

Verwalten von Site Recovery Manager

Site Recovery Manager 5.5



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	8
Aktualisierte Informationen	9
1 Site Recovery Manager -Rechte, -Rollen und -Berechtigungen	11
Wie Site Recovery Manager Berechtigungen handhabt	12
Site Recovery Manager und die vCenter Server -Administratorrolle	14
Site Recovery Manager - und vSphere Replication -Rollen	14
Verwalten von Berechtigungen in einer Konstellation mit gemeinsam genutzter Wiederherstellungs-Site	15
Zuweisen von Site Recovery Manager -Rollen und -Berechtigungen	17
Rollenreferenzen für Site Recovery Manager	20
vSphere Replication -Rollenreferenz	25
2 Replizieren von virtuellen Maschinen	28
Auswirkungen des RPO (Recovery Point Objective) auf die Replizierungsplanung	28
Replizieren einer virtuellen Maschine und Aktivieren mehrerer Zeitpunktinstanzen	29
Verwenden von vSphere Replication mit Virtual SAN Storage	30
Konfigurieren der Replizierung für eine einzelne virtuelle Maschine	33
Konfigurieren der Replizierung für mehrere virtuelle Maschinen	35
Replizieren virtueller Maschinen mithilfe von Replizierungsspeichern	38
Neukonfigurieren von Replizierungen	40
Beenden der Replizierung einer virtuellen Maschine	41
3 Erstellen von Schutzgruppen	42
Grundlegendes zu Array-basierten Schutzgruppen und Datenspeicherguppen	43
Wie Site Recovery Manager Datenspeicherguppen berechnet	44
Erstellen Array-basierter Schutzgruppen	45
Bearbeiten von Array-basierten Schutzgruppen	47
Erstellen von vSphere Replication -Schutzgruppen	47
Bearbeiten von vSphere Replication -Schutzgruppen	48
Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe	48
4 Erstellen, Testen und Ausführen von Wiederherstellungsplänen	50
Testen eines Wiederherstellungsplans	52
Test- und Datacenter-Netzwerke	52

Durchführen einer geplanten Migration oder einer Notfallwiederherstellung durch Ausführung eines Wiederherstellungsplans	53
Ausführen einer Wiederherstellung mit erzwungener Wiederherstellung	54
Unterschiede zwischen dem Test und der Ausführung eines Wiederherstellungsplans	55
So interagiert Site Recovery Manager während der Wiederherstellung mit DPM und DRS	56
So interagiert Site Recovery Manager mit Storage DRS oder Storage vMotion	57
Verwenden von Site Recovery Manager mit Array-basierter Replizierung auf Sites mit Storage DRS oder Storage vMotion	57
Verwenden von Site Recovery Manager mit vSphere Replication auf Sites mit Storage DRS oder Storage vMotion	58
Wie Site Recovery Manager mit vSphere High Availability interagiert	59
Schützen von Microsoft Cluster Server und fehlertoleranten virtuellen Maschinen	59
Erstellen, Testen und Ausführen eines Wiederherstellungsplans	61
Erstellen eines Wiederherstellungsplans	62
Bearbeiten eines Wiederherstellungsplans	63
Anhalten virtueller Maschinen, wenn ein Wiederherstellungsplan ausgeführt wird	63
Testen eines Wiederherstellungsplans	64
Bereinigen nach dem Testen eines Wiederherstellungsplans	65
Ausführen eines Wiederherstellungsplans	66
Wiederherstellen eines Point-in-Time-Snapshots einer virtuellen Maschine	67
Schritte zum Exportieren des Wiederherstellungsplans	68
Ansicht und Export des Verlaufs des Wiederherstellungsplans	68
Abbrechen eines Tests oder einer Wiederherstellung	69
Löschen eines Wiederherstellungsplans	69
5 Erneuter Schutz virtueller Maschinen nach einer Wiederherstellung	71
So führt Site Recovery Manager den erneuten Schutz durch	72
Vorbedingungen zum Durchführen des erneuten Schutzes	73
Erneutes Schützen virtueller Maschinen	74
Zustände beim erneuten Schutz	75
6 Wiederherstellen der ursprünglichen Konfiguration der Wiederherstellungs-Site durch Failback	76
Durchführen eines Failbacks	78
7 Konfigurieren eines Wiederherstellungsplans	80
Schritte für den Wiederherstellungsplan	81
Festlegen der Wiederherstellungspriorität einer virtuellen Maschine	82
Erstellen von benutzerdefinierten Wiederherstellungsschritten	82
Typen von benutzerdefinierten Wiederherstellungsschritten	84
Wie Site Recovery Manager mit Fehlschlägen bei benutzerdefinierten Wiederherstellungsschritten umgeht	85

Erstellen von Befehlsschritten der obersten Ebene	85
Erstellen von Meldungsaufforderungsschritten der obersten Ebene	86
Erstellen von Befehlsschritten für einzelne virtuelle Maschinen	87
Erstellen von Meldungsaufforderungsschritten für einzelne virtuelle Maschinen	87
Richtlinien zum Schreiben von Befehlsschritten	88
Umgebungsvariablen für Befehlsschritte	89
Anpassen der Wiederherstellung einer einzelnen virtuellen Maschine	90
8 Anpassen der IP-Eigenschaften für virtuelle Maschinen	91
Anpassen der IP-Eigenschaften für eine einzelne virtuelle Maschine	92
Melden von IP-Adresszuordnungen für Wiederherstellungspläne	94
Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen	95
Syntax des Tools „DR IP Customizer“	96
Struktur der DR IP Customizer-CSV-Datei	98
Ändern der CSV-Datei für DR IP Customizer	101
Ausführen von DR IP Customizer, um die IP-Eigenschaften für mehrere virtuelle Maschinen anzupassen	108
9 Erweiterte Site Recovery Manager -Konfiguration	110
Konfigurieren des Schutzes für eine virtuelle Maschine oder eine Vorlage	110
Konfigurieren der Ressourcenzuordnungen für eine virtuelle Maschine	112
Festlegen eines nicht replizierten Datenspeichers für Auslagerungsdateien	112
Wiederherstellen von virtuellen Maschinen über mehrere Hosts an der Wiederherstellungs-Site hinweg	113
Ändern der Größe von Festplattendateien virtueller Maschinen während einer Replizierung mithilfe von Replizierungsspeichern	114
Ändern der Größe von Festplattendateien virtueller Maschinen während einer Replizierung ohne die Verwendung von Replizierungsspeichern	115
Neukonfigurieren der Site Recovery Manager -Einstellungen	115
Ändern der Einstellungen der lokalen Site	116
Ändern der Protokollierungseinstellungen	117
Ändern von Wiederherstellungseinstellungen	119
Ändern der Einstellungen für Remote-Sites	121
Ändern der Zeitüberschreitung für das Erstellen von Platzhalter-VMs	121
Ändern der Speichereinstellungen	122
Ändern der Speicheranbietereinstellungen	122
Ändern der vSphere Replication -Einstellungen	125
Ändern der Einstellungen, um große Site Recovery Manager -Umgebungen auszuführen	126
10 Fehlerbehebung bei Site Recovery Manager	130
Einschränkungen beim Schutz und der Wiederherstellung von virtuellen Maschinen	130
Einschränkungen von vSphere Replication	134

Site Recovery Manager -Ereignisse und -Alarmer	135
So überwacht Site Recovery Manager die Verbindungen zwischen Sites	135
Konfigurieren von Site Recovery Manager -Alarmen	136
Site Recovery Manager -Ereignisreferenz	137
vSphere Replication -Ereignisse und -Alarmer	148
Konfigurieren der vSphere Replication -Alarmer	148
Liste mit vSphere Replication -Ereignissen	148
Erfassen von Site Recovery Manager -Protokolldateien	152
Sammeln von Site Recovery Manager -Protokolldateien über die Site Recovery Manager -Benutzeroberfläche	152
Manuelles Erfassen von Site Recovery Manager -Protokolldateien	153
Zugreifen auf die vSphere Replication -Protokolle	156
Manuelles Zugreifen auf die vSphere Replication -Protokolle	157
Beheben von Site Recovery Manager -Betriebsproblemen	157
Site Recovery Manager verdoppelt die Anzahl der umgekehrten Schrägstriche, wenn Callouts ausgeführt werden	157
Das Einschalten mehrerer virtueller Maschinen gleichzeitig auf der Wiederherstellungs-Site kann zu Fehlern führen	158
Die Einstellung LVM.enableResignature=1 bleibt nach einem Site Recovery Manager -Test-Failover bestehen	159
Hinzufügen von virtuellen Maschinen zu einer Schutzgruppe schlägt mit einem Fehler des Typs „Nicht aufgelöste Geräte“ fehl	160
Die Konfiguration des Schutzes schlägt mit einem Fehler bezüglich der Platzhaltererstellung fehl	161
Die geplante Migration schlägt aufgrund eines falschen Status des Hosts fehl	162
Wiederherstellung schlägt bei einigen virtuellen Maschinen während der Netzwerkanpassung mit einem Zeitüberschreitungsfehler fehl	162
Die Wiederherstellung schlägt mit dem Fehler „Host und Datenspeicher nicht verfügbar“ fehl	163
Erneutes Schützen schlägt mit einem vSphere Replication -Zeitüberschreitungsfehler fehl	164
Der Wiederherstellungsplan läuft während des Wartens auf VMware Tools ab	164
Fehlschlag des erneuten Schützens nach dem Neustart von vCenter Server	165
Erneutes Prüfen von Datenspeichern schlägt fehl, da Speichergeräte nicht bereit sind	165
Skalierbarkeitsprobleme beim Replizieren vieler virtueller Maschinen mit einem knappen RPO auf einen gemeinsam genutzten VMFS-Datenspeicher auf ESXi -Server 5.0	166
Anwendungsstilllegung ändert sich in Dateisystemstilllegung während der Verschiebung durch vMotion auf einen älteren Host	167
Neukonfigurieren der Replizierung auf virtuellen Maschinen ohne Datenspeicherzuordnung	168
Das Konfigurieren der Replizierung schlägt für virtuelle Maschinen mit zwei Festplatten auf unterschiedlichen Datenspeichern fehl	169
vSphere Replication - RPO-Verstöße	169
Kein Starten von vSphere Replication nach dem Verschieben des Hosts	170
Unerwarteter vSphere Replication -Fehler führt zu einem generischen Fehler	171

Das Generieren von Support-Paketen beeinträchtigt die Wiederherstellung von
vSphere Replication 172

Anfängliche vollständige Synchronisierung der Dateien virtueller Maschinen zum VMware Virtual SAN-Speicher ist langsam 173

vSphere Replication -Vorgänge werden bei ansteigender Anzahl an Replizierungen langsam
ausgeführt 173

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

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

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

Revision	Beschreibung
001112-07	<ul style="list-style-type: none">■ Funktion von <code>defaultMaxBootAndShutdownOpsPerCluster</code> und <code>defaultMaxBootAndShutdownOpsPerHost</code> 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<ul style="list-style-type: none">■ 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 Beschreibung der Einstellung <code>allowOtherSolutionTagInRecovery</code> wurde unter Ändern der vSphere Replication-Einstellungen aktualisiert.
001112-06	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.
001112-05	<ul style="list-style-type: none">■ Die Syntax des Tools „DR IP Reporter“ wurde unter Melden von IP-Adresszuordnungen für Wiederherstellungspläne korrigiert.■ 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.
001112-04	Unter Verwenden von vSphere Replication mit Virtual SAN Storage , Konfigurieren der Replizierung für eine einzelne virtuelle Maschine und Konfigurieren der Replizierung für mehrere virtuelle Maschinen wurde korrigierend ergänzt, dass die Verwendung von vSphere Replication mit Virtual SAN-Speicher sowohl auf den Quell- als auch auf den Ziel-Sites unterstützt wird.
001112-03	<ul style="list-style-type: none">■ Im Abschnitt Rollenreferenzen für Site Recovery Manager wurde erläutert, was bei Deinstallation von Site Recovery Manager mit Berechtigungen für Site Recovery Manager geschieht.■ Im Abschnitt Wie Site Recovery Manager mit Fehlschlägen bei benutzerdefinierten Wiederherstellungsschritten umgeht wurde erläutert, was beim Fehlschlagen von Schritten für Befehle pro virtueller Maschine geschieht.■ In den Abschnitten Wiederherstellungsereignisse und Speicher- und Speicheranbieter-Ereignisse wurden die Ereignisnamen korrigiert.

Revision	Beschreibung
001112-02	<ul style="list-style-type: none">■ Es wurden Ausführungen über die vollständige Unterstützung für VMware Virtual SAN in vSphere 5.5u1 und vSphere Replication 5.5.1 hinzugefügt.■ Es wurde in Replizieren einer virtuellen Maschine und Aktivieren mehrerer Zeitpunktinstanzen und Wiederherstellen eines Point-in-Time-Snapshots einer virtuellen Maschine hinzugefügt, dass Site Recovery Manager die IP-Anpassung nur für den neuesten Point-in-Time-Snapshot anwendet.■ Es wurden Abschnitte zu Grenzwerten und Point-in-Time-Snapshots zum Abschnitt Verwenden von vSphere Replication mit Virtual SAN Storage hinzugefügt.■ Es wurde in Konfigurieren der Replizierung für eine einzelne virtuelle Maschine und Konfigurieren der Replizierung für mehrere virtuelle Maschinen hinzugefügt, dass Sie den vSphere Web Client zum Konfigurieren von vSphere Replication für den Virtual SAN-Speicher verwenden müssen.■ Es wurden Empfehlungen zum Konfigurieren von vSphere Replication in Stapeln von 30 virtuellen Maschinen bei Verwendung des Virtual SAN-Speichers zum Abschnitt Konfigurieren der Replizierung für mehrere virtuelle Maschinen hinzugefügt.■ Es wurden Informationen zur E/A-Latenz bei Verwendung von vSphere Replication mit dem Virtual SAN-Speicher zum Abschnitt Testen eines Wiederherstellungsplans hinzugefügt.■ Beschreibungen der Befehls-Wiederherstellungsschritte unter Typen von benutzerdefinierten Wiederherstellungsschritten wurden verdeutlicht.■ Es wurden unter Ändern von Wiederherstellungseinstellungen die Einstellungen aufgelistet, die zu dem Zeitpunkt, zu dem Sie den Schutz konfigurieren, auf eine virtuelle Maschine angewendet werden.■ Es wurden neue erweiterte Einstellungen für Site Recovery Manager 5.5.1 zum Abschnitt Ändern der Speichereinstellungen hinzugefügt.
001112-01	Typen von benutzerdefinierten Wiederherstellungsschritten wurde um zusätzliche Informationen zu dem Benutzerkonto, in dem Befehlsschritte ausgeführt werden, ergänzt.
001112-00	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 und die vCenter Server-Administratorrolle**

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

- **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.

- **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 Kunde über ausreichende Berechtigungen zum Konfigurieren und Verwenden von Site Recovery Manager verfügt, aber kein Kunde Zugriff auf Ressourcen hat, die anderen Kunden gehören.

- **Zuweisen von Site Recovery Manager-Rollen und -Berechtigungen**

Während der Installation werden der vCenter Server-Administratorrolle Site Recovery Manager-Administratorrechte zugewiesen. Zu diesem Zeitpunkt können sich vCenter Server-Administratoren bei Site Recovery Manager anmelden, sofern sie nicht explizit anderen Benutzern Zugriff gewähren.

- **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.

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 zu teilen**. 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 vCenter Server-Administratorrolle auf einer vCenter Server-Instanz erhält während der Site Recovery Manager-Installation sämtliche Site Recovery Manager-Berechtigungen.

Site Recovery Manager führt nach der Installation keine Überprüfung von Rollen oder Berechtigungen durch. 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 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 Kunde über ausreichende Berechtigungen zum Konfigurieren und Verwenden von Site Recovery Manager verfügt, aber kein Kunde Zugriff auf Ressourcen hat, die anderen Kunden gehören.

Im Kontext einer gemeinsam genutzten Wiederherstellungs-Site ist ein Kunde der Besitzer eines Paares der Site Recovery Manager Server-Instanzen. Kunden 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 eine separate Benutzergruppe für jeden Kunden erstellen. Kunden-Benutzerkonten 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. Weitere Informationen zur Liste dieser Site Recovery Manager-Rollen, die auf dem Site Recovery Manager Server Befehle ausführen, finden Sie unter [Rollenreferenzen für Site Recovery Manager](#).

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 Kundenressourcen

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

- Alle Kunden müssen über Lesezugriff auf alle Ordner des vCenter Server auf der gemeinsam genutzten Wiederherstellungs-Site verfügen.
- Erteilen Sie einem Kunden nicht die Berechtigung, das Datacenter oder den Host umzubenennen, zu verschieben oder zu löschen.
- Erteilen Sie einem Kunden nicht die Berechtigung, virtuelle Maschinen außerhalb der Ordner, die für den Kunden reserviert sind, und der Ressourcenpools zu erstellen.
- Erteilen Sie einem Kunden nicht die Berechtigung, Rollen zu ändern oder Berechtigungen für Objekte zuzuweisen, die nicht für die eigene Verwendung des Kunden 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, Datacenter und Hosts des vCenter Server weiter.

Richtlinien zum Isolieren von Kundenressourcen

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

- Weisen Sie jedem Kunden einen separaten Ordner der virtuellen Maschine in der vCenter Server-Bestandsliste zu.
 - Legen Sie die Berechtigungen für diesen Ordner fest, um das Platzieren der virtuellen Maschinen anderer Kunden in diesen Ordner zu verhindern. Legen Sie beispielsweise die Administratorrolle fest und aktivieren Sie auf diesem Kunden-Ordner für einen Kunden die Option „Weitergeben“. Diese Konfiguration verhindert „Doppelter Name“-Fehler, die ansonsten möglicherweise auftreten, wenn mehrere Kunden virtuelle Maschinen schützen, die identische Namen haben.

- Platzieren Sie alle Platzhalter-VMs des Kunden in diesen Ordner, sodass sie seine Berechtigungen übernehmen können.
- Weisen Sie Zugriffsberechtigungen für diesen Ordner nicht anderen Kunden zu.
- Weisen Sie allen Kunden dedizierte Ressourcenpools, Datenspeicher und Netzwerke zu und konfigurieren Sie Berechtigungen auf dieselbe Weise wie für Ordner.

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 Kunden können alle Aufgaben sehen, die andere Benutzer auf einer freigegebenen Ressource durchführen. Alle Benutzer können beispielsweise die Aufgaben sehen, die auf einem freigegebenen Host, Datacenter 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 werden der vCenter Server-Administratorrolle Site Recovery Manager-Administratorrechte zugewiesen. Zu diesem Zeitpunkt können sich 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 in der Site Recovery Manager-Benutzeroberfläche Berechtigungen gewähren. Die Zuweisung von Berechtigungen erfolgt pro Site. 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-Clients. Sie können nach dem Verbinden der Schutz- und Wiederherstellungs-Sites die Site Recovery Manager-Berechtigungen über die gleiche Benutzeroberfläche auf beiden Sites 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](#).

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, und wählen Sie die Site aus, auf der Berechtigungen zugewiesen werden sollen.
- 2 Klicken Sie auf die Registerkarte **Berechtigungen**.
- 3 Klicken Sie mit der rechten Maustaste an einer beliebigen Stelle im Bereich für die lokalen bzw. Remote-Sites und wählen Sie **Berechtigung hinzufügen**.
- 4 Klicken Sie auf **Hinzufügen**.
- 5 Identifizieren Sie einen Benutzer oder eine Gruppe für die Rolle.
 - a Wählen Sie im Dropdown-Menü **Domäne** die Domäne aus, die den Benutzer oder die Gruppe enthält.
 - b Geben Sie einen Benutzer- oder Benutzergruppennamen im Textfeld **Suchen** ein, oder wählen Sie in der Liste **Name** einen Namen aus.
 - c Klicken Sie auf **Hinzufügen** und anschließend auf **OK**.
- 6 Wählen Sie im Dropdown-Menü **Zugewiesene Rolle** eine Rolle aus, um sie dem ausgewählten Benutzer bzw. der 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 Site Recovery Manager-Administratorrolle zu.
Genehmigt einem Benutzer oder einer Benutzergruppe die Verwaltung und Modifizierung von Schutzgruppen und die Schutzkonfiguration auf virtuellen Maschinen.	Weist die Administratorrolle für Site Recovery Manager-Schutzgruppen zu.
Genehmigt einem Benutzer oder einer Benutzergruppe die Durchführung und das Testen von Wiederherstellungen.	Weist die Administratorrolle für Site Recovery Manager-Wiederherstellungen zu.

Option	Aktion
Genehmigt einem Benutzer oder einer Benutzergruppe das Erstellen, Modifizieren und Testen von Wiederherstellungsplänen.	Weist die Administratorrolle für Site Recovery Manager-Wiederherstellungspläne zu.
Genehmigt einem Benutzer oder einer Benutzergruppe das Testen von Wiederherstellungsplänen.	Weist die Administratorrolle für Site Recovery Manager-Wiederherstellungstests 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.

- 7 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.

- 8 Klicken Sie auf **OK**, um die Rolle und deren zugehörige Berechtigungen dem Benutzer oder der Benutzergruppe zuzuweisen.
- 9 Wiederholen Sie [Schritt 1](#) bis [Schritt 8](#), 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 Administratorrolle für Site Recovery Manager-Wiederherstellungspläne zu.

- 3 Weisen Sie der anderen Gruppe die Administratorrolle für Site Recovery Manager-Wiederherstellungen zu.
- 4 Nehmen Sie den Benutzer in beide Gruppen auf.

Da er Mitglied von Gruppen ist, in denen beide Administratorrollen sowohl für Site Recovery Manager-Wiederherstellungspläne als auch für Site Recovery Manager-Wiederherstellungen vorhanden sind, kann der Benutzer 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	<p>Der Site Recovery Manager-Administrator gewährt die Berechtigung zur Durchführung aller Site Recovery Manager-Konfigurations- und -Verwaltungsvorgänge.</p> <ul style="list-style-type: none"> ■ 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. <p>Benutzer mit dieser Rolle können keine Wiederherstellungen ausführen. Wiederherstellungen können ausschließlich von Benutzern mit der Administratorrolle für Site Recovery Manager-Wiederherstellungen ausgeführt werden.</p>	<p>Site Recovery Manager.Erweiterte Einstellungen.Ändern</p> <p>Site Recovery Manager.Array-Manager.Konfigurieren</p> <p>Site Recovery Manager.Diagnose.Export</p> <p>Site Recovery Manager.Bestandslistenvoreinstellungen.Ändern</p> <p>Site Recovery Manager.Platzhalterdatenspeicher.Konfigurieren</p> <p>Site Recovery Manager.DiagnoseExport</p> <p>Site Recovery Manager.Schutzgruppe.Einem Plan zuweisen</p> <p>Site Recovery Manager.Schutzgruppe.Erstellen</p> <p>Site Recovery Manager.Schutzgruppe.Ändern</p> <p>Site Recovery Manager.Schutzgruppe.Entfernen</p> <p>Site Recovery Manager.Schutzgruppe.Aus Plan entfernen</p> <p>Site Recovery Manager.Wiederherstellungsverlauf.Gelöschte Pläne anzeigen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Konfigurieren</p> <p>Site Recovery Manager.Wiederherstellungsplan.Erstellen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Ändern</p> <p>Site Recovery Manager.Wiederherstellungsplan.Entfernen</p>	<ul style="list-style-type: none"> ■ 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
		<p>Site Recovery Manager.Wiederherstellungsplan.Neu schützen</p> <p>Site Recovery Manager.Wiederherstellungsplan .Testen</p> <p>Site Recovery Manager.Remote-Site.Ändern</p> <p>Datenspeicher.Replizierung.Schützen</p> <p>Datenspeicher.Replizierung.Schutz aufheben</p> <p>Ressource.Verwendung der Wiederherstellung</p> <p>Virtuelle Maschine.SRM-Schutz.Schützen</p> <p>Virtuelle Maschine.SRM-Schutz.Beenden</p>	
<p>Administrator für Site Recovery Manager-Schutzgruppen</p>	<p>Mit der Administratorrolle für Site Recovery Manager-Schutzgruppen können Benutzer Schutzgruppen verwalten.</p> <ul style="list-style-type: none"> ■ 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. <p>Benutzer mit dieser Rolle können weder Wiederherstellungen durchführen oder testen noch Wiederherstellungspläne erstellen oder ändern.</p>	<p>Site Recovery Manager.Schutzgruppe.Erstellen</p> <p>Site Recovery Manager.Schutzgruppe.Ändern</p> <p>Site Recovery Manager.Schutzgruppe.Entfernen</p> <p>Datenspeicher.Replizierung.Schützen</p> <p>Datenspeicher.Replizierung.Schutz aufheben</p> <p>Ressource.Verwendung der Wiederherstellung</p> <p>Virtuelle Maschine.SRM-Schutz.Schützen</p> <p>Virtuelle Maschine.SRM-Schutz.Beenden</p>	<ul style="list-style-type: none"> ■ 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	<p>Die Administratorrolle für Site Recovery Manager-Wiederherstellungen ermöglicht Benutzern die Durchführung von Wiederherstellungen und Vorgängen zum erneuten Schützen.</p> <ul style="list-style-type: none"> ■ 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. <p>Benutzer mit dieser Rolle können weder den Schutz auf virtuellen Maschinen konfigurieren noch Wiederherstellungspläne erstellen oder ändern.</p>	<p>Site Recovery Manager.Schutzgruppe.Aus Plan entfernen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Ändern</p> <p>Site Recovery Manager.Wiederherstellungsplan .Testen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Wiederherstellen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Neu schützen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Befehle konfigurieren</p> <p>Site Recovery Manager.Wiederherstellungsverlauf.Gelöschte Pläne anzeigen</p>	<ul style="list-style-type: none"> ■ 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	<p>Die Administratorrolle für Site Recovery Manager-Wiederherstellungspläne ermöglicht Benutzern das Erstellen und Testen von Wiederherstellungsplänen.</p> <ul style="list-style-type: none"> ■ Schutzgruppen zu Wiederherstellungsplänen hinzufügen. ■ Schutzgruppen aus Wiederherstellungsplänen entfernen. ■ Benutzerdefinierte Befehlschritte auf virtuellen Maschinen konfigurieren. ■ Erstellen von Wiederherstellungsplänen. ■ Wiederherstellungspläne testen. ■ Tests von Wiederherstellungsplänen abbrechen. ■ Wiederherstellungseigenschaften von virtuellen Maschinen bearbeiten. <p>Benutzer mit dieser Rolle können weder den Schutz auf virtuellen Maschinen konfigurieren noch Wiederherstellungen oder Vorgänge zum erneuten Schützen durchführen.</p>	<p>Site Recovery Manager.Schutzgruppe.Einem Plan zuweisen</p> <p>Site Recovery Manager.Schutzgruppe.Aus Plan entfernen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Befehle konfigurieren</p> <p>Site Recovery Manager.Wiederherstellungsplan.Erstellen</p> <p>Site Recovery Manager.Wiederherstellungsplan.Ändern</p> <p>Site Recovery Manager.Wiederherstellungsplan.Entfernen</p> <p>Site Recovery Manager.Wiederherstellungsplan .Testen</p> <p>Ressource.Verwendung der Wiederherstellung</p>	<ul style="list-style-type: none"> ■ Schutzgruppen ■ Wiederherstellungspläne ■ vCenter Server-Ordner ■ Datenspeicher ■ Ressourcenpools ■ Netzwerke
Administrator für Site Recovery Manager-Tests	<p>Die Administratorrolle für Site Recovery Manager-Tests ermöglicht Benutzern lediglich das Testen von Wiederherstellungsplänen.</p> <ul style="list-style-type: none"> ■ Wiederherstellungspläne testen. ■ Tests von Wiederherstellungsplänen abbrechen. ■ Wiederherstellungseigenschaften von virtuellen Maschinen bearbeiten. <p>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.</p>	<p>Site Recovery Manager.Wiederherstellungsplan.Ändern</p> <p>Site Recovery Manager.Wiederherstellungsplan .Testen</p>	Wiederherstellungspläne

vSphere Replication -Rollenreferenz

vSphere Replication enthält mehrere Rollen. Jede Rolle enthält mehrere Rechte, damit die Benutzer mit diesen Rollen verschiedene Aktionen ausführen können.

