

# Storage Replication Adapter der Dell EMC ME4-Serie für vSphere

Benutzerhandbuch

## Anmerkungen, Vorsichtshinweise und Warnungen

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.
-  **VORSICHT:** Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.
-  **WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

# Inhaltsverzeichnis

<b>1 Installation und Konfiguration des SRA.....</b>	<b>4</b>
Informationen zu VMware Site Recovery Manager.....	4
Geplante Migration.....	4
Disaster Recovery.....	4
Gesicherte Standorte und Recovery-Standorte.....	5
SRM-Anforderungen.....	5
Konfigurieren der Speichersysteme der ME4-Serie.....	5
Konfigurieren der Replikation.....	5
Installation von SRM-Software.....	6
Installation der SRA-Software.....	6
Konfigurieren von SRM.....	7
<b>2 Verwenden von SRM für die Disaster Recovery.....</b>	<b>8</b>
Volume-Erkennung.....	8
Erstellen eines Recovery-Plans.....	8
Testen eines Recovery-Plans.....	9
Failover und Failback.....	9
Automatisches Failover.....	10
Erneute Sicherung.....	10
Automatisches Failback.....	10
<b>3 Fehlerbehebung.....</b>	<b>12</b>
<b>4 Optimale Geschäftsabläufe.....</b>	<b>15</b>

# Installation und Konfiguration des SRA

Der Storage Replication Adapter (SRA) der Dell EMC ME4-Serie für vSphere ermöglicht die umfassende Nutzung des VMware vCenter Site Recovery Manager (SRM) Version 6.5 oder höher. Wenn Sie die Replikationsfunktion des Speichersystems der ME4-Serie mit dem vCenter SRM kombinieren, bietet SRA eine automatisierte Lösung für die Implementierung und das Testen von Disaster Recovery zwischen geografisch getrennten Standorten. Außerdem können Sie dadurch SRM für geplante Migrationen zwischen zwei Standorten verwenden.

Themen:

- [Informationen zu VMware Site Recovery Manager](#)
- [Gesicherte Standorte und Recovery-Standorte](#)
- [SRM-Anforderungen](#)
- [Konfigurieren der Speichersysteme der ME4-Serie](#)
- [Installation von SRM-Software](#)
- [Installation der SRA-Software](#)
- [Konfigurieren von SRM](#)

## Informationen zu VMware Site Recovery Manager

Der vCenter Site Recovery Manager (SRM) ist eine Lösung für Business Continuity und Disaster Recovery, mit der Sie die Recovery von virtuellen vCenter-Maschinen zwischen einem Standort (dem gesicherten Standort) und einem anderen Standort (dem Recovery-Standort) planen, testen und durchführen können.

Zwei Arten von Recovery stehen zur Verfügung – geplante Migration und Disaster Recovery.

### Geplante Migration

Eine geplante Migration ist die ordnungsgemäße Stilllegung von virtuellen Maschinen am gesicherten Standort und die Inbetriebnahme derselben Maschinen am Recovery-Standort. Damit eine geplante Migration erfolgreich ausgeführt werden kann, müssen beide Standorte verfügbar und voll funktionsfähig sein.

### Disaster Recovery

Die Disaster Recovery ähnelt der geplanten Migration, erfordert jedoch nicht, dass beide Standorte verfügbar sind. Während einer Disaster Recovery werden Fehler bei den Vorgängen am gesicherten Standort gemeldet, aber ansonsten ignoriert.

SRM koordiniert den Recovery-Vorgang mit den zugrunde liegenden Replikationsmechanismen, sodass die virtuellen Maschinen am gesicherten Standort ordnungsgemäß heruntergefahren (für den Fall, dass die virtuellen Maschinen des gesicherten Standorts weiterhin verfügbar sind) und die replizierten virtuellen Maschinen eingeschaltet werden können. Die Recovery der gesicherten virtuellen Maschinen am Recovery-Standort orientiert sich an einem Recovery-Plan, der festlegt, in welcher Reihenfolge virtuelle Maschinen gestartet werden. Der Recovery-Plan gibt auch Netzwerkparameter an, wie z. B. IP-Adressen, und kann vom Benutzer angegebene Skripte umfassen, die ausgeführt werden können, um benutzerdefinierte Recovery-Maßnahmen durchzuführen.

Nachdem eine Recovery durchgeführt wurde, werden die ausgeführten virtuellen Maschinen nicht mehr gesichert. Um diesen verringerten Schutz auszugleichen, unterstützt SRM einen Vorgang für die erneute Sicherung von virtuellen Maschinen. Dieser Vorgang kehrt die Rollen

der zwei Standorte nach dem Backup des ursprünglich gesicherten Standorts um. Der Standort, bei dem es sich zuvor um den Recovery-Standort handelte, wird nun zum gesicherten Standort und der zuvor gesicherte Standort wird zum Recovery-Standort.

