 Sekunden.

13 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Einstellungen für große Site Recovery Manager -Umgebungen

Wenn Sie eine große Anzahl an virtuellen Maschinen schützen möchten, können Sie die Site Recovery Manager-Standardeinstellungen ändern, um die bestmöglichen Wiederherstellungszeiten in Ihrer Umgebung einzurichten oder um Zeitüberschreitungen zu vermeiden.

Sie können in den Menüs der **Erweiterten Einstellungen** im vSphere Web Client oder im Client-Plug-In von Site Recovery Manager gewisse Optionen ändern. Zum Ändern anderer Einstellungen bearbeiten Sie die Konfigurationsdatei `vmware-dr.xml` auf dem Site Recovery Manager Server. Verwenden Sie zum Ändern der Einstellungen immer die Client-Menüs, wenn es Optionen gibt. Wenn Sie die Einstellungen ändern, müssen Sie dieselben Änderungen auf den Instanzen von Site Recovery Manager Server und vCenter Server auf der Schutz- und der Wiederherstellungs-Site vornehmen.

Informationen zum Ändern der Einstellungen finden Sie unter Ändern der Einstellungen, um große Site Recovery Manager-Umgebungen auszuführen.

Tabelle 10-1. Einstellungen, die die Anzahl der gleichzeitigen Ein- bzw. Ausschaltvorgänge ändern

Option	Beschreibung
srmMaxBootShutdownOps	Bestimmt die maximale Anzahl gleichzeitiger Einschaltvorgänge für einen bestimmten Cluster. Über diesen Wert wird das Herunterfahren von Gastbetriebssystemen, aber nicht das erzwungene Ausschalten gedrosselt. Das Herunterfahren von Gastbetriebssystemen tritt beim Herunterfahren der primären Site (geplantes Failover) und bei IP-Anpassungs-Workflows auf. Ändern Sie diese Option pro Cluster im vSphere Web Client, indem Sie mit der rechten Maustaste auf einen Cluster klicken und **Einstellungen** auswählen. Klicken Sie auf **vSphere DRS** und anschließend auf **Bearbeiten > Erweiterte Optionen**. Geben Sie diese Option ein, um den **defaultMaxBootAndShutdownOpsPerCluster**-Wert zu überschreiben, den Sie in der Datei `vmware-dr.xml` überschreiben können. Sie können in der Datei **vmware-dr.xml** den globalen Wert `defaultMaxBootAndShutdownOpsPerCluster` festlegen und anschließend unterschiedliche **srmMaxBootShutdownOps**-Werte für einzelne Cluster im vSphere Web Client festlegen. Standardmäßig ist die Drosselung ausgeschaltet.
defaultMaxBootAndShutdownOpsPerCluster	Legt die maximale Anzahl gleichzeitiger Einschaltvorgänge für alle Cluster fest, die von Site Recovery Manager geschützt werden. Über diesen Wert wird das Herunterfahren von Gastbetriebssystemen, aber nicht das erzwungene Ausschalten gedrosselt. Das Herunterfahren von Gastbetriebssystemen tritt beim Herunterfahren der primären Site (geplantes Failover) und bei IP-Anpassungs-Workflows auf. Sie ändern diese Einstellung in der Datei `vmware-dr.xml`. Der Wert **srmMaxBootShutdownOps**, den Sie im vSphere Web Client festlegen können, überschreibt den Wert **defaultMaxBootAndShutdownOpsPerCluster**. Sie können in der Datei **vmware-dr.xml** den globalen Wert `defaultMaxBootAndShutdownOpsPerCluster` festlegen und anschließend unterschiedliche **srmMaxBootShutdownOps**-Werte für einzelne Cluster im vSphere Web Client festlegen. Standardmäßig ist die Drosselung ausgeschaltet.
defaultMaxBootAndShutdownOpsPerHost	Bestimmt die maximale Anzahl gleichzeitiger Einschaltvorgänge für einen eigenständigen Host. Sie können die Option nur in der Datei `vmware-dr.xml` festlegen. Standardmäßig ist die Drosselung ausgeschaltet.

Tabelle 10-2. Einstellungen, die Zeitlimits für Zeitüberschreitungen ändern

Option	Beschreibung
vrReplication.synchronizationTimeout	Site Recovery Manager erzwingt eine Zeitüberschreitung, um eine Online- oder Offline-Synchronisierung für virtuelle Maschinen abzuschließen, die während eines Tests oder Failovers von vSphere Replication repliziert wurden. Wenn eine Synchronisierung nicht während eines bestimmten Zeitraums abgeschlossen wurde, z. B. aufgrund einer langsamen Netzwerkverbindung oder einer großen virtuellen Maschine, meldet Site Recovery Manager während eines Tests oder Failovers einen Fehler. Ändern Sie diese Option im vSphere Web Client. Wählen Sie in **Site- Wiederherstellung** eine Site aus. Wählen Sie auf der Registerkarte **Verwalten** die Option **Erweiterte Einstellungen > vSphere Replication**. Der Standardwert ist 7200 und entspricht einer Zeitüberschreitungsperiode für Synchronisierungsvorgänge von 14400 Sekunden.
storage.commandTimeout	Die Zeitüberschreitung zur Ausführung von SRA-Befehle in ABR-bezogenen Workflows. In einigen Fällen, wie bei Surfacing-LUNs und Snapshots benötigen einige Arrays länger als die Standardzeit, um zu reagieren. Ändern Sie diese Option im vSphere Web Client. Wählen Sie in **Site- Wiederherstellung** eine Site aus. Wählen Sie auf der Registerkarte **Verwalten** die Option **Erweiterte Einstellungen > Speicher**. Die Standardeinstellung beträgt 300 Sekunden.

Site Recovery Manager - Ereignisse und -Alarme

11

Site Recovery Manager unterstützt die Ereignisprotokollierung. Zu jedem Ereignis gehört ein entsprechender Alarm, den Site Recovery Manager auslösen kann, wenn das Ereignis eintritt. Dies bietet eine Möglichkeit zum Verfolgen des Systemzustands Ihres Systems, sodass potenzielle Probleme gelöst werden können, bevor sie den von Site Recovery Manager gebotenen Schutz beeinträchtigen.

Dieses Kapitel behandelt die folgenden Themen:

- So überwacht Site Recovery Manager die Verbindungen zwischen Sites
- Konfigurieren von Site Recovery Manager-Alarmen

So überwacht Site Recovery Manager die Verbindungen zwischen Sites

Site Recovery Manager überwacht die Verbindung zwischen der Schutz- und der Wiederherstellungs-Site und protokolliert die Ereignisse, wenn die Remote-Site nicht mehr antwortet.

Wenn Site Recovery Manager die Verbindung zwischen zwei gekoppelten
Site Recovery Manager Server-Instanzen einrichtet, sendet der Site Recovery Manager Server, der die Verbindung initiiert hat, den Befehl `RemoteSiteUpEvent`.

Wenn Site Recovery Manager erkennt, dass die überwachte Verbindung getrennt wurde, beginnt er mit regelmäßigen Verbindungsüberprüfungen, indem er einen `Ping`-Befehl an die Remote-Site sendet.
Site Recovery Manager überwacht die Verbindungsüberprüfungen und protokolliert Ereignisse.

- Site Recovery Manager sendet Ping-Befehle in regelmäßigen Intervallen. Sie können das Intervall mithilfe der Einstellung `remoteSiteStatus.pingInterval` konfigurieren. Die Standardeinstellung ist 300 Sekunden.
- Die Verbindungsüberwachung überspringt eine Anzahl an fehlgeschlagenen Pings. Sie können diese Anzahl mithilfe der Einstellung `remoteSiteStatus.pingFailedDelay` konfigurieren. Die Standardeinstellung ist 2.
- Wenn die Anzahl an übersprungenen fehlgeschlagenen Pings den Wert von `remoteSiteStatus.pingFailedDelay` überschreitet, sendet Site Recovery Manager das Ereignis `RemoteSitePingFailedEvent`.

- Wenn die Anzahl an übersprungenen fehlgeschlagenen Pings einen höheren Grenzwert übersteigt, sendet Site Recovery Manager bei jedem fehlgeschlagenen Ping-Befehl das Ereignis `RemoteSiteDownEvent` und sendet keine `RemoteSitePingFailedEvent`-Ereignisse mehr. Sie können diesen höheren Grenzwert für fehlgeschlagene Ping-Befehle mithilfe der Einstellung `remoteSiteStatus.panicDelay` konfigurieren. Die Standardeinstellung ist 5.
- Site Recovery Manager fährt mit dem Senden von `RemoteSiteDownEvent`-Ereignissen fort, bis die Verbindung erneut hergestellt wurde.
- Wenn eine Verbindung mit dem Site Recovery Manager-Server der Remote-Site neu hergestellt wird, sendet Site Recovery Manager `RemoteSiteUpEvent`-Ereignisse.

Konfigurieren von Site Recovery Manager -Alarmen

Site Recovery Manager fügt Alarme zu den Alarmen hinzu, die vCenter Server unterstützt. Sie können Site Recovery Manager-Alarme so konfigurieren, dass eine E-Mail-Benachrichtigung gesendet, ein SNMP-Trap gesendet oder ein Skript auf dem vCenter Server-Host ausgeführt wird.

Auf der Registerkarte **Alarmdefinitionen** unter **Verwalten** im vSphere Web Client finden Sie eine Liste aller Site Recovery Manager-Alarme. Sie können die Einstellungen für jeden Alarm bearbeiten, um die Aktion anzugeben, die Site Recovery Manager ergreifen soll, wenn ein Ereignis den Alarm auslöst. Standardmäßig führt ein Site Recovery Manager-Alarm eine Aktion erst dann durch, wenn Sie den Alarm konfiguriert haben.

Hinweis In einer Umgebung mit mehr als einem vCenter Server zeigt Site Recovery Manager alle Ereignisse von den Site Recovery Manager-Servern an, die als Erweiterungen registriert sind, selbst wenn Sie die Ereignisse nur für einen bestimmten vCenter Server auswählen.