Hinweis Wenn Sie Berechtigungen ohne Weitergabe zuweisen, stellen Sie sicher, dass Sie mindestens über die Berechtigung „Nur Lesen“ für alle übergeordneten Objekte verfügen.

Tabelle 1-2. vSphere Replication -Rollen

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
VRM-Replizierungsansicht	<ul style="list-style-type: none"> ■ Replizierungen anzeigen. ■ Replizierungsparameter können nicht geändert werden. 	<p>VRM remote.VR anzeigen</p> <p>VRM remote.VRM anzeigen</p> <p>VRM-Datenspeicher-Mapper.Anzeigen</p> <p>Host.vSphere Replication.Replizierung verwalten</p> <p>Virtuelle Maschine.vSphere Replication.Replizierung überwachen</p>	<p>vCenter Server-Root-Ordner mit Weitergabe an der Quell-Site (ausgehende Replizierungen) und der Ziel-Site (eingehende Replizierungen).</p> <p>Alternativ vCenter Server-Root-Ordner ohne Weitergabe an beiden Sites und virtuelle Maschine ohne Weitergabe an der Quell-Site.</p>
VRM-VM-Replizierungsbenutzer	<ul style="list-style-type: none"> ■ Replizierungen anzeigen. ■ Datenspeicher verwalten. ■ Replizierungen konfigurieren und die Konfigurierung aufheben. ■ Replizierungen verwalten und überwachen. <p>Erfordert einen entsprechenden Benutzer mit der gleichen Rolle auf der Ziel-Site und außerdem die vSphere Replication-Zieldatenspeicher-Benutzerrolle im Zieldatencenter, im Datenspeicherordner oder in jedem Zieldatenspeicher.</p>	<p>Datenspeicher.Datenspeicher durchsuchen</p> <p>VRM remote.VR anzeigen</p> <p>VRM remote.VRM anzeigen</p> <p>VRM-Datenspeicher-Mapper.Verwalten</p> <p>VRM-Datenspeicher-Mapper.Anzeigen</p> <p>Host.vSphere Replication.Replizierung verwalten</p> <p>Virtuelle Maschine.vSphere Replication.Replizierung konfigurieren</p> <p>Virtuelle Maschine.vSphere Replication.Replizierung verwalten</p> <p>Virtuelle Maschine.vSphere Replication.Replizierung überwachen</p>	<p>vCenter Server-Root-Ordner mit Weitergabe an beiden Sites.</p> <p>Alternativ vCenter Server-Root-Ordner ohne Weitergabe an beiden Sites, virtuelle Maschine ohne Weitergabe an der Quell-Site, Quelldatenspeicher ohne Weitergabe an der Quell-Site.</p>

Tabelle 1-2. vSphere Replication -Rollen (Fortsetzung)

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
VRM-Administrator	Schließt alle vSphere Replication-Rechte ein.	VRM remote.VR verwalten VRM remote.VR anzeigen VRM remote.VRM verwalten VRM remote.VRM anzeigen VRM-Datenspeicher-Mapper.Verwalten VRM-Datenspeicher-Mapper.Anzeigen VRM-Diagnose.Verwalten VRM-Sitzung.Beenden Datenspeicher.Datenspeicher durchsuchen Datenspeicher.Dateivorgänge auf niedriger Ebene Host.vSphere Replication.Replizierung verwalten Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen Virtuelle Maschine.Konfiguration.Vorhandene Festplatte hinzufügen Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen Virtuelle Maschine.Interaktion.Einschalten Virtuelle Maschine.Interaktion.Geräteverbindung Virtuelle Maschine.Bestandsliste.Registrieren Virtuelle Maschine.vSphere Replication.Replizierung konfigurieren Virtuelle Maschine.vSphere Replication.Replizierung verwalten Virtuelle Maschine.vSphere Replication.Replizierung überwachen	vCenter Server-Root-Ordner mit Weitergabe an beiden Sites. Alternativ vCenter Server-Root-Ordner ohne Weitergabe an beiden Sites, virtuelle Maschine ohne Weitergabe an der Quell-Site, Zieldatenspeicher, Ordner der virtuellen Zielmaschine mit Weitergabe an der Ziel-Site, Zielhost oder -cluster mit Weitergabe an der Ziel-Site.
VRM-Diagnose	Protokollpakete generieren, abrufen und löschen.	VRM remote.VR anzeigen VRM remote.VRM anzeigen VRM-Diagnose.Verwalten	vCenter Server-Root-Ordner an beiden Sites.

Tabelle 1-2. vSphere Replication -Rollen (Fortsetzung)

Rolle	Mit dieser Rolle zulässige Aktionen	In dieser Rolle enthaltene Berechtigungen	Objekte im vCenter Server-Bestand, auf die diese Rolle Zugriff hat
VRM-Zieldatenspeicherbenutzer	<p>Replizierungen konfigurieren und neu konfigurieren.</p> <p>Wird auf der Ziel-Site in Kombination mit der VRM-VM-Replizierungsbenutzerrolle an beiden Sites verwendet.</p>	<p>Datenspeicher.Datenspeicher durchsuchen</p> <p>Datenspeicher.Dateivorgänge auf niedriger Ebene</p>	Datenspeicherobjekte an der Ziel-Site oder Datenspeicherordner mit Weitergabe an der Ziel-Site oder Zieldatencenter mit Weitergabe.
VRM-VM-Wiederherstellungsbenu- tzer	Wiederherstellen virtueller Maschinen.	<p>Datenspeicher.Datenspeicher durchsuchen</p> <p>Datenspeicher.Dateivorgänge auf niedriger Ebene</p> <p>Host.vSphere Replication.Replizierung verwalten</p> <p>Virtuelle Maschine.Konfiguration.Vorhandene Festplatte hinzufügen</p> <p>Virtuelle Maschine.Konfiguration.Gerät hinzufügen oder entfernen</p> <p>Virtuelle Maschine.Interaktion.Einschalten</p> <p>Virtuelle Maschine.Interaktion.Geräteverbindung</p> <p>Virtuelle Maschine.Bestandsliste.Registrieren</p> <p>Ressource.Virtuelle Maschine zu Ressourcenpool zuweisen</p>	<p>Sekundärer vCenter Server-Root-Ordner mit Weitergabe.</p> <p>Alternativ sekundärer vCenter Server-Root-Ordner ohne Weitergabe, Zieldatenspeicher ohne Weitergabe, Ordner der virtuellen Zielmaschine mit Weitergabe, Zielhost oder -cluster mit Weitergabe.</p>

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.

Diese Informationen betreffen die Replizierung unter Verwendung von vSphere Replication. Um die Array-basierte Replizierung auf virtuellen Maschinen zu konfigurieren, lesen Sie die Dokumentation des Anbieters Ihres Speicher-Array-Managers (SRA).

Dieses Kapitel behandelt die folgenden Themen:

- [Auswirkungen des RPO \(Recovery Point Objective\) auf die Replizierungsplanung](#)
- [Replizieren einer virtuellen Maschine und Aktivieren mehrerer Zeitpunktinstanzen](#)
- [Verwenden von vSphere Replication mit Virtual SAN Storage](#)
- [Konfigurieren der Replizierung für eine einzelne virtuelle Maschine](#)
- [Konfigurieren der Replizierung für mehrere virtuelle Maschinen](#)
- [Replizieren virtueller Maschinen mithilfe von Replizierungsspeichern](#)
- [Neukonfigurieren von Replizierungen](#)
- [Beenden der Replizierung einer virtuellen Maschine](#)

Auswirkungen des RPO (Recovery Point Objective) auf die Replizierungsplanung

Der Wert für das RPO (Recovery Point Objective), den Sie während der Konfiguration der Replizierung festlegen, wirkt sich auf die Replizierungsplanung aus.

Wenn Sie ein RPO von x Minuten einstellen, kann die neueste verfügbare Replizierungsinstanz keinen Zustand widerspiegeln, der mehr als x Minuten alt ist. Eine Replizierungsinstanz spiegelt den Zustand einer virtuellen Maschine zum Zeitpunkt des Beginns der Replizierung wider.

Sie legen das RPO während der Replizierungskonfiguration auf 15 Minuten fest. Wenn die Replizierung um 12 Uhr beginnt und die Übertragung auf die Ziel-Site fünf Minuten dauert, steht die Instanz auf der Ziel-Site um 12.05 Uhr zur Verfügung, spiegelt jedoch den Zustand der virtuellen Maschine von 12 Uhr wider. Die nächste Replizierung kann nicht später als 12.10 Uhr starten. Diese Replizierungsinstanz steht dann um 12.15 Uhr zur Verfügung, wenn die erste Replizierungsinstanz (mit Beginn um 12 Uhr) abläuft.

Wenn Sie das RPO auf 15 Minuten festlegen und die Replizierung 7:30 Minuten braucht, um eine Instanz zu übertragen, überträgt vSphere Replication stets eine Instanz. Falls die Replizierung mehr als 7:30 Minuten benötigt, treten bei der Replizierung regelmäßig RPO-Verstöße auf. Wenn die Replizierung beispielsweise um 12:00 Uhr beginnt und es 10 Minuten dauert, um eine Instanz zu übertragen, wird die Replizierung um 12:10 Uhr beendet. Sie können eine weitere umgehend starten, aber diese wird um 12:20 Uhr beendet. Während der Zeit von 12:15 - 12:20 Uhr tritt ein RPO-Verstoß auf, weil die neueste verfügbare Instanz um 12:00 Uhr gestartet wurde und somit zu alt ist.

Der Replizierungs-Scheduler versucht, durch Überlappen von Replizierungen diese Einschränkungen zu berücksichtigen, indem er die Nutzung der Bandbreite optimiert, und startet möglicherweise Replizierungen für einige virtuellen Maschinen früher als erwartet.

Zum Ermitteln der Übertragungszeit bei der Replizierung greift der Replizierungs-Scheduler auf die Dauern der letzten Instanzen zurück, um die Dauer der nächsten Übertragung abzuschätzen.

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.

Hinweis Sie können mit der Site Recovery Manager-Benutzeroberfläche keine Replizierungen konfigurieren, die Point-in-Time-Snapshots (PIT) verwenden. Um PIT-Snapshots zu aktivieren, konfigurieren Sie Replizierungen einer virtuellen Maschine anhand von vSphere Web Client. Siehe [Konfigurieren der Replizierung für eine einzelne virtuelle Maschine](#) unter *Verwaltung von vSphere Replication*.

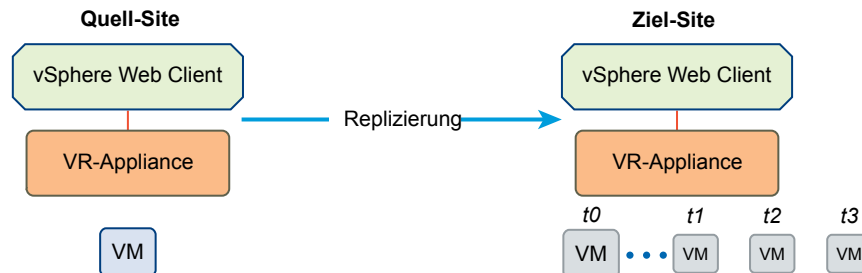
Wenn Sie die Replizierung einer virtuellen Maschine konfigurieren, können Sie in den Wiederherstellungseinstellungen des Assistenten „Replizierung konfigurieren“ mehrere Zeitpunktinstanzen aktivieren. vSphere Replication behält eine Reihe von Snapshot-Instanzen der virtuellen Maschine auf der Ziel-Site 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 den letzten bekannten guten Zustand einer Datenbank auch unter Verwendung der Zeitpunk-
tinstanzen wiederherstellen.

Hinweis vSphere Replication repliziert keine VM-Snapshots.

Abbildung 2-1. 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-Benutzer-
oberfläche 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 vSphere Replication mit Virtual SAN Storage

Sie können beim Konfigurieren von Replizierungen VMware Virtual SAN-Datenspeicher als Quell- und Zieldatenspeicher verwenden. Folgen Sie den Richtlinien beim Verwenden von vSphere Replication mit Virtual SAN-Speicher.

Hinweis VMware Virtual SAN ist eine vollständig unterstützte Funktion von vSphere 5.5u1.

- Sie können Virtual SAN in Produktionsumgebungen mit vSphere Replication 5.5.1 und vSphere 5.5u1 verwenden.
- Virtual SAN ist eine experimentelle Funktion in vSphere 5.5. Sie können Tests mit Virtual SAN in vSphere Replication 5.5.0 und vSphere 5.5 durchführen, die Verwendung der Funktion in Produktionsumgebungen wird jedoch nicht unterstützt. In den Versionshinweisen zu vSphere Replication 5.5.0 finden Sie Informationen zur Aktivierung von Virtual SAN in vSphere 5.5.

vSphere Replication unterstützt nicht das Replizieren oder Wiederherstellen virtueller Maschinen in Root-Ordern mit benutzerfreundlichen Namen auf Virtual SAN-Datenspeichern. Diese Namen können sich ändern, was zu Replizierungsfehlern führt. Wählen Sie bei der Auswahl von Virtual SAN-Datenspeichern stets Ordner mit UUID-Namen aus, die sich nicht ändern.

Konfigurieren von Replizierungen

Beim Konfigurieren von Replizierungen für eine einzelne virtuelle Maschine erstellt vSphere Replication den von Ihnen ausgewählten Zielordner, ruft die UUID-Referenz für diesen Ordner ab und verwendet anschließend den UUID-Namen anstelle des benutzerfreundlichen Namens. Der UUID-Name ist sichtbar, wenn vSphere Replication beim Neukonfigurieren von Replizierungen die Zielordner anzeigt.

Wenn Sie die Replizierung für mehrere virtuelle Maschinen konfigurieren, erstellen Sie einen Root-Ordner im Datenspeicher für Virtual SAN, rufen Sie dessen UUID-Namen ab und verwenden Sie den Ordner, der von der UUID im Replizierungsassistenten identifiziert wird.

Konfigurieren Sie vSphere Replication auf Gruppen von maximal 30 virtuellen Maschinen gleichzeitig.

Konfigurieren von Replizierungen mithilfe von Replizierungsspeichern

Beim Kopieren von Replizierungsspeicherdateien in den Zieldatenspeicher können Sie den vSphere Web Client zum Erstellen eines neuen Root-Ordners auf einem Datenspeicher für Virtual SAN verwenden oder Sie können die Dateien in einem vorhandenen Ordner speichern. Wenn Sie Replizierungen konfigurieren, die Replizierungsspeicher verwenden, müssen Sie den Ordner anhand seines UUID-Namens auswählen. Die Auswahl von benutzerfreundlichen Ordernamen wird nicht unterstützt.

Neukonfigurieren von Replizierungen

Wenn Sie den Zielordner für eine Festplatte oder die VM-Konfigurationsdateien ändern möchten, müssen Sie die folgenden Optionen verwenden:

- Wählen Sie den UUID-Namen eines vorhandenen Ordners aus.
- Lassen Sie vSphere Replication einen neuen Ordner erstellen und dessen UUID-Namen abrufen.

Einschränkungen bei der Verwendung von vSphere Replication mit Virtual SAN-Speicher

Aus Gründen der Last und E/A-Latenz gelten für den Virtual SAN-Speicher Einschränkungen hinsichtlich der Anzahl von Hosts, die Sie in einem Virtual SAN-Cluster hinzufügen können, und der Anzahl von virtuellen Maschinen, die Sie auf jedem Host ausführen können. Weitere Informationen finden Sie im Abschnitt „Einschränkungen“ im *Handbuch für VMware Virtual SAN Design und Sizing* unter <http://www.vmware.com/products/virtual-san/resources.html>.

Durch das Verwenden von vSphere Replication wird die Last auf dem Speicher erhöht. Jede virtuelle Maschine generiert reguläre Lese- oder Schreibvorgänge. Beim Konfigurieren von vSphere Replication auf den virtuellen Maschinen wird ein weiterer Lesevorgang zu den regulären Lese- oder Schreibvorgängen hinzugefügt, wodurch die E/A-Latenz auf dem Speicher erhöht wird. Die genaue Anzahl der virtuellen Ma-

schinen, die Sie unter Verwendung von vSphere Replication auf den Virtual SAN-Speicher replizieren können, hängt von Ihrer Infrastruktur ab. Wenn die Reaktionszeiten langsamer werden, während Sie vSphere Replication für virtuelle Maschinen im Virtual SAN-Speicher konfigurieren, überwachen Sie die E/A-Latenz der Virtual SAN-Infrastruktur. Reduzieren Sie möglicherweise die Anzahl der virtuellen Maschinen, die Sie im Virtual SAN-Datenspeicher replizieren können.

Beibehalten der Point-in-Time-Snapshots bei der Verwendung des Virtual SAN-Speichers

Der Virtual SAN-Speicher speichert Festplattendateien virtueller Maschinen als Satz von Objekten und Komponenten. Jedes Festplattenobjekt in einem Virtual SAN-Speicher enthält Spiegel- und Zeugen-Objekte. In der Standardrichtlinie des Virtual SAN-Speichers enthält ein Festplattenobjekt zwei Spiegel und einen Zeugen. Die Anzahl der Spiegel-Komponenten wird durch die Größe der Festplatte der virtuellen Maschine und durch die Anzahl der zulässigen Fehler bestimmt, die Sie in Ihrer Richtlinie des Virtual SAN-Speichers festlegen. Ein Spiegel-Objekt ist in Komponenten mit einer maximalen Größe von jeweils 256 GB unterteilt.

- Wenn eine virtuelle Maschine eine 256-GB-Festplatte enthält und Sie die Standardrichtlinie des Virtual SAN-Speichers verwenden, enthält das Festplattenobjekt zwei Spiegel-Komponenten mit jeweils 256 GB und einen Zeugen, d. h. insgesamt drei Komponenten.
- Wenn eine virtuelle Maschine eine 512-GB-Festplatte enthält und Sie die Standardrichtlinie des Virtual SAN-Speichers verwenden, enthält das Festplattenobjekt vier Spiegel-Komponenten mit jeweils 256 GB und einen Zeugen, d. h. insgesamt fünf Komponenten.

Weitere Informationen zu Objekten, Komponenten, Spiegeln, Zeugen und Richtlinien des Virtual SAN-Speichers finden Sie im *Handbuch für VMware Virtual SAN Design und Sizing* unter <http://www.vmware.com/products/virtual-san/resources.html>.

Wenn Sie mehrere Point-in-Time-Snapshots (PIT) aktivieren, müssen Sie Zuteilungen für zusätzliche Komponenten durchführen, die jeder Snapshot im Virtual SAN-Speicher erstellt, basierend auf der Anzahl der Festplatten pro virtueller Maschine, der Größe der Festplatten, der Anzahl der beizubehaltenden PIT-Snapshots und der Anzahl der zulässigen Fehler. Beim Beibehalten von PIT-Snapshots und Verwenden des Virtual SAN-Speichers müssen Sie die Anzahl der zusätzlichen Komponenten berechnen, die Sie für jede virtuelle Maschine benötigen:

Anzahl der Festplatten x Anzahl der PIT-Snapshots x Anzahl der Spiegel- und Zeugen-Komponenten

Beispiele für die Verwendung dieser Formel zeigen, dass durch das Beibehalten von PIT-Snapshots die Anzahl von Komponenten im Virtual SAN-Speicher für jede virtuelle Maschine schnell steigt, die Sie für vSphere Replication konfigurieren:

- Sie verfügen über eine virtuelle Maschine mit zwei 256-GB-Festplatten, für die Sie 10 MPIT-Snapshots beibehalten, und setzen die Standardrichtlinie des Virtual SAN-Speichers fest:
 - 2 (Anzahl der Festplatten) \times 10 (Anzahl der PIT-Snapshots) \times 3 (2 Spiegel-Komponenten + 1 Zeuge) = 60 Komponenten für diese virtuelle Maschine.

- Sie verfügen über eine virtuelle Maschine mit zwei 512-GB-Festplatten, für die Sie 10 PIT-Snapshots beibehalten, und setzen die Standardrichtlinie des Virtual SAN-Speichers fest:
 - 2 (Anzahl der Festplatten) \times 10 (Anzahl der PIT-Snapshots) \times 5 (4 Spiegel-Komponenten mit jeweils 256 GB + 1 Zeuge) = 100 Komponenten für diese virtuelle Maschine.

Die Anzahl der PIT-Snapshots, die Sie beibehalten, kann die E/A-Latenz auf dem Virtual SAN-Speicher erhöhen.

Konfigurieren der Replizierung für eine einzelne virtuelle Maschine

vSphere Replication kann einzelne virtuelle Maschinen und ihre virtuellen Festplatten schützen, indem es sie an einen anderen Speicherort repliziert.

Wenn Sie die Replizierung konfigurieren, legen Sie ein RPO (Recovery Point Objective) fest, um den Zeitraum zwischen Replizierungen festzulegen. Ein RPO von 1 Stunde soll z. B. sicherstellen, dass eine virtuelle Maschine während der Wiederherstellung nicht mehr als eine Stunde an Daten verliert. Bei kleineren RPO-Werten gehen weniger Daten bei einer Wiederherstellung verloren, jedoch wird mehr Netzwerkbandbreite belegt, um das Replikat aktuell zu halten.

Jedes Mal, wenn eine virtuelle Maschine ihr RPO-Ziel erreicht, protokolliert vSphere Replication etwa 3800 Bytes an Daten in der Datenbank für vCenter Server-Ereignisse. Wenn Sie einen kurzen RPO-Zeitraum festlegen, kann dies schnell zu einem hohen Datenvolumen in der Datenbank führen. Um zu vermeiden, dass die Datenbank für vCenter Server-Ereignisse zu groß wird, begrenzen Sie die Anzahl der Tage, die vCenter Server Ereignisdaten aufbewahrt. Weitere Informationen finden Sie unter „Konfigurieren einer Datenbankaufbewahrungsrichtlinie“ im *Handbuch für vCenter Server und Hostverwaltung*. Alternativ dazu können Sie einen höheren RPO-Wert festlegen.

Hinweis Sie können mit der Site Recovery Manager-Benutzeroberfläche keine Replizierungen konfigurieren, die Point-in-Time-Snapshots (PIT) verwenden. Um PIT-Snapshots zu aktivieren, konfigurieren Sie Replizierungen einer virtuellen Maschine anhand von vSphere Web Client. Siehe [Konfigurieren der Replizierung für eine einzelne virtuelle Maschine](#) unter *Verwaltung von vSphere Replication*.

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](#).

vSphere Replication garantiert Absturzkonsistenz unter allen Festplatten, die zu einer virtuellen Maschine gehören. Wenn Sie die Stilllegung mit VSS verwenden, können Sie möglicherweise eine höhere Konsistenzstufe erzielen. Die verfügbaren Typen für das Stilllegen werden durch das Betriebssystem der virtuellen Maschine festgelegt. Weitere Informationen darüber, wie der Microsoft Volume Shadow Copy Service (VSS) das Stilllegen von virtuellen Windows-Maschinen unterstützt, finden Sie unter [Kompatibilitätstabellen für vSphere Replication 5.5](#).

Sie können vSphere Replication mit einem Virtual SAN-Datenspeicher auf den Quell- und Ziel-Sites verwenden. Sie müssen bei der Replizierung in den Virtual SAN-Speicher jedoch den vSphere Web Client verwenden, um vSphere Replication zu konfigurieren. Der Site Recovery Manager-Client lässt beim Auswählen des Zieldatenspeichers keine Auswahl eines virtuellen SAN-Speichers zu.

Hinweis VMware Virtual SAN ist eine vollständig unterstützte Funktion von vSphere 5.5u1.

- Sie können Virtual SAN in Produktionsumgebungen mit vSphere Replication 5.5.1 und vSphere 5.5u1 verwenden.
 - Virtual SAN ist eine experimentelle Funktion in vSphere 5.5. Sie können Tests mit Virtual SAN in vSphere Replication 5.5.0 und vSphere 5.5 durchführen, die Verwendung der Funktion in Produktionsumgebungen wird jedoch nicht unterstützt. In den Versionshinweisen zu vSphere Replication 5.5.0 finden Sie Informationen zur Aktivierung von Virtual SAN in vSphere 5.5.
-

Voraussetzungen

Vergewissern Sie sich, dass Sie vSphere Replication-Appliances und die Site Recovery Manager Server-Instanzen auf jeder Site bereitgestellt und verbunden haben.

Vorgehensweise

- 1 Klicken Sie auf der Startseite des vSphere-Clients auf **VMs und Vorlagen**.
- 2 Durchsuchen Sie die Bestandsliste nach der einzelnen virtuellen Maschine, die mithilfe von vSphere Replication repliziert werden soll.
- 3 Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **vSphere Replikation** aus.
- 4 Verwenden Sie den Schieberegler „RPO (Recovery Point Objective)“ oder geben Sie einen Wert ein, um die maximale Datenmenge festzulegen, die im Falle des Ausfalls einer Site verloren gehen darf. Der verfügbare RPO-Bereich geht von 15 Minuten bis 24 Stunden.
- 5 Wählen Sie die Stilllegungskonfiguration des Gastbetriebssystems aus, sofern dies für das Betriebssystem der virtuellen Quellmaschine zutrifft.
- 6 Wenn kein Speicherort für die Zieldatei angegeben wurde oder Sie den von den Datenspeicherzuordnungen festgelegten Standardspeicherort überschreiben möchten, klicken Sie auf **Durchsuchen**, um einen Zielspeicherort für die virtuelle Maschine auszuwählen.

Option	Beschreibung
Platzieren der virtuellen Maschine direkt in einem Datenspeicher	Wählen Sie einen Datenspeicher aus und klicken Sie auf OK .
Platzieren der virtuellen Maschine in einem bestimmten Ordner im Datenspeicher	Wählen Sie Datenspeicherordner angeben , klicken Sie zum Suchen des Ordners auf Durchsuchen und doppelklicken Sie anschließend auf den gewünschten Ordner.

- 7 Wählen Sie ein Replizierungsziel für jedes Medium der virtuellen Maschine aus.

Die nächsten Seiten werden je nach den auf der virtuellen Maschine installierten Mediengeräten dynamisch erstellt. Sie können mehrere virtuelle Laufwerke enthalten, die Sie alle einzeln konfigurieren können. Die konfigurierbaren Einstellungen umfassen Informationen darüber, ob das virtuelle Laufwerk repliziert wird, was das Replizierungsziel des virtuellen Laufwerks ist sowie darüber, wie das replizierte virtuelle Laufwerk konfiguriert ist. Wenn die Festplatte repliziert werden soll, wählen Sie für die Festplatte ein Replizierungsziel aus, bevor Sie fortfahren.

- 8 Akzeptieren Sie die automatische Zuweisung eines vSphere Replication-Servers oder wählen Sie einen bestimmten Server an der Ziel-Site aus.

- 9 Überprüfen Sie die Einstellungen und klicken Sie auf **Beenden**, um die Replizierung einzurichten.

vSphere Replication startet eine anfängliche vollständige Synchronisierung der Dateien der virtuellen Maschinen in den festgelegten Datenspeicher auf der Ziel-Site.

- 10 (Optional) Wählen Sie die Ansicht vSphere Replication in der Site Recovery Manager-Benutzeroberfläche aus.

- 11 (Optional) Wählen Sie die vSphere ReplicationRemote-Site aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.

Sie können den Fortschritt der anfänglichen vollständigen Synchronisierung der Dateien der virtuellen Maschinen auf die Ziel-Site überwachen.