SRM ermöglicht es Ihnen, Recovery-Pläne zu testen. Sie können Tests unter Verwendung einer vorübergehenden Kopie der replizierten Daten so durchführen, dass der laufende Betrieb an den beiden Standorten nicht unterbrochen wird. Zudem können Sie Tests nach einem Vorgang zur erneuten Sicherung durchführen, um sicherzustellen, dass die neue Konfiguration des gesicherten Standorts/Recovery-Standorts gültig ist.

## Gesicherte Standorte und Recovery-Standorte

In einer typischen SRM-Installation bietet ein gesicherter Standort geschäftskritische Rechenzentrumsdienste. Bei dem gesicherten Standort kann es sich um einen beliebigen Standort handeln, an dem vCenter geschäftskritische Geschäftsanforderungen unterstützt.

Der Recovery-Standort ist eine alternative Einrichtung, zu dem diese Dienste migriert werden können. Der Recovery-Standort kann sich Tausende von Kilometern entfernt befinden. In der Regel befindet er sich in einer Einrichtung, die mit einer hohen Wahrscheinlichkeit nicht durch Umweltfaktoren, Infrastruktur oder andere Störungen beeinflusst wird, die sich auf den gesicherten Standort auswirken.

**ANMERKUNG:** Das SRA der ME4-Serie verbindet VMware SRM mit der Replikationsfunktion des Speichersystems, sodass Ihnen eventuell unterschiedliche Terminologie mit ähnlichen Bedeutungen begegnet. In der VMware-Benutzeroberfläche und -Dokumentation ist zum Beispiel von gesicherten und Recovery-Standorten die Rede. In der ME Storage Manager (MESM)-Benutzeroberfläche und -Replikationsdokumentation finden Sie die Begriffe primäre und sekundäre Volumes und Standorte.

## SRM-Anforderungen

Eine typische SRM-Konfiguration umfasst zwei geografisch getrennte Standorte mit TCP/IP-Verbindung, den gesicherten Standort und den Recovery-Standort. Der gesicherte Standort ist der Standort, der auf den Recovery-Standort zum Zwecke der Disaster Recovery repliziert wird. Jeder Standort enthält ein Speichersystem der Dell EMC ME4-Serie, VMware ESX-Server, einen Virtual Center (vCenter) Server und einen SRM-Server, der den SRM ausführt.

Nach dem Einrichten des gesicherten Standorts und des Recovery-Standorts und der Installation der erforderlichen Infrastruktur für den Netzwerkbetrieb zwischen den beiden Standorten können Sie die Software installieren und konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren der Speichersysteme der ME4-Serie](#).

## Konfigurieren der Speichersysteme der ME4-Serie

Wenn Ihre Speichersysteme der ME4-Serie noch nicht konfiguriert sind:

- 1 Befolgen Sie die Installationsanweisungen im *Dell EMC ME4-Serie der Dell EMC ME4-Serie*.
- 2 Stellen Sie sicher, dass beide Speichersysteme die gleiche Host-Schnittstellenkonfiguration (iSCSI oder FC oder Hybrid-FC/-iSCSI) aufweisen.

## Konfigurieren der Replikation

**ANMERKUNG:** Stellen Sie sicher, dass Sie den Namen des Speichersystems, die Benutzeranmeldedaten und die IP-Adressen für beide Speichersysteme festlegen, bevor Sie den SRA konfigurieren. Der SRA verwendet die gleichen Benutzeranmeldedaten für das lokale und das Remotespeichersystem. Wenn also unter „Benutzer verwalten“ an beiden Standorten dasselbe Kennwort vorhanden ist, erstellen Sie eine neue user ID für den SRA mit manage auf beiden Systemen. Weitere Informationen zur Einrichtung finden Sie unter [Optimale Geschäftsabläufe](#).

- 1 Verwenden Sie den ME Storage Manager (MESM), um Replikationssoftware zu konfigurieren. Befolgen Sie dabei die Anweisungen im Abschnitt „Replikation“ des Administratorhandbuchs, einschließlich der folgenden Einstellungen für SRA:
  - Snapshot-Anzahl: 3 (oder höher)
  - Snapshot-Verlauf: both
  - Snapshot-Aufbewahrung: high

- Auftragswarteschlange: `queue-latest`
- (optional) Snapshot-Basisname: `same-as-volume-name`

**ANMERKUNG:** Das Einstellen des Basisnamens wie angegeben erleichtert das Troubleshooting, da Replikations-Snapshots den gleichen Namen wie das Basis-Volume mit `_nnnn` angehängt haben (zeigt die Replikationsgenerierungsnummer an).