Voraussetzungen

Damit Alarme E-Mail-Benachrichtigungen senden können, konfigurieren Sie die **Mail**-Einstellungen im Menü **vCenter Server-Einstellungen**. Information dazu finden Sie in der *ESXi- und vCenter Server-Dokumentation*.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf einen vCenter Server.
2. Klicken Sie auf der Registerkarte **Verwalten** auf die Registerkarte **Alarmdefinitionen**, um die Liste der vCenter Server-Alarme anzuzeigen.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Alarm hinzuzufügen.
4. Geben Sie auf der Seite **Allgemein** einen Namen und eine Beschreibung für den Alarm ein und wählen Sie das zu überwachende Objekt aus der Dropdown-Liste aus.
5. Wählen Sie ein bestimmtes Ereignis für das Objekt aus.
6. Aktivieren Sie das Kontrollkästchen **Diesen Alarm aktivieren**, um die Aktion für diesen Alarm zu aktivieren, und klicken Sie auf **Weiter**.

7 Klicken Sie auf der Seite **Auslöser** auf **Hinzufügen**, um einen Ereignisauslöser hinzuzufügen.

8 Wählen Sie ein Ereignis aus der Dropdown-Liste und den entsprechenden Status aus.

Wenn Sie in der Liste wiederholte Ereignisse sehen, stellt jedes Ereignis eine einzelne Site Recovery Manager-Instanz dar und löst einen Alarm für die Erweiterung aus, mit der sie registriert ist. In einem Szenario mit mehreren Site Recovery Manager-Instanzen können Sie zum Beispiel `RecoveryPlanCreated (SRM 1)` und `RecoveryPlanCreated (SRM 2)` für das gleiche Ereignis auf beiden Erweiterungen verwenden.

9 Um eine Bedingung hinzuzufügen, die den Alarm auslöst, klicken Sie auf **Hinzufügen**, wählen Sie ein Argument aus der Dropdown-Liste, den Operator und den Übergang von Warnung zu kritischem Zustand aus.

10 Klicken Sie auf **Weiter**.

11 Wählen Sie aus der Dropdown-Liste auf der Seite **Aktionen** eine Aktion aus, geben Sie in der Konfigurationsspalte die relevanten Informationen ein, geben Sie an, wann die Aktion ausgeführt werden soll, sowie die Anzahl der Minuten, wenn eine Aktion wiederholt werden soll, und klicken Sie auf **Beenden**.

Weiter

Zum Bearbeiten einer Alarmdefinition klicken Sie mit der rechten Maustaste auf einen Alarm und wählen **Bearbeiten** aus.

Site Recovery Manager -Ereignisreferenz

Site Recovery Manager überwacht verschiedenen Typen von Ereignissen.

Site-Statusereignisse

Site-Statusereignisse bieten Informationen zum Status von Schutz- und Wiederherstellungs-Sites sowie der Verbindung zwischen ihnen.

Tabelle 11-1. Site-Statusereignisse

Ereignisname	Ereignistyp	Ereignisbeschreibung	Kategorie
unbekannter Status	`UnknownStatusEvent`	Der Status des Site Recovery Manager Server ist nicht verfügbar	Info
Remote-Site nicht bereit	`RemoteSiteDownEvent`	Site Recovery Manager Server hat die Verbindung zum Remote-Site Recovery Manager Server verloren.	Fehler
Anpingen der Remote-Site fehlgeschlagen	`RemoteSitePingFailedEvent`	Ausfälle an der Remote-Site oder Probleme mit der Netzwerkverbindung.	Warnung
Remote-Site erstellt	`RemoteSiteCreatedEvent`	Die lokale Site wurde erfolgreich mit der Remote-Site gekoppelt.	Info
Remote-Site bereit	`RemoteSiteUpEvent`	Site Recovery Manager Server hat die Verbindung zum Remote-Site Recovery Manager Server wiederhergestellt.	Info

Tabelle 11-1. Site-Statusereignisse (Fortsetzung)

Ereignisname	Ereignistyp	Ereignisbeschreibung	Kategorie
Remote-Site gelöscht	`RemoteSiteDeletedEvent`	Remote-Site Recovery Manager-Site wurde gelöscht.	Info
Eine von vSphere Replication replizierte virtuelle Maschine wird zu einer Schutzgruppe hinzugefügt	`HbrGroupVmAssociatedEvent`	Eine von vSphere Replication replizierte virtuelle Maschine wird zu einer Schutzgruppe hinzugefügt.	Info
Eine von vSphere Replication replizierte virtuelle Maschine wurde aus einer Schutzgruppe entfernt	`HbrGroupVmDisassociatedEvent`	Eine von vSphere Replication replizierte virtuelle Maschine wurde aus einer Schutzgruppe entfernt.	Info
Lokaler vSphere Replication-Server ist ausgefallen	`LocalHmsConnectionDownEvent`	Wiederholte Verbindungsversuche zu vSphere Replication sind fehlgeschlagen.	Fehler
Die Verbindung mit dem lokalen vSphere Replication-Server wurde wiederhergestellt	`LocalHmsConnectionUpEvent`	Verbindung zu vSphere Replication ist hergestellt.	Info
Der lokale vSphere Replication-Server antwortet nicht	`LocalHmsPingFailedEvent`	Es konnte keine Verbindung zum lokalen vSphere Replication-Server hergestellt werden	Warnung
Der lokale Inventory Service ist ausgefallen	`LocalQsConnectionDownEvent`	Es konnte keine Verbindung mit dem lokalen Inventory Service-Server hergestellt werden. Sie können die Anzahl der internen, zu überspringenden Pings angeben, bevor Site Recovery Manager `LocalQsConnectionDownEvent` ausgibt, indem Sie `<connections><qsPanicDelay>`*`Ganzzahl`*`</qsPanicDelay></connections>` in die Konfigurationsdatei `vmware-dr.xml` einfügen.	Fehler
Die Verbindung mit dem lokalen Inventory Service wurde wiederhergestellt	`LocalQsConnectionUpEvent`	Die Verbindung mit dem lokalen Inventory Service ist hergestellt. Sie können das Intervall zwischen Pings vom Site Recovery Manager zum Inventory Service angeben, indem Sie `<connections><qsPingInterval>`*`Sekundenanzahl`*`</qsPingInterval></connections>` in die Konfigurationsdatei `vmware-dr.xml` einfügen.	Info
Der lokale Inventory Service antwortet nicht	`LocalQsPingFailedEvent`	Der Verbindungsversuch mit dem lokalen Inventory Service ist fehlgeschlagen. Sie können die Anzahl der internen, zu überspringenden Pings angeben, bevor Site Recovery Manager `LocalQsPingFailedEvent` ausgibt, indem Sie `<connections><qsPingFailedDelay>`*`Ganzzahl`*`</qsPingFailedDelay></connections>` in die Konfigurationsdatei `vmware-dr.xml` einfügen.	Warnung
Wenig Speicherplatz	`LowDiskSpaceEvent`	Der freie Speicherplatz auf der lokalen Site ist gering.	Warnung

Tabelle 11-1. Site-Statusereignisse (Fortsetzung)

Ereignisname	Ereignistyp	Ereignisbeschreibung	Kategorie
Wenig Arbeitsspeicher	LowMemoryEvent	Der verfügbare Arbeitsspeicher auf der lokalen Site ist gering.	Warnung
SRM-Serverzertifikat noch nicht gültig	SrmCertificateNotValidEvent	Das SSL/TLS-Zertifikat für den angegebenen SRM-Server liegt in der Zukunftist zukünftig.	Fehler
Ablaufender SRM-Serverzertifikat läuft abr	SrmCertificateExpiringEvent	Das SSL/TLS-Zertifikat für den angegebenen SRM-Server läuft in der angegebenen Anzahl an Tagen ab.	Info
Zertifikat für SRM-Serverzertifikat ist abgelaufen	SrmCertificateExpiredEvent	Das SSL/TLS-Zertifikat für den angegebenen SRM-Server ist abgelaufen.	Fehler

Schutzgruppenereignisse

Schutzgruppenereignisse bieten im Zusammenhang mit Schutzgruppen Informationen zu Aktionen und zum Status.

Tabelle 11-2. Ereignisse zur Schutzgruppenreplizierung

Ereignis	Beschreibung	Ursache	Kategorie
CreatedEvent	Schutzgruppe wurde erstellt.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Erstellens einer Schutzgruppe gepostet.	Info
RemovedEvent	Schutzgruppe wurde entfernt.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Entfernens einer Schutzgruppe gepostet.	Info
ReconfiguredEvent	Schutzgruppe wurde neu konfiguriert.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Neukonfigurierens einer Schutzgruppe gepostet.	Info
ProtectedVmCreatedEvent	Die virtuelle Maschine in der Gruppe ist für den Schutz konfiguriert.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Schutzes einer virtuellen Maschine gepostet.	Info
ProtectedVmRemovedEvent	Die virtuelle Maschine in der Gruppe ist nicht mehr für den Schutz konfiguriert.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen der Aufhebung des Schutzes einer virtuellen Maschine gepostet.	Info
ProtectedVmReconfiguredProtectionSettingsEvent	Neu konfigurierte Schutzeinstellungen für VM.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Neukonfigurierens der VM-Schutzeinstellungen gepostet.	Info
ProtectedVmReconfiguredRecoveryLocationSettingsEvent	Neu konfigurierte Einstellungen des Wiederherstellungsspeicherorts für VM.	Wird nur bei erfolgreichem Abschluss der Neukonfiguration der Wiederherstellungsspeicherort-Einstellungen für eine geschützte virtuelle Maschine auf dem vCenter Server der Schutz-Site gepostet.	Info

Tabelle 11-2. Ereignisse zur Schutzgruppenreplizierung (Fortsetzung)