Konfigurieren der Replizierung für mehrere virtuelle Maschinen

Mit dem Assistenten zum Konfigurieren mehrerer Replizierungen können Sie die Replizierung für mehrere virtuelle Maschinen konfigurieren.

Wenn Sie die Replizierung konfigurieren, legen Sie ein RPO (Recovery Point Objective) fest, um den Zeitraum zwischen Replizierungen festzulegen. Ein RPO von 1 Stunde soll z. B. sicherstellen, dass eine virtuelle Maschine während der Wiederherstellung nicht mehr als eine Stunde an Daten verliert. Bei kleineren RPO-Werten gehen weniger Daten bei einer Wiederherstellung verloren, jedoch wird mehr Netzwerkbandbreite belegt, um das Replikat aktuell zu halten.

Jedes Mal, wenn eine virtuelle Maschine ihr RPO-Ziel erreicht, protokolliert vSphere Replication etwa 3800 Bytes an Daten in der Datenbank für vCenter Server-Ereignisse. Wenn Sie einen kurzen RPO-Zeitraum festlegen, kann dies schnell zu einem hohen Datenvolumen in der Datenbank führen. Um zu vermeiden, dass die Datenbank für vCenter Server-Ereignisse zu groß wird, begrenzen Sie die Anzahl der Tage, die vCenter Server Ereignisdaten aufbewahrt. Weitere Informationen finden Sie unter „Konfigurieren einer Datenbankaufbewahrungsrichtlinie“ im *Handbuch für vCenter Server und Hostverwaltung*. Alternativ dazu können Sie einen höheren RPO-Wert festlegen.

Hinweis Sie können die Site Recovery Manager-Benutzeroberfläche nicht dazu verwenden, Replizierungen zu konfigurieren, die Point-in-Time-Snapshots (PIT) verwenden. Um PIT-Snapshots zu aktivieren, konfigurieren Sie die Replizierung virtueller Maschinen, indem Sie den vSphere Web Client verwenden. Weitere Details finden Sie unter [Konfigurieren der Replizierung für mehrere virtuelle Maschinen in vSphere Replication](#).

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](#).

vSphere Replication garantiert Absturzkonsistenz unter allen Festplatten, die zu einer virtuellen Maschine gehören. Wenn Sie die Stilllegung mit VSS verwenden, können Sie möglicherweise eine höhere Konsistenzstufe erzielen. Die verfügbaren Typen für das Stilllegen werden durch das Betriebssystem der virtuellen Maschine festgelegt. Weitere Informationen darüber, wie der Microsoft Volume Shadow Copy Service (VSS) das Stilllegen von virtuellen Windows-Maschinen unterstützt, finden Sie unter [Kompatibilitätstabellen für vSphere Replication 5.5](#).

Sie können vSphere Replication mit einem Virtual SAN-Datenspeicher auf den Quell- und Ziel-Sites verwenden. Sie müssen bei der Replizierung in den Virtual SAN-Speicher jedoch den vSphere Web Client verwenden, um vSphere Replication zu konfigurieren. Der Site Recovery Manager-Client lässt beim Auswählen des Zieldatenspeichers keine Auswahl eines virtuellen SAN-Speichers zu.

Hinweis VMware Virtual SAN ist eine vollständig unterstützte Funktion von vSphere 5.5u1.

- Sie können Virtual SAN in Produktionsumgebungen mit vSphere Replication 5.5.1 und vSphere 5.5u1 verwenden.
 - Virtual SAN ist eine experimentelle Funktion in vSphere 5.5. Sie können Tests mit Virtual SAN in vSphere Replication 5.5.0 und vSphere 5.5 durchführen, die Verwendung der Funktion in Produktionsumgebungen wird jedoch nicht unterstützt. In den Versionshinweisen zu vSphere Replication 5.5.0 finden Sie Informationen zur Aktivierung von Virtual SAN in vSphere 5.5.
-

Wenn Virtual SAN-Speicher verwendet und vSphere Replication auf einer großen Zahl von virtuellen Maschinen gleichzeitig konfiguriert wird, kann dies dazu führen, dass die anfängliche vollständige Synchronisierung der Dateien der virtuellen Maschinen sehr langsam ist. Die anfängliche vollständige Synchronisierung generiert einen hohen E/A-Datenverkehr und das Konfigurieren zu vieler Replikate gleichzeitig kann zu einer Überlastung des Virtual SAN-Speichers führen. Konfigurieren Sie vSphere Replication auf Gruppen von maximal 30 virtuellen Maschinen gleichzeitig.

Voraussetzungen

Um virtuelle Maschinen unter Verwendung von vSphere Replication zu replizieren, müssen Sie die vSphere Replication-Appliance auf den Quell- und Ziel-Sites bereitstellen. Sie müssen die virtuellen Maschinen einschalten, um mit der Replizierung zu beginnen.

Konfigurieren Sie vor der Replizierung mehrerer Maschinen die Datenspeicherzuordnungen über die Site Recovery Manager-Benutzeroberfläche. Sie konfigurieren die Zuordnungen, damit Site Recovery Manager die Informationen zu den Zieldatenspeichern für die Replizierung erhält.

Vorgehensweise

- 1 Klicken Sie auf der Startseite von vSphere Web Client auf **VMs und Vorlagen**.
- 2 Wählen Sie einen Ordner oder ein Datacenter im linken Bereich aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
- 3 Wählen Sie die zu replizierenden virtuellen Maschinen unter Verwendung der Strg- bzw. Umschalttaste aus.
- 4 Klicken Sie mit der rechten Maustaste auf die virtuellen Maschinen und wählen Sie **vSphere Replication**.
- 5 Verwenden Sie den Schieberegler „RPO (Recovery Point Objective)“ oder geben Sie einen Wert ein, um die maximale Datenmenge festzulegen, die im Falle des Ausfalls einer Site verloren gehen darf.
Der verfügbare RPO-Bereich geht von 15 Minuten bis 24 Stunden.
- 6 Wählen Sie die Stilllegungskonfiguration des Gastbetriebssystems aus, sofern dies für das Betriebssystem der virtuellen Quellmaschine zutrifft.
- 7 (Optional) Wählen Sie, ob die Option **Anfängliche Kopien der .vmdk-Dateien wurden auf dem Zieldatenspeicher platziert** aktiviert werden soll.
Wählen Sie diese Option, wenn Sie VMDK-Dateien physisch auf die Ziel-Site für die Verwendung als Replizierungsspeicher kopiert haben. Site Recovery Manager verwendet Datenspeicherzuordnungen und die Informationen von Quell-VMs, um die anfänglichen Kopien zu suchen und zu verwenden. Site Recovery Manager zeigt den Fortschritt und den Status der Suche nach anfänglichen Kopien an. Sie können den Suchvorgang anhalten oder ihn erneut starten.
- 8 Akzeptieren Sie die automatische Zuweisung eines vSphere Replication-Servers oder wählen Sie einen bestimmten Server an der Ziel-Site aus.
- 9 Überprüfen Sie die Einstellungen und klicken Sie auf **Beenden**, um die Replizierung einzurichten.
vSphere Replication startet eine anfängliche vollständige Synchronisierung der Dateien der virtuellen Maschinen in den festgelegten Datenspeicher auf der Ziel-Site.
- 10 (Optional) Wählen Sie die Ansicht vSphere Replication in der Site Recovery Manager-Benutzeroberfläche aus.

- 11 (Optional) Wählen Sie die vSphere ReplicationRemote-Site aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.

Sie können den Fortschritt der anfänglichen vollständigen Synchronisierung der Dateien der virtuellen Maschinen auf die Ziel-Site überwachen.

Weiter

Wenn Sie vor dem Konfigurieren der Replizierung die Datenspeicherzuordnungen für vSphere Replication nicht konfiguriert haben, werden die virtuellen Maschinen auf der Registerkarte **vSphere Replication > Virtuelle Maschinen** rot und mit dem Status Datenspeicherzuordnungen wurden nicht konfiguriert angezeigt. Konfigurieren Sie die Datenspeicherzuordnungen und konfigurieren Sie dann vSphere Replication auf den virtuellen Maschinen neu.

Replizieren virtueller Maschinen mithilfe von Replizierungsspeichern

Sie können die erste Replizierung von VMDK-Dateien effizienter gestalten, indem Sie Dateien physisch auf ein Speichermedium verschieben. vSphere Replication verwendet die physisch verschobenen Dateien als Replizierungsspeicher.

Möglicherweise müssen Sie Replizierungsspeicher verwenden, wenn es nicht praktikabel ist, die Dateien über das Netzwerk zu kopieren, weil die Datenmenge zu groß ist, die verfügbare Bandbreite zu klein ist oder eine Kombination aus diesen beiden Faktoren vorliegt.

Vergewissern Sie sich bei der Replizierung von virtuellen Maschinen, dass virtuelle Maschinen in Unterverzeichnisse von Datenspeichern repliziert werden. Kopierte Festplatten funktionieren, wenn die Übertragungsmethode die Identitätsinformationen in der VMDK-Datei aufbewahrt.

Voraussetzungen

- Sie haben die vSphere Replication-Appliance auf beiden Sites bereitgestellt.
- Sie haben die Site Recovery Manager Server-Instanzen auf jeder Site gekoppelt. Außerdem haben Sie die vSphere Replication-Appliances gekoppelt.
- Schalten Sie die virtuelle Quellmaschine aus, bevor Sie die VMDK-Dateien, die als Speicher für die Replizierung genutzt werden sollen, herunterladen. Die Replizierung beginnt, wenn die virtuelle Maschine eingeschaltet wird.

Vorgehensweise

- 1 Verwenden Sie den vSphere-Client, um eine Verbindung zu einem vCenter Server herzustellen, über die die virtuellen Maschinen verwaltet werden können, die physisch verschoben werden sollen.
- 2 Klicken Sie auf **Datenspeicher**.
- 3 Suchen Sie im linken Bereich den Datenspeicher, der die Dateien für die virtuelle Maschine enthält, wählen Sie den Datenspeicher aus und klicken Sie im rechten Bereich auf **Diesen Datenspeicher durchsuchen**.

- 4 Wählen Sie die Ordner für alle virtuellen Maschinen aus, die physisch verschoben werden sollen, klicken Sie mit der rechten Maustaste auf die Auswahl und klicken Sie dann auf **Herunterladen**.
- 5 Wählen Sie ein Ziel aus, an das die Dateien kopiert werden sollen, und klicken Sie auf **OK**.
- 6 Klicken Sie auf **Ja**.
- 7 Wenn der Download abgeschlossen ist, übertragen Sie die Dateien zu einem Speicherort an der gekoppelten Site, um sie hochzuladen.
- 8 Klicken Sie auf der Startseite des vSphere-Clients auf der gekoppelten Site auf **Datenspeicher**.
- 9 Suchen Sie im linken Bereich den Datenspeicher, der die Dateien für die virtuelle Maschine enthalten soll, wählen Sie den Datenspeicher aus und klicken Sie im rechten Bereich auf **Diesen Datenspeicher durchsuchen**.
- 10 Wählen Sie den Ordner aus, der die Kopien der virtuellen Maschinen enthalten soll, klicken Sie mit der rechten Maustaste auf die Auswahl und klicken Sie auf **Ordner hochladen**.
- 11 Wählen Sie den Ordner aus, der die virtuellen Maschinen enthält, und klicken Sie auf **OK**.
- 12 Klicken Sie an der geschützten Site mit der rechten Maustaste auf die zu replizierende virtuelle Maschine, und wählen Sie **vSphere Replication** aus.
- 13 Richten Sie den Speicherort für Recovery-Point-Objective und Zieldatei als normal ein, und klicken Sie auf **Weiter**.
- 14 Klicken Sie im Bereich „Speicherort der Zielfestplattendatei“ auf **Durchsuchen**.
- 15 Wählen Sie den Zieldatenspeicher aus, aktivieren Sie das Kontrollkästchen **Datenspeicherordner angeben**, und klicken Sie auf **Durchsuchen**.
- 16 Wählen Sie den Zieldatenspeicher aus, und klicken Sie auf **Öffnen**.
- 17 Wählen Sie den Datenspeicherordner aus, der die Speicherdateien enthält, ändern Sie den Dateityp in „Alle Dateien“, wählen Sie die als Replizierungsspeicher zu verwendende VMDK-Datei aus, und klicken Sie auf **OK**.
- 18 Klicken Sie zur Bestätigung, dass Sie diese Datei als eine anfängliche Kopie verwenden möchten, auf „Ja“.
- 19 Folgen Sie den Anweisungen zur Auswahl eines vSphere Replication-Servers, und klicken Sie auf **Beenden**, um die Konfiguration abzuschließen.

Neukonfigurieren von Replizierungen

Sie können die Replizierung neu konfigurieren, um eine Festplattendatei einer virtuellen Maschine für die Replizierung zu aktivieren oder zu deaktivieren, und Replizierungsoptionen ändern, wie z. B. RPO oder die Stilllegungsmethode. Sie können auch einen anderen Zieldatenspeicher für die Replizierungskonfigurations- und Festplattendateien angeben und die virtuelle Maschine auf einen anderen vSphere Replication-Server verschieben.

Voraussetzungen

Sie können vSphere Replication auf einer oder mehreren virtuellen Maschinen konfigurieren.

Vorgehensweise

- 1 Wählen Sie die Ansicht vSphere Replication auf der Site Recovery Manager-Benutzeroberfläche aus.
- 2 Wählen Sie einen vSphere Replication-Server aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
- 3 Wählen Sie eine virtuelle Maschine aus oder verwenden Sie die Strg- bzw. Umschalttasten, um mehrere virtuelle Maschinen auszuwählen, klicken Sie auf die rechte Maustaste und wählen Sie **Replizierung konfigurieren** aus.
- 4 (Optional) Verwenden Sie den Schieberegler „RPO (Recovery Point Objective)“ oder geben Sie einen Wert ein, um die maximale Datenmenge festzulegen, die im Falle des Ausfalls einer Site verloren gehen darf.

Der verfügbare RPO-Bereich geht von 15 Minuten bis 24 Stunden.

- 5 (Optional) Ändern Sie die Stilllegungskonfiguration des Gastbetriebssystems, sofern dies für das Betriebssystem der virtuellen Maschine zutrifft.
- 6 (Optional) Ändern Sie den Zielspeicherort für die Dateien der virtuellen Maschine.

Option	Beschreibung
Replizierung für eine einzelne virtuelle Maschine neu konfigurieren	Klicken Sie auf Durchsuchen , um den Zielspeicherort für die Dateien der virtuellen Maschine zu ändern.
Replizierung mehrerer virtueller Maschinen neu konfigurieren	Wählen Sie Anfängliche Kopien der .vmdk-Dateien wurden auf den Zieldatenspeichern platziert aus, wenn Sie die Replizierungsspeicher auf einen neuen Zieldatenspeicher kopiert haben.

- 7 (Optional) Ändern Sie das Replizierungsziel für jedes Mediengerät der virtuellen Maschine.

Die nächsten Seiten werden je nach den auf der virtuellen Maschine installierten Mediengeräten dynamisch erstellt. Sie können mehrere virtuelle Laufwerke enthalten, die Sie alle einzeln konfigurieren können. Die konfigurierbaren Einstellungen umfassen Informationen darüber, ob das virtuelle Laufwerk repliziert wird, was das Replizierungsziel des virtuellen Laufwerks ist sowie darüber, wie das replizierte virtuelle Laufwerk konfiguriert ist. Wenn die Festplatte repliziert werden soll, wählen Sie für die Festplatte ein Replizierungsziel aus, bevor Sie fortfahren.

- 8 (Optional) Wählen Sie einen anderen vSphere Replication-Server aus, um die Replizierung dieser virtuellen Maschine zu verwalten.
- 9 Überprüfen Sie die Einstellungen und klicken Sie auf **Beenden**, um die Replizierung einzurichten.
vSphere Replication startet eine anfängliche vollständige Synchronisierung der Dateien der virtuellen Maschinen in den festgelegten Datenspeicher auf der Ziel-Site.

Beenden der Replizierung einer virtuellen Maschine

Wenn die Replizierung einer virtuellen Maschine nicht erforderlich ist, können Sie sie beenden.

Durch das Beenden der Replizierung einer virtuellen Maschine wird diese nicht aus den Schutzgruppen entfernt, zu denen sie gehört.

Voraussetzungen

Sie haben vSphere Replication auf einer virtuellen Maschine konfiguriert, die nicht mehr geschützt zu werden braucht.

Vorgehensweise

- 1 Wählen Sie die Ansicht vSphere Replication auf der Site Recovery Manager-Benutzeroberfläche aus.
- 2 Wählen Sie einen vSphere Replication-Server aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
- 3 Wählen Sie eine virtuelle Maschine aus und klicken Sie auf **Replizierung entfernen**.
- 4 Klicken Sie auf **Ja**, um das Beenden der Replizierung dieser virtuellen Maschine zu bestätigen.
- 5 Wählen Sie auf der Site Recovery Manager-Oberfläche die Schutzgruppenansicht aus.
- 6 Wählen Sie die Schutzgruppe aus, zu der die virtuelle Maschine gehört, und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
- 7 Wählen Sie die virtuelle Maschine aus, deren Replizierung Sie beendet haben, und klicken Sie auf **Schutz entfernen**.
- 8 Klicken Sie auf **Ja**, um die Aufhebung des Schutzes für diese virtuelle Maschine zu bestätigen.

Die virtuelle Maschine repliziert nicht auf die Ziel-Site.

Die virtuelle Maschine gehört keiner Schutzgruppe mehr an.

Erstellen von Schutzgruppen

Nachdem Sie eine Replizierungslösung konfiguriert haben, können Sie Schutzgruppen erstellen. Bei einer Schutzgruppe handelt es sich um eine Sammlung von virtuellen Maschinen und Vorlagen, die Sie mithilfe von Site Recovery Manager zusammen schützen.

Sie nehmen eine oder mehrere Schutzgruppen in jedem Wiederherstellungsplan auf. Ein Wiederherstellungsplan gibt die Art an, wie Site Recovery Manager die virtuellen Maschinen in den Schutzgruppen, die es enthält, wiederherstellt.

Sie müssen die virtuellen Maschinen in einer Schutzgruppe konfigurieren, sodass Site Recovery Manager sie in die vCenter Server-Bestandsliste auf der Wiederherstellungs-Site aufnehmen kann.

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 jedoch Array-basierte Schutzgruppen und vSphere Replication-Schutzgruppen in denselben Wiederherstellungsplan aufnehmen.

- [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.

- [Erstellen von vSphere Replication-Schutzgruppen](#)

Sie können Schutzgruppen mit virtuellen Maschinen erstellen, die vSphere Replication schützt.

- [Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe](#)

Wenn Sie virtuelle Maschinen zu einer Schutzgruppe hinzufügen oder wenn virtuelle Maschinen den Schutz verlieren, können Sie in einem Schritt den Schutz für alle nicht konfigurierten virtuellen Maschinen mithilfe vorhandener Bestandslistenzuordnungen konfigurieren.

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.

Sie können virtuelle Maschinen zu einer Schutzgruppe hinzufügen, indem Sie sie auf einem der Datenspeicher erstellen, die den Datenspeichergruppen angehören, die Site Recovery Manager der Schutzgruppe zuordnet. Sie können virtuelle Maschinen auch unter Verwendung von Storage vMotion zur Schutzgruppe hinzufügen, indem Sie ihre Speicher auf einen der Datenspeicher der Datenspeichergruppe verschieben. Sie können ein Mitglied aus einer Schutzgruppe entfernen, indem Sie die Dateien der virtuellen Maschine auf einen anderen Datenspeicher verschieben.

Wenn Sie den Schutz auf einer virtuellen Maschine deaktivieren, müssen Sie die Dateien dieser virtuellen Maschine auf einen ungeschützten Datenspeicher verschieben. Wenn Sie die Dateien einer ungeschützten virtuellen Maschine in einem geschützten Datenspeicher speichern, schlägt die Wiederherstellung für alle virtuellen Maschinen in diesem Datenspeicher fehl.

Zum Konfigurieren der Array-basierten Replizierung müssen Sie jede virtuelle Maschine einem auf der Wiederherstellungs-Site vorhandenen Ressourcenpool, Ordner und Netzwerk zuweisen. Sie können Standardwerte für diese Zuweisungen angeben, indem Sie Bestandslistenzuordnungen auswählen. Site Recovery Manager wendet die Bestandslistenzuordnungen an, wenn Sie die Schutzgruppe erstellen. Wenn Sie keine Bestandslistenzuordnungen angeben, müssen Sie sie für jedes Mitglied der Schutzgruppe einzeln konfigurieren. Virtuelle Maschinen, die Sie für die Replizierung nicht bzw. fehlerhaft konfiguriert haben, werden von Site Recovery Manager nicht geschützt, auch wenn sie sich auf einem geschützten Datenspeicher befinden.

Sofern Ihr Storage-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 Storage-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.

■ [Erstellen Array-basierter Schutzgruppen](#)

Sie erstellen Array-basierte Schutzgruppen, um den Schutz von virtuellen Maschinen in Datenspeichergruppen zu aktivieren, die Sie für die Verwendung der Array-basierten Replizierung konfigurieren.

- **Bearbeiten von Array-basierten Schutzgruppen**

Sie können den Namen und die Beschreibung einer Array-basierten Schutzgruppe ändern sowie die zu einer Schutzgruppe gehörigen Datenspeichergruppen hinzufügen oder entfernen.

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.

Erstellen Array-basierter Schutzgruppen

Sie erstellen Array-basierte Schutzgruppen, um den Schutz von virtuellen Maschinen in Datenspeichergruppen zu aktivieren, die Sie für die Verwendung der Array-basierten Replizierung konfigurieren.

Site Recovery Manager berechnet die Datastore-Gruppen, wenn Sie das Array-Paar konfigurieren oder wenn Sie die Geräteliste aktualisieren.

Nachdem Sie eine Schutzgruppe erstellt haben, erstellt Site Recovery Manager Platzhalter-VMs und wendet Bestandslistenzuordnungen für jede virtuelle Maschine in der Gruppe an. Falls Site Recovery Manager einem Ordner, Netzwerk und 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.

Schutzgruppen können in Ordnern organisiert werden. Verschiedene Ansichten in der Wiederherstellungsschnittstelle zeigen die Namen der Schutz-Gruppen, aber nicht die Namen der Ordner an. Wenn Sie zwei Schutzgruppen mit demselben Namen in unterschiedlichen Ordnern abgelegt haben, ist es möglicherweise schwer, sie in einigen Ansichten der Benutzeroberfläche für die Wiederherstellung 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.

Vorgehensweise

- 1 Klicken Sie auf **Schutzgruppen** auf der Site Recovery Manager-Benutzeroberfläche und danach auf **Schutzgruppe erstellen**.
- 2 Legen Sie auf der Seite „Site und Schutzgruppentyp auswählen“ fest, welche Site geschützt werden soll, und wählen Sie **Array-basierte Replizierung**.
- 3 Wählen Sie ein Array-Paar aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie in der Liste eine Datenspeichergruppe aus und klicken Sie auf **Weiter**.

Wenn Sie eine Datenspeichergruppe auswählen, werden die virtuellen Maschinen in dieser Datenspeichergruppe unter „Virtuelle Maschinen“ im Bereich „Ausgewählter Datenspeicher“ aufgeführt. Sie sind für die Aufnahme in die Schutzgruppe markiert, sobald Sie die Schutzgruppe eingerichtet haben.

- 5 Geben Sie einen Namen und optional eine Beschreibung für die Schutzgruppe ein und klicken Sie auf **Weiter**.
- 6 Klicken Sie auf **Beenden**, um die Schutzgruppe zu erstellen und den Schutz der angegebenen virtuellen Maschinen zu aktivieren.

Sie können im Bereich „Kürzlich bearbeitete Aufgaben“ des vSphere-Clients den Fortschritt der Aufgaben für das Erstellen der Schutzgruppe und das Schützen der virtuellen Maschinen verfolgen.

Weiter

Erstellen Sie einen Wiederherstellungsplan, den Sie Ihren Schutzgruppen zuordnen. Weitere Informationen hierzu finden Sie unter [Erstellen eines Wiederherstellungsplans](#).

Bearbeiten von Array-basierten Schutzgruppen

Sie können den Namen und die Beschreibung einer Array-basierten Schutzgruppe ändern sowie die zu einer Schutzgruppe gehörigen Datenspeichergruppen hinzufügen oder entfernen.

Vorgehensweise

- 1 Klicken Sie auf **Schutzgruppen**, klicken Sie dann mit der rechten Maustaste auf eine Array-basierte Schutzgruppe und wählen Sie **Schutzgruppe bearbeiten**.
- 2 Klicken Sie auf **Weiter**.
- 3 Fügen Sie Datenspeichergruppen zur Schutzgruppe hinzu bzw. entfernen Sie diese und klicken Sie auf **Weiter**.
- 4 Bearbeiten Sie den Namen und die Beschreibung der Schutzgruppe und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Beenden**.

Erstellen von vSphere Replication -Schutzgruppen

Sie können Schutzgruppen mit virtuellen Maschinen erstellen, die vSphere Replication schützt.

Schutzgruppen können in Ordnern organisiert werden. Verschiedene Ansichten in der Wiederherstellungsschnittstelle zeigen die Namen der Schutz-Gruppen, aber nicht die Namen der Ordner an. Wenn Sie zwei Schutzgruppen mit demselben Namen in unterschiedlichen Ordnern abgelegt haben, ist es möglicherweise schwer, sie in einigen Ansichten der Benutzeroberfläche für die Wiederherstellung 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.

Wenn Sie eine vSphere Replication-Schutzgruppe erstellen, können Sie die virtuellen Maschinen, die Sie für vSphere Replication konfiguriert haben, zur Schutzgruppe hinzufügen.

Voraussetzungen

Verwenden Sie den vSphere-Client, um vSphere Replication für virtuelle Maschinen zu konfigurieren. Siehe [Konfigurieren der Replizierung für eine einzelne virtuelle Maschine](#) oder [Konfigurieren der Replizierung für mehrere virtuelle Maschinen](#).

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Schutzgruppen** und danach auf **Schutzgruppe erstellen**.
- 2 Wählen Sie die Site aus, die als Schutz-Site dienen soll, wählen Sie **vSphere Replication** und klicken Sie auf **Weiter**.

- 3 Wählen Sie virtuelle Maschinen in der Liste aus und klicken Sie auf **Weiter**.

Nur virtuelle Maschinen, die Sie für vSphere Replication konfiguriert haben und sich nicht bereits in einer Schutzgruppe befinden, werden in der Liste angezeigt.

- 4 Geben Sie einen Namen und optional eine Beschreibung für die Schutzgruppe ein und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Beenden**, um die Schutzgruppe zu erstellen.

Weiter

Erstellen Sie einen Wiederherstellungsplan, den Sie Ihren Schutzgruppen zuordnen. Weitere Informationen hierzu finden Sie unter [Erstellen eines Wiederherstellungsplans](#).

Bearbeiten von vSphere Replication -Schutzgruppen

Sie können eine vSphere Replication-Schutzgruppe bearbeiten, um deren Namen zu ändern und virtuelle Maschinen zur Gruppe hinzuzufügen oder virtuelle Maschinen zu entfernen.

Vorgehensweise

- 1 Klicken Sie im linken Bereich auf **Schutzgruppen** und klicken Sie mit der rechten Maustaste auf eine vSphere Replication-Schutzgruppe.
- 2 Wählen Sie **Schutzgruppe bearbeiten** und klicken Sie auf **Weiter**.
Sie können die Einstellungen **Schutz-Site** und **Schutzgruppentyp** nicht ändern.
- 3 Fügen Sie virtuelle Maschinen zur Schutzgruppe hinzu und klicken Sie auf **Weiter**.
- 4 Bearbeiten Sie den Namen und die Beschreibung der Schutzgruppe und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Beenden**.
- 6 (Optional) Um eine virtuelle Maschine aus einer vSphere Replication-Schutzgruppe zu entfernen, klicken Sie auf die Registerkarte **Virtuelle Maschinen**, wählen Sie eine virtuelle Maschine aus und klicken Sie auf **Schutz entfernen**.