Ereignis	Beschreibung	Ursache	Kategorie
PlaceholderVmCreatedEvent	Die Platzhalter-VM wurde in der vCenter Server-Bestandsliste erstellt.	Wird auf dem vCenter Server der Wiederherstellungs-Site gepostet, wenn die Platzhalter-VM als Ergebnis eines Schutz- oder Reparaturvorgangs erstellt wird.	Info
PlaceholderVmCreatedFrom-OldProductionVmEvent	Die Platzhalter-VM wurde in der Bestandsliste des vCenter Server unter Verwendung der Identität der alten geschützten virtuellen Maschine erstellt.	Auf dem vCenter Server der Wiederherstellungs-Site wird gepostet, dass die Platzhalter-VM als Ergebnis des Austauschs der alten geschützten virtuellen Maschine durch die Platzhalter-VM während oder nach dem erneuten Schutz erstellt wird.	Info
VmFullyProtectedEvent	Virtuelle Maschine in Gruppe: Nicht aufgelöste Geräte wurden alle aufgelöst.	Die zuvor nicht aufgelösten Geräte einer geschützten virtuellen Maschine wurden alle aufgelöst.	Warnung
VmNotFullyProtectedEvent	Virtuelle Maschine in Gruppe: Mindestens ein Gerät muss für den Schutz konfiguriert werden.	Wird nur beim Aktualisieren der Wiederherstellungsspeicherort-Einstellungen für die Gerätebehandlung, wobei ein nicht leerer unresolvedDevices festgelegt ist, auf dem vCenter Server der Schutz-Site gepostet. Dies kann durch Änderungen an der geschützten virtuellen Maschine oder während des erneuten Schutzes einer virtuellen Maschine ausgelöst werden.	Warnung
PlaceholderVmUnexpectedly-DeletedEvent	Virtuelle Maschine in Gruppe: Die Platzhalter-VM wurde aus der vCenter Server-Bestandsliste entfernt.	Wird auf dem vCenter Server der Wiederherstellungs-Site gepostet, wenn Site Recovery Manager erkennt, dass die Platzhalter-VM unerwarteterweise gelöscht oder aus der vCenter Server-Bestandsliste entfernt wurde.	Warnung
ProductionVmDeletedEvent	Virtuelle Maschine in Gruppe: Die geschützte virtuelle Maschine wurde aus der vCenter Server-Bestandsliste der virtuellen Maschine entfernt.	Wird gepostet, wenn eine geschützte virtuelle Maschine aus der vCenter Server-Bestandsliste gelöscht oder daraus entfernt wird.	Fehler
ProductionVmInvalidEvent	Virtuelle Maschine in Gruppe: Die Dateispeicherorte der geschützten virtuellen Maschine können zwecks Replizierung nicht aufgelöst werden.	Wird gepostet, wenn der Replizierungs-Provider die Dateien der geschützten virtuellen Maschine, die repliziert werden sollen, nicht finden kann.	Fehler

Wiederherstellungsereignisse

Wiederherstellungsereignisse bieten Informationen zu Aktionen und zum Status in Zusammenhang mit Site Recovery Manager-Wiederherstellungsvorgängen.

Tabelle 11-3. Wiederherstellungsereignisse

Ereignisname	Ereignistyp	Ereignisbeschreibung	Kategorie
Der Wiederherstellungsplan hat damit begonnen, die angegebene virtuelle Maschine wiederherzustellen.	`RecoveryVmBegin`	Wird signalisiert, wenn die Wiederherstellungs-VM erfolgreich erstellt wurde. Wenn ein Fehler aufgetreten ist, bevor die VM-ID bekannt ist, wird das Ereignis nicht ausgelöst.	Info
Der Wiederherstellungsplan hat die Wiederherstellung der virtuellen Maschine beendet.	`RecoveryVmEnd`	Wird signalisiert, nachdem das letzte Skript nach dem Einschalten abgeschlossen ist oder nachdem bei der virtuelle Maschine ein Fehler aufgetreten ist, der die Wiederherstellung unterbricht.	Info
Der Wiederherstellungsplan *Hostname* wurde erstellt.	`PlanCreated`	Wird signalisiert, wenn ein neuer Plan erstellt wird. Wird an jede vCenter Server-Instanz gesendet, auf der der Plan gehostet wird.	Info
Der Wiederherstellungsplan wurde gelöscht.	`PlanDestroy`	Wird signalisiert, wenn ein Plan aus der Site gelöscht wurde. Beachten Sie, dass auf der Site, auf der die Löschung des Plans angefordert wurde, eine wesentliche Verzögerung auftreten kann, während auf die Löschung des Plans auf der anderen Site gewartet wird. Wird an jede vCenter Server-Instanz gesendet, auf der der Plan gehostet wird.	Info
Der Wiederherstellungsplan wurde geändert.	`PlanEdit`	Wird signalisiert, wenn ein vorhandener Plan bearbeitet wird.	Info
Der Wiederherstellungsplan hat einen Test begonnen.	`PlanExecTestBegin`	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Wiederherstellungstest initiiert wird.	Info
Der Wiederherstellungsplan hat einen Test abgeschlossen.	`PlanExecTestEnd`	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Wiederherstellungstest abgeschlossen ist.	Info
Der Wiederherstellungsplan hat eine Testbereinigung begonnen.	`PlanExecCleanupBegin`	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Testbereinigung initiiert wird.	Info
Der Wiederherstellungsplan hat eine Testbereinigung abgeschlossen.	`PlanExecCleanupEnd`	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Testbereinigung abgeschlossen ist.	Info
Der Wiederherstellungsplan hat eine Wiederherstellung begonnen.	`PlanExecBegin`	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Wiederherstellung initiiert wird.	Info
Der Wiederherstellungsplan hat eine Wiederherstellung abgeschlossen.	`PlanExecEnd`	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Wiederherstellung abgeschlossen ist.	Info

Tabelle 11-3. Wiederherstellungsereignisse (Fortsetzung)

Ereignisname	Ereignistyp	Ereignisbeschreibung	Kategorie
Der Wiederherstellungsplan hat damit begonnen, einen Vorgang zum erneuten Schützen durchzuführen.	`PlanExecReprotectBegin`	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Vorgang zum erneuten Schützen initiiert wird.	Info
Der Wiederherstellungsplan hat einen Vorgang zum erneuten Schützen abgeschlossen.	`PlanExecReprotectEnd`	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Vorgang zum erneuten Schützen abgeschlossen ist.	Info
Der Wiederherstellungsplan zeigt eine Eingabeaufforderung an und wartet auf eine Eingabe des Benutzers.	`PlanPromptDisplay`	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Eingabeaufforderungsschritt erkannt wird. Der Schlüssel ist ein eindeutiger Bezeichner für die Eingabeaufforderung.	Info
Der Wiederherstellungsplan hat eine Antwort auf die Eingabeaufforderung erhalten.	`PlanPromptResponse`	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Eingabeaufforderungsschritt geschlossen wird.	Info
Der Wiederherstellungsplan hat damit begonnen, einen Befehl auf der Site Recovery Manager Server-Maschine auszuführen.	`PlanServerCommandBegin`	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager mit der Ausführung eines Callout-Befehls auf der Site Recovery Manager Server-Maschine begonnen hat.	Info
Der Wiederherstellungsplan hat die Ausführung eines Befehls auf der Site Recovery Manager Server-Maschine abgeschlossen.	`PlanServerCommandEnd`	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager die Ausführung eines Callout-Befehls auf der Site Recovery Manager Server-Maschine abgeschlossen hat.	Info
Der Wiederherstellungsplan hat damit begonnen, einen Befehl auf einer wiederhergestellten virtuellen Maschine auszuführen.	`PlanVmCommandBegin`	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager mit der Ausführung eines Callout-Befehls auf einer wiederhergestellten virtuellen Maschine begonnen hat.	Info
Der Wiederherstellungsplan hat die Ausführung eines Befehls auf einer wiederhergestellten virtuellen Maschine abgeschlossen.	`PlanVmCommandEnd`	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager die Ausführung eines Callout-Befehls auf einer wiederhergestellten virtuellen Maschine abgeschlossen hat.	Info

Speicher- und Speicheranbieter-Ereignisse

Speicher- und Speicheranbietereereignisse bieten Informationen zu Aktionen und statusbezogenem Speicher bzw. zu statusbezogenen Speicheranbietern.

Tabelle 11-4. SRA-Ereignisse

Ereignis	Beschreibung	Ursache	Kategorie
StorageAdaptLoadEvent	Der angegebene SRA wurde geladen.	Site Recovery Manager hat neue SRA erkannt, entweder während der Startphase oder während des vom Benutzer initiierten Neuladens von SRAs.	Info
StorageAdaptReloadFailEvent	Das Laden des SRA vom angegebenen Pfad ist fehlgeschlagen.	Site Recovery Manager konnte einen bereits bekannten SRA nicht neu laden, entweder während der Startphase oder während des vom Benutzer initiierten Neuladens von SRAs.	Fehler
StorageAdaptChangeEvent	Eine neue Version des angegebenen SRAs wurde geladen.	Site Recovery Manager hat erkannt, dass ein bereits bekannter SRA aktualisiert wurde.	Info

Tabelle 11-5. Array-Manager-Ereignisse

Ereignis	Beschreibung	Ursache	Kategorie
SAManagerAddedEvent	Der angegebene Array-Manager wurde mithilfe des angegebenen SRAs erstellt.	Der Benutzer hat einen Array-Manager hinzugefügt.	Info
SAManagerRemovedEvent	Der angegebene Array-Manager wurde gelöscht.	Der Benutzer hat einen Array-Manager entfernt.	Info
SAManagerReconfigEvent	Der angegebene Array-Manager wurde neu konfiguriert.	Der Benutzer hat die Eigenschaften eines Array-Managers bearbeitet.	Info
SAManagerPingOkEvent	Das Anpingen des angegebenen Array-Managers war erfolgreich.	Der Site Recovery Manager Server hat einen Array-Manager erfolgreich angepingt.	Info
SAManagerPingFailEvent	Anpingen des angegebenen Array-Managers fehlgeschlagen.	Beim Anpingen des Array-Managers ist ein Fehler aufgetreten.	Fehler

Tabelle 11-6. Array-Paar-Ereignisse

Ereignis	Beschreibung	Ursache	Kategorie
SAPairDiscoveredEvent	Ein repliziertes Array-Paar wurde mit Array-Manager erkannt.	Ein vom Benutzer erstellter Array-Manager hat replizierte Array-Paare erkannt.	Info
SAPairEnabledEvent	Ein repliziertes Array-Paar wurde mit Array-Manager aktiviert.	Der Benutzer hat ein Array-Paar aktiviert.	Info
SAPairDisabledEvent	Ein repliziertes Array-Paar wurde mit Array-Manager deaktiviert.	Der Benutzer hat ein Array-Paar deaktiviert.	Info
SAPairPingOkEvent	Das Anpingen des replizierten Array-Paars war erfolgreich.	Der Site Recovery Manager Server hat das Array-Paar erfolgreich angepingt.	Info
SAPairPingFailEvent	Das Anpingen des replizierten Array-Paars ist fehlgeschlagen.	Beim Anpingen des Array-Paars ist ein Fehler aufgetreten.	Fehler