Anwenden von Bestandslistenzuordnungen auf alle Mitglieder einer Schutzgruppe

Wenn Sie virtuelle Maschinen zu einer Schutzgruppe hinzufügen oder wenn virtuelle Maschinen den Schutz verlieren, können Sie in einem Schritt den Schutz für alle nicht konfigurierten virtuellen Maschinen mithilfe vorhandener Bestandslistenzuordnungen konfigurieren.

Vorgehensweise

- 1 Klicken Sie im linken Bereich auf **Schutzgruppen**, wählen Sie eine Schutzgruppe aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.

2 Klicken Sie auf **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.

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. Diese verschiedenen Wiederherstellungspläne ermöglichen Ihnen zu entscheiden, wie Sie die Wiederherstellung durchführen.

Durch das Testen eines Wiederherstellungsplans wird der Plan durchgeführt, ohne die Dienste auf der Schutz- und der Wiederherstellungs-Site zu beeinträchtigen, mit Ausnahme des Anhaltens von nicht-kritischen virtuellen Maschinen auf der Wiederherstellungs-Site, sofern Sie den Wiederherstellungsplan entsprechend konfiguriert haben. Sie können geplante Migrationen von der Schutz- auf die Wiederherstellungs-Site oder Notfallwiederherstellungen durchführen, indem Sie einen Wiederherstellungsplan ausführen.

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.

- [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.

- [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.

- [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.

- [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.

- [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.

- [Ansicht und Export des Verlaufs des Wiederherstellungsplans](#)

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

- [Abbrechen eines Tests oder einer Wiederherstellung](#)

Sie können den Test eines Wiederherstellungsplans jederzeit abbrechen. Das Abbrechen einer geplanten Migration oder Notfallwiederherstellung während der Ausführung ist zu bestimmten Zeiten möglich.

- [Löschen eines Wiederherstellungsplans](#)

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

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 Operationen 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 eine Bereinigung nach der Durchführung eines Tests ausführen, entfernt der vSphere Replication-Server die Redo-Protokolle von den Festplattendateien auf der Wiederherstellungs-Site.

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

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 Datacenter-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 Netzwerkeinstellungen bei der Ausführung eines Tests konfigurieren.

Ein Datacenter-Netzwerk ist ein Netzwerk, das in der Regel vorhandene virtuelle Maschinen auf der Wiederherstellungs-Site unterstützt. 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.

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.

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 virtuellen Maschinen auf der Wiederherstellungs-Site mit den virtuellen Maschinen auf der Schutz-Site. Anschließend wird die Replizierung gestoppt. Site Recovery Manager versucht, alle virtuellen Maschinen zu replizieren und die geschützten Maschinen ordnungsgemäß herunterzufahren. 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 stellt Site Recovery Manager die virtuellen Maschinen auf der Wiederherstellungs-Site mit dem zuletzt verfügbaren Status entsprechend des Recovery Point Objective (RPO) wieder her. 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. In diesem Fall ist ein automatischer erneuter Schutz möglicherweise nicht möglich.

Wenn Site Recovery Manager erkennt, dass sich ein Datenspeicher an der Schutz-Site im Status „Keine Pfade verfügbar“ befindet, und verhindert, dass eine virtuelle Maschine heruntergefahren wird, wartet Site Recovery Manager, bevor es erneut versucht, 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 verwendet den Heartbeat der VMware Tools, um zu erkennen, 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 müssen Sie VMware Tools auf geschützten virtuellen Maschinen 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 normalen Aufgaben nicht ausführen kann, 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.

Die erzwungene Wiederherstellung soll verwendet werden, wenn Speicher-Arrays an der Schutz-Site ausfallen 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.

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

Das Ausführen der erzwungenen Wiederherstellung mit Array-basierter Replizierung kann die Spiegelung zwischen dem Speicher-Array für den Schutz und dem 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.

Wenn Sie die erzwungene Wiederherstellung aktivieren, 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 hinzu-

gefügt 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.

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.

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.
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 sie jedoch nicht zum gewünschten Ergebnis führen, ignoriert Site Recovery Manager die Fehler.

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

Unterschiede	Testen eines Wiederherstellungsplans	Ausführen eines Wiederherstellungsplans
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 einem Datacenter-Netzwerk.
Unterbrechung eines Wiederherstellungsplans	Sie können einen Test jederzeit abbrechen.	In einigen Fällen können Sie die Wiederherstellung abbrechen.

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 vorübergehend DPM für den Cluster und stellt sicher, dass alle darin enthaltenen Hosts eingeschaltet werden, bevor die Wiederherstellung beginnt. Nachdem die Wiederherstellung und der Test abgeschlossen wurden, reaktiviert Site Recovery Manager DPM für den Cluster. Die darin enthaltenen Hosts bleiben im aktuellen Zustand, 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 während des Einschaltens wiederhergestellter virtueller Maschinen durch Site Recovery Manager andere virtuelle Maschinen, um die Last noch besser auf die Cluster zu verteilen. 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.

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.

- Sofern Ihr Storage-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 Storage-Array keine Konsistenzgruppen unterstützt, können Sie Storage DRS oder Storage vMotion nicht in Verbindung mit Site Recovery Manager verwenden.
- Wenn Sie Storage DRS auf der Schutz-Site aktivieren, darf ein Datenspeicher-Cluster nur genau eine Konsistenzgruppe enthalten. Nehmen Sie keine Datenspeicher in den Cluster auf, die nicht zur Konsistenzgruppe gehören. Wenn ein Cluster mehrere Konsistenzgruppen enthält, kann dies dazu führen, dass virtuelle Maschinen während der Wiederherstellung verloren gehen. Diese Richtlinie gilt auch für die Wiederherstellungs-Site, wenn Storage DRS auf der Wiederherstellungs-Site aktiviert ist.
- 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.
- Das Verschieben einer geschützten Festplatte in eine andere Konsistenzgruppe führt zu den gleichen Problemen wie das Verschieben einer kompletten virtuellen Maschine. Diese Probleme treten auf, wenn Sie eine Festplatte in eine andere Konsistenzgruppe innerhalb derselben Schutzgruppe verschieben oder wenn Sie die Festplatte in eine andere Schutzgruppe verschieben. Site Recovery Manager hindert Sie nicht, diese Aktion auszuführen, aber wenn eine Festplatte in eine andere Konsistenzgruppe verschoben wurde, 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.

- vSphere Replication ist mit vSphere Storage vMotion und vSphere Storage DRS an der Schutz-Site kompatibel. Sie können Storage vMotion und Storage DRS zum Verschieben der Festplattendateien einer von vSphere Replication geschützten virtuellen Maschine verwenden, ohne dass dies Auswirkungen auf die Replizierung hat.
- 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.

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.

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](#).
- vSphere unterstützt nicht vSphere vMotion für virtuelle MSCS-Maschinen.

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.

- Da vSphere nicht vSphere vMotion für virtuelle MSCS-Maschinen unterstützt, müssen Sie die DRS-Regel VM zu Host festlegen, sodass DRS nicht vMotion auf MSCS-Knoten durchführt. Legen Sie die VM zu Host-Regel für die virtuellen Maschinen auf der Schutz-Site und für den Schatten virtueller Maschinen auf der Wiederherstellungs-Site fest.
- 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.

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 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.

3 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.

4 Testen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan testen, führt Site Recovery Manager den Wiederherstellungsplan auf 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 Wiederherstellungsplan

Nach dem Testen eines Wiederherstellungsplans können Sie den Wiederherstellungsplan wieder in den Status 'Bereit' versetzen, indem Sie einen Bereinigungsverfahren durchführen.

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.

Erstellen eines Wiederherstellungsplans

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

Isolieren Sie beim Testen die virtuellen Maschinen, die Site Recovery Manager wiederherstellt. Wenn Site Recovery Manager duplizierte Maschinen online zur Verfügung stellt und sie mit nicht geschützten virtuellen Maschinen in Ihrem Produktionsnetzwerk zu interagieren beginnen, können Fehler auftreten.

Vorgehensweise

- 1 Klicken Sie auf **Wiederherstellungspläne**, dann auf die Registerkarte **Übersicht** und schließlich auf **Wiederherstellungsplan erstellen**.
- 2 Wählen Sie die Wiederherstellungs-Site aus.
- 3 Wählen Sie eine oder mehrere Schutzgruppen für den Plan aus, der wiederhergestellt werden soll, und klicken Sie auf **Weiter**.
- 4 Wählen Sie ein Wiederherstellungs-Site-Netzwerk aus, mit dem sich die wiederhergestellten virtuellen Maschinen während der Wiederherstellungsplantests verbinden, und klicken Sie auf **Weiter**.

Bei Testwiederherstellungen können Sie das Wiederherstellen von virtuellen Maschinen durch Site Recovery Manager isolieren, indem Sie **Auto** wählen, bei dem es sich um ein isoliertes Netzwerk handelt, oder indem Sie ein manuell erstelltes Netzwerk auswählen, das nicht mit anderen Netzwerken verbunden ist.

- 5 Geben Sie im Textfeld **Name des Wiederherstellungsplans** einen Namen für den Plan ein, fügen Sie optional eine Beschreibung hinzu und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die Zusammenfassung der Angaben und klicken Sie auf **Beenden**, um den Wiederherstellungsplan zu erstellen.

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

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 auf **Wiederherstellungspläne**, klicken Sie mit der rechten Maustaste auf einen Wiederherstellungsplan und wählen Sie **Wiederherstellungsplan bearbeiten**.
- 2 Klicken Sie auf **Weiter**.
Sie können die Wiederherstellungs-Site nicht ändern.
- 3 Wählen Sie eine oder mehrere Schutzgruppen für den Plan aus, der wiederhergestellt werden soll, und klicken Sie auf **Weiter**.
- 4 Wählen Sie ein Wiederherstellungs-Site-Netzwerk aus, mit dem sich die wiederhergestellten virtuellen Maschinen während der Wiederherstellungsplantests verbinden, und klicken Sie auf **Weiter**.
- 5 Ändern Sie im Textfeld **Name des Wiederherstellungsplans** den Namen des Plans und fügen Sie eine optionale Beschreibung hinzu.
- 6 Klicken Sie 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.

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-Datencentrumgebungen 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.

Sie können nur virtuelle Maschinen hinzufügen, die an der Wiederherstellungs-Site angehalten werden sollen. Um virtuelle Maschinen sowohl an der Schutz- als auch an der Wiederherstellungs-Site anzuhalten, müssen Sie eine Wiederherstellung durchführen und anschließend den Schutz umkehren, indem Sie den Vorgang zum erneuten Schützen ausführen, bevor Sie virtuelle Maschinen hinzufügen, die an der ursprünglichen Schutz-Site angehalten werden sollen. Wenn Sie virtuellen Maschinen zum Anhalten an beiden Sites konfigurieren, sorgt der Plan dafür, dass bei jedem ausgeführten Wiederherstellungsvorgang die virtuellen Maschinen an einer Site gestartet und an der anderen Site angehalten werden.

Vorgehensweise

- 1 Klicken Sie an der Wiederherstellungs-Site im linken Bereich auf **Wiederherstellungspläne** und wählen Sie den zu bearbeitenden Wiederherstellungsplan aus.
- 2 Klicken Sie auf die Registerkarte **Wiederherstellungsschritte** und klicken Sie auf **Nicht kritische VM hinzufügen**.
- 3 Erweitern Sie die hierarchische Liste, um diejenigen virtuellen Maschinen an der Wiederherstellungs-Site auszuwählen, die während eines Wiederherstellungsvorgangs angehalten werden sollen.
- 4 Klicken Sie auf **OK**.

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

Testen eines Wiederherstellungsplans

Wenn Sie einen Wiederherstellungsplan testen, führt Site Recovery Manager den Wiederherstellungsplan auf 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 Ausschalten 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 auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**.
- 2 Wählen Sie den Wiederherstellungsplan aus, den Sie testen möchten, und klicken Sie auf **Testen**.
- 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 **Starten**.

- 6 Klicken Sie auf die Registerkarte **Wiederherstellungsschritte**, um den Testfortschritt zu überwachen und auf Meldungen zu reagieren.

Auf der Registerkarte **Wiederherstellungsschritte** wird der Fortschritt der einzelnen Schritte angezeigt. Auf der Registerkarte **Übersicht** wird der Gesamtfortschritt des Plans angezeigt.

Hinweis Site Recovery Manager initiiert die Wiederherstellungsschritte in der vorgeschriebenen Reihenfolge, mit einer Ausnahme. Er wartet nicht darauf, bis der Schritt zum Vorbereiten des Speichers für alle Schutzgruppen beendet ist, bevor er mit den nächsten Schritten fortfährt.

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 Bereinigungsverfahren durchführen.

Site Recovery Manager führt nach dem Test mehrere Bereinigungsverfahren 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 auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, wählen Sie den Wiederherstellungsplan aus, den Sie getestet haben, und klicken Sie auf **Bereinigen**.
- 2 Überprüfen Sie die Bereinigungsverfahren und klicken Sie auf **Weiter**.
- 3 Klicken Sie auf **Starten**.
- 4 Falls nach Abschluss der Bereinigung Fehler gemeldet werden, führen Sie den Bereinigungsverfahren 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. Im Fall einer Array-basierten Replizierung müssen wiederhergestellte virtuelle Maschinen und Dienste möglicherweise für eine gewisse Zeit auf der Wiederherstellungs-Site unterstützt werden. Eine Rücknahme dieser Änderungen nimmt möglicherweise viel Zeit und Aufwand in Anspruch und kann zu längeren Dienstausschfallzeiten 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 linken Bereich auf **Wiederherstellungspläne**, wählen Sie den auszuführenden Wiederherstellungsplan aus und klicken Sie auf **Wiederherstellen**.
- 2 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**.
- 3 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.

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

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

- 5 Klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die Wiederherstellungsinformationen und klicken Sie auf **Starten**.

7 Klicken Sie auf die Registerkarte **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](#).

Hinweis Sie können mit der Site Recovery Manager-Benutzeroberfläche keine Replizierungen konfigurieren, die Point-in-Time-Snapshots (PIT) verwenden. Um PIT-Snapshots zu aktivieren, konfigurieren Sie Replizierungen einer virtuellen Maschine anhand von vSphere Web Client. Siehe [Konfigurieren der Replizierung für eine einzelne virtuelle Maschine](#) unter *Verwaltung von vSphere Replication*.

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](#).

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** setzen.
- 2 Verwenden Sie den vSphere Web Client zur Konfiguration der Replizierung einer virtuellen Maschine, indem Sie die Option zur Beibehaltung mehrerer PIT-Snapshots auswählen.
- 3 Fügen Sie auf der Site Recovery Manager-Benutzeroberfläche 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.

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 in der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, wählen Sie einen Wiederherstellungsplan aus und klicken Sie auf die Registerkarte **Wiederherstellungsschritte**.
- 2 Klicken Sie auf **Schritte exportieren**.
Sie können die Schritte eines Wiederherstellungsplans als MS Word-, Excel-, HTML-, CSV- oder XML-Dokument speichern.

Ansicht und Export des Verlaufs des 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 des Wiederherstellungsplans nicht exportieren, während eine Testwiederherstellung, eine echte Wiederherstellung oder eine Testbereinigung läuft.

Voraussetzungen

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

Vorgehensweise

- 1 Klicken Sie in der Site Recovery Manager-Schnittstelle auf **Wiederherstellungspläne**, wählen Sie einen Wiederherstellungsplan aus und klicken Sie auf die Registerkarte **Verlauf**.
- 2 (Optional) Klicken Sie für die Durchführung eines Wiederherstellungsplans, einen Test oder einen Bereinigungsvorgang auf **Ansicht**.

Der Verlauf wird in einem Browser geöffnet.

- 3 (Optional) Klicken Sie für die Durchführung eines Wiederherstellungsplans, einen Test oder einen Bereinigungsvorgang auf **Export**.

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

Abbrechen eines Tests oder einer Wiederherstellung

Sie können den Test eines Wiederherstellungsplans jederzeit abbrechen. Das Abbrechen einer geplanten Migration oder Notfallwiederherstellung während der Ausführung ist zu bestimmten Zeiten möglich.

Wenn Sie einen Test oder eine Wiederherstellung abbrechen, startet Site Recovery Manager keine neuen Schritte. Schritte, die bereits ausgeführt werden, werden unter Einhaltung bestimmter Regeln angehalten.

- Schritte, 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.
- Schritte, 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 Schritte ab, die derzeit ausgeführt werden.

Vorgehensweise

- ◆ Klicken Sie zum Abbrechen eines Tests oder einer Wiederherstellung auf der Wiederherstellungsplan-Symbolleiste auf die Schaltfläche **Abbrechen**.

Löschen eines Wiederherstellungsplans

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

Beim Löschen eines Wiederherstellungsplans wird der Verlauf des Plans nicht gelöscht. Er wird auf der Registerkarte **Alle Wiederherstellungspläne > Gesamter Verlauf** weiterhin angezeigt.

Vorgehensweise

- 1 Klicken Sie auf **Wiederherstellungspläne** und wählen Sie den zu löschenden Wiederherstellungsplan aus.
- 2 (Optional) Klicken Sie auf die Registerkarte **Verlauf** und dann auf **Liste exportieren**, um den Verlauf des Plans herunterzuladen.

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

Erneuter Schutz virtueller Maschinen nach einer Wiederherstellung

5

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 dann abschließen, nachdem eine Wiederherstellung 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.

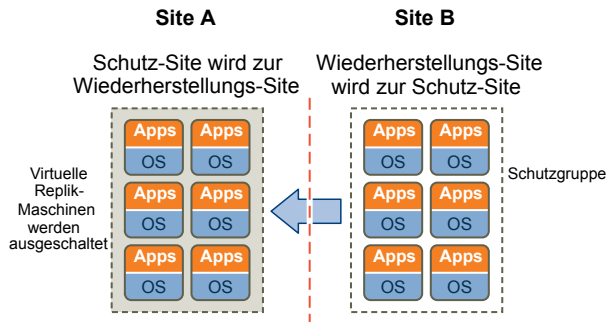
Sie können Schutzgruppen, die virtuellen Maschinen enthalten, die sowohl für die Array-basierte Replizierung als auch für vSphere Replication konfiguriert sind, erneut schützen.

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, stellt Site Recovery Manager die geschützten virtuellen Maschinen auf Site B wieder her. Nach der Wiederherstellung werden die geschützten virtuellen Maschinen von Site A auf Site B ohne Schutz gestartet.

Wenn Site A wieder online ist, können Sie einen Vorgang des erneuten Schutzes ausführen, 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 5-1. Site Recovery Manager -Vorgang des erneuten Schutzes



Richtung der Replizierung wird nach einer geplanten Migration umgekehrt

- **So führt Site Recovery Manager den erneuten Schutz durch**

Der erneute Schutz wird in zwei Stufen durchgeführt. Site Recovery Manager kehrt 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. Mit dem erneuten Schutz können Sie virtuelle Maschinen nach einer Wiederherstellung 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.

So führt Site Recovery Manager den erneuten Schutz durch

Der erneute Schutz wird in zwei Stufen durchgeführt. Site Recovery Manager kehrt 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 oder vSphere Replication 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 erstellt den Platzhalter und alle nachfolgend wiederhergestellten virtuellen Maschinen unter Verwendung der Identität der ursprünglich geschützten virtuellen Maschine. 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. Wenn Sie dies nicht tun, schlägt der erneute Schutz möglicherweise fehl.

Beim Durchführen des Vorgangs zum erneuten Schützen 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 erneute Schutz abgeschlossen ist.

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.

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. Mit dem erneuten Schutz können Sie virtuelle Maschinen nach einer Wiederherstellung auf der ursprünglichen Site wiederherstellen.

Voraussetzungen

Weitere Informationen hierzu finden Sie unter [Vorbedingungen zum Durchführen des erneuten Schutzes](#).

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, wählen Sie einen Wiederherstellungsplan aus, und klicken Sie auf **Neu schützen**.
- 2 Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Ihnen bewusst ist, dass das erneute Schützen nicht rückgängig gemacht werden kann.
- 3 Überprüfen Sie die Informationen zum erneuten Schutz und klicken Sie auf **Starten**.
- 4 Klicken Sie auf die Registerkarte **Wiederherstellungsschritte**, um den Fortschritt des erneuten Schutzes zu überwachen.

Bestimmte Schritte gelten nicht für alle virtuellen Maschinen. Virtuelle Maschinen, die Sie für die Array-basierte Replizierung konfiguriert haben, erscheinen beispielsweise unter **Speicher für die umgekehrte Richtung konfigurieren > Schutzgruppe > VR-Replizierung konfigurieren**, obwohl für sie bei diesem Schritt keine Aktionen durchgeführt werden. Diese virtuellen Maschinen werden als „Nicht anwendbar“ gekennzeichnet, wenn der Schritt ausgeführt wird.

- 5 Wenn der Vorgang zum erneuten Schutz beendet wird, wählen Sie den Wiederherstellungsplan aus, und klicken Sie auf **Verlauf** und danach auf **Ansicht**, um diesen Vorgang einzusehen.

Der Verlaufsbericht für den Vorgang zum erneuten Schutz wird in einem Browser geöffnet. 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 5-1. 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.	<ul style="list-style-type: none"> ■ 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, sind Wiederherstellungen 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 einer der Site Recovery Manager-Server während des Vorgangs zum erneuten Schutz unerwartet beendet wird.	Stellen Sie sicher, dass beide Site Recovery Manager-Server ausgeführt werden, und starten Sie die Aufgabe zum erneuten Schutz erneut.

Wiederherstellen der ursprünglichen Konfiguration der Wiederherstellungs-Site durch Failback

6

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 5 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 durchführen, 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.

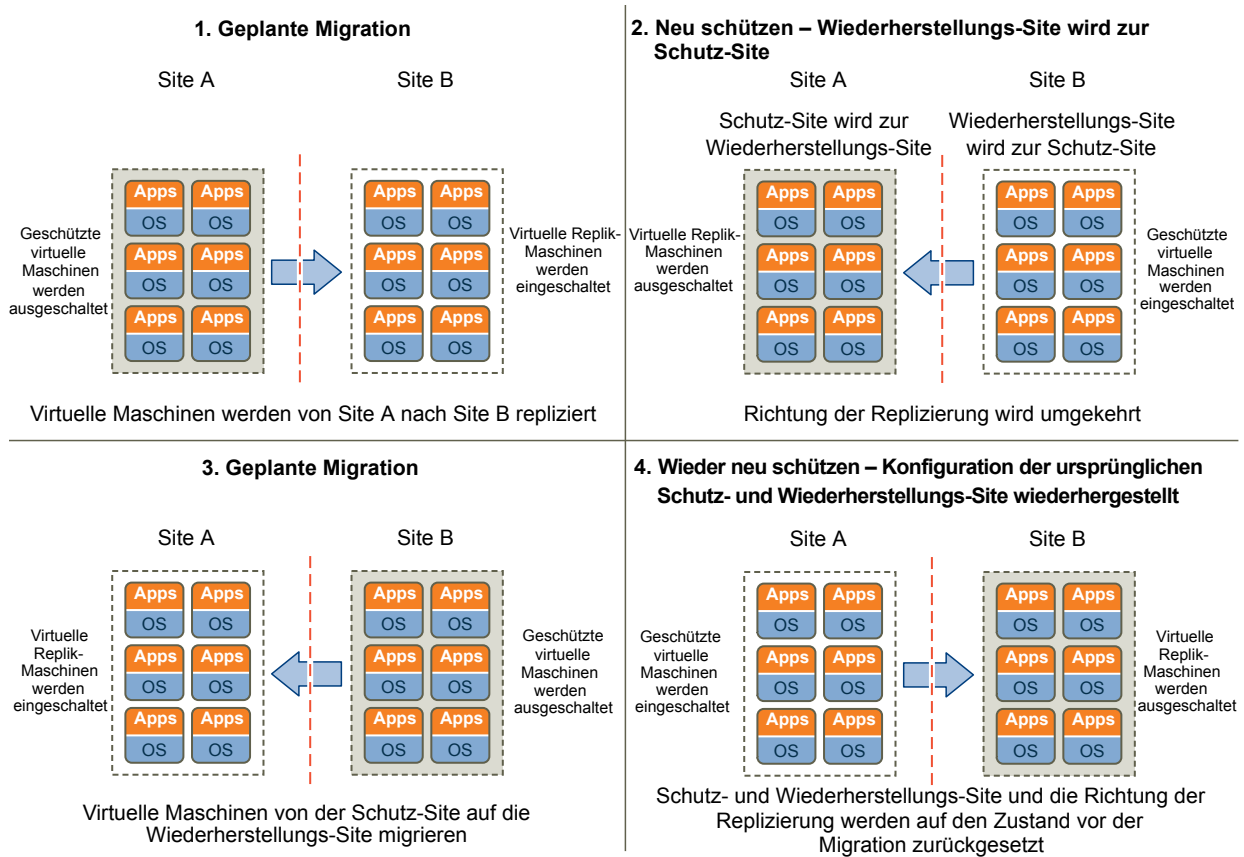
Sie können ein Failback konfigurieren und ausführen, wenn Sie bereit sind, die Dienste auf der ursprünglichen Schutz-Site wiederherzustellen, nachdem die Site nach einem Vorfall wieder online ist.

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.

- 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.
- Führen Sie eine geplante Migration durch, um die geschützten virtuellen Maschinen von Site B an Site A wiederherzustellen.
- Führen Sie einen zweiten Vorgang zum erneuten Schutz neu aus. Site A wird zur Schutz-Site und Site B wird zur Wiederherstellungs-Site.

Abbildung 6-1. 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 Schutz-Site, Site A, wieder ausgeführt werden.
- Nach der Wiederherstellung haben Sie den erneuten Schutz nicht durchgeführt.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, wählen Sie einen Wiederherstellungsplan aus, und klicken Sie auf **Neu schützen**.
- 2 Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Ihnen bewusst ist, dass das erneute Schützen nicht rückgängig gemacht werden kann.
- 3 Überprüfen Sie die Informationen zum erneuten Schutz und klicken Sie auf **Starten**.
- 4 Überwachen Sie den Fortschritt des erneuten Schutzes auf der Registerkarte **Wiederherstellungsschritte**, bis der Vorgang abgeschlossen ist.
- 5 (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.
- 6 (Optional) Klicken Sie auf **Testen** und folgen Sie den Anweisungen zum Testen des Wiederherstellungsplans.
Mit dem Testen des Wiederherstellungsplans stellen Sie sicher, dass der Wiederherstellungsplan nach dem erneuten Schutz ordnungsgemäß funktioniert.
- 7 Klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsplan als geplante Migration auszuführen.

- 8 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**.
- 9 Wählen Sie **Geplante Migration** und klicken Sie auf **Weiter**. Klicken Sie anschließend auf **Starten**.
- 10 Überwachen Sie den Status der geplanten Migration auf der Registerkarte **Wiederherstellungsschritte**, bis der Vorgang abgeschlossen ist.

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 auf **Neu schützen** und führen Sie die Anweisungen des Assistenten aus, 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.

Konfigurieren eines Wiederherstellungsplans

7

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 eine Reihe von Schritten aus, die in einer bestimmten Reihenfolge erfolgen 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.

■ 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 vermindern.

■ Erstellen von benutzerdefinierten Wiederherstellungsschritten

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

- [Anpassen der Wiederherstellung einer einzelnen virtuellen Maschine](#)

Sie können eine virtuelle Maschine in einem Wiederherstellungsplan so konfigurieren, dass sie eine vorgeschriebene Anpassungsspezifikation verwendet oder Meldungs- bzw. Befehlsschritte ausführt, wenn sie wiederhergestellt wird.

Schritte für den Wiederherstellungsplan

Ein Wiederherstellungsplan führt eine Reihe von Schritten aus, die in einer bestimmten Reihenfolge erfolgen 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.

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 vermindern.

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 verwendet den Heartbeat der VMware Tools, um zu erkennen, wenn eine virtuelle Maschine auf der Wiederherstellungs-Site ausgeführt wird. Auf diese Weise kann Site Recovery Manager sicherstellen, dass alle virtuellen Maschinen einer gegebenen 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 linken Bereich auf **Wiederherstellungspläne**, wählen Sie einen Wiederherstellungsplan aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen** oder die Registerkarte **Wiederherstellungsschritte**.
- 2 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Priorität**.
- 3 Wählen Sie eine neue Priorität für die virtuelle Maschine aus.
Die höchste Priorität ist 1. Die niedrigste Priorität ist 5.
- 4 Klicken Sie auf **Ja** und bestätigen Sie die Änderung der Priorität.

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.

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 Befehlsschritten der obersten Ebene](#)

Sie können Befehle der obersten Ebene überall im Wiederherstellungsplan hinzufügen.

- [Erstellen von Meldungsaufforderungsschritten der obersten Ebene](#)

Sie können Meldungsaufforderungen der obersten Ebene überall im Wiederherstellungsplan hinzufügen.

- [Erstellen von Befehlsschritten für einzelne virtuelle Maschinen](#)

Sie können benutzerdefinierte Wiederherstellungsschritte konfigurieren, um Aufgaben für eine virtuelle Maschine durchzuführen, bevor Site Recovery Manager sie ein- und nachdem es sie ausschaltet.

- [Erstellen von Meldungsaufforderungsschritten für einzelne virtuelle Maschinen](#)

Sie können benutzerdefinierte Wiederherstellungsschritte konfigurieren, um Benutzer aufzufordern, Aufgaben für eine virtuelle Maschine durchzuführen, bevor die virtuelle Maschine eingeschaltet wird und nachdem sie eingeschaltet wurde.

- [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 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, besteht darin, auf **OK** zu klicken. Dadurch wird die Meldung ausgeblendet und die Wiederherstellung kann fortgesetzt werden.

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 Befehlsschritten der obersten Ebene

Sie können Befehle der obersten Ebene überall im Wiederherstellungsplan hinzufügen.

Voraussetzungen

Sie haben einen Wiederherstellungsplan, dem benutzerdefinierte Schritte hinzugefügt werden sollen.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, und wählen Sie einen Wiederherstellungsplan aus.
- 2 Klicken Sie auf die Registerkarte **Wiederherstellungsschritte**.

- 3 Klicken Sie mit der rechten Maustaste auf einen Schritt davor oder danach, um einen benutzerdefinierten Schritt hinzuzufügen, und wählen Sie **Schritt hinzufügen**.
- 4 Wählen Sie **Befehl auf SRM-Server**.
- 5 Geben Sie in das Textfeld **Name** einen Namen für den Schritt ein.
- 6 Geben Sie in das Textfeld **Inhalt** die Befehle ein, die bei diesem Schritt ausgeführt werden sollen.
- 7 (Optional) Ändern Sie die Einstellung **Zeitüberschreitung**.
- 8 Wählen Sie, wo in der Schrittfolge der neue Schritt eingefügt werden soll.
 - **Vor ausgewähltem Schritt**
 - **Nach ausgewähltem Schritt**
- 9 Klicken Sie auf **OK**, um den Schritt zum Wiederherstellungsplan hinzuzufügen.

Erstellen von Meldungsaufforderungsschritten der obersten Ebene

Sie können Meldungsaufforderungen der obersten Ebene überall im Wiederherstellungsplan hinzufügen.

Voraussetzungen

Sie haben einen Wiederherstellungsplan, dem benutzerdefinierte Schritte hinzugefügt werden sollen.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, und wählen Sie einen Wiederherstellungsplan aus.
- 2 Klicken Sie auf die Registerkarte **Wiederherstellungsschritte**.
- 3 Klicken Sie mit der rechten Maustaste auf einen Schritt davor oder danach, um einen benutzerdefinierten Schritt hinzuzufügen, und wählen Sie **Schritt hinzufügen**.
- 4 Wählen Sie **Eingabeaufforderung**.
- 5 Geben Sie in das Textfeld **Name** einen Namen für den Schritt ein.
- 6 Geben Sie in das Textfeld **Inhalt** eine Meldung für die Eingabeaufforderung ein.
- 7 Wählen Sie, wo in der Schrittfolge der neue Schritt eingefügt werden soll.
 - **Vor ausgewähltem Schritt**
 - **Nach ausgewähltem Schritt**
- 8 Klicken Sie auf **OK**, um den Schritt zum Wiederherstellungsplan hinzuzufügen.

Erstellen von Befehlsschritten für einzelne virtuelle Maschinen

Sie können benutzerdefinierte Wiederherstellungsschritte konfigurieren, um Aufgaben für eine virtuelle Maschine durchzuführen, bevor Site Recovery Manager sie ein- und nachdem es sie ausschaltet.

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

Voraussetzungen

Sie haben einen Wiederherstellungsplan, dem benutzerdefinierte Schritte hinzugefügt werden sollen.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, und wählen Sie einen Wiederherstellungsplan aus.
- 2 Klicken Sie auf die Registerkarte **Virtuelle Maschinen (Virtual Machines)**.
- 3 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und klicken Sie auf **Konfigurieren**.
- 4 Wählen Sie im linken Bereich **Schritte vor dem Einschalten** oder **Schritte nach dem Einschalten** und klicken Sie auf **Hinzufügen**.
- 5 Wählen Sie **Befehl auf SRM-Server** oder **Befehl auf wiederhergestellter VM**.
- 6 Geben Sie in das Textfeld **Name** einen Namen für den Schritt ein.
- 7 Geben Sie in das Textfeld **Inhalt** die Befehle ein, die bei diesem Schritt ausgeführt werden sollen.
- 8 (Optional) Ändern Sie die Einstellung **Zeitüberschreitung**.
- 9 Klicken Sie auf **OK**, um den Schritt zum Wiederherstellungsplan hinzuzufügen.
- 10 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.

Erstellen von Meldungsaufforderungsschritten für einzelne virtuelle Maschinen

Sie können benutzerdefinierte Wiederherstellungsschritte konfigurieren, um Benutzer aufzufordern, Aufgaben für eine virtuelle Maschine durchzuführen, bevor die virtuelle Maschine eingeschaltet wird und nachdem sie eingeschaltet wurde.

Site Recovery Manager ordnet einer geschützten virtuellen Maschine Meldungsaufforderungsschritte in der gleichen Art und Weise zu wie Anpassungsinformationen. Wenn unterschiedliche Wiederherstellungspläne dieselbe virtuelle Maschine enthalten, sind die Befehle und Eingabeaufforderungen identisch.

Voraussetzungen

Sie haben einen Wiederherstellungsplan, dem benutzerdefinierte Schritte hinzugefügt werden sollen.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne**, und wählen Sie einen Wiederherstellungsplan aus.
- 2 Klicken Sie auf die Registerkarte **Virtuelle Maschinen (Virtual Machines)**.
- 3 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und klicken Sie auf **Konfigurieren**.
- 4 Wählen Sie im linken Bereich **Schritte vor dem Einschalten** oder **Schritte nach dem Einschalten** und klicken Sie auf **Hinzufügen**.
- 5 Wählen Sie **Eingabeaufforderung**.
- 6 Geben Sie in das Textfeld **Name** einen Namen für den Schritt ein.
- 7 Geben Sie in das Textfeld **Inhalt** eine Meldung für die Eingabeaufforderung ein.
- 8 Klicken Sie auf **OK**, um den Schritt zum Wiederherstellungsplan hinzuzufügen.
- 9 Klicken Sie auf **OK**, um die virtuelle Maschine so neu zu konfigurieren, dass vor oder nach dem Einschalten der virtuellen Maschine für den Benutzer eine Meldung angezeigt 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-Befehlshell 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 7-1. Umgebungsvariablen, die allen Befehlsschritten zur Verfügung stehen

Name	Wert	Beispiel
<i>VMware_RecoveryName</i>	Name des Wiederherstellungsplans, der gerade ausgeführt wird.	Plan A
<i>VMware_RecoveryMode</i>	Wiederherstellungsmodus	Test oder Wiederherstellung
<i>VMware_VC_Host</i>	Hostname von vCenter Server auf der Wiederherstellungs-Site.	vc_hostname.example.com
<i>VMware_VC_Port</i>	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 7-2. Umgebungsvariablen, die Befehlsschritten pro virtueller Maschine zur Verfügung stehen

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

Anpassen der Wiederherstellung einer einzelnen virtuellen Maschine

Sie können eine virtuelle Maschine in einem Wiederherstellungsplan so konfigurieren, dass sie eine vorgeschriebene Anpassungsspezifikation verwendet oder Meldungs- bzw. Befehlsschritte ausführt, wenn sie wiederhergestellt wird.

Meldungs- und Befehlsschritte, die zu den Wiederherstellungsschritten für eine virtuelle Maschine hinzugefügt werden, fungieren wie Meldungs- oder Befehlsschritte, die zu einem Wiederherstellungsplan hinzugefügt werden. Weitere Informationen hierzu finden Sie unter [Richtlinien zum Schreiben von Befehlsschritten](#).

Vorgehensweise

- 1 Verbinden Sie den vSphere-Client mit der vCenter Server-Instanz auf der Wiederherstellungs-Site.
- 2 Klicken Sie im linken Bereich auf der Site Recovery Manager-Benutzeroberfläche auf **Wiederherstellungspläne** und anschließend auf den anzupassenden Plan.
- 3 Klicken Sie auf die Registerkarte **Wiederherstellungsschritte** oder **Virtuelle Maschinen**.
- 4 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine in der Liste und klicken Sie auf **Konfigurieren**.
- 5 Klicken Sie auf **IP-Einstellungen**.

Darüber hinaus können Sie eine Beschreibung der von Ihnen angewendeten Spezifikation eingeben. Nur die IP-Eigenschaften der ausgewählten Spezifikation werden angewendet. Wenn Sie den Befehl `dr-ip-customizer.exe` verwendet haben, um die virtuellen Maschinen im Wiederherstellungsplan anzupassen, müssen Sie diese Anpassung hier nicht angeben.

- 6 Wählen Sie den entsprechenden Eintrag, um einen Meldungs- oder Befehlsschritt hinzuzufügen, der ausgeführt wird, bevor die Maschine eingeschaltet wird.
- 7 Wählen Sie den entsprechenden Eintrag aus, um einen Meldungs- oder Befehlsschritt hinzuzufügen, der nach dem Einschalten der Maschine ausgeführt wird.

Die von Ihnen angegebenen Anpassungen werden der geschützten virtuellen Maschine zugeordnet. Folglich werden die Einstellungen von allen Wiederherstellungsplänen, die sich auf diese virtuelle Maschine beziehen, gemeinsam genutzt.

Hinweis Wenn Sie den Schutz einer virtuellen Maschine entfernen, gehen alle Wiederherstellungsanpassungen verloren.

Anpassen der IP-Eigenschaften für virtuelle Maschinen



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.

In der [Kompatibilitätstabelle für vCenter Site Recovery Manager 5.5](#) finden Sie die Liste der Gastbetriebssysteme, für die Site Recovery Manager IP-Anpassungen unterstützt.

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 eine Netzwerkkarte auf einer Site nicht anpassen, verwendet die Netzwerkkarte die IP-Einstellungen der anderen Site.

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>.

- [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 anpassen.
- [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 Netzanforderungen eines Wiederherstellungsplans zu verstehen.
- [Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen](#)
Das manuelle Konfigurieren der IP-Einstellungen für viele virtuelle Maschinen einer Wiederherstellungs-Site kann zeitaufwändig sein und es können Fehler in der Konfiguration auftreten. Site Recovery Manager enthält das Tool „DR IP Customizer“, um den Konfigurationsvorgang für mehrere virtuelle Maschinen zu vereinfachen.

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 anpassen.

Vorgehensweise

- 1 Klicken Sie auf **Wiederherstellungspläne** und wählen den Wiederherstellungsplan aus, den Sie anpassen möchten.

- 2 Klicken Sie auf die Registerkarte **Virtuelle Maschinen**, klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Konfigurieren**.
- 3 Wählen Sie die Netzwerkkarte aus, für die Sie IP-Einstellungen ändern möchten.
- 4 Aktivieren Sie zum Anpassen der Einstellungen die Option **IP-Einstellungen während der Wiederherstellung anpassen**.
- 5 Klicken Sie je nach dem, welchen Satz an IP-Einstellungen Sie konfigurieren möchten, auf **Schutz konfigurieren** oder **Wiederherstellung konfigurieren**.
- 6 Klicken Sie auf die Registerkarte **Allgemein**, um Einstellungen zu konfigurieren.
 - a Wählen Sie die Art der Adressierung aus, die verwendet werden soll.

Zu den verfügbaren Optionen gehören DHCP, statische IPv4- oder statische IPv6-Adressen.
 - b Geben Sie für statische 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 **Aktualisieren** klicken, um die aktuellen Einstellungen, die auf der virtuellen Maschine konfiguriert sind, zu importieren.
- 7 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**.
- 8 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.
- 9 Wiederholen Sie die Schritte [Schritt 5](#) bis [Schritt 8](#), um die Wiederherstellungs- oder Schutzeinstellungen zu konfigurieren, falls erforderlich.

Wenn Sie beispielsweise IP-Einstellungen für die Schutz-Site konfiguriert haben, können Sie die Einstellungen für die Wiederherstellungs-Site konfigurieren.
- 10 Wiederholen Sie den Konfigurationsvorgang für andere Netzwerkkarten, sofern erforderlich, indem Sie anfänglich eine andere Netzwerkkarte auswählen, wie in Schritt [Schritt 3](#) beschrieben.

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, wie in diesem Beispiel dargestellt.

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out Pfad_zur_Melddatei.xml
--vc vCenter_Server-Adresse
```

Um die Liste der Netzwerke auf die von einem bestimmten Wiederherstellungsplan benötigten einzuschränken, verwenden Sie in der Befehlszeile die Option `-plan`, wie in diesem Beispiel dargestellt:

```
dr-ip-reporter.exe
--cfg ..\config\vmware-dr.xml
--out Pfad_zur_Melddatei.xml
--vc vCenter_Server-Adresse
--plan Name_des_Wiederherstellungsplans
```

Hinweis Der Befehl fordert Sie normalerweise dazu auf, die von den Zertifikaten angegebenen Fingerabdrücke auf jeder Site zu überprüfen. Sie können die Überprüfungsanforderung unterdrücken, indem Sie die Option `-I` verwenden.

Anpassen der IP-Eigenschaften für mehrere virtuelle Maschinen

Das manuelle Konfigurieren der IP-Einstellungen für viele virtuelle Maschinen einer Wiederherstellungs-Site kann zeitaufwändig sein und es können Fehler in der Konfiguration auftreten.

Site Recovery Manager enthält das Tool „DR IP Customizer“, um den Konfigurationsvorgang für mehrere virtuelle Maschinen zu vereinfachen.

Sie verwenden das Tool „DR IP Customizer“, um benutzerdefinierte Netzwerkeinstellungen auf virtuelle Maschinen anzuwenden, wenn sie auf der Wiederherstellungs-Site gestartet werden. Sie übergeben dem Tool „DR IP Customizer“ die benutzerdefinierten 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.

In der [Kompatibilitätstabelle für vCenter Site Recovery Manager 5.5](#) finden Sie die Liste der Gastbetriebssysteme, für die Site Recovery Manager IP-Anpassungen unterstützt.

■ 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.

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.

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]
[--vc vCenter Server-Adresse]
[--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 8-1. DR IP Customizer-Optionen

Option	Beschreibung	Obligatorisch
-h [--help]	Zeigt Nutzungsinformationen zu dr-ip-customizer.exe an.	Nein
--cfg arg	Pfad zur XML-Konfigurationsdatei der Datei vmware-dr.xml des Site Recovery Manager Server.	Ja
--cmd arg	<p>Sie verwenden verschieden Befehle, um DR IP Customizer in verschiedenen Modi auszuführen.</p> <ul style="list-style-type: none"> ■ Der Befehl <code>apply</code> wendet die Netzwerkanpassungseinstellungen aus einer vorhandenen CSV-Datei auf die Wiederherstellungspläne auf den Site Recovery Manager Server-Instanzen an. ■ Der Befehl <code>generate</code> generiert eine Basis-CSV-Datei für alle virtuellen Maschinen, die Site Recovery Manager für eine vCenter Server-Instanz schützt. ■ Der Befehl <code>drop</code> entfernt die Wiederherstellungseinstellungen von den in der Eingabe-CSV-Datei angegebenen virtuellen Maschinen. <p>Geben Sie stets dieselbe vCenter Server-Instanz für die Befehle <code>apply</code> und <code>drop</code> an, die Sie zum Generieren der CSV-Datei verwendet haben.</p>	Ja
--csv arg	Pfad zur CSV-Datei, die als Eingabe verwendet werden soll.	Ja, wenn die Befehle <code>apply</code> und <code>drop</code> ausgeführt werden.
-o [--out] arg	Name der neuen CSV-Ausgabedatei, die mit dem Befehl <code>generate</code> erstellt werden soll. Wenn Sie den Namen einer vorhandenen CSV-Datei angeben, überschreibt der Befehl <code>generate</code> den aktuellen Inhalt.	Ja, wenn Sie den Befehl <code>generate</code> ausführen.
--vc arg	vCenter Server-Hostname. VM-IDs für die geschützten virtuellen Maschinen sind auf jeder Site unterschiedlich. Verwenden Sie dieselbe vCenter Server-Instanz zum Erstellen und Anwenden der CSV-Datei.	Ja
-i [--ignore-thumbprint]	Ignoriert die Eingabeaufforderung der vCenter Server-Fingerabdruckbestätigung.	Nein

Tabelle 8-1. DR IP Customizer-Optionen (Fortsetzung)

Option	Beschreibung	Obligatorisch
-e [--extra-dns-columns]	Veraltet.	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

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.

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 8-2. 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 einzelne 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 beider Sites verwendet werden.

Tabelle 8-2. 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.	<p>Anpassbar. Darf nicht leer sein.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ■ Eine Zeile, die alle Informationen zur virtuellen Maschine und einen DNS-Host enthält. ■ Eine Zeile, die nur den zweiten DNS-Host enthält. <p>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.</p>
DNS-Domäne	DNS-Domäne für diesen Adapter.	<p>Anpassbar. Darf leer bleiben.</p> <p>Wenn Sie einen Wert eingeben, müssen Sie das Format beispiel.firma.com verwenden.</p>
Net BIOS	Wählen Sie, ob auf diesem Adapter NetBIOS aktiviert werden soll.	<p>Anpassbar. Darf leer bleiben.</p> <p>Wenn die Spalte nicht leer bleibt, muss sie eine der folgenden Zeichenfolgen enthalten: <code>disableNetBIOS</code>, <code>enableNetBIOS</code> oder <code>enableNetBIOSviaDhcp</code>.</p>
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 8-2. 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 oder einer statischen IPv6-Adresse konfigurieren. Wenn Sie beispielsweise für IPv4 eine statische IP-Adresse festlegen, müssen Sie die IPv6-Adresse auf DHCP einstellen.
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 IPv4-Adresse oder einer statischen IPv6-Adresse konfigurieren. Wenn Sie beispielsweise für IPv6 eine statische IP-Adresse festgelegt haben, müssen Sie die IPv4-Adresse auf DHCP einstellen. Wenn Sie den 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. Daher 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 8-2. 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.

Eine Herausforderung bei der Darstellung von VM-Netzwerkconfigurationen 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 mehrere IP-Adressen für einen Netzwerkadapter oder mehrere DNS-Server-Adressen angegeben werden sollen, 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.

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 8-3. 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
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 8-4. 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

Tabelle 8-4. Festlegen statischer und DHCP 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	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 8-5. Festlegen statischer und DHCP IPv4- und IPv6-Adressen in einer geänderten CSV-Datei

VM-ID	VM-Nam e	vCen ter Ser- ver	Adap ter- ID	Pri- mä- rer WIN S	Se- kund ärer WIN S	IP-Ad- resse	Sub- netz- maske	Gate- way(s)	IPv6- Adres- se	Länge des IPv6- Sub- netz- präfi- xes	IPv6- Gate- way(s)	DNS- Server	DNS- Suf- fix(e)
protec- ted- vm-10 301	vm-3- win	vcen- ter- ser- ver- site-B	0										exam- ple.com
protec- ted- vm-10 301	vm-3- win	vcen- ter- ser- ver- site-B	0										eng.exa mple.co m
protec- ted- vm-10 301		vcen- ter- ser- ver- site-B	1	2.2.3. 4	2.2.3. 5	192.16 8.1.21	255.25 5.255. 0	192.16 8.1.1	dhcp			1.1.1.1	
protec- ted- vm-10 301		vcen- ter- ser- ver- site-B	2	2.2.3. 4	2.2.3. 5	dhcp			::ffff: 192.16 8.1.22	32	::ffff: 192.16 8.1.1	1.1.1.2	
protec- ted- vm-10 301	vm-3- win	vcen- ter- ser- ver- site-A	0										exam- ple.com
protec- ted- vm-10 301	vm-3- win	vcen- ter- ser- ver- site-A	0										eng.exa mple.co m
protec- ted- vm-10 301		vcen- ter- ser- ver- site-A	1			dhcp			::ffff: 192.16 8.0.22	32	::ffff: 192.16 8.0.1	::ffff: 192.16 8.0.25 0	

Tabelle 8-5. Festlegen statischer und DHCP IPv4- und IPv6-Adressen in einer geänderten CSV-Datei (Fortsetzung)

VM-ID	VM-Nam e	vCen ter Ser- ver	Adap ter- ID	Pri- mä- rer WIN S	Se- kund ärer WIN S	IP-Ad- resse	Sub- netz- maske	Gate- way(s)	IPv6- Adres- se	Länge des IPv6- Sub- netz- präfi- xes	IPv6- Gate- way(s)	DNS- Server	DNS- Suf- fix(e)
protec- ted- vm-10 301		vcen- ter- ser- ver- site-A	1									::ffff: 192.16 8.0.25 1	
protec- ted- vm-10 301		vcen- ter- ser- ver- site-A	2	1.2.3. 4	1.2.3. 5	192.16 8.0.22	255.25 5.255. 0	192.16 8.0.1				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.

Voraussetzungen

Verwenden Sie das Tool „DR IP Customizer“ auf einem Computer, der auf die vCenter Server-Instanzen in Ihrer Umgebung zugreifen kann.

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.

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

In diesem Beispiel verweist `dr-ip-customizer.exe` auf die Datei `vmware-dr.xml` des Site Recovery Manager Server und generiert die Datei `MassIPCust-generate-output.csv` für die vCenter Server-Instanz `vc04.eng.example.com`.

- 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.

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

In diesem Beispiel verweist `dr-ip-customizer.exe` auf die Datei `vmware-dr.xml` des Site Recovery Manager Server und wendet die Änderungen in der Datei `MassIPCustCSVs\MassIPCust-ipv6.csv` auf die vCenter Server-Instanz `vc04.eng.example.com` 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.

Erweiterte Site Recovery Manager - Konfiguration

9

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:

- [Konfigurieren des Schutzes für eine virtuelle Maschine oder eine Vorlage](#)
- [Konfigurieren der Ressourcenzuordnungen für eine virtuelle Maschine](#)
- [Festlegen eines nicht replizierten Datenspeichers für Auslagerungsdateien](#)
- [Wiederherstellen von virtuellen Maschinen über mehrere Hosts an der Wiederherstellungs-Site hinweg](#)
- [Ändern der Größe von Festplattendateien virtueller Maschinen während einer Replizierung mithilfe von Replizierungsspeichern](#)
- [Ändern der Größe von Festplattendateien virtueller Maschinen während einer Replizierung ohne die Verwendung von Replizierungsspeichern](#)
- [Neukonfigurieren der Site Recovery Manager-Einstellungen](#)

Konfigurieren des Schutzes für eine virtuelle Maschine oder eine Vorlage

Sie können die Schutzeigenschaften einer virtuellen Maschine oder Vorlage in einer Schutzgruppe ändern. Sie können die Ressourcenzuordnungen, angeschlossene Speichergeräte und ihre Datenspeicher sowie andere Eigenschaften der Konfiguration ändern, anhand derer Site Recovery Manager die virtuelle Maschine wiederherstellt.

Sie müssen den Schutz für virtuelle Maschinen konfigurieren, die den Status „Nicht konfiguriert“ oder „Zuordnung fehlt“ haben.

Wenn Sie eine Array-basierte Replizierung verwenden, kann das Bearbeiten der Eigenschaften einer virtuellen Maschine zum Hinzufügen oder Ändern von Speichergeräten, z. B. von Festplatten oder DVD-Laufwerken, den Schutz dieser Maschine beeinflussen, wenn Sie ein Gerät hinzufügen, das auf einem Datenspeicher gespeichert wird, der nicht repliziert wird oder von einer anderen Schutzgruppe geschützt wird.

- Wenn das neue Gerät auf einem replizierten Datenspeicher erstellt wird, der nicht Teil einer Schutzgruppe ist, wird der Datenspeicher zur geschützten Datenspeichergruppe der virtuellen Maschine hinzugefügt, ohne dass der Schutz der virtuellen Maschine beeinträchtigt wird.
- Wenn das neue Gerät auf einem replizierten Datenspeicher erstellt wird, der von einer anderen Schutzgruppe geschützt wird, verliert der Schutz der virtuellen Maschine seine Gültigkeit.
- Wenn das neue Gerät auf einem nicht replizierten Datenspeicher erstellt wird, verliert der Schutz der virtuellen Maschine seine Gültigkeit.
- Wenn Sie Storage vMotion zum Verschieben einer virtuellen Maschine auf einen nicht replizierten Datenspeicher oder auf einen replizierten Datenspeicher auf einem Array verwenden, für dessen Verwaltung (über einen SRA) Site Recovery Manager nicht konfiguriert wurde, 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.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Schutzgruppen** und wählen Sie die Schutzgruppe aus, die die zu konfigurierende virtuelle Maschine enthält.
- 2 Klicken Sie auf der Registerkarte **Virtuelle Maschinen** mit der rechten Maustaste auf eine virtuelle Maschine und wählen Sie **Schutz konfigurieren**.
- 3 Überprüfen und konfigurieren Sie im Fenster **Eigenschaften virtueller Maschinen** die Eigenschaften bei Bedarf.
 - a Klicken Sie auf **Ordner**, um einen alternativen Zielordner anzugeben.
 - b Klicken Sie auf **Wiederherstellungs-Pool**, um einen alternativen Ressourcenpool anzugeben, in den die wiederhergestellte virtuelle Maschine platziert wird.
 - c Wenn Sie den Schutz für eine Vorlage konfigurieren, klicken Sie auf **Wiederherstellungs-Host**, um einen alternativen Host anzugeben, der zum Wiederherstellen der virtuellen Maschine verwendet wird.

Dieser Schritt gilt nur für Vorlagen.
 - d Klicken Sie auf **Netzwerk**, um ein alternatives Wiederherstellungsnetzwerk für das Wiederherstellen der virtuellen Maschine anzugeben.
- 4 Klicken Sie auf **OK**, um die neue Konfiguration für die ausgewählte virtuelle Maschine zu übernehmen.

Konfigurieren der Ressourcenzuordnungen für eine virtuelle Maschine

Wenn Sie keine Bestandslistenzuordnungen für Ihre Site angegeben haben, müssen Sie Ressourcenzuordnungen für einzelne virtuelle Maschinen konfigurieren. Sie können Ressourcenzuordnungen nur dann konfigurieren, wenn keine Bestandslistenzuordnungen für die gesamte Site eingerichtet worden sind.

Wenn für eine Site Bestandslistenzuordnungen eingerichtet wurden, können Sie sie nicht außer Kraft setzen, indem Sie den Schutz einzelner virtueller Maschinen konfigurieren. Wenn Sie Bestandslistenzuordnungen für einige Mitglieder einer Schutzgruppe außer Kraft setzen müssen, verwenden Sie den vSphere-Client, um eine Verbindung zur Wiederherstellungs-Site aufzubauen und die Einstellungen der Platzhalter zu bearbeiten oder sie in einen anderen Ordner oder Ressourcenpool zu verschieben.

Vorgehensweise

- 1 Klicken Sie auf **Schutzgruppen** und navigieren Sie zu der Schutzgruppe, die die virtuelle Maschine enthält, die Sie konfigurieren möchten.
- 2 Klicken Sie auf der Seite „Virtuelle Maschinen“ mit der rechten Maustaste auf eine virtuelle Maschine und klicken Sie auf **Schutz konfigurieren**.

Sofern Sie Bestandslistenzuordnungen eingerichtet haben, werden diese angewendet.

- 3 Konfigurieren Sie die Zuordnungen nach Bedarf.

Bei den meisten virtuellen Maschinen können Sie die Ordner- und Rechenressourcenzuordnungen ändern. Weitere Informationen finden Sie unter [Konfigurieren des Schutzes für eine virtuelle Maschine oder eine Vorlage](#).

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 sie in einem nicht replizierten Datenspeicher erstellt werden.

Vorsicht Unter normalen Umständen sollten die Auslagerungsdateien im selben Datenspeicher wie die anderen 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 ebenfalls, dass Auslagerungsdateien nicht repliziert werden. Verhindern Sie die Replizierung von Auslagerungsdateien nur dann, wenn es absolut erforderlich ist.

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

Vorgehensweise

- 1 Klicken Sie im vSphere-Client mit der rechten Maustaste auf einen ESXi-Cluster und dann auf **Einstellungen bearbeiten**.
- 2 Klicken Sie auf der Seite „Einstellungen“ des Clusters auf **Speicherort der Auslagerungsdatei**, wählen Sie **Die Auslagerungsdatei in dem Datenspeicher speichern, der durch den Host angegeben ist** und klicken Sie auf **OK**.
- 3 Wählen Sie für jeden Host im Cluster einen nicht replizierten Datenspeicher.
 - a Wählen Sie einen Host und klicken Sie auf die Registerkarte **Konfiguration**.
 - b Klicken Sie im Bereich „Software“ auf **Speicherort der VM-Auslagerungsdatei** und dann in der oberen rechten Ecke des Hauptbereichs auf **Bearbeiten**.
 - c Wählen Sie auf der Seite „Speicherort der VM-Auslagerungsdatei“ einen nicht replizierten Datenspeicher aus und klicken Sie auf **OK**.
- 4 Bei eigenständigen Hosts, die nicht Teil eines Clusters sind, wählen Sie den Host aus und klicken Sie auf die Registerkarte **Konfiguration**.
- 5 Klicken Sie im Bereich „Software“ auf **Speicherort der VM-Auslagerungsdatei** und dann in der oberen rechten Ecke des Hauptbereichs auf **Bearbeiten**.
- 6 Wählen Sie **Speichern Sie die Auslagerungsdatei in einem der unten ausgewählten Datenspeicher für Auslagerungsdateien**, wählen Sie den Datenspeicher aus und klicken Sie auf **OK**.
- 7 Schalten Sie die virtuellen Maschinen im Cluster 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.
- 8 Durchsuchen Sie den Datenspeicher, den Sie für Auslagerungsdateien ausgewählt haben, und vergewissern Sie sich, dass VSWP-Dateien für die virtuellen Maschinen im Cluster vorhanden sind.

Wiederherstellen 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, in ihr eigenes Testnetzwerk gestellt. Jeder Test-Switch ist zwischen den Hosts isoliert. Folglich sind virtuelle Maschinen im sel-

ben Plan isoliert, wenn die Wiederherstellung beendet wird. 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.

Ändern der Größe von Festplattendateien virtueller Maschinen während einer Replizierung mithilfe von Replizierungsspeichern

vSphere Replication verhindert Sie daran, die Größe der Festplattendatei einer virtuellen Maschine während der Replizierung zu ändern. Wenn Sie Replizierungsspeicher für die Zielfestplatte verwendet haben, können Sie die Größe der Festplatte manuell ändern.

Vorgehensweise

- 1 Heben Sie die Konfiguration der Replizierung auf der virtuellen Maschine auf.
- 2 Ändern Sie die Größe der Festplatte auf der Quell-Site.
- 3 Ändern Sie die Größe der Zielfestplatte, die verbleibt, nachdem Sie die Konfiguration der Replizierung aufheben.
- 4 Konfigurieren Sie die Replizierung auf der virtuellen Maschine neu.

Ändern der Größe von Festplattendateien virtueller Maschinen während einer Replizierung ohne die Verwendung von Replizierungsspeichern

vSphere Replication verhindert Sie daran, die Größe der Festplattendatei einer virtuellen Maschine während der Replizierung zu ändern. Falls Sie während der Konfiguration der Zielfestplatte keine Replizierungsspeicher verwendet haben, löscht vSphere Replication die Zielfestplatte, wenn Sie die Replizierung beenden.

Wenn Sie anfänglich keine Replizierungsspeicher verwendet haben und die Größe einer VM-Festplatte ändern möchten, müssen Sie eine Testwiederherstellung durchführen, die wiederhergestellte virtuelle Maschine klonen und die Festplatte mithilfe von Replizierungsspeichern manuell neu konfigurieren.

Vorgehensweise

- 1 Führen Sie eine Testwiederherstellung der virtuellen Maschine durch.
- 2 Klonen Sie die wiederhergestellte virtuelle Maschine auf demselben Datenspeicher, auf dem die Replizierung erfolgt, nachdem Sie die Replizierung neu konfiguriert haben.
- 3 Stellen Sie die Testwiederherstellung wieder her.
- 4 Heben Sie die Konfiguration der Replizierung auf.
- 5 Ändern Sie die Größe der Festplatte auf der Quell-Site.
- 6 Ändern Sie die Größe der Festplatte der geklonten virtuellen Maschine auf der Ziel-Site.
- 7 Heben Sie die Registrierung der geklonten virtuellen Maschine auf der Ziel-Site auf, aber löschen Sie die Festplatten nicht.
- 8 Aktivieren Sie die Replizierung, indem Sie die Festplatten der geklonten virtuellen Maschine als Speicher verwenden.

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.

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 auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **localSiteStatus**.
- 3 Ändern Sie die Einstellungen nach Bedarf.

Option	Aktion
Ändern des Zeitraums, in dem Site Recovery Manager die CPU-Nutzung, den Festplattenspeicher und den freien Arbeitsspeicher auf der lokalen Site prüft	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.
Ändern des Zeitlimits, das Site Recovery Manager abwartet, um Alarme zur CPU-Nutzung, zum Festplattenspeicher und zum freien Arbeitsspeicher auf der lokalen Site auszulösen	Geben Sie einen neuen Wert im Textfeld localSiteStatus.eventFrequency ein.
Ändern des Prozentsatzes der CPU-Nutzung, der dazu führt, dass Site Recovery Manager ein Ereignis des Typs „Hohe CPU-Nutzung“ auslöst	Geben Sie einen neuen Wert im Textfeld localSiteStatus.maxCpuUsage ein.
Ändern des Prozentsatzes des freien Festplattenspeichers, der dazu führt, dass Site Recovery Manager ein Ereignis des Typs „Wenig Festplattenspeicher“ auslöst	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	Geben Sie einen neuen Wert im Textfeld localSiteStatus.minMemory ein.

- 4 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.

Beim Site Recovery Manager Server finden Protokollaustausche statt. Wenn Sie den Site Recovery Manager Server neu starten oder wenn eine Protokolldatei sehr groß wird, erstellt der Site Recovery Manager Server eine neue Protokolldatei und nimmt nachfolgende Protokollmeldungen in die neue Protokolldatei auf. Wenn der 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.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **logManager**.
- 3 Ändern Sie die Protokollierungseinstellungen.

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	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.Default aus.
Protokollierungsebene für das externe API-Modul einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.ExternalAPI aus.
Protokollierungsebene für vSphere Replication einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.HbrProvider aus.
Protokollierungsebene für das IP-Anpassungstool einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.IPCustomizer aus.
Protokollierungsebene für die Bestandszuordnung einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.InventoryMapper aus.
Protokollierungsebene für Lizenzierungsprobleme einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.Licensing aus.
Protokollierungsebene für Persistenzprobleme einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.Persistence aus.
Protokollierungsebene für Wiederstellungsvorgänge einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.Recovery aus. Standardmäßig ist die Wiederherstellungsprotokollierung auf Ausführlich (erweitert) gesetzt.
Protokollierungsebene für Wiederstellungskonfigurationsvorgänge einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.RecoveryConfig aus.
Protokollierungsebene für Array-basierte Replizierungsvorgänge einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.Replication aus.
Protokollierungsebene für Autorisierungsprobleme zwischen dem Site Recovery Manager Server und vCenter Server einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.ServerAuthorization aus.
Protokollierungsebene für die Sitzungsverwaltung einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.SessionManager aus.
Protokollierungsebene für den SOAP-Webservices-Adapter einstellen	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.

Option	Beschreibung
Protokollierungsebene für Speicherprobleme einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.Storage aus.
Protokollierungsebene für Meldungen aus dem Array-basierten Speicheranbieter einstellen	Wählen Sie eine Protokollierungsebene im Dropdown-Menü logManager.StorageProvider aus.

- 4 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-Services 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.customizationTimeout`
- `recovery.skipGuestShutdown`
- `recovery.powerOffTimeout`

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 wird durch den Systemaufbau bedingt, da im Falle, dass Site Recovery Manager geänderte erweiterte Einstellungen auf virtuelle Maschinen anwenden musste, auf denen Sie bereits den Schutz konfiguriert haben, dies zu unerwünschten Änderungen am Schutz dieser virtuellen Maschinen führen könnte.

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. Es

ist auch möglich, alle neuen erweiterten Einstellungen zu übernehmen. Entfernen Sie dazu den Schutz von einer virtuellen Maschine, indem Sie diese aus der Schutzgruppe entfernen, und fügen Sie sie anschließend wieder zur Schutzgruppe hinzu. Beim erneuten Hinzufügen der virtuellen Maschine zur Schutzgruppe werden die neueren erweiterten Einstellungen für die virtuelle Maschine übernommen.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **recovery**.
- 3 Ändern Sie die Einstellungen der Wiederherstellungs-Site.

Option	Aktion
Ändern der Zeitüberschreitung für die IP-Anpassung	Geben Sie einen neuen Wert im Textfeld recovery.customizationTimeout ein.
Ändern der Standardpriorität für das Wiederherstellen einer virtuellen Maschine	Geben Sie einen neuen Wert im Textfeld recovery.defaultPriority ein.
Aktivieren oder Deaktivieren der erzwungenen Wiederherstellung	Aktivieren Sie das Kontrollkästchen recovery.forceRecovery bzw. heben Sie die Aktivierung auf. Sie sollten die erzwungene Wiederherstellung nur dann aktivieren, wenn RTO durch eine mangelhafte Konnektivität zur Schutz-Site erheblich beeinträchtigt wird.
Ändern der Zeitüberschreitung für das Einschalten von Hosts in einem Cluster	Geben Sie einen neuen Wert im Textfeld recovery.hostPowerOnTimeout ein.
Ändern der Zeitüberschreitung für das Ausschalten des Gastbetriebssystems	Geben Sie einen neuen Wert im Textfeld recovery.powerOffTimeout ein. Der neue Wert für Zeitüberschreitungen gilt für alle Ausschaltungsaufgaben für virtuelle Maschinen an der Wiederherstellungs-Site.
Ändern der Verzögerung beim Starten von abhängigen Aufgaben nach dem Einschalten einer virtuellen Maschine	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	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	Aktivieren Sie das Kontrollkästchen recovery.skipGuestShutdown bzw. heben Sie die Aktivierung auf. Sie müssen diese Option auswählen, wenn auf geschützten virtuellen Maschinen VMware Tools nicht installiert ist und die Zeitüberschreitung für das Herunterfahren des Gasts nicht auf „0“ gesetzt ist. Wenn Sie diese Option nicht auswählen und VMware Tools nicht installiert ist, wird eine Wiederherstellung nach dem Schritt zum Herunterfahren der VMs auf der Wiederherstellungs-Site nicht fortgesetzt.

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

Ändern der Einstellungen für Remote-Sites

Sie können die Standardwerte ändern, die der Site Recovery Manager Server auf der Schutz-Site verwendet, um festzustellen, ob der Site Recovery Manager Server auf der Remote-Site zur Verfügung steht.

Site Recovery Manager überwacht die Verbindung zwischen der Schutz- 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 ändern, in der Site Recovery Manager Alarme auslöst.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **remoteSiteStatus**.
- 3 Ändern Sie die Einstellungen.

Option	Aktion
Ändern der Anzahl an Statusprüfungen von Remote-Sites (Ping-Befehle), die versucht werden, bevor die Prüfung als fehlgeschlagen betrachtet wird	Geben Sie einen neuen Wert im Textfeld remoteSiteStatus.pingFailedDelay ein.
Ändern der Anzahl an fehlgeschlagenen Ping-Befehlen, die ein Ereignis des Typs „Site ausgefallen“ auslöst	Geben Sie einen neuen Wert im Textfeld remoteSiteStatus.panicDelay ein.
Ändern des Zeitraums, in dem Site Recovery Manager prüft, ob der Site Recovery Manager Server auf der Remote-Site zur Verfügung steht	Geben Sie einen neuen Wert im Textfeld remoteSiteStatus.pingInterval ein.

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

Ändern der Zeitüberschreitung für das Erstellen von Platzhalter-VMs

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 auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **replication**.

- 3 Ändern Sie die Einstellung **replication.placeholderVmCreationTimeout**, um die Wartezeit (in Sekunden) beim Erstellen einer Platzhalter-VM zu ändern.
- 4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Ändern der Speichereinstellungen

Sie können die Einstellungen Ihres Speicher-Arrays anpassen, um festzulegen, wie Site Recovery Manager und vCenter Server mit dem Speicherreplizierungsadapter (SRA) kommunizieren.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **storage**.
- 3 Ändern Sie die Speichereinstellungen.

Option	Aktion
Ändern der Zeitüberschreitung für SRA-Updates	Geben Sie einen neuen Wert im Textfeld storage.commandTimeout ein.
Ändern der maximalen Anzahl gleichzeitiger SRA-Vorgänge	Geben Sie einen neuen Wert im Textfeld storage.maxConcurrentCommandCnt ein.
Ändern des Mindestabstands (in Sekunden) zwischen Datenspeichergruppen-Berechnungen	Geben Sie einen neuen Wert im Textfeld storage.minDsGroupComputationInterval ein.
Ändern des Zeitintervalls zwischen Status-Updates für laufende Datensynchronisierungsvorgänge	Geben Sie einen neuen Wert im Textfeld storage.querySyncStatusPollingInterval ein.
Ändern des Zeitintervalls zwischen Erkennungsprüfungen von Speicher-Arrays	Geben Sie einen neuen Wert im Textfeld storage.storagePingInterval ein.
Ändern der maximal zulässigen Dauer für Datensynchronisierungsvorgänge	Geben Sie einen neuen Wert im Textfeld storage.syncTimeout ein.

- 4 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 Speicherreplikationsadapter (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 ändern. Weitere Informationen zu diesen Werten finden Sie in der SRA-Dokumentation Ihres Array-Anbieters.

Vorgehensweise

- 1 Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **storageProvider**.
- 3 Ändern Sie die Einstellungen für den SAN-Anbieter.

Option	Aktion
Site Recovery Manager zwingen, Verbindungen von LUNs mit doppelten Volumes zu trennen und neu zu verbinden	Aktivieren Sie das Kontrollkästchen storageProvider.autoDetachLUNsWithDuplicateVolume .
Festlegen des Flags LVM.EnableResignature auf ESXi-Hosts während des Testens und der Wiederherstellung	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 dieses Flag auf 0 eingestellt gelassen, signiert Site Recovery Manager nur die von ihm verwalteten VMFS-Snapshot-Volumes neu.
Entfernen des snap-xx -Präfixes, das den Namen von wiederhergestellten Datenspeichern vorangestellt wird, nach einer ordnungsgemäßen Wiederherstellung erzwingen	Aktivieren Sie das Kontrollkästchen storageProvider.fixRecoveredDatastoreNames .
Hostprüfungen während des Testens und der Wiederherstellung verzögern	<p>SRAAs 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.</p> <p>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.</p> <p>Ändern Sie diesen Wert nur, wenn Probleme auftreten, weil Datenspeicher nicht verfügbar sind.</p>
Hostprüfungen während des Testens und der Wiederherstellung wiederholen	<p>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.</p> <p>In früheren Versionen haben Sie möglicherweise den Parameter <code>storageProvider.hostRescanRepeatCnt</code> verwendet, um eine Verzögerung bei Wiederherstellungen festzulegen. Verwenden Sie stattdessen den Parameter <code>storageProvider.hostRescanDelaySec</code>.</p>
Ändern des Zeitraums, den Site Recovery Manager wartet, bis eine erneute HBA-Prüfung abgeschlossen wird	Geben Sie einen neuen Wert im Textfeld storageProvider.hostRescanTimeoutSec ein.

Option	Aktion
Festlegen der Anzahl der Versuche von Site Recovery Manager, um ein VMFS-Volumen neu zu signieren	Geben Sie einen neuen Wert im Textfeld storageProvider.resignatureFailure-RetryCount ein.
Zeitüberschreitung für Neusignierung eines VMFS-Volumens einstellen	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.
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	Diese Option ist standardmäßig ausgewählt. Deaktivieren Sie das Kontrollkästchen storageProvider.storageVmotionVmxSearch , um diese Option zu deaktivieren.
VMX-Dateipfade festlegen, die Site Recovery Manager nach einem Storage vMotion-Vorgang nicht als mögliche VMX-Kandidatendateien berücksichtigen soll	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.
Ändern des Zeitraums, den Site Recovery Manager wartet, bis wiederhergestellte Datenspeicher zugänglich werden	Geben Sie einen neuen Wert im Textfeld storageProvider.waitForAccessibleDatastoreTimeoutSec ein. Ändern Sie diesen Wert, wenn Zeitüberschreitungen auftreten, die dadurch verursacht werden, dass Site Recovery Manager Datenspeicher überprüft, die noch nicht verfügbar sind. Diese Einstellung ist in Site Recovery Manager 5.5.1 und höheren Versionen verfügbar.
Ändern des Zeitraums, den Site Recovery Manager wartet, bis wiederhergestellte Datenspeicher zu vCenter Server hinzugefügt werden	Geben Sie einen neuen Wert im Textfeld storageProvider.waitForRecoveredDatastoreTimeoutSec ein. Ändern Sie diesen Wert, wenn Zeitüberschreitungen auftreten, die dadurch verursacht werden, dass Site Recovery Manager Datenspeicher überprüft, die noch nicht von vCenter Server erkannt wurden. Diese Einstellung ist in Site Recovery Manager 5.5.1 und höheren Versionen verfügbar.
Ändern des Zeitraums, den Site Recovery Manager wartet, bis VMFS-Volumen gemountet werden	Geben Sie einen neuen Wert im Textfeld storageProvider.waitForVmfsVolumesMountedStateTimeoutSec ein. Ändern Sie diesen Wert, wenn Zeitüberschreitungen auftreten, die dadurch verursacht werden, dass Site Recovery Manager VMFS-Volumen überprüft, bei denen das Mounten viel Zeit in Anspruch nimmt. Diese Einstellung ist in Site Recovery Manager 5.5.1 und höheren Versionen verfügbar.

- 4 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 auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- 2 Klicken Sie auf **vrReplication**.
- 3 Ändern Sie die vSphere Replication-Einstellungen.

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- (Point-in-Time-)Snapshots während Wiederherstellungen beibehalten	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 umgekehrte Replizierung während Vorgängen zum erneuten Schützen ändern	Geben Sie im Textfeld reverseReplicationTimeout 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 während Vorgängen zum erneuten Schützen die Replizierung umkehrt.
Zeitüberschreitungsperiode für vSphere Replication-Synchronisierungsvorgänge ändern	Geben Sie im Textfeld synchronizationTimeout einen neuen Wert ein. Ändern Sie diesen Wert, falls Zeitüberschreitungsfehler auftreten, wenn vSphere Replication virtuelle Maschinen an der Wiederherstellungs-Site synchronisiert.
Standard-RPO-Einstellungen für Replizierungen ändern	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.

- 4 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 von **Erweiterte Einstellungen** im vSphere-Client oder im Site Recovery Manager-Client-Plug-In bestimmte Optionen ändern. Zum Ändern anderer Einstellungen können Sie die Konfigurationsdatei `vmware-dr.xml` bearbeiten, die sich auf dem Site Recovery Manager Server befindet. 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 Klicken Sie mit der rechten Maustaste in der vCenter Server-Bestandsliste auf einen Cluster und wählen Sie **Einstellungen bearbeiten > vSphere DRS > Erweiterte Optionen** aus.
- 2 Legen Sie die Einstellung `srmMaxBootShutdownOps` fest.