Tabelle 11-7. Datenspeicherereignisse

Ereignis	Beschreibung	Ursache	Kategorie
StorageDsDiscoveredEvent	Replizierter Datenspeicher wurde erkannt.	Der Site Recovery Manager Server hat einen replizierten Datenspeicher erkannt.	Info
StorageDsLostEvent	Der angegebene Datenspeicher wird nicht mehr repliziert.	Der Benutzer hat die Replizierung von den Datenspeicher stützenden Speichergeräten ausgeschaltet.	Info
StorageRdmDiscoveredEvent	Eine an der angegebenen virtuellen Maschine angehängte replizierte RDM wurde erkannt.	Der Site Recovery Manager Server hat eine replizierte RDM erkannt. Dieses Problem tritt auf, wenn Sie eine RDM-Festplatte zu einer geschützten virtuellen Maschine hinzufügen.	Info
StorageRdmLostEvent	Eine an der angegebenen virtuellen Maschine angehängte RDM wird nicht mehr repliziert.	Der Benutzer hat die Replizierung der die RDM stützenden LUN ausgeschaltet.	Info

Tabelle 11-8. Schutzereignisse

Ereignis	Beschreibung	Ursache	Kategorie	Ereignis-Ziel
SPDsProtEvent	Geschützter Datenspeicher wurde zur angegebenen Schutzgruppe hinzugefügt.	Der Benutzer hat den Datenspeicher in eine neue oder vorhandene Schutzgruppe aufgenommen.	Info	Datenspeicher
SPDsUnprotEvent	Der Schutz des angegebenen Datenspeichers wurde aufgehoben.	Der Benutzer hat den Datenspeicher aus der Schutzgruppe entfernt oder die Schutzgruppe, in der dieser Datenspeicher enthalten war, gelöscht. Dieses Problem tritt auf, wenn Sie den Schutz eines Datenspeichers aufheben, entweder indem Sie ihn aus einer Schutzgruppe entfernen oder indem Sie die Schutzgruppe entfernen.	Info	Datenspeicher
SPVmDiscoveredEvent	Eine replizierte virtuelle Maschine wurde erkannt.	Der Benutzer hat eine virtuelle Maschine auf einem replizierten Datenspeicher erstellt.	Info	Virtuelle Maschine
SPVmLostEvent	Die angegebene virtuelle Maschine wird nicht mehr repliziert.	Der Benutzer hat eine virtuelle Maschine aus dem replizierten Datenspeicher migriert.	Info	Virtuelle Maschine
SPDsProtMissingEvent	Der replizierte Datenspeicher muss in die angegebene Schutzgruppe aufgenommen werden, befindet sich jedoch in einer alternativen Schutzgruppe.	Dieses Problem tritt auf, wenn Sie einen Datenspeicher haben, der zusammengeführt werden muss, aber noch nicht geschützt ist. Beim Konfliktereignis ist der Datenspeicher schon geschützt.	Warnung	Datenspeicher
SPDsProtConflictEvent	Replizierter Datenspeicher muss in die angegebene Schutzgruppe aufgenommen werden.	Dieses Problem tritt auf, wenn Sie einen Datenspeicher haben, der zusammengeführt werden muss, aber noch nicht geschützt ist. Beim Konfliktereignis ist der Datenspeicher schon geschützt.	Fehler	Datenspeicher
SPDsReplicationLostEvent	Der Datenspeicher in der angegebenen Schutzgruppe wird nicht mehr repliziert	Der Benutzer hat die Replizierung für Geräte ausgeschaltet, die den Datenspeicher stützen.	Fehler	Datenspeicher
SPGroupProtRestoredEvent	Der Schutz der angegebenen Schutzgruppe wurde wiederhergestellt	Die vorherigen (nicht leeren) Probleme einer Schutzgruppe wurden bereinigt.	Info	Schutzgruppe

Tabelle 11-8. Schutzereignisse (Fortsetzung)

Ereignis	Beschreibung	Ursache	Kategorie	Ereignis-Ziel
SPVmDsProtMissingEvent	Der von der virtuellen Maschine verwendete Datenspeicher muss in die angegebene Schutzgruppe aufgenommen werden.	Wenn Sie einer VM, die schon durch eine Schutzgruppe geschützt wird, einen Datenspeicher hinzufügen, der nicht zu dieser Schutzgruppe gehört, müssen Sie ihn der Schutzgruppe hinzufügen.	Warnung	Datenspeicher
SPVmDsProtConflictEvent	Der Datenspeicher, der von der angegebenen virtuellen Maschine verwendet wird, muss in die angegebene Schutzgruppe aufgenommen werden, er wird jedoch zurzeit von einer alternativen Schutzgruppe verwendet.	Wenn Sie einer VM, die schon durch eine Schutzgruppe geschützt wird, einen Datenspeicher hinzufügen, der nicht zu dieser Schutzgruppe gehört, müssen Sie ihn der Schutzgruppe hinzufügen.	Fehler	Datenspeicher
SPVmDsReplicationLostEvent	Der von der angegebenen virtuellen Maschine verwendete Datenspeicher, der sich in der angegebenen Schutzgruppe befindet, wird nicht mehr repliziert.	Siehe Beschreibung.	Fehler	Datenspeicher
SPVmProtRestoredEvent	Der Schutz für die angegebene virtuelle Maschine in der angegebenen Schutzgruppe wurde wiederhergestellt.	Die vorherigen (nicht leeren) Probleme einer geschützten virtuellen Maschine wurden bereinigt. Das Ereignis wird nicht festgehalten, wenn Probleme, die nicht geschützte virtuelle Maschinen betreffen, bereinigt werden.	Info	Virtuelle Maschine
SPCgSpansProtGroupsEvent	Die angegebene Konsistenzgruppe umfasst die angegebenen Schutzgruppen.	Dieses Problem tritt auf, wenn Sie zwei Datenspeicher haben, die in unterschiedlichen Schutzgruppen geschützt werden, die Sie jedoch später zu einer einzelnen Konsistenzgruppe in einem Array zusammenfassen.	Fehler	Datenspeicher
SPCgDsMissingProtEvent	Der Datenspeicher der angegebenen Konsistenzgruppe muss in die angegebene Schutzgruppe aufgenommen werden.	Siehe Beschreibung.	Fehler	Datenspeicher

Tabelle 11-8. Schutzereignisse (Fortsetzung)

Ereignis	Beschreibung	Ursache	Kategorie	Ereignis-Ziel
SPDsSpansConsistGroupsEvent	Der Datenspeicher umfasst Geräte aus unterschiedlichen Konsistenzgruppen.	Dieses Problem tritt auf, wenn Sie zusätzlich zu mehreren LUNs über einen Datenspeicher verfügen, aber diese LUNs nicht derselben Konsistenzgruppe angehören.	Fehler	Datenspeicher
SPNfsDsUrlConflictEvent	Die URLs der NFS-Datenspeicher, die vom angegebenen Volume gemountet wurden, weisen andere URLs auf als die, die vom Remotehost gemountet wurden. Der Remotepfad hat die angegebene URL und der Datenspeicher, der vom anderen Host gemountet wurde, hat die angegebene URL.	Dasselbe NFS-Volume wurde unter Verwendung der verschiedenen IP-Adressen desselben NFS-Servers in zwei unterschiedlichen Datenspeichern gemountet.	Fehler	Datenspeicher

Lizenzierungsereignisse

Lizenzierungsereignisse bieten Informationen zu Änderungen des Site Recovery Manager-Lizenzierungsstatus.

Tabelle 11-9. Lizenzierungsereignisse

Ereignis	Beschreibung	Ursache
LicenseExpiringEvent	Die Site Recovery Manager-Lizenz an der angegebenen Site läuft in der angegebenen Anzahl von Tagen ab.	Alle 24 Stunden werden ablaufende Nicht-Testlizenzen auf die Anzahl der verbleibenden Tage überprüft. Dieses Ereignis wird mit den Ergebnissen gepostet.
EvaluationLicenseExpiringEvent	Die Site Recovery Manager-Testlizenz an der angegebenen Site läuft in der angegebenen Anzahl von Tagen ab.	Alle 24 Stunden werden Testlizenzen auf die Anzahl der verbleibenden Tage überprüft. Dieses Ereignis wird mit den Ergebnissen gepostet.
LicenseExpiredEvent	Die Site Recovery Manager-Lizenz an der angegebenen Site ist abgelaufen.	Alle 30 Minuten posten abgelaufene (Nicht-Test-)Lizenzen dieses Ereignis.
EvaluationLicenseExpiredEvent	Die Site Recovery Manager-Testlizenz an der angegebenen Site ist abgelaufen.	Alle 30 Minuten posten Testlizenzen dieses Ereignis.

Tabelle 11-9. Lizenzierungsereignisse (Fortsetzung)

Ereignis	Beschreibung	Ursache
`UnlicensedFeatureEvent`	Die Site Recovery Manager-Lizenz an der angegebenen Site ist durch die angegebene Anzahl an Lizenzen überreserviert.	Alle 24 Stunden und beim Schützen oder Aufheben des Schutzes einer virtuellen Maschine wird dieses Ereignis gepostet, wenn die Gesamtzahl an Lizenzen die Kapazität der Lizenz überschreitet.
`LicenseUsageChangedEvent`	Die Site Recovery Manager-Lizenz an der angegebenen Site verwendet die angegebene Anzahl von der Gesamtzahl der Lizenzen.	Alle 24 Stunden und beim Schützen oder Aufheben des Schutzes einer virtuellen Maschine wird dieses Ereignis gepostet, wenn die Gesamtzahl an Lizenzen die Kapazität der Lizenz nicht überschreitet.

Berechtigungsereignisse

Berechtigungsereignisse enthalten Informationen zu Änderungen an den Site Recovery Manager-Berechtigungen.

Tabelle 11-10. Berechtigungsereignisse

Ereignis	Beschreibung	Ursache
`PermissionsAddedEvent`	Berechtigung erstellt für das Element auf Site Recovery Manager.	Es wurde mithilfe der angegebenen Rolle eine Berechtigung für das Element erstellt. Das Flag `IsPropagate` gibt an, ob die Berechtigung in der Elementhierarchie nach unten weitergegeben wird.
`PermissionsDeletedEvent`	Berechtigungsregel entfernt für das Element auf Site Recovery Manager.	Eine Berechtigung für das Element wurde gelöscht.
`PermissionsUpdatedEvent`	Berechtigung geändert für das Element auf Site Recovery Manager.	Eine Berechtigung für das angegebene Element wurde geändert.

SNMP-Traps

Site Recovery Manager sendet SNMP-Traps an in vCenter Server definierte Community-Ziele. Sie können sie mit dem vSphere Web Client konfigurieren. Wenn Sie „localhost“ oder „127.0.0.1“ als einen Zielhost für SNMP-Traps eingeben, verwendet Site Recovery Manager die IP-Adresse oder den Hostnamen des vSphere-Servers, wie vom Site Recovery Manager-Installationsprogramm konfiguriert.