Option	Beschreibung
Textfeld Option	Geben Sie <code>srmMaxBootShutdownOps</code> 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.

- 3 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
- 4 Melden Sie sich beim Site Recovery Manager Server-Host an.

- 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`.

- 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.

- Starten Sie den Site Recovery Manager Server neu, damit die neuen Einstellungen wirksam werden.
- Klicken Sie auf der Site Recovery Manager-Benutzeroberfläche auf **Sites**, klicken Sie mit der rechten Maustaste auf die Site, deren Einstellungen Sie ändern möchten, und wählen Sie **Erweiterte Einstellungen** aus.
- Wählen Sie **vrReplication** und erhöhen Sie den Wert der Einstellung `synchronizationTimeout`.
Der Standardwert ist 7200 und entspricht einer Zeitüberschreitungsperiode für Synchronisierungsvorgänge von 14400 Sekunden.
- Wählen Sie **storage** und erhöhen Sie den Wert der Einstellung `commandTimeout`.
Erhöhen Sie den Wert der Einstellung `commandTimeout` auf beispielsweise 3600 Sekunden.
- 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 von **Erweiterte Einstellungen** im vSphere-Client oder im Site Recovery Manager-Client-Plug-In bestimmte Optionen ändern. Zum Ändern anderer Einstellungen können Sie die Konfigurationsdatei `vmware-dr.xml` bearbeiten, die sich auf dem Site Recovery Manager Server befindet. 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 9-1. 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-Client, indem Sie mit der rechten Maustaste auf einen Cluster klicken und Einstellungen bearbeiten > vSphere DRS > Erweiterte Optionen auswählen. Durch diese Einstellung wird der Wert defaultMaxBootAndShutdownOpsPerCluster überschrieben, den Sie in der Datei <code>vmware-dr.xml</code> festlegen können. Sie können in der Datei <code>vmware-dr.xml</code> den globalen Wert defaultMaxBootAndShutdownOpsPerCluster festlegen und anschließend unterschiedliche srmMaxBootShutdownOps -Werte für einzelne Cluster im vSphere-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 <code>vmware-dr.xml</code> . Der Wert srmMaxBootShutdownOps , den Sie im vSphere-Client festlegen können, überschreibt den Wert defaultMaxBootAndShutdownOpsPerCluster . Sie können in der Datei <code>vmware-dr.xml</code> den globalen Wert defaultMaxBootAndShutdownOpsPerCluster festlegen und anschließend unterschiedliche srmMaxBootShutdownOps -Werte für einzelne Cluster im vSphere-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 <code>vmware-dr.xml</code> festlegen. Standardmäßig ist die Drosselung ausgeschaltet.

Tabelle 9-2. Einstellungen, die Zeitlimits für Zeitüberschreitungen ändern

Option	Beschreibung
synchronizationTimeout	<p>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 unter Erweiterte Einstellungen > vrReplication im Site Recovery Manager-Client-Plug-In. Der Standardwert ist 7200 und entspricht einer Zeitüberschreitungsperiode für Synchronisierungsvorgänge von 14400 Sekunden.</p>
commandTimeout	<p>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 unter Erweiterte Einstellungen > Speicher im Site Recovery Manager-Client-Plug-In. Der Standardwert ist fünf Minuten.</p>

Fehlerbehebung bei Site Recovery Manager

10

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:

- [Einschränkungen beim Schutz und der Wiederherstellung von virtuellen Maschinen](#)
- [Site Recovery Manager-Ereignisse und -Alarmer](#)
- [vSphere Replication-Ereignisse und -Alarmer](#)
- [Erfassen von Site Recovery Manager-Protokolldateien](#)
- [Zugreifen auf die vSphere Replication-Protokolle](#)
- [Beheben von Site Recovery Manager-Betriebsproblemen](#)

Einschränkungen beim Schutz und der Wiederherstellung von virtuellen Maschinen

Der Schutz und die Wiederherstellung von virtuellen Maschinen durch Site Recovery Manager unterliegen Einschränkungen.

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, sodass nach der Wiederherstellung Snapshots nicht mehr zur Verfügung stehen.

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 mit RDM-Festplattengeräten verbundenen virtuellen Maschinen

Der Schutz und die Wiederherstellung von mit einem RDM-Festplattengerät verbundenen virtuellen Maschinen werden anders 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 Modus.
- vSphere Replication unterstützt RDM-Geräte nur im virtuellen Modus sowohl für das Quell- als auch für das Zielgerät.

Geplante Migration von virtuellen Maschinen auf Datenspeichern, die SIOC verwenden

Sie können Site Recovery Manager nicht zum Durchführen einer geplanten Migration von virtuellen Maschinen auf Datenspeichern verwenden, bei denen Storage I/O Control (SIOC) aktiviert ist. Das Unmounten von Datenspeichern mit aktivierter SIOC ist nicht möglich. Sie können also nicht Teil einer geplanten Migration sein. Sie müssen SIOC auf in einem Wiederherstellungsplan enthaltenen Datenspeichern deaktivieren, bevor Sie eine geplante Migration durchführen.

Notfallwiederherstellung und neuer Schutz von virtuellen Maschinen auf Datenspeichern, die SIOC verwenden

Wenn Sie einen Wiederherstellungsvorgang mit aktivierter SIOC durchführen, wird die Wiederherstellung mit Fehlern durchgeführt. Nach der Wiederherstellung müssen Sie SIOC auf der Schutz-Site manuell deaktivieren und erneut eine geplante Migrationswiederherstellung durchführen. Sie können den Vorgang zum erneuten Schützen erst dann durchführen, wenn Sie eine geplante Migration erfolgreich durchgeführt haben.

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 beiden 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.

Schutz und Wiederherstellung von Active Directory-Domänencontrollern

Verwenden Sie Site Recovery Manager nicht, um Active Directory-Domänencontroller zu schützen. Active Directory bietet eine eigene Replizierungstechnologie und einen eigenen Wiederherstellungsmodus. Verwenden Sie die Active Directory-Replizierungstechnologie und Wiederherstellungsmodus-Technologien, um Notfallwiederherstellungssituationen zu bewältigen.

Verwendung 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 Wiederherstellungs-Plans 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.

Einschränkungen von vSphere Replication

vSphere Replication ist beim Replizieren virtueller Maschinen einigen Einschränkungen unterworfen.

Replizierung großer Mengen

vSphere Replication kann virtuelle Maschinen, die größer als 2 TB sind, mit den folgenden Einschränkungen replizieren:

- Wenn Sie eine virtuelle Maschine mit replizierten Festplatten über 2032 GB zurück auf eine ältere Version verschieben, kann vSphere Replication die virtuellen Maschinen nicht replizieren oder einschalten.
- Eine vollständige Synchronisierung großer Festplatten kann Tage dauern.
- vSphere Replication muss geänderte Blöcke verfolgen und belegt mehr Arbeitsspeicher auf größeren Festplatten.

- vSphere Replication verfolgt größere Blöcke auf Festplatten über 2 TB. Die Replizierungsleistung auf Festplatten über 2 TB kann sich von der Leistung auf Festplatten über 2 TB bei gleicher Arbeitslast unterscheiden, je nach Größe des Teils der Festplatte, der für einen bestimmten Satz geänderter Blöcke über das Netzwerk wechselt.
- Die Replikation verbraucht möglicherweise mehr oder weniger Bandbreite, je nach Arbeitslast und dem Wechsel der Blöcke auf der Festplatte während des RPO-Intervalls.

Unterstützung gemeinsam genutzter Festplatten

vSphere Replication kann in dieser Version keine virtuellen Maschinen replizieren, die vmdk-Dateien gemeinsam nutzen.

Site Recovery Manager -Ereignisse und -Alarmer

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.

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 fünf Minuten.
- Die Verbindungsüberwachung überspringt eine Anzahl an fehlgeschlagenen `Pings`. Sie können diese Anzahl mithilfe der Einstellung `remoteSiteStatus.pingFailedDelay` konfigurieren.
- 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.
- Site Recovery Manager fährt mit dem Senden von `RemoteSiteDownEvent`-Ereignissen fort, bis die Verbindung erneut hergestellt wurde.

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 **Alarme** der Site Recovery Manager-Benutzeroberfläche werden alle Site Recovery Manager-Alarme aufgelistet. 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.

Voraussetzungen

Damit Alarme E-Mail-Benachrichtigungen senden können, müssen Sie die **Mail**-Einstellungen im Menü **vCenter Server-Einstellungen** konfigurieren.

Vorgehensweise

- 1 Klicken Sie im linken Bereich auf **Sites** und wählen Sie eine Site aus.
- 2 Klicken Sie auf die Registerkarte **Alarme**, um eine Liste der Site Recovery Manager-Alarme anzuzeigen.
- 3 Klicken Sie mit der rechten Maustaste auf einen Alarm und wählen Sie anschließend **Einstellungen bearbeiten**.
- 4 Klicken Sie auf die Registerkarte **Aktionen**.
- 5 Klicken Sie auf **Hinzufügen**, um eine Aktion hinzuzufügen, die durchgeführt werden soll, wenn dieser Alarm ausgelöst wird.
- 6 Wählen Sie im Dropdown-Menü eine Aktion aus.

Option	Beschreibung
E-Mail senden	Die Standardaktion. Geben Sie im Textfeld Wert eine E-Mail-Adresse ein.
SNMP-Trap senden	Geben Sie im Textfeld Wert den Namen eines SNMP-Traps ein.
Skript ausführen	Geben Sie im Textfeld Wert den Pfad des auszuführenden Skripts ein.

- 7 Klicken Sie auf die Registerkarte **Allgemein**.

- 8 Aktivieren Sie das Kontrollkästchen **Diesen Alarm aktivieren**, um die Aktion für diesen Alarm zu aktivieren.

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 10-1. Site-Statusereignisse

Ereignisschlüssel	Ereignisbeschreibung	Ursache
UnknownStatusEvent	Unbekannter Status	Der Status des Site Recovery Manager Server ist nicht verfügbar
RemoteSiteDownEvent	Remote-Site nicht bereit	Site Recovery Manager Server hat die Verbindung zum Remote-Site Recovery Manager Server verloren.
RemoteSitePingFailedEvent	Anpingen der Remote-Site fehlgeschlagen	Ausfälle an der Remote-Site oder Probleme mit der Netzwerkverbindung.
RemoteSiteCreatedEvent	Remote-Site erstellt	Remote-Site wurde erstellt.
RemoteSiteUpEvent	Remote-Site bereit	Site Recovery Manager Server hat die Verbindung zum Remote-Site Recovery Manager Server wiederhergestellt.
RemoteSiteDeletedEvent	Remote-Site gelöscht	Remote-Site wurde gelöscht.

Schutzgruppenereignisse

Schutzgruppenereignisse bieten im Zusammenhang mit Schutzgruppen Informationen zu Aktionen und zum Status.

Diese Ereignisse lassen sich in drei Kategorien unterteilen:

- Informationsereignisse zur Schutzgruppenreplizierung
- Warnungsereignisse zur Schutzgruppenreplizierung
- Fehlerereignisse zur Schutzgruppenreplizierung

Tabelle 10-2. Informationsereignisse zur Schutzgruppenreplizierung

Ereignisschlüssel	Ereignisbeschreibung	Ursache
ProtectionGroup > CreatedEvent	Schutzgruppe wurde erstellt.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Erstellens einer Schutzgruppe gepostet.
ProtectionGroup > RemovedEvent	Schutzgruppe wurde entfernt.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Entfernens einer Schutzgruppe gepostet.
ProtectionGroup > ReconfiguredEvent	Schutzgruppe wurde neu konfiguriert.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Neukonfigurierens einer Schutzgruppe gepostet.
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.
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.
ProtectedVmReconfiguredProtectionSettingsEvent	Neu konfigurierte Schutzeinstellungen für VM.	Wird auf beiden vCenter Servern bei Abschluss der Festschreibungsphase im Rahmen des Neukonfigurierens der VM-Schutzeinstellungen gepostet.
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.
PlaceholderVmCreatedEvent	Die Platzhalter-VM wurde in der Bestandsliste des VMware vCenter Server erstellt.	Wird nur dann auf dem vCenter Server der Wiederherstellungs-Site gepostet, wenn die Platzhalter-VM als Ergebnis von Schutz oder Reparatur erstellt wird.
PlaceholderVmCreatedFromOldProductionVmEvent	Die Platzhalter-VM wurde in der Bestandsliste des VMware vCenter Server unter Verwendung der Identität der alten geschützten virtuellen Maschine erstellt.	Wird nur dann auf dem vCenter Server der Wiederherstellungs-Site gepostet, wenn die Platzhalter-VM als Ergebnis der Auslagerung für die alte geschützte virtuelle Maschine während oder nach dem erneuten Schutz erstellt wird.

Tabelle 10-3. Warnungseignisse zur Schutzgruppenreplizierung

Ereignisschlüssel	Ereignisbeschreibung	Ursache
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.
PlaceholderVmUnexpectedlyDeletedEvent	Virtuelle Maschine in Gruppe: Die Platzhalter-VM wurde aus der Bestandsliste des VMware vCenter Server entfernt.	Wird nur dann auf dem vCenter Server der Wiederherstellungs-Site gepostet, wenn erkannt wird, dass die Platzhalter-VM unerwarteterweise gelöscht oder aus der vCenter-Bestandsliste entfernt wurde.

Tabelle 10-4. Fehlerereignisse zur Schutzgruppenreplizierung

Ereignisschlüssel	Ereignisbeschreibung	Ursache
ProductionVmDeletedEvent	Virtuelle Maschine in Gruppe: Die geschützte virtuelle Maschine wurde aus der VMware vCenter Server-Bestandsliste entfernt.	Wird gepostet, wenn erkannt wird, dass die geschützte virtuelle Maschine gelöscht oder aus der vCenter-Bestandsliste entfernt wurde.
ProductionVmInvalidEvent	Virtuelle Maschine in Gruppe: Die Dateispeicherorte der geschützten virtuellen Maschine können zwecks Replizierung nicht aufgelöst werden.	Wird gepostet, wenn Geräte- oder Wiederherstellungsspeicherort-Änderungen gehandhabt werden, jedoch festgestellt wird, dass der Anbieter die Dateien der geschützten virtuellen Maschine nicht finden kann, um sie zu replizieren.

Wiederherstellungseignisse

Wiederherstellungseignisse bieten Informationen zu Aktionen und zum Status in Zusammenhang mit Site Recovery Manager-Wiederherstellungsvorgängen.

Tabelle 10-5. Wiederherstellungseignisse

Ereignis	Beschreibung	Ursache
RecoveryVmBegin	Der Wiederherstellungsplan hat damit begonnen, die angegebene virtuelle Maschine wiederherzustellen.	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.
RecoveryVmEnd	Der Wiederherstellungsplan hat die Wiederherstellung der virtuellen Maschine beendet.	Wird signalisiert, nachdem das letzte Skript nach dem Einschalten abgeschlossen ist oder nachdem bei der virtuellen Maschine ein Fehler aufgetreten ist, der die Wiederherstellung unterbricht.

Tabelle 10-5. Wiederherstellungsereignisse (Fortsetzung)

Ereignis	Beschreibung	Ursache
PlanCreated	Der Wiederherstellungsplan <i>Hostname</i> wurde erstellt.	Wird signalisiert, wenn ein neuer Plan erstellt wird. Wird an jede vCenter Server-Instanz gesendet, auf der der Plan gehostet wird.
PlanDestroy	Der Wiederherstellungsplan wurde gelöscht.	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.
PlanEdit	Der Wiederherstellungsplan wurde geändert.	Wird signalisiert, wenn ein vorhandener Plan bearbeitet wird.
PlanExecTestBegin	Der Wiederherstellungsplan hat einen Test begonnen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Wiederherstellungstest initiiert wird.
PlanExecTestEnd	Der Wiederherstellungsplan hat einen Test abgeschlossen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Wiederherstellungstest abgeschlossen ist.
PlanExecCleanupBegin	Der Wiederherstellungsplan hat eine Testbereinigung begonnen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Testbereinigung initiiert wird.
PlanExecCleanupEnd	Der Wiederherstellungsplan hat eine Testbereinigung abgeschlossen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Testbereinigung abgeschlossen ist.
PlanExecBegin	Der Wiederherstellungsplan hat eine Wiederherstellung begonnen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Wiederherstellung initiiert wird.
PlanExecEnd	Der Wiederherstellungsplan hat eine Wiederherstellung abgeschlossen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn eine Wiederherstellung abgeschlossen ist.
PlanExecReprotectBegin	Der Wiederherstellungsplan hat damit begonnen, einen Vorgang zum erneuten Schützen durchzuführen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Vorgang zum erneuten Schützen initiiert wird.
PlanExecReprotectEnd	Der Wiederherstellungsplan hat einen Vorgang zum erneuten Schützen abgeschlossen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Vorgang zum erneuten Schützen abgeschlossen ist.
PlanPromptDisplay	Der Wiederherstellungsplan zeigt eine Eingabeaufforderung an und wartet auf eine Eingabe des Benutzers.	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Eingabeaufforderungsschritt erkannt wird. Der Schlüssel ist ein eindeutiger Bezeichner für die Eingabeaufforderung.

Tabelle 10-5. Wiederherstellungsereignisse (Fortsetzung)

Ereignis	Beschreibung	Ursache
PlanPromptResponse	Der Wiederherstellungsplan hat eine Antwort auf die Eingabeaufforderung erhalten.	Wird auf der Wiederherstellungs-Site signalisiert, wenn ein Eingabeaufforderungsschritt geschlossen wird.
PlanServerCommandBegin	Der Wiederherstellungsplan hat damit begonnen, einen Befehl auf der Site Recovery Manager Server-Maschine auszuführen.	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.
PlanServerCommandEnd	Der Wiederherstellungsplan hat die Ausführung eines Befehls auf der Site Recovery Manager Server-Maschine abgeschlossen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager die Ausführung eines Callout-Befehls auf der Site Recovery Manager Server-Maschine abgeschlossen hat.
PlanVmCommandBegin	Der Wiederherstellungsplan hat damit begonnen, einen Befehl auf einer wiederhergestellten virtuellen Maschine auszuführen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager mit der Ausführung eines Callout-Befehls auf einer wiederhergestellten virtuellen Maschine begonnen hat.
PlanVmCommandEnd	Der Wiederherstellungsplan hat die Ausführung eines Befehls auf einer wiederhergestellten virtuellen Maschine abgeschlossen.	Wird auf der Wiederherstellungs-Site signalisiert, wenn Site Recovery Manager die Ausführung eines Callout-Befehls auf einer wiederhergestellten virtuellen Maschine abgeschlossen hat.

Speicher- und Speicheranbieter-Ereignisse

Speicher- und Speicheranbieterereignisse bieten Informationen zu Aktionen und statusbezogenem Speicher bzw. zu statusbezogenen Speicheranbietern.

Tabelle 10-6. SRA-Ereignisse

Ereignis	Beschreibung	Ursache
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.
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.
StorageAdaptChangeEvent	Eine neue Version des angegebenen SRAs wurde geladen.	Site Recovery Manager hat erkannt, dass ein bereits bekannter SRA aktualisiert wurde.

Tabelle 10-7. Array-Manager-Ereignisse

Ereignis	Beschreibung	Ursache
SAManagerAddedEvent	Der angegebene Array-Manager wurde mithilfe des angegebenen SRAs erstellt.	Der Benutzer hat einen Array-Manager hinzugefügt.
SAManagerRemovedEvent	Der angegebene Array-Manager wurde gelöscht.	Der Benutzer hat einen Array-Manager entfernt.
SAManagerReconfigEvent	Der angegebene Array-Manager wurde neu konfiguriert.	Der Benutzer hat die Eigenschaften eines Array-Managers bearbeitet.
SAManagerPingOkEvent	Das Anpingen des angegebenen Array-Managers war erfolgreich.	Der Site Recovery Manager Server hat einen Array-Manager erfolgreich angepingt.
SAManagerPingFailEvent	Anpingen des angegebenen Array-Managers fehlgeschlagen.	Beim Anpingen des Array-Managers ist ein Fehler aufgetreten.

Tabelle 10-8. Array-Paar-Ereignisse

Ereignis	Beschreibung	Ursache
SAPairDiscoveredEvent	Ein repliziertes Array-Paar wurde mit Array-Manager erkannt.	Ein vom Benutzer erstellter Array-Manager hat replizierte Array-Paare erkannt.
SAPairEnabledEvent	Ein repliziertes Array-Paar wurde mit Array-Manager aktiviert.	Der Benutzer hat ein Array-Paar aktiviert.
SAPairDisabledEvent	Ein repliziertes Array-Paar wurde mit Array-Manager deaktiviert.	Der Benutzer hat ein Array-Paar deaktiviert.
SAPairPingOkEvent	Das Anpingen des replizierten Array-Paars war erfolgreich.	Der Site Recovery Manager Server hat das Array-Paar erfolgreich angepingt.
SAPairPingFailEvent	Das Anpingen des replizierten Array-Paars ist fehlgeschlagen.	Beim Anpingen des Array-Paars ist ein Fehler aufgetreten.

Tabelle 10-9. Datenspeicherereignisse

Ereignis	Beschreibung	Ursache
StorageDsDiscoveredEvent	Replizierter Datenspeicher wurde erkannt.	Der Site Recovery Manager Server hat einen replizierten Datenspeicher erkannt.
StorageDsLostEvent	Der angegebene Datenspeicher wird nicht mehr repliziert.	Der Benutzer hat die Replizierung von den Datenspeicher stützenden Speichergeräten ausgeschaltet.
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.
StorageRdmLostEvent	Eine an der angegebenen virtuellen Maschine angehängte RDM wird nicht mehr repliziert.	Der Benutzer hat die Replizierung der die RDM stützenden LUN ausgeschaltet.

Tabelle 10-10. Schutzereignisse

Ereignis	Beschreibung	Ursache
SPDsProtEvent	Geschützter Datenspeicher wurde zur angegebenen Schutzgruppe hinzugefügt.	Der Benutzer hat den Datenspeicher in eine neue oder vorhandene Schutzgruppe aufgenommen.
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.
SPVmDiscoveredEvent	Eine replizierte virtuelle Maschine wurde erkannt.	Der Benutzer hat eine virtuelle Maschine auf einem replizierten Datenspeicher erstellt.
SPVmLostEvent	Die angegebene virtuelle Maschine wird nicht mehr repliziert.	Der Benutzer hat eine virtuelle Maschine aus dem replizierten Datenspeicher migriert.
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.
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.
SPDsReplicationLostEvent	Der Datenspeicher in der angegebenen Schutzgruppe wird nicht mehr repliziert.	Der Benutzer hat die Replizierung für Geräte ausgeschaltet, die den Datenspeicher stützen.
SPGroupProtRestoredEvent	Der Schutz der angegebenen Schutzgruppe wurde wiederhergestellt.	Die vorherigen (nicht leeren) Probleme einer Schutzgruppe wurden bereinigt.
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.
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.

Tabelle 10-10. Schutzereignisse (Fortsetzung)

Ereignis	Beschreibung	Ursache
SPVmdsReplicationLostEvent	Der von der angegebenen virtuellen Maschine verwendete Datenspeicher, der sich in der angegebenen Schutzgruppe befindet, wird nicht mehr repliziert.	Siehe Beschreibung.
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.
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.
SPCgDsMissingProtEvent	Der Datenspeicher der angegebenen Konsistenzgruppe muss in die angegebene Schutzgruppe aufgenommen werden.	Siehe Beschreibung.
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.
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.

Lizenzierungsereignisse

Lizenzierungsereignisse bieten Informationen zu Änderungen des Site Recovery Manager-Lizenzierungsstatus.

Tabelle 10-11. Lizenzierungsereignisse

Typ	Beschreibung	Inhalt
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.
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 bieten Informationen zu Änderungen an Site Recovery Manager-Berechtigungen.

Tabelle 10-12. Berechtigungsereignisse

Typ	Beschreibung	Inhalt
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 10-13. 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.

Tabelle 10-13. SNMP-Traps (Fortsetzung)

Ereignis	Beschreibung	Ursache
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.
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.

vSphere Replication -Ereignisse und -Alarme

vSphere Replication unterstützt die Ereignisprotokollierung. Sie können Alarme für jedes Ereignis definieren, das den Alarm auslöst, wenn das Ereignis eintritt. Mit dieser Funktion können Sie den Zustand Ihres Systems überwachen und potenzielle Probleme lösen, um eine zuverlässige Replizierung der virtuellen Maschine sicherzustellen.

Konfigurieren der vSphere Replication -Alarme

Sie können Alarme definieren und bearbeiten, um bei Eintreten eines bestimmten vSphere Replication-Ereignisses benachrichtigt zu werden.

Sie können einen Alarm erstellen, der bei Eintreten eines bestimmten Ereignisses ausgelöst wird, z. B. nach dem Konfigurieren einer virtuellen Maschine für die Replizierung. Siehe *Anzeigen und Bearbeiten der Alarmeinstellungen im vSphere Web Client* in der vSphere Web Client-Dokumentation.

Liste mit vSphere Replication -Ereignissen

vSphere Replication-Replizierung überwacht Replizierungen und die zugrunde liegende Replizierungsinfrastruktur und generiert unterschiedliche Arten von Ereignissen.

Tabelle 10-14. vSphere Replication -Ereignisse

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie	Ereignis-Ziel
vSphere Replication konfiguriert	Virtuelle Maschine wurde für vSphere Replication konfiguriert	com.vmware.vcHms.replication-ConfiguredEvent	Info	Virtuelle Maschine
Konfiguration von vSphere Replication wurde aufgehoben	Die Konfiguration der virtuellen Maschine für vSphere Replication wurde aufgehoben	com.vmware.vcHms.replication-UnconfiguredEvent	Info	Virtuelle Maschine
Der Host ist für vSphere Replication konfiguriert	Host wurde für vSphere Replication konfiguriert	com.vmware.vcHms.hostConfiguredForHbrEvent	Info	Hostsystem
Konfiguration des Hosts für vSphere Replication aufgehoben	Für einen Host mit der ID <Host Moid> des verwalteten Objekts wurde die Konfiguration für vSphere Replication aufgehoben	com.vmware.vcHms.hostUnconfiguredForHbrEvent	Info	Ordner
Virtuelle Maschine wurde nicht für vSphere Replication konfiguriert	Die virtuelle Maschine hat Probleme mit vSphere Replication und muss neu konfiguriert werden	com.vmware.vcHms.vmMissingReplicationConfigurationEvent	Fehler	Virtuelle Maschine

Tabelle 10-14. vSphere Replication -Ereignisse (Fortsetzung)

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie	Ereignis-Ziel
VM aus vSphere Replication entfernt	Die virtuelle Maschine wurde aus der vSphere Replication-Konfiguration entfernt	com.vmware.vcHms.vmReplicationConfigurationRemovedEvent	Info	Virtuelle Maschine
Gegen RPO verstoßen	Es wurde um <x> Minuten gegen das vSphere Replication-RPO der virtuellen Maschine verstoßen	com.vmware.vcHms.rpoViolatedEvent	Fehler	Virtuelle Maschine
RPO wiederhergestellt	Es liegt keine Verletzung des vSphere Replication-RPO der virtuellen Maschine mehr vor	com.vmware.vcHms.rpoRestoredEvent	Info	Virtuelle Maschine
Die vSphere Replication-Remote-Site ist getrennt	Die Verbindung zur vSphere Replication-Remote-Site <siteName> ist unterbrochen	com.vmware.vcHms.remoteSiteDownEvent	Fehler	Ordner
Die vSphere Replication-Remote-Site ist verbunden	Die Verbindung zur vSphere Replication-Remote-Site <siteName> wurde hergestellt	com.vmware.vcHms.remoteSiteUpEvent	Info	Ordner
VR-Server getrennt	vSphere Replication-Server <VR Server> getrennt	com.vmware.vcHms.hbrDisconnectedEvent	Info	Ordner
VR-Server erneut verbunden	vSphere Replication-Server <VR Server> erneut verbunden	com.vmware.vcHms.hbrReconnectedEvent	Info	Ordner
Ungültige vSphere Replication bereinigt	Die virtuelle Maschine <VM name> wurde von vCenter Server entfernt und ihr vSphere Replication-Zustand wurde bereinigt	com.vmware.vcHms.replicationCleanedUpEvent	Info	Ordner
Virtuelle Maschine von Replikat wiederhergestellt	Die virtuelle Maschine <VM Name> wurde von einem vSphere Replication-Image wiederhergestellt	com.vmware.vcHms.vmRecoveredEvent	Info	Virtuelle Maschine
vSphere Replication kann nicht auf den Datenspeicher zugreifen	vSphere Replication-Server kann nicht auf den Datenspeicher zugreifen	com.vmware.vcHms.datastoreInaccessibleEvent	Fehler	Datenspeicher

Tabelle 10-14. vSphere Replication -Ereignisse (Fortsetzung)

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie	Ereignis-Ziel
vSphere Replication hat das Hinzufügen einer Festplatte zu einer virtuellen Maschine gehandhabt	Eine Festplatte, die zur virtuellen Maschine <VM name> hinzugefügt wurde, wurde von vSphere Replication erkannt und behandelt. Hinzugefügte Festplatten: <Disk name>	com.vmware.vchms.handledVmDiskAddEvent	Info	Virtuelle Maschine
vSphere Replication hat das Entfernen einer Festplatte auf einer virtuellen Maschine gehandhabt	Eine Festplatte, die zur virtuellen Maschine <VM name> hinzugefügt wurde, wurde von vSphere Replication erkannt und behandelt. Hinzugefügte Festplatten: <Disk name>	com.vmware.vchms.handledVmDiskRemoveEvent	Info	Virtuelle Maschine
Speicherrichtlinie konnte nicht aufgelöst werden	Eine bestimmte Speicherrichtlinie für das bereitgestellte Storage Profile mit der ID <profile ID> und den bereitgestellten Datenspeicher mit der Managed-Objekt-ID <Moid> konnte nicht aufgelöst werden	com.vmware.vchms.failedResolvingStoragePolicyEvent	Fehler	Datenspeicher
vSphere Replication wurde angehalten	vSphere Replication wurde als Folge einer Konfigurationsänderung angehalten, z. B. wegen einer hinzugefügten Festplatte oder der Wiederherstellung eines Snapshots mit unterschiedlichem Festplattenstatus	hbr.primary.SystemPausedReplication	Fehler	Virtuelle Maschine
Ungültige vSphere Replication-Konfiguration	Ungültige vSphere Replication-Konfiguration	hbr.primary.InvalidVmReplicationConfigurationEvent	Fehler	Virtuelle Maschine
Synchronisierung gestartet	Synchronisierung gestartet	hbr.primary.DeltaStartedEvent	Info	Virtuelle Maschine
Anwendungskonsistente Synchronisierung abgeschlossen	Anwendungskonsistente Synchronisierung abgeschlossen	hbr.primary.AppQuiescedDeltaCompletedEvent	Info	Virtuelle Maschine

Tabelle 10-14. vSphere Replication -Ereignisse (Fortsetzung)

Ereignisname	Ereignisbeschreibung	Ereignistyp	Kategorie	Ereignis-Ziel
Dateisystemkonsistente Synchronisierung abgeschlossen	Dateisystemkonsistente Synchronisierung abgeschlossen	hbr.primary.FSQuiescedDeltaCompletedEvent	Warnung	Virtuelle Maschine
Nicht stillgelegte, absturzkonsistente Synchronisierung abgeschlossen	Nicht stillgelegte, absturzkonsistente Synchronisierung wurde abgeschlossen. Die Stilllegung ist fehlgeschlagen oder die virtuelle Maschine ist ausgeschaltet.	hbr.primary.UnquiescedDeltaCompletedEvent	Warnung	Virtuelle Maschine
Absturzkonsistente Synchronisierung abgeschlossen	Absturzkonsistente Synchronisierung abgeschlossen	hbr.primary.DeltaCompletedEvent	Info	Virtuelle Maschine
Starten der Synchronisierung fehlgeschlagen	Starten der Synchronisierung fehlgeschlagen	hbr.primary.FailedToStartDeltaEvent	Fehler	Virtuelle Maschine
Vollsynchronisierung gestartet	Vollsynchronisierung gestartet	hbr.primary.SyncStartedEvent	Info	Virtuelle Maschine
Vollsynchronisierung abgeschlossen	Vollsynchronisierung abgeschlossen	hbr.primary.SyncCompletedEvent	Info	Virtuelle Maschine
Vollsynchronisierung konnte nicht gestartet werden	Vollsynchronisierung konnte nicht gestartet werden	hbr.primary.FailedToStartSyncEvent	Fehler	Virtuelle Maschine
Synchronisieren abgebrochen	Synchronisieren abgebrochen	hbr.primary.DeltaAbortedEvent	Warnung	Virtuelle Maschine
Keine Verbindung zum VR-Server	Keine Verbindung zum vSphere Replication-Server	hbr.primary.NoConnectionToHbrServerEvent	Warnung	Virtuelle Maschine
Verbindung zum VR-Server wiederhergestellt	Verbindung zum VR-Server wurde wiederhergestellt	hbr.primary.ConnectionRestoredToHbrServerEvent	Info	Virtuelle Maschine
Die vSphere Replication-Konfiguration wurde geändert	Die vSphere Replication-Konfiguration wurde geändert	hbr.primary.VmReplicationConfigurationChangedEvent	Info	Virtuelle Maschine

Erfassen von Site Recovery Manager -Protokolldateien

Site Recovery Manager legt mehrere Protokolldateien mit Informationen an, die dem VMware-Support bei der Diagnose von Problemen helfen können. Sie können den Site Recovery Manager-Protokoll-Collector dazu verwenden, 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. Die Site Recovery Manager-Client-Protokolldateien enthalten Informationen zur Clientkonfiguration sowie Meldungen, die die Client-Plug-In-Vorgänge betreffen. 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.

Site Recovery Manager sorgt auch für das Erfassen von vSphere Replication-Protokolldateien als Teil des Site Recovery Manager-Protokollpakets. 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.

- [Sammeln von Site Recovery Manager-Protokolldateien über die Site Recovery Manager-Benutzeroberfläche](#)

Sie können Protokolle für Site Recovery Manager, die vSphere Replication-Appliance und vSphere Replication-Server auf einen vom Benutzer angegebenen Speicherort 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.

Sammeln von Site Recovery Manager -Protokolldateien über die Site Recovery Manager -Benutzeroberfläche

Sie können Protokolle für Site Recovery Manager, die vSphere Replication-Appliance und vSphere Replication-Server auf einen vom Benutzer angegebenen 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 auf **Sites** und wählen Sie eine Site aus.
- 2 Klicken Sie auf die Registerkarte **Übersicht** und klicken Sie auf **Systemprotokolle exportieren**.
- 3 Geben Sie im Textfeld **Speicherort für Downloads** einen Pfad ein oder klicken Sie auf **Durchsuchen**, um einen Speicherort auszuwählen.

- 4 (Optional) Deaktivieren Sie das Kontrollkästchen **VR-Systemprotokolle einbeziehen**, um das Herunterladen der vSphere Replication-Protokolldaten zu deaktivieren.

Standardmäßig werden vSphere Replication-Systemprotokolle heruntergeladen. Diese Protokolle enthalten Informationen zu vSphere Replication Management Server (VRMS), vSphere Replication-Servern und Replizierungsereignissen.

- 5 Klicken Sie zum Herunterladen der Protokolle auf **OK**.

Das Fenster **Systemprotokollpakete werden heruntergeladen** enthält Informationen zu den Protokollpaketen.

- Eine Liste mit allen Hostsystemen, dem Downloadstatus ihrer Protokollpakete und weitere Details.
- „Download-Details“ enthält Informationen zu Dateiname und Zielspeicherort des Protokollpakets.

Bei diesem Prozess werden keine Client-Protokolle gesammelt. Client-Protokolle müssen getrennt gesammelt werden.

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 **Startmenü** 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**.
- 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.

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 Ändern Sie den Speicherort der Core-Dumps auf dem Site Recovery Manager Server.

Ändern Sie hierzu den Abschnitt `<coreDump>` im Abschnitt `<log>`.