SNMP-Traps für Site Recovery Manager 5.x sind mit Site Recovery Manager 4.0 und höheren Versionen abwärtskompatibel.

Tabelle 11-11. SNMP-Traps

Ereignis	Beschreibung	Ursache
`RecoveryPlanExecuteTestBeginTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan einen Test startet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand.
`RecoveryPlanExecuteTestEndTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan einen Test beendet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Ergebnisstatus.
`RecoveryPlanExecuteCleanupBeginTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan eine Testbereinigung startet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand.
`RecoveryPlanExecuteCleanupEndTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan eine Testbereinigung beendet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Ergebnisstatus.
`RecoveryPlanExecuteBeginTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan eine Wiederherstellung startet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand.
`RecoveryPlanExecuteEndTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan eine Wiederherstellung beendet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Ergebnisstatus.
`RecoveryPlanExecuteReprotectBeginTrap`	Dieses Trap wird gesendet, wenn Site Recovery Manager den Workflow zum erneuten Schützen für einen Wiederherstellungsplan startet.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand.
`RecoveryPlanExecuteReprotectEndTrap`	Dieses Trap wird gesendet, wenn Site Recovery Manager den Workflow zum erneuten Schützen für einen Wiederherstellungsplan abgeschlossen hat.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Ergebnisstatus.
`RecoveryVmBeginTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan mit der Wiederherstellung einer virtuellen Maschine beginnt.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungsstatus, Name der virtuellen Maschine, UUID der virtuellen Maschine.
`RecoveryVmEndTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan die Wiederherstellung einer virtuellen Maschine abgeschlossen hat.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungsstatus, Name der virtuellen Maschine, UUID der virtuellen Maschine, Ergebnisstatus.
`RecoveryPlanServerCommandBeginTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan mit der Ausführung eines Befehls-Callouts auf der Maschine des Site Recovery Manager Server beginnt.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Befehlsname.

Tabelle 11-11. SNMP-Traps (Fortsetzung)

Ereignis	Beschreibung	Ursache
`RecoveryPlanServerCommandEndTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan die Ausführung eines Befehls-Callouts auf der Maschine des Site Recovery Manager Server beendet hat.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungsstatus, Befehlsname, Ergebnisstatus.
`RecoveryPlanVmCommandBeginTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan mit der Ausführung eines Befehls-Callouts auf einer wiederhergestellten virtuellen Maschine beginnt.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungsstatus, Befehlsname, Name der virtuellen Maschine, UUID der virtuellen Maschine.
`RecoveryPlanVmCommandEndTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan die Ausführung eines Befehls-Callouts auf einer wiederhergestellten virtuellen Maschine beendet hat.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Befehlsname, Name der virtuellen Maschine, UUID der virtuellen Maschine, Ergebnisstatus.
`RecoveryPlanPromptDisplayTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan Benutzereingaben benötigt, um fortfahren zu können.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp, Ausführungszustand, Zeichenfolge der Eingabeaufforderung.
`RecoveryPlanPromptResponseTrap`	Dieses Trap wird gesendet, wenn ein Wiederherstellungsplan keine weiteren Benutzereingaben benötigt, um fortfahren zu können.	Site Recovery Manager-Site-Name, Name des Wiederherstellungsplans, Wiederherstellungstyp und Ausführungszustand.

Zusammenstellen von Site Recovery Manager - Protokolldateien

12

Um die Ursache von Problemen zu identifizieren, die bei der täglichen Ausführung von Site Recovery Manager auftreten, müssen Sie möglicherweise Site Recovery Manager-Protokolldateien zusammenstellen, um diese zu überprüfen oder an den VMware-Support zu senden.

Site Recovery Manager legt mehrere Protokolldateien an, die Informationen enthalten, die dem VMware-Support bei der Diagnose von Problemen helfen können. Sie können den Site Recovery Manager-Protokoll-Collector verwenden, um das Erfassen von Protokolldateien zu vereinfachen.

Der Site Recovery Manager Server und der Client nutzen unterschiedliche Protokolldateien.

Die Site Recovery Manager Server-Protokolldateien enthalten Informationen über die Serverkonfiguration sowie Meldungen, die die Servervorgänge betreffen. Das Site Recovery Manager Server-Protokollpaket enthält zudem Systeminformationen und Verlaufsberichte für die Ausführungen des neuesten Wiederherstellungsplans.

Die Site Recovery Manager-Client-Protokolldateien enthalten Informationen zur Clientkonfiguration sowie Meldungen, die die Client-Plug-In-Vorgänge betreffen. Das Site Recovery Manager-Paket enthält zudem Protokolldateien des Installationsprogramms und die Inhalte des Unterverzeichnisses für die Speicherreplizierungsadapter (SRA) im Protokollverzeichnis.

Protokolldateien aus vCenter Server-Instanzen und ESXi-Serverinstanzen, die Teil Ihres Site Recovery Manager-Systems sind, enthalten möglicherweise Informationen, die bei der Diagnose von Site Recovery Manager-Problemen nützlich sind.

Für die Site Recovery Manager-Protokolldatei werden die Dateien erfasst oder abgerufen, in einer ZIP-Datei komprimiert und in einem von Ihnen angegebenen Verzeichnis gespeichert.

Fehler, die während der Site Recovery Manager-Vorgänge auftreten, werden in den Fehlerdialogfeldern oder im Fenster **Kürzlich bearbeitete Aufgaben** angezeigt. Die meisten Fehler erzeugen auch einen Eintrag in einer Site Recovery Manager-Protokolldatei. Überprüfen Sie die kürzlich bearbeiteten Aufgaben und die Protokolldateien der Wiederherstellungs-Site und der Schutz-Site.

Dieses Kapitel behandelt die folgenden Themen:

Erfassen von Daten in Site Recovery Manager - Protokolldateien mit der Site Recovery Manager - Schnittstelle

Sie können Protokolle für Site Recovery Manager an einen benutzerdefinierten Speicherort herunterladen.

Anhand dieser Informationen können Sie Probleme analysieren und beheben. Sammeln Sie Protokolle von jeder Site, um die besten Ergebnisse zu erzielen.

Vorgehensweise

1. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites** und wählen Sie eine Site aus.
2. Wählen Sie im Menü **Aktionen** die Option **SRM-Protokoll exportieren** aus. Sie können auch mit der rechten Maustaste auf die Site klicken und **SRM-Protokoll exportieren** wählen.
3. Klicken Sie im Assistenten **SRM-Protokoll exportieren** auf **Protokoll generieren** und warten Sie, bis der Vorgang abgeschlossen ist.
4. Klicken Sie zum Herunterladen der Protokolle auf **Protokoll herunterladen**.

Manuelles Erfassen von Site Recovery Manager - Protokolldateien

Sie können Site Recovery Manager Server-Protokolldateien in einem Protokollpaket herunterladen, das Sie manuell generieren. Dies ist nützlich, wenn Sie nicht auf den vSphere-Client zugreifen können.

Das Protokollpaket, das von diesen Prozeduren generiert wird, ist identisch mit den Protokollen, die Sie mithilfe des vSphere-Clients generieren.

Vorgehensweise

- Starten Sie den Vorgang zum Erfassen der Site Recovery Manager Server-Protokolldateien vom **Start**menü aus:
  a. Melden Sie sich beim Site Recovery Manager Server-Host an.
  b. Wählen Sie **Start > Programme > VMware > VMware Site Recovery Manager > vCenter Site Recovery Manager-Protokollpaket generieren** aus.

- Starten Sie den Vorgang zum Erfassen der Site Recovery Manager Server-Protokolldateien von der Windows-Befehlszeile aus:
  a Starten Sie eine Windows-Befehlsshell auf dem Site Recovery Manager Server-Host.
  b Wechseln Sie zum Verzeichnis `C:\Programme\VMware\VMware vCenter Site Recovery Manager\bin`.
  c Führen Sie den folgenden Befehl aus.

```
cscript srm-support.wsf
```

Die einzelnen Protokolldateien werden in einer Datei namens `srm-support-MM-TT-JJJJ-HH-MM.zip` erfasst, wobei *MM-TT-JJJJ-HH-MM* den Monat, den Tag, das Jahr, die Stunde und die Minute der Erstellung der Protokolldateien angibt. Das Protokollpaket wird standardmäßig auf dem Desktop gespeichert.

Ändern der Größe und Anzahl der Site Recovery Manager Server -Protokolldateien

Sie können die Größe und Anzahl sowie den Speicherort der Site Recovery Manager Server-Protokolldateien ändern.

Sie können die Site Recovery Manager-Protokolleinstellungen in der Konfigurationsdatei `vmware-dr.xml` auf dem Site Recovery Manager Server ändern.

Vorgehensweise

1. Melden Sie sich beim Site Recovery Manager Server-Host an.
2. Öffnen Sie die Datei `vmware-dr.xml` in einem Texteditor.

   Sie finden die Datei `vmware-dr.xml` im Ordner `C:\Programme\VMware\VMware vCenter Site Recovery Manager\config`.
3. Suchen Sie den Abschnitt `<log>` in der Datei `vmware-dr.xml`.
4. Legen Sie für die Protokolldateien die maximale Größe in Byte fest.

   Fügen Sie hierzu den Abschnitt `<maxFileSize>` in den Abschnitt `<log>` ein. Die Standardeinstellung beträgt 5242880 Byte.

```
<log>

   <maxFileSize>5242880</maxFileSize>

</log>
```

5 Legen Sie die maximale Anzahl der beizubehaltenden Protokolldateien fest.

Fügen Sie hierzu den Abschnitt <maxFileNum> in den Abschnitt <log> ein. Der Standardwert ist 10 Protokolldateien.

```
<log>

   <maxFileNum>50</maxFileNum>

</log>
```

6 Ändern Sie den Speicherort der Protokolldateien auf dem Site Recovery Manager Server.

Ändern Sie hierzu den Abschnitt <directory> im Abschnitt <log>.

```
<log>

   <directory>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\Logs</directory>

</log>
```

7 Ändern Sie das Standardpräfix für Protokolldateien.

Ändern Sie hierzu den Abschnitt <name> im Abschnitt <log>.

```
<log>

   <name>vmware-dr</name>

</log>
```

8 Ändern Sie die Protokollierungsebene.

Ändern Sie hierzu den Abschnitt <level> im Abschnitt <log>. Die verfügbaren Protokollierungsebenen sind „error“, „warning“, „info“, „trivia“ und „verbose“.

```
<log>

   <level>verbose</level>

</log>
```

9 (Optional) Legen Sie die Protokollierungsebene für die Site Recovery Manager Server-Komponenten fest.

Sie können bestimmte Protokollierungsebenen für Komponenten festlegen, indem Sie die entsprechenden `<level>`-Abschnitte ändern. Die verfügbaren Protokollierungsebenen sind „error“, „warning“, „info“, „trivia“ und „verbose“. Beispielsweise können Sie die Protokollierungsebene für eine Wiederherstellung auf „Ausführlich (erweitert)“ festlegen.

```
<level id="Recovery">
   <logName>Recovery</logName>
   <logLevel>trivia</logLevel>
</level>
```

10 (Optional) Legen Sie die Protokollierungsebene für Speicherreplizierungsadapter fest.

Beim Festlegen der Site Recovery Manager-Protokollierungsebene wird die Protokollierungsebene für SRAs nicht festgelegt. Um die SRA-Protokollierungsebene zu ändern, fügen Sie den Abschnitt `<level id="SraCommand">` in die Datei `vmware-dr.xml` ein. Die verfügbaren Protokollierungsebenen sind „error“, „warning“, „info“, „trivia“ und „verbose“.

```
<level id="SraCommand">
   <logName>SraCommand</logName>
   <logLevel>trivia</logLevel>
</level>
```

11 Starten Sie den Dienst Site Recovery Manager Server neu, damit die Änderungen wirksam werden.

Konfigurieren von Site Recovery Manager-Core-Dumps

Sie können die Site Recovery Manager-Core-Dump-Einstellungen konfigurieren, um den Speicherort der Core-Dump-Dateien zu ändern und diese zu komprimieren.

Sie können die Site Recovery Manager-Core-Dump-Einstellungen in der Konfigurationsdatei `vmware-dr.xml` auf dem Site Recovery Manager Server ändern.

Der untergeordnete Site Recovery Manager Server-Prozess `rundll32.exe` überwacht den primären Site Recovery Manager Server-Prozess auf Notfallalarm-Abbrüche und übernimmt dann das Generieren des Core-Dumps.

Vorgehensweise

1 Melden Sie sich beim Site Recovery Manager Server-Host an.

2 Öffnen Sie die Datei `vmware-dr.xml` in einem Texteditor.

Sie finden die Datei `vmware-dr.xml` im Ordner `C:\Programme\VMware\VMware vCenter Site Recovery Manager\config`.

3 Ändern Sie den Speicherort der Core-Dumps auf dem Site Recovery Manager Server.

Ändern Sie hierzu den Abschnitt `<coreDump>`.

```
<coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles</coreDump>
```

Der Standardpfad lautet `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\DumpFiles`, es sei denn, dieser Ort ist nicht vorhanden oder nicht beschreibbar. In diesem Fall verwendet Site Recovery Manager Server den Pfad `C:\ProgramData\VMware`.

4 Verwenden Sie die Core-Dump-Systemparameter, um die Anzahl der erstellten und komprimierten Dump-Dateien einzuschränken.

```
<debug>
  <dumpCoreCompression>true,false</dumpCoreCompression>
  <dumpFullCore>true,false</dumpFullCore>
</debug>
```

Option	Beschreibung
dumpCoreCompression	Wird kein Wert angegeben, lautet der Standardwert „false“. Beim Erstellen von Core-Dump-Dateien werden frühere Core-Dump-Dateien von Site Recovery Manager Server nicht komprimiert. Wenn Sie „true“ auswählen, werden alle älteren Core-Dump-Dateien von Site Recovery Manager Server komprimiert, sobald eine neue Core-Dump-Datei generiert wird.
dumpFullCore	Wird kein Wert angegeben, lautet der Standardwert „false“. Site Recovery Manager Server generiert eine mehrere MB große Core-Dump-Datei, die im Falle eines Problems Unterstützung bietet. Wenn Sie diesen Wert auf „true“ setzen, generiert Site Recovery Manager Server eine vollständige Core-Dump-Datei, die möglicherweise mehrere GB groß ist, je nach Arbeitslast zu dem Zeitpunkt, an dem der Core-Dump auftritt. Diese größere Datei kann im Falle eines Problems mehr Unterstützung bieten. Wenn der Speicherplatz auf der Festplatte es zulässt, legen Sie diesen Wert auf „true“ fest.

5 Um die maximale Anzahl von Core-Dump-Dateien zu ändern, fügen Sie eine Zeile zum Abschnitt `<debug>` hinzu.

```
<maxCoreDumpFiles>max files</maxCoreDumpFiles>
```

Wird kein Wert angegeben, lautet der Standardwert „4“. Dieser Wert legt die maximale Anzahl der im Core-Dump-Verzeichnis gespeicherten Core-Dump-Dateien fest. Wenn Site Recovery Manager Server Core-Dumps erstellt, werden ältere bei Bedarf von Site Recovery Manager Server gelöscht, um zu verhindern, dass der Höchstwert überschritten und zu viel Speicherplatz auf der Festplatte belegt wird, insbesondere, wenn `dumpFullCore` zutrifft.

Fehlerbehebung bei Site Recovery Manager

13

Wenn Probleme beim Erstellen von Schutzgruppen und Wiederherstellungsplänen, bei der Wiederherstellung oder bei der Gastanpassung auftreten, können Sie das Problem über die Fehlerbehebung lösen.

Überprüfen Sie auf der Suche nach der Ursache eines Problems auch die VMware-Knowledgebase unter http://kb.vmware.com/.

Dieses Kapitel behandelt die folgenden Themen:

Beim Ausführen von Callouts verdoppelt Site Recovery Manager die Anzahl der umgekehrten Schrägstriche in der Befehlszeile

Wenn ein umgekehrter Schrägstrich Teil der Callout-Befehlszeile ist, verdoppelt Site Recovery Manager alle umgekehrten Schrägstriche.

Problem

Der Systeminterpreter für die Befehlszeile behandelt doppelte umgekehrte Schrägstriche nur in Dateipfaden als einfache umgekehrte Schrägstriche. Wenn der Callout-Befehl einen umgekehrten Schrägstrich in einem anderen Parameter als dem Dateipfad benötigt und doppelte umgekehrte Schrägstriche vom Befehl nicht in einfache umgekehrte Schrägstriche umgewandelt werden, wird die Ausführung des Callout-Befehls möglicherweise mit einem Fehler beendet.

Als Beispiel können Sie dem Workflow einen Callout-Schritt hinzufügen und den folgenden Text als Befehl eingeben:

```
c:\Windows\system32\cmd.exe /C "C:\myscript.cmd" a/b/c \d\e\f \\g\\h c:\myscript.log
```

Als Ergebnis des Callout-Schritts führt Site Recovery Manager den folgenden Befehl aus:

```
c:\\Windows\\system32\\cmd.exe /C "C:\\myscript.cmd" a/b/c \\d\\e\\f \\\\g\\\\h c:\\myscript.log
```

Wenn der doppelte umgekehrte Schrägstrich nicht durch `myscript.cmd` in einen einfachen umgekehrten Schrägstrich geändert wird und bei den Parametern `\d\e\f` und `\\g\\h` die Anzahl der umgekehrten Schrägstriche berücksichtigt wird, schlägt `myscript.cmd` möglicherweise fehl.

Lösung

1. Erstellen Sie eine weitere Befehlszeilen-Batchdatei, die Befehle und alle erforderlichen Parameter enthält. Der Callout-Schritt führt diese zusätzliche Batchdatei ohne ein Argument aus. Die folgende Lösung ist beispielsweise möglich:
   a. Erstellen Sie in einem Texteditor wie dem Windows-Editor die Datei `c:\SRM_callout.cmd` mit dem folgenden Inhalt: **`C:\myscript.cmd a/b/c \d\e\f \\g\\h c:\myscript.log`**
   b. Geben Sie in einem Callout-Schritt des Wiederherstellungsplans diesen auszuführenden Befehl ein: **`c:\\Windows\\system32\\cmd.exe /C c:\SRM_callout.cmd`**

2 Fügen Sie einen Code zur ursprünglichen Skriptdatei hinzu, durch den die doppelten umgekehrten Schrägstriche durch einfache umgekehrte Schrägstriche ersetzt werden.

   a Fügen Sie einen Code ähnlich dem folgenden Beispiel an den Anfang der Skriptdatei `c:\myscript.cmd` ein.

   ```
   @echo off
   set arg2=%2
   set arg3=%3
   set fixed_arg2=%arg2:\\=\%
   set fixed_arg3=%arg3:\\=\%
   ```

   Wenn Sie den Umschalt-Befehl in einem Skript einsetzen, werden alle Parameter mit doppelten umgekehrten Schrägstrichen auf diese Weise gehandhabt.

   b Wenn Sie den Umschalt-Befehl in einem Skript verwenden, nehmen Sie die folgenden Änderungen vor:

   Ersetzen Sie `%2` durch `%fixed_arg2%`.

   Ersetzen Sie `%3` durch `%fixed_arg3%`.

   c Ändern Sie nicht den Befehl des Callout-Schritts.

Das Einschalten mehrerer virtueller Maschinen gleichzeitig auf der Wiederherstellungs-Site kann zu Fehlern führen

Wenn viele virtuelle Maschinen gleichzeitig Startvorgänge durchführen, treten während der Array-basierten Wiederherstellung und der Wiederherstellung per vSphere Replication möglicherweise Fehler auf.

Problem

Wenn Sie auf der Wiederherstellungs-Site viele virtuelle Maschinen gleichzeitig starten, sehen Sie in den Berichten zum Wiederherstellungsverlauf möglicherweise die folgenden Fehler:

- `Den Befehl 'echo "Starting IP customization on Windows ..." > > % VMware_GuestOp_OutputFile%.`
- `Die Anpassung kann nicht abgeschlossen werden, möglicherweise wegen des Laufzeitfehlers eines Skripts oder wegen ungültiger Skriptparameter.`
- `Beim Hochladen von Dateien auf die Gast-VM ist ein Fehler aufgetreten.`
- `Zeitüberschreitung beim Warten auf VMware Tools nach 600 Sekunden.`

Ursache

Standardmäßig legt Site Recovery Manager für die Anzahl an gleichzeitigen Einschaltvorgängen keine Begrenzung fest. Wenn beim Einschalten der virtuellen Maschinen auf der Wiederherstellungs-Site Fehler auftreten, können Sie in der Datei `vmware-dr.xml` die Anzahl an gleichzeitigen Einschaltvorgängen für virtuelle Maschinen begrenzen.