```
<log>
  <coreDump>C:\ProgramData\VMware\VMware vCenter Site Recovery
    Manager\DumpFiles</coreDump>
</log>
```

10 (Optional) Legen Sie die Protokollierungsebene für bestimmte Site Recovery Manager Server-Komponenten fest.

Sie können bestimmte Protokollierungsebenen für die Komponenten SoapAdapter, SanConfigManager, Recovery, Folders, Libs und HttpConnectionPool festlegen, indem Sie die entsprechenden `<level>`-Abschnitte ändern. Die verfügbaren Protokollierungsebenen sind „error“, „warning“, „info“, „trivia“ und „verbose“.

```
<level id="Recovery">
  <logName>Recovery</logName>
  <logLevel>trivia</logLevel>
</level>
```

11 (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>
```

12 Starten Sie den Dienst Site Recovery Manager Server neu, damit die Änderungen wirksam werden.

Zugreifen auf die vSphere Replication -Protokolle

Sie können die vSphere Replication-Protokolle zur Systemüberwachung und zur Fehlerbehebung verwenden. Möglicherweise benötigt ein VMware-Support-Mitarbeiter diese Protokolle bei einem Support-Anruf.

Wenn Sie auf die vSphere Replication-Protokolle zugreifen und sie herunterladen möchten, benötigen Sie Zugriff auf das Virtual Appliance Management Interface (VAMI) von vSphere Replication.

vSphere Replication wechselt die Protokolldatei, wenn sie eine Größe von 50 MB erreicht hat, und behält maximal 12 komprimierte Protokolldateien bei.

Informationen zum manuellen Kopieren der Protokolldateien finden Sie unter [Manuelles Zugreifen auf die vSphere Replication-Protokolle](#).

Voraussetzungen

- Stellen Sie sicher, dass die vSphere Replication-Appliance eingeschaltet ist.

Vorgehensweise

- 1 Stellen Sie in einem Webbrowser eine Verbindung zum VAMI der vSphere Replication-Appliance her.

Die URL des VAMI lautet `https://Adresse_der_VR-Appliance:5480`.

Sie können auf das VAMI auch über die Site Recovery Manager-Benutzeroberfläche zugreifen, indem Sie innerhalb der Ansicht vSphere Replication auf der Registerkarte **Übersicht auf VR-Appliance konfigurieren** klicken.

- 2 Klicken Sie auf die Registerkarte **VRM** und klicken Sie auf **Unterstützung**.

- 3 Klicken Sie auf **Generieren**, um ein .zip-Paket der aktuellen vSphere Replication-Protokolle zu generieren.

Es wird ein Link zu dem Paket angezeigt, das die Replizierungs- und Systemprotokolle enthält. Protokolldateien der vSphere Replication-Appliance und alle zusätzlich verbundenen vSphere Replication-Server sind in demselben Paket enthalten.

- 4 Klicken Sie auf den Link, um das Paket herunterzuladen.

- 5 (Optional) Klicken Sie auf **Löschen** neben den vorhandenen Protokollpaketen, um sie einzeln zu löschen.

Manuelles Zugreifen auf die vSphere Replication -Protokolle

Sie können die vSphere Replication-Protokolle zur Systemüberwachung und zur Fehlerbehebung kopieren und verwenden. Möglicherweise benötigt ein VMware-Support-Mitarbeiter diese Protokolle bei einem Support-Anruf.

Mit SCP oder Win SCP können Sie die Protokollordner und -dateien von der vSphere Replication-Appliance und von allen zusätzlichen vSphere Replication-Servern kopieren.

- /opt/vmware/hms/logs/
- /opt/vmware/var/log/lighttpd/
- /var/log/vmware/
- /var/log/boot.msg

Beheben von Site Recovery Manager -Betriebsproblemen

Wenn Probleme beim Erstellen von Schutzgruppen und Wiederherstellungsplänen, beim Failover, bei der Wiederherstellung oder bei der Gastanpassung auftreten, können Sie das Problem über die Fehlerbehebung lösen.

Site Recovery Manager verdoppelt die Anzahl der umgekehrten Schrägstriche, wenn Callouts ausgeführt werden

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-basierenden 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 einem Site Recovery Manager -Test-Failover bestehen

Site Recovery Manager unterstützt keine ESXi-Umgebungen, bei denen das Flag `LVM.enableResignature` auf 0 festgelegt ist.

Problem

Während eines Test- oder eines tatsächlichen Failovers legt Site Recovery Manager das Flag `LVM.enableResignature` auf 1 fest, sofern es nicht bereits festgelegt wurde. 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 ein Test-Failover durchführen oder ein tatsächliches Failover erfolgt.

Das Festlegen 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 eines Test-Failovers oder eines tatsächlichen Failover-Vorgangs 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 Zeitüberschreitung für das Erstellen von Platzhalter-VMs](#).

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.

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 eines Failovers werden einige virtuelle Maschinen innerhalb des Standardzeitlimits 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.
- Der Datenspeicher auf der Wiederherstellungs-Site ist voll.

Lösung

- 1 Überprüfen Sie, ob VMware Tools auf der virtuellen Maschine, die Sie wiederherstellen, installiert ist.

2 Überprüfen Sie die verfügbare Kapazität des Datenspeichers auf der Wiederherstellungs-Site.

Falls der Datenspeicher voll bzw. fast voll ist, kann das Problem behoben werden, indem das Zeitlimit für Gastanpassungen erhöht wird.

- a Wählen Sie im vSphere-Client den Host aus und klicken Sie auf **Konfiguration > Erweiterte Einstellungen**.
- b Ändern Sie den Parameter für die Anpassungszeitüberschreitung auf 1200 Sekunden.

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](#).

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 Speicheranbieterereinstellungen](#).

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`.

Skalierbarkeitsprobleme beim Replizieren vieler virtuellen Maschinen mit einem knappen RPO auf einen gemeinsam genutzten VMFS-Datenspeicher auf ESXi -Server 5.0

Die Leistung wird möglicherweise beeinträchtigt, wenn Sie eine große Anzahl an virtuellen Maschinen mit einem knappen RPO (Recovery Point Objective) auf eine einzige VMFS-Datenspeicher replizieren, auf den mehrere Hosts an der Wiederherstellungs-Site zugreifen können.

Problem

Dieses Problem tritt auf, wenn ESXi Server 5.0 an der Wiederherstellungs-Site ausgeführt wird. Es kann dazu führen, dass RPO-Ziele verfehlt werden.

Die Anzahl an virtuellen Maschinen, die erfolgreich auf einen einzigen gemeinsam genutzten VMFS-Datenspeicher repliziert werden können, erhöht sich bei großzügigeren RPO-Zielen.

Folgen Sie den Richtlinien beim Berechnen der Anzahl an virtuellen Maschinen, die Sie auf ein einziges VMFS-Volume an der Wiederherstellungs-Site replizieren sollen.

- Wenn alle Ihre virtuellen Maschinen ein RPO von 15 Minuten haben, wird die Leistung beeinträchtigt, wenn 50 bis 100 virtuelle Maschinen auf denselben VMFS-Datenspeicher repliziert werden.

- Wenn alle Ihre virtuellen Maschinen ein RPO von 30 Minuten haben, wird die Leistung beeinträchtigt, wenn 100 bis 200 virtuelle Maschinen auf denselben VMFS-Datenspeicher repliziert werden.

Wenn Sie heterogene RPO-Ziele in einer Schutzgruppe haben, berechnen Sie das harmonische Mittel der RPO-Ziele, wenn Sie die Anzahl an virtuellen Maschinen berechnen, die Sie auf ein einziges VMFS-Volume replizieren können. Wenn Sie beispielsweise 100 virtuelle Maschinen mit einem RPO von 20 Minuten und 50 virtuelle Maschinen mit einem RPO von 600 Minuten haben, berechnen Sie das harmonische Mittel des RPO folgendermaßen:

$$150 / (100/20 + 50/600) = \sim 30$$

In diesem Beispiel ähnelt die Konfiguration einem Setup mit 150 virtuellen Maschinen, wobei jede Maschine ein RPO von ungefähr 30 Minuten hat. In diesem Fall wird die Leistung beeinträchtigt, wenn diese 150 virtuellen Maschinen auf ein einziges VMFS-Volume repliziert werden.

Ursache

Dieses Problem betrifft nur VMFS-Datenspeicher, die von mehreren Hosts gemeinsam genutzt werden. Es tritt nicht bei Datenspeichern, die lokal für einen Host sind, oder bei anderen Datenspeichertypen auf, z. B. NFS. Dieses Problem betrifft nur Installationen, bei denen ESXi Server 5.0 ausgeführt wird.

Die Anzahl der vSphere Replication-Server spielt dabei keine Rolle. Diese Beschränkungen gelten für die Anzahl an virtuellen Maschinen, die Sie auf einen einzigen VMFS-Datenspeicher replizieren können.

Lösung

- 1 Führen Sie ein Upgrade von ESXi Server auf Version 5.1 oder höher auf der Wiederherstellungs-Site durch.
- 2 Falls Sie kein Upgrade von ESXi Server auf Version 5.1 oder höher durchführen können, verteilen Sie die replizierten virtuellen Maschinen neu oder passen Sie deren RPO an.
 - Reduzieren Sie die Anzahl an virtuellen Maschinen mit einem knappen RPO, die auf ein einziges VMFS-Volume repliziert werden, indem Sie beispielsweise eine große Anzahl an kleineren Datenspeichern einsetzen.
 - Erhöhen Sie das RPO der virtuellen Maschine, die auf ein einziges VMFS-Volume repliziert werden, um ein längeres, harmonisches, mittleres RPO zu erstellen.

Anwendungsstilllegung ändert sich in Dateisystemstilllegung während der Verschiebung durch vMotion auf einen älteren Host

vSphere Replication kann ein Replikat mit Anwendungsstilllegung für virtuelle Maschinen mit Windows Server 2008- und Windows 8-Gastbetriebssystemen erstellen, die auf einem Host mit ESXi 5.1 oder höher ausgeführt werden.

Problem

Der Host mit ESXi 5.1 oder höher befindet sich in einem Cluster mit Hosts älterer Versionen, und Sie verwenden vMotion, um die replizierte virtuelle Maschine auf einen älteren Host zu verschieben.

vSphere Replication erstellt anschließend ein Dateisystemstilllegungs-Replikat.

Ursache

Eine Mischung von Hosts mit ESXi 5.1 (oder höher) und älteren Hosts im Cluster erstellt ein Dateisystemstilllegungs-Replikat während der Verschiebung durch vMotion auf einen älteren Host. Der Vorgang sollte stattdessen ein Anwendungsstilllegungs-Replikat erstellen.

Lösung

Stellen Sie sicher, dass alle Hosts im Cluster ESXi 5.1 oder höher ausführen, bevor Sie mit vMotion eine virtuelle Windows Server 2008- bzw. Windows 8-Maschine mit Anwendungsstilllegung verschieben.

Neukonfigurieren der Replizierung auf virtuellen Maschinen ohne Datenspeicherzuordnung

Wenn Sie vor dem Konfigurieren von vSphere Replication auf mehreren virtuellen Maschinen die Datenspeicherzuordnungen nicht konfiguriert haben, schlägt die Konfiguration der Replizierung fehl.

Problem

Auf der Registerkarte **Virtuelle Maschinen** einer vSphere Replication-Site werden virtuelle Maschinen rot mit dem Status Datenspeicherzuordnungen wurden für diese VM nicht konfiguriert dargestellt.

Ursache

Sie haben vor dem Konfigurieren der Replizierung auf mehreren virtuellen Maschinen keine Datenspeicherzuordnungen konfiguriert. Sie müssen die Replizierung für jede virtuelle Maschine einzeln neu konfigurieren.

Lösung

- 1 Wählen Sie die Ansicht vSphere Replication in der Site Recovery Manager-Benutzeroberfläche aus.
- 2 Wählen Sie die vSphere Replication-Remote-Site aus und klicken Sie auf die Registerkarte **Virtuelle Maschinen**.
- 3 Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine mit dem Status Datenspeicherzuordnungen wurden für diese VM nicht konfiguriert und wählen Sie **Replizierung konfigurieren**.

Der RPO-Wert und etwaige Stilllegungsmethoden, die Sie festgelegt haben, als Sie versuchten, mehrere virtuellen Maschinen zu konfigurieren, sind bereits festgelegt.

- 4 Klicken Sie auf **Durchsuchen**, um den Zieldatenspeicher für die VMX-Datei auszuwählen, und dann auf **Weiter**.
- 5 Klicken Sie auf **Durchsuchen**, um den Zieldatenspeicher für die VMDK-Datei auszuwählen, und dann auf **Weiter**.
- 6 Wählen Sie einen vSphere Replication-Server an der Ziel-Site aus und klicken Sie auf **Weiter**.
- 7 Klicken Sie auf **Beenden**.

Nach Abschluss der Neukonfiguration wird die virtuelle Maschine mit der Ziel-Site synchronisiert.

- 8 Wiederholen Sie [Schritt 3](#) bis [Schritt 7](#) für alle virtuellen Maschinen, die den Status Datenspeicherzuordnungen wurden für diese VM nicht konfiguriert aufweisen.

Das Konfigurieren der Replizierung schlägt für virtuelle Maschinen mit zwei Festplatten auf unterschiedlichen Datenspeichern fehl

Wenn Sie versuchen, vSphere Replication auf einer virtuellen Maschine mit zwei in unterschiedlichen Datenspeichern enthaltenen Festplatten zu konfigurieren, schlägt die Konfiguration fehl.

Problem

Das Konfigurieren der Replizierung schlägt mit folgendem Fehler fehl: Mehrere Quellfestplatten mit den Geräteschlüsseln *Geräteschlüssel* verweisen auf denselben Zieldatenspeicher und Dateipfad.

Die Replizierungsgruppe verbleibt im Fehlerzustand.

Ursache

Dieses Problem tritt auf, weil vSphere Replication weder einen eindeutigen Datenspeicherpfad noch einen eindeutigen Dateinamen für die virtuelle Zielplatte generiert.

Lösung

Wenn Sie unterschiedliche Datenspeicher für die VMDK-Dateien an der geschützten Site auswählen, müssen Sie auch unterschiedliche Datenspeicher für die VMDK-Zieldateien an der sekundären Site auswählen.

Alternativ können Sie einen eindeutigen Datenspeicherpfad erstellen, indem Sie an der sekundären Site die VMDK-Dateien in getrennte Ordner eines einzelnen Zieldatenspeichers verschieben.

vSphere Replication - RPO-Verstöße

Es treten möglicherweise auch dann RPO-Verstöße auf, wenn vSphere Replication ordnungsgemäß auf der Wiederherstellungs-Site ausgeführt wird.

Problem

Wenn Sie virtuelle Maschinen replizieren, treten möglicherweise RPO-Verstöße ein.

Ursache

RPO-Verstöße treten möglicherweise aus einem der folgenden Gründen ein:

- Problem mit der Netzwerkkonnektivität zwischen Quellhosts und vSphere Replication-Servern auf der Ziel-Site.
- Das Ändern der IP-Adresse führt dazu, dass der vSphere Replication-Server eine andere IP-Adresse erhält.
- Der vSphere Replication-Server kann nicht auf den Zieldatenspeicher zugreifen.
- Langsame Bandbreite zwischen den Quellhosts und den vSphere Replication-Servern.

Lösung

- Durchsuchen Sie die Datei `vmkernel.log` am Quellhost nach der IP-Adresse des vSphere Replication-Servers, um zu sehen, ob es Netzwerkkonnektivitätsprobleme gibt.
- Stellen Sie sicher, dass es sich um dieselbe IP-Adresse des vSphere Replication-Servers handelt. Falls es eine andere IP-Adresse ist, konfigurieren Sie alle Replizierungen neu, sodass die Quellhosts die neue IP-Adresse verwenden.
- Durchsuchen Sie `/var/log/vmware/*hbrsrv*` auf der vSphere Replication-Appliance auf der Ziel-Site, um zu sehen, ob es Probleme mit dem Server beim Zugriff auf einen Zieldatenspeicher gibt.
- Weitere Informationen zum Berechnen der Bandbreitenanforderungen finden Sie unter KB 2037268 <http://kb.vmware.com/kb/2037268>.

Kein Starten von vSphere Replication nach dem Verschieben des Hosts

Wenn Sie den ESXi Server, auf dem die vSphere Replication-Appliance ausgeführt wird, in die Bestandsliste einer anderen vCenter Server-Instanz verschieben, sind vSphere Replication-Vorgänge nicht verfügbar. Dies gilt auch, wenn Sie vCenter Server erneut installieren.

Problem

Wenn die Verbindung zwischen der ESXi-Instanz, auf der vSphere Replication läuft, und vCenter Server getrennt wird und mit einer anderen vCenter Server-Instanz verbunden wird, kann nicht mehr auf die vSphere Replication-Funktionen zugegriffen werden. Wenn Sie versuchen, vSphere Replication neu zu starten, startet der Dienst nicht.

Ursache

Die OVF-Umgebung für die vSphere Replication-Appliance ist in der vCenter Server-Datenbank gespeichert. Wenn der ESXi-Host aus der vCenter Server-Bestandsliste entfernt wird, geht die OVF-Umgebung für die vSphere Replication-Appliance verloren. Diese Aktion deaktiviert die Mechanismen, die die vSphere Replication-Appliance verwendet, um sich bei vCenter Server zu authentifizieren.

Lösung

- 1 (Optional) Stellen Sie, sofern möglich, die vSphere Replication-Appliance erneut bereit und konfigurieren Sie alle Replizierungen. Dabei sollten Sie, sofern möglich, die vorhandenen `.vmdk`-Dateien als anfängliche Kopien wiederverwenden.
 - a Schalten Sie die alten vSphere Replication-Appliances aus.
 - b Entfernen Sie alle temporären `hbr*`-Dateien aus den Ordnern des Zieldatenspeichers.
 - c Stellen Sie neue vSphere Replication-Appliances bereit und verbinden Sie die Sites.
 - d Konfigurieren Sie alle Replizierungen, wobei Sie die `.vmdk`-Dateien des vorhandenen Replikats als anfängliche Kopien wiederverwenden.

- 2 (Optional) Wenn Sie die vSphere Replication-Appliance nicht erneut bereitstellen können, verwenden Sie die VAMI, um vSphere Replication mit der ursprünglichen vCenter Server-Instanz zu verbinden.
 - a Stellen Sie eine neue Verbindung zwischen dem ESXi-Host und vCenter Server her.
 - b Stellen Sie eine Verbindung mit der VAMI des vSphere Replication-Servers unter `https://vr-server-address:5480` her.
 - c Wählen Sie die Registerkarte **Konfiguration (Configuration)**.
 - d Geben Sie **username:password@vcenter_server_address** in das vCenter Server-Adressfeld ein, wobei "username" und "password" die Anmeldedaten des vCenter Server-Administrators sind.
 - e Geben Sie die korrekte ID des verwalteten Objekts der Appliance-VM in **ID des verwalteten Objekts der Appliance-VM** ein. Verwenden Sie den vCenter Server-Browser für verwaltete Objekte (MOB), um die Appliance-ID abzurufen.
 - f Klicken Sie auf **Speichern und Dienst neu starten**.

Wenn Sie die VAMI-Lösung verwenden, müssen Sie die Schritte jedes Mal, wenn Sie das vSphere Replication-Zertifikat ändern, wiederholen.

Unerwarteter vSphere Replication -Fehler führt zu einem generischen Fehler

vSphere Replication fügt eine generische Fehlermeldung in das Protokoll ein, wenn bestimmte unerwartete Fehler auftreten.

Problem

Bestimmte unerwartete vSphere Replication-Fehler führen zu der Fehlermeldung VRM-Server – generischer Fehler. Suchen Sie in der Dokumentation nach Informationen zur Fehlerbehebung.

Zusätzlich zu dem generischen Fehler enthält die Meldung detailliertere Informationen zu dem Problem, ähnlich den folgenden Beispielen.

- VRM-Server – generischer Fehler. Suchen Sie in der Dokumentation nach Informationen zur Fehlerbehebung. Die detaillierte Ausnahme ist: 'org.apache.http.conn.HttpHostConnectException: Verbindung mit `https://vCenter_Server-Adresse` verweigert'. Dieser Fehler bezieht sich auf Probleme beim Verbindungsaufbau zu vCenter Server.
- Fehler – VR-Synchronisierung für VRM-Gruppe *VM-Bezeichnung* fehlgeschlagen. Synchronisierungsüberwachung abgebrochen. Überprüfen Sie den Replizierungsdatenverkehr zwischen Quell-Host und VR-Zielservers auf mögliche Verbindungsprobleme. Die Synchronisierung wird automatisch fortgesetzt, sobald die Verbindungsprobleme behoben sind.. Dieses Problem bezieht sich auf einen Fehler im Synchronisierungsvorgang.

- Fehler – Die Replikation der virtuellen Maschine '*VM-Bezeichnung*' kann nicht umgekehrt werden. VRM-Server – generischer Fehler. Suchen Sie in der Dokumentation nach Informationen zur Fehlerbehebung. Die detaillierte Ausnahme ist: 'org.hibernate.exception.LockAcquisitionException: Transaction (Process ID 57) was deadlocked on lock resources with another process and has been chosen as the deadlock victim. Führen Sie die Transaktion erneut aus. Dieses Problem bezieht sich auf einen Deadlock in Microsoft SQL Server.

Ursache

vSphere Replication sendet diese Meldung, wenn Konfigurations- oder Infrastrukturfehler auftreten. Dies sind beispielsweise Netzwerkprobleme, Probleme mit der Datenbankverbindung oder eine Hostüberlastung.

Lösung

Prüfen Sie die detaillierte Ausnahmemeldung auf Informationen über das Problem. Je nach den Details der Meldung können Sie versuchen, den fehlgeschlagenen Vorgang zu wiederholen, vSphere Replication neu zu starten oder das Infrastrukturproblem zu beheben.

Das Generieren von Support-Paketen beeinträchtigt die Wiederherstellung von vSphere Replication

Wenn Sie ein vSphere Replication-Protokollpaket generieren und gleichzeitig versuchen, eine Wiederherstellung auszuführen, schlägt die Wiederherstellung möglicherweise fehl.

Problem

Das Generieren von Support-Paketen in stark ausgelasteten Umgebungen kann bei Wiederstellungsvorgängen vSphere Replication-Verbindungsprobleme verursachen. Die Wiederherstellung schlägt mit dem Fehler

```
„VRM-Server – generischer Fehler. Suchen Sie in der Dokumentation nach Informationen zur Fehlerbehebung.“ fehl. Die detaillierte Ausnahme ist: 'Fehlgeschlagenes Schreibschutzobjekt: object_ID'.
```

Ursache

Der vSphere Replication-Server ist blockiert, wenn das Protokollpaket generiert wird. Diese Situation tritt dann auf, wenn der Speicher für die virtuelle vSphere Replication überladen ist.

Lösung

Führen Sie die Wiederherstellung erneut durch. Wenn die Wiederherstellung immer noch fehlschlägt, überprüfen Sie die Anforderungen an die Speicherbandbreite des Clusters, auf dem vSphere Replication ausgeführt wird, sowie die Netzwerkbandbreite, falls es sich bei dem Speicher um NAS handelt.

Anfängliche vollständige Synchronisierung der Dateien virtueller Maschinen zum VMware Virtual SAN-Speicher ist langsam

Bei Verwendung des VMware Virtual SAN-Speichers und beim Konfigurieren von vSphere Replication auf mehreren virtuellen Maschinen nimmt die anfängliche vollständige Synchronisierung viel Zeit in Anspruch.

Problem

Wenn vSphere Replication mit dem Virtual SAN-Speicher verwendet und vSphere Replication auf einer großen Anzahl von virtuellen Maschinen gleichzeitig konfiguriert wird, führt dies dazu, dass die anfängliche vollständige Synchronisierung der Dateien der virtuellen Maschinen sehr langsam ist.

Ursache

Die anfängliche vollständige Synchronisierung generiert einen hohen E/A-Datenverkehr. Das gleichzeitige Konfigurieren zu vieler Replizierungen kann den Virtual SAN-Speicher überlasten.

Lösung

Konfigurieren Sie vSphere Replication auf Gruppen von maximal 30 virtuellen Maschinen gleichzeitig.

vSphere Replication -Vorgänge werden bei ansteigender Anzahl an Replizierungen langsam ausgeführt

Bei ansteigender Anzahl an virtuellen Maschinen, die Sie replizieren, können vSphere Replication-Vorgänge langsamer ausgeführt werden.

Problem

Die Reaktionszeiten für vSphere Replication-Vorgänge können bei der Replizierung mehrerer virtueller Maschinen steigen. Möglicherweise treten Zeitüberschreitungen bei der Wiederherstellung oder Fehler für einige virtuelle Maschinen sowie RPO-Verstöße auf.

Ursache

Jede virtuelle Maschine in einem Datenspeicher generiert reguläre Lese- oder Schreibvorgänge. Beim Konfigurieren von vSphere Replication auf den virtuellen Maschinen wird ein anderer Lesevorgang zu den regulären Lese- oder Schreibvorgängen hinzugefügt, wodurch die E/A-Last auf dem Speicher erhöht wird. Die Leistung von vSphere Replication hängt von der E/A-Last der virtuellen Maschinen ab, die Sie replizieren, und von den Funktionen der Speicherhardware. Wenn die durch die virtuellen Maschinen generierte Last, kombiniert mit den zusätzlichen E/A-Vorgängen, die vSphere Replication einführt, die Funktionen Ihrer Speicherhardware überschreitet, treten möglicherweise langsame Reaktionszeiten auf.

Lösung

Wenn die Reaktionszeiten beim Ausführen von vSphere Replication 30 ms übersteigen, reduzieren Sie die Anzahl der virtuellen Maschinen, die Sie auf den Datenspeicher replizieren. Erhöhen Sie alternativ die Hardwareleistung. Wenn Sie den Verdacht haben, dass die E/A-Last auf dem Speicher ein Problem darstellt, und Sie den VMware Virtual SAN-Speicher verwenden, überwachen Sie die E/A-Latenz unter Verwendung des Überwachungs-Tools in der Schnittstelle für Virtual SAN.