Falls diese Fehler auftreten, begrenzen Sie die Anzahl der Einschaltvorgänge auf der Wiederherstellungs-Site gemäß der Kapazität Ihrer Umgebung für einen eigenständigen Host oder einen Cluster.

Lösung

1. Wechseln Sie auf dem Wiederherstellungsserver zu `C:\Programme\VMware\VMware vCenter Site Recovery Manager\config`.
2. Öffnen Sie die Datei `vmware-dr.xml` in einem Texteditor.
3. Ändern Sie die Werte für `defaultMaxBootAndShutdownOpsPerCluster` und `defaultMaxBootAndShutdownOpsPerHost`, um die Anzahl der Einschaltvorgänge auf der Wiederherstellungs-Site zu begrenzen.

   Im folgenden Beispiel wurde die Anzahl der Einschaltvorgänge pro Cluster auf 32 und pro eigenständigem Host auf 4 begrenzt.

   ```
   <config>
     <defaultMaxBootAndShutdownOpsPerCluster>32</defaultMaxBootAndShutdownOpsPerCluster>
     <defaultMaxBootAndShutdownOpsPerHost>4</defaultMaxBootAndShutdownOpsPerHost>
   </config>
   ```

4. Starten Sie den Site Recovery Manager-Server-Dienst neu.

Die Einstellung „LVM.enableResignature=1“ bleibt nach einer Site Recovery Manager -Testwiederherstellung unverändert

Site Recovery Manager unterstützt keine ESXi-Umgebungen, bei denen das Flag `LVM.enableResignature` auf 0 festgelegt ist.

Problem

Während einer Testwiederherstellung oder einer tatsächlichen Wiederherstellung legt Site Recovery Manager `LVM.enableResignature` auf 1 fest, sofern das Flag nicht bereits gesetzt ist. Site Recovery Manager legt dieses Flag fest, um die Snapshot-Volumes neu zu signieren, und mountet sie zur Wiederherstellung auf ESXi-Hosts. Nachdem der Vorgang durchgeführt wurde, behält das Flag den Wert 1 bei.

Ursache

Site Recovery Manager prüft nicht, wie den ESXi-Hosts Snapshot-Volumes präsentiert werden. Site Recovery Manager unterstützt nicht das Festlegen des Flags `LVM.enableResignature` auf 0. Wenn Sie den Wert des Flags von 1 auf 0 ändern, könnte eine virtuelle Maschine jedes Mal ausfallen, wenn Sie eine Testwiederherstellung durchführen oder eine tatsächliche Wiederherstellung erfolgt.

Das Setzen des Flags `LVM.enableResignature` auf ESXi-Hosts ist ein hostweiter Vorgang. Wenn das Flag auf 1 festgelegt ist, werden während der erneuten Hostprüfung oder des nächsten Neustarts des Hosts alle Snapshot-LUNs neu signiert, die für den ESXi-Host sichtbar sind und neu signiert werden können.

Wenn Snapshot-Volumes, die nicht mit Site Recovery Manager in Zusammenhang stehen, auf ESXi-Hosts der Wiederherstellungs-Site erzwungenermaßen gemountet werden, werden diese LUNs als Teil einer erneuten Hostprüfung während einer Testwiederherstellung oder einer tatsächlichen Wiederherstellung neu signiert. Als Folge davon werden alle virtuellen Maschinen in diesen Volumes unzugänglich.

Lösung

Um Ausfälle zu verhindern, vergewissern Sie sich, dass keine Snapshot-LUNs, die nicht mit Site Recovery Manager in Zusammenhang stehen und erzwungenermaßen gemountet werden, für ESXi-Hosts auf der Wiederherstellungs-Site sichtbar sind.

Hinzufügen von virtuellen Maschinen zu einer Schutzgruppe schlägt mit einem Fehler des Typs „Nicht aufgelöste Geräte“ fehl

Das Hinzufügen von virtuellen Maschinen zu einer Schutzgruppe schlägt mit einer Fehlermeldung fehl, wenn Sie die entsprechenden Bestandslistenzuordnungen nicht eingerichtet haben.

Problem

Wenn Sie eine virtuelle Maschine zu einer Schutzgruppe hinzufügen, wird die Fehlermeldung `Die VM 'Name der VM' kann aufgrund von nicht aufgelösten Geräten nicht geschützt werden` ausgegeben.

Ursache

Sie haben keine Bestandslistenzuordnungen konfiguriert, um die Geräte der virtuellen Maschine auf der Schutz-Site den entsprechenden Geräten auf der Wiederherstellungs-Site zuzuordnen.

Lösung

Konfigurieren Sie die Bestandslistenzuordnungen, wie unter *Installation und Konfiguration von Site Recovery Manager* beschrieben.

Die Konfiguration des Schutzes schlägt mit einem Fehler bezüglich der Platzhaltererstellung fehl

Wenn Sie einen Schutz auf mehreren virtuellen Maschinen konfigurieren, schlägt die Konfiguration mit einem Fehler bezüglich der Platzhaltererstellung fehl.

Problem

Gleichzeitiges Erstellen des Schutzes auf vielen virtuellen Maschinen schlägt entweder mit einem Zeitüberschreitungsfehler oder einem Benennungsfehler bezüglich der Platzhaltererstellung fehl.

- `Fehler bezüglich der Erstellung einer Platzhalter-VM:Zeit für Vorgang überschritten:300 Sekunden`
- `Fehler bezüglich der Erstellung einer Platzhalter-VM:Der Name '`*`Platzhaltername`*`' ist bereits vorhanden`

Dieses Problem tritt auf, wenn Sie den Schutz auf unterschiedliche Art und Weise konfigurieren:

- Sie erstellen eine Schutzgruppe, die einen oder mehrere Datenspeicher mit einer großen Anzahl von virtuellen Maschinen enthält.
- Sie benutzen die Option **Schutzgruppen > Virtuelle Maschinen > Alle wiederherstellen** in der Site Recovery Manager-Schnittstelle für eine große Anzahl von virtuellen Maschinen.
- Sie verwenden die Site Recovery Manager-API, um eine große Anzahl an virtuellen Maschinen manuell zu schützen.

Ursache

Die Infrastruktur der Wiederherstellungs-Site kann das Volumen der gleichzeitigen Erstellung mehrerer Platzhalter-VMs nicht handhaben.

Lösung

Erhöhen Sie die Einstellung `replication.placeholderVmCreationTimeout` (Standardwert ist 300 Sekunden). Weitere Informationen hierzu finden Sie unter Ändern der Replizierungseinstellungen.

Sie müssen den Site Recovery Manager Server nach Änderung dieser Einstellung nicht neu starten. Site Recovery Manager übernimmt die Einstellung, wenn Sie das nächste Mal einen Schutz für eine virtuelle Maschine konfigurieren.

Schnelles Löschen und Neuerstellen von Platzhaltern schlägt fehl

Wenn Sie alle Platzhalter-VMs aus einem Datenspeicher löschen, den Datenspeicher unmounten und anschließend den Datenspeicher erneut mounten, schlägt das Neuerstellen der Platzhalter-VMs möglicherweise fehl.

Problem

Wenn Sie nach dem Unmounten des Datenspeichers die Platzhalter zu schnell neu erstellen, kann der Vorgang mit dem Fehler `NoCompatibleHostFound` fehlschlagen.

Ursache

Die Verknüpfungen zwischen ESXi-Hosts und Datenspeichern werden alle 10 Minuten aktualisiert. Wenn Sie nach dem Unmounten und erneuten Mounten des Datenspeichers, aber vor der nächsten Aktualisierung die Platzhalter neu erstellen, wird der Host nicht gefunden.

Lösung

Warten Sie länger als 10 Minuten nach dem Unmounten und erneuten Mounten des Datenspeichers, bevor Sie die Platzhalter-VMs neu erstellen.

Die geplante Migration schlägt aufgrund eines falschen Status des Hosts fehl

Wenn Sie den ESXi-Host auf der Wiederherstellungs-Site während einer geplanten Migration in den Wartungsmodus versetzen, schlägt die geplante Migration fehl.

Problem

Die geplante Migration schlägt mit der Fehlermeldung `Fehler – Der Vorgang ist im aktuellen Hostzustand nicht zulässig` fehl.

Ursache

Site Recovery Manager kann virtuelle Maschinen auf der Wiederherstellungs-Site nicht einschalten, wenn sich der ESXi-Host auf der Wiederherstellungs-Site im Wartungsmodus befindet.

Lösung

Beenden Sie den Wartungsmodus auf dem ESXi-Host auf der Wiederherstellungs-Site und führen Sie die geplante Migration erneut aus.

Wiederherstellung schlägt bei einigen virtuellen Maschinen während der Netzwerkanpassung mit einem Zeitüberschreitungsfehler fehl

Während einer Wiederherstellung werden einige virtuelle Maschinen nicht wiederhergestellt und es kommt zu einem Zeitüberschreitungsfehler bei der Netzwerkanpassung.

Problem

Während einer Wiederherstellung werden einige virtuelle Maschinen innerhalb des Standard-Zeitlimits von 120 Sekunden nicht wiederhergestellt.

Ursache

Dieses Problem kann aus einem der folgenden Gründe auftreten.

- Das VMware Tools-Paket ist auf der virtuellen Maschine, die Sie wiederherstellen, nicht installiert.
- Beim Versuch, gleichzeitig mehrere virtuelle Maschinen wiederherzustellen, weist der Cluster auf der Wiederherstellungs-Site eine erhebliche Ressourcennutzung auf. In diesem Fall können Sie bestimmte Zeitüberschreitungseinstellungen erhöhen, um Aufgaben mehr Zeit für die Durchführung zuzuteilen. Siehe Ändern von Wiederherstellungseinstellungen.

Lösung

1. Überprüfen Sie, ob VMware Tools auf der virtuellen Maschine, die Sie wiederherstellen, installiert ist.
2. Prüfen Sie die verfügbare Kapazität auf der Wiederherstellungs-Site.

   Falls auf der Wiederherstellungs-Site eine hohe Ressourcennutzung zu beobachten ist, kann das Problem behoben werden, indem das Zeitlimit für Gastanpassungen erhöht wird.

   a. Klicken Sie im vSphere Web Client auf **Site-Wiederherstellung > Sites**, wählen Sie eine Site aus und klicken Sie auf **Verwalten > Erweiterte Einstellungen**.

   b. Wählen Sie **Wiederherstellen** und klicken Sie auf **Bearbeiten**.

   c. Erhöhen Sie den Standardwert (600 Sekunden) des Parameters `recovery.customizationTimeout`.

   d. Erhöhen Sie den Standardwert (300 Sekunden) des Parameters `recovery.powerOnTimeout`.
3. Führen Sie die Wiederherstellung erneut aus.

Die Wiederherstellung schlägt mit dem Fehler „Host und Datenspeicher nicht verfügbar“ fehl

Wenn Sie eine Wiederherstellung oder eine Testwiederherstellung durchführen, kurz nachdem die vCenter Server-Bestandsliste geändert wurde, schlägt die Wiederherstellung oder der Test aufgrund nicht verfügbarer Hosthardware und Datenspeicher fehl.

Problem

Die Wiederherstellung oder Testwiederherstellung schlägt mit folgender Fehlermeldung fehl: `Kein Host mit Hardwareversion '7' und Datenspeicher 'ds_id', die eingeschaltet und nicht im Wartungsmodus sind, sind verfügbar....`

Ursache

Der Site Recovery Manager Server bewahrt den Hostbestandslistenstatus in seinem Cache auf. Wenn in letzter Zeit Änderungen in der Bestandsliste vorgenommen wurden, beispielsweise wenn ein Host nicht mehr verfügbar ist, wenn er getrennt wird oder seine Verbindung mit einigen Datenspeichern verliert, kann es vorkommen, dass der Site Recovery Manager Server bis zu 15 Minuten zum Aktualisieren des Caches benötigt. Wenn der Site Recovery Manager Server den falschen Hostbestandslistenstatus in seinem Cache bewahrt, kann eine Wiederherstellung oder eine Testwiederherstellung fehlschlagen.

Lösung

Warten Sie 15 Minuten, bevor Sie eine Wiederherstellung durchführen, wenn Sie die Hostbestandsliste geändert haben. Wenn Sie den oben genannten Fehler erneut erhalten, warten Sie 15 Minuten und führen Sie die Wiederherstellung dann erneut durch.

Erneutes Schützen schlägt mit einem vSphere Replication -Zeitüberschreitungsfehler fehl

Wenn Sie das erneute Schützen auf einem Wiederherstellungsplan ausführen, der vSphere Replication-Schutzgruppen enthält, tritt bei dem Vorgang eine Zeitüberschreitung mit einem Fehler auf.

Problem

Vorgänge zum erneuten Schutz auf Wiederherstellungspläne, die vSphere Replication-Schutzgruppen enthalten, schlagen mit der Fehler `Zeitüberschreitung beim Vorgang: 7200 Sekunden VR-Synchronisierung für die VRM-Gruppe fehlgeschlagen <Nicht verfügbar> fehl. Zeitüberschreitung beim Vorgang: 7200 Sekunden`.

Ursache

Wenn Sie den Vorgang zum erneuten Schützen ausführen, führt Site Recovery Manager eine Online-Synchronisierung für die vSphere Replication-Schutzgruppe aus, wodurch eine Zeitüberschreitung auftreten kann. Der Standardwert für die Zeitüberschreitung beträgt zwei Stunden und entspricht einer Zeitüberschreitungsperiode für Synchronisierungsvorgänge von vier Stunden.

Lösung

Erhöhen Sie den Wert der Zeitüberschreitung `synchronizationTimeout` unter "Erweiterte Einstellungen". Weitere Informationen hierzu finden Sie unter Ändern der vSphere Replication-Einstellungen.

Der Wiederherstellungsplan läuft während des Wartens auf VMware Tools ab

Die Ausführung eines Wiederherstellungsplans schlägt beim Warten auf den Start von VMware Tools mit einer Zeitüberschreitung fehl.

Problem

Wiederherstellungsvorgänge schlagen beim Schritt „Herunterfahren der VMs“ oder „Warten auf den Start von VMware Tools“ des Wiederherstellungsplans fehl.

Ursache

Site Recovery Manager erkennt anhand des Taktsignalstatus von VMware Tools, wann wiederhergestellte virtuelle Maschinen auf der Wiederherstellungs-Site ausgeführt werden. Wiederherstellungsvorgänge erfordern die Installation von VMware Tools auf den geschützten virtuellen Maschinen. Die Wiederherstellung schlägt fehl, wenn VMware Tools auf den geschützten virtuellen Maschinen nicht installiert wurde oder wenn Site Recovery Manager so konfiguriert wurde, dass die Ausführung erst nach dem Start von VMware Tools erfolgt.

Lösung

Installieren Sie VMware Tools auf den geschützten virtuellen Maschinen. Wenn Sie VMware Tools auf geschützten virtuellen Maschinen nicht installieren oder nicht installieren können, müssen Sie Site Recovery Manager so konfigurieren, dass nicht auf den Start von VMware Tools in den wiederhergestellten virtuellen Maschinen gewartet wird und die Schritte zum Herunterfahren des Gastbetriebssystems übersprungen werden. Weitere Informationen hierzu finden Sie unter Ändern von Wiederherstellungseinstellungen.

Die Synchronisierung schlägt für vSphere Replication - Schutzgruppen fehl

Während einer Testwiederherstellung, einer geplanten Migration und des erneuten Schützens von Wiederherstellungsplänen, die vSphere Replication-Schutzgruppen enthalten, schlägt der VM-Synchronisierungsschritt mit einem Fehler fehl.

Problem

Die Synchronisierung von virtuellen Maschinen in einer vSphere Replication-Schutzgruppe schlägt mit der Fehlermeldung fehl: `Fehler – VR-Synchronisierung für VRM-Gruppe fehlgeschlagen <nicht verfügbar>. Das Objekt wurde bereits gelöscht oder noch nicht vollständig erstellt.`

Ursache

Übermäßiger E/A-Datenverkehr auf einer oder mehreren der virtuellen Maschinen in der Schutzgruppe sorgt dafür, dass es bei der Synchronisation zu einer Zeitüberschreitung kommt, bevor sie abgeschlossen wird. Dies kann auf einen hohen Datenverkehr zurückzuführen sein. So kann beispielsweise das Festlegen der Protokollierungsebene auf den Modus „Ausführlich (erweitert)“ für einen hohen E/A-Datenverkehr sorgen.

Lösung

1. Melden Sie sich beim Site Recovery Manager Server-Host an.
2. Öffnen Sie die Datei `vmware-dr.xml` in einem Texteditor.

   Sie finden die Datei `vmware-dr.xml` im Ordner `C:\Programme\VMware\VMware vCenter Site Recovery Manager\config`.
3. Fügen Sie ein Element des Typs `<topology><drTaskCleanupTime>` zur Datei `vmware-dr.xml` hinzu.

   Sie können das `<topology>`-Element an einer beliebigen Stelle der obersten Ebene der `<Config>`-Tags hinzufügen. Legen Sie den Wert von `<drTaskCleanupTime>` auf mindestens 300 Sekunden fest. Wenn Sie die Protokollierungsebene auf „Ausführlich (erweitert)“ festlegen, legen Sie `<drTaskCleanupTime>` auf 1000 Sekunden fest.

   ```
   <topology>
      <drTaskCleanupTime>1000</drTaskCleanupTime>
   </topology>
   ```
4. Speichern und schließen Sie die Datei `vmware-dr.xml`.
5. Starten Sie den Site Recovery Manager Server-Dienst neu, damit die neuen Einstellungen wirksam werden.

Fehlschlag des erneuten Schützens nach dem Neustart von vCenter Server

Nachdem Sie vCenter Server bei der Verwendung von vSphere Replication neu gestartet haben, schlagen die Vorgänge zum erneuten Schützen gelegentlich fehl.

Problem

Nachdem Sie vCenter Server bei der Verwendung von vSphere Replication neu gestartet haben, schlagen die Vorgänge zum erneuten Schützen mit dem folgenden Fehler fehl:

```
Fehler – Die Replizierung für die virtuelle Maschine
     'Virtuelle_Maschine' kann nicht umgekehrt werden. Die Sitzung wurde nicht authentifiziert.
```

Ursache

Nach dem Neustart von vCenter Server können einige Sitzungen nicht wiederhergestellt werden, die Site Recovery Manager verwendet, um mit vSphere Replication zu kommunizieren, und daher schlägt der erneute Schutz fehl.

Lösung

Starten Sie die Site Recovery Manager-Dienste auf beiden Sites neu.

Erneutes Prüfen von Datenspeichern schlägt fehl, da Speichergeräte nicht bereit sind

Wenn Sie eine Testwiederherstellung oder eine Wiederherstellung starten, senden einige SRAs Antworten an Site Recovery Manager, bevor ein heraufgestuftes Speichergerät auf der Wiederherstellungs-Site für die ESXi-Hosts verfügbar ist. Site Recovery Manager prüft die Speichergeräte erneut, und die Prüfung schlägt fehl.

Problem

Wenn die Speichergeräte noch nicht vollständig verfügbar sind, erkennt der ESXi-Server sie nicht und Site Recovery Manager findet die replizierten Geräte beim Durchführen der erneuten Prüfungen nicht. Das kann mehrere Probleme verursachen.

- Datenspeicher werden nicht erstellt und wiederhergestellte virtuelle Maschinen können nicht gefunden werden.
- ESXi-Hosts reagieren nicht mehr auf vCenter Server-Taktsignale und trennen die Verbindung zu vCenter Server. In diesem Fall sendet vCenter Server einen Fehler an Site Recovery Manager und eine Testwiederherstellung oder echte Wiederherstellung schlägt fehl.
- Der ESXi-Host ist verfügbar, aber erneutes Prüfen und das erneute Signieren von Festplatten überschreiten die angegebenen Zeitlimits in Site Recovery Manager oder vCenter Server, wodurch eine Site Recovery Manager-Fehlermeldung generiert wird.

Ursache

Die Speichergeräte sind nicht einsatzbereit, wenn Site Recovery Manager eine erneute Prüfung startet.

Lösung

Um den Start von erneuten Speicherprüfungen zu verzögern, bis die Speichergeräte auf den ESXi-Hosts einsatzbereit sind, erhöhen Sie die Einstellung `storageProvider.hostRescanDelaySec` auf einen Wert zwischen 20 und 180 Sekunden. Weitere Informationen hierzu finden Sie unter Ändern der Speicheranbietereinstellungen.

Hinweis In Site Recovery Manager 5.1 und älteren Versionen haben Sie möglicherweise den Parameter `storageProvider.hostRescanRepeatCnt` verwendet, um eine Verzögerung bei Wiederherstellungen festzulegen. Verwenden Sie stattdessen den Parameter `storageProvider.hostRescanDelaySec`.