- 2 Verwenden Sie den MESM auf jedem System, um das andere System im Replikationssatz als Remotesystem zu definieren.
- 3 Verwenden Sie den MESM, um mindestens eine Replikation durchzuführen.
- 4 Verwenden Sie den MESM zum Planen von Replikationen vom gesicherten Standort zum Recovery-Standort. Dadurch wird sichergestellt, dass der SRM bei einem Notfall, bei dem der gesicherte Standort deaktiviert wird oder Hardware oder Dateien beschädigt werden, die zuletzt replizierte Kopie am Recovery-Standort für die Disaster Recovery verwenden kann. Es ist wichtig, bei der Verwendung von geplanten Replikation zu überprüfen, ob die Quelle der letzten Replikation sich in einem gültigen Status befand.

## Installation von SRM-Software

Sie müssen einen SRM-Server am gesicherten Standort und auch am Recovery-Standort installieren. Nachdem Sie die SRM-Server installiert haben, laden Sie das SRM-Client-Plug-in von einem der SRM-Server unter Verwendung des Menüs **Plug-ins verwalten** über den vSphere Client herunter. Verwenden Sie das SRM-Client-Plug-in für die Konfiguration und Verwaltung von SRM an jedem Standort.

SRM erfordert die Installation eines vCenter Servers an jedem Standort, bevor SRM installiert werden kann. Das SRM-Installationsprogramm muss in der Lage sein, während der Installation eine Verbindung mit diesem Server herzustellen. VMware empfiehlt die Installation von SRM auf einem System, das sich von dem System unterscheidet, auf dem vCenter Server installiert ist. Wenn SRM und vCenter Server auf dem gleichen System installiert sind, lassen sich administrative Aufgaben möglicherweise schwieriger ausführen. Wenn Sie ein Upgrade von SRM durchführen, werden nur Sicherungsgruppen und Recovery-Pläne während des Upgrades gespeichert, die sich in einem gültigen Status befinden. Sicherungsgruppen oder Recovery-Pläne in einem ungültigen Status werden verworfen.

So installieren Sie die SRM-Software:

- 1 Richten Sie vCenter Server an jedem Standort ein.
- 2 Erstellen Sie ein einzelnes Rechenzentrum in jeder Instanz von vCenter Server.
- 3 Fügen Sie die lokalen Hosts zu diesen Rechenzentren hinzu.
- 4 Laden Sie die VMware Site Recovery Manager-Software über den Link zum Produkt-Download unter dem folgendem Link auf der VMware-Website herunter:

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

- 5 Installieren Sie VMware Site Recovery Manager 6.5 oder höher an jedem Standort und befolgen Sie dabei die Anweisungen im VMware-Handbuch für *Site Recovery Manager Administration*.

Das Handbuch und die Versionshinweise für Ihre SRM-Version finden Sie auf der VMware-Dokumentationswebsite: <https://docs.vmware.com/en/Site-Recovery-Manager/index.html>

- 6 Konfigurieren Sie SRM zu diesem Zeitpunkt noch nicht. Zuerst [Installation der SRA-Software](#).

## Installation der SRA-Software

Laden Sie die Software für den SRA der Dell EMC ME4-Serie für Ihre Version von VMware SRM herunter und installieren Sie sie:

- 1 Rufen Sie <https://www.dell.com/support> auf.
- 2 Machen Sie die SRA-Software auf der Supportseite für das Speichersystem der ME4-Serie ausfindig.
- 3 Öffnen Sie die SRA-Setup-Datei und führen Sie sie aus.

Nachdem der SRA an jedem Standort installiert wurde, können Sie den SRM konfigurieren, wodurch das Plug-in die zwischen den Standorten replizierten Volumes erkennen kann.

# Konfigurieren von SRM

Nachdem Sie sowohl SRM als auch SRA installiert haben, führt die Registerkarte **Erste Schritte** des Hauptfensters von SRM Sie durch die erforderlichen Schritte für die Konfiguration. Detaillierte SRM-Konfigurationsanweisungen finden Sie im VMware-Handbuch zu *Site Recovery Manager Administration*.

Zum Konfigurieren von Speichersystemen der ME4-Serie in SRM ist Folgendes erforderlich:

- Die IP-Adressen der Speichersysteme der ME4-Serie.
- Ein Benutzername und ein Passwort für jedes Speichersystem (konfiguriert im MESM).

Nehmen Sie die folgenden Änderungen an den SRM-Einstellungen vor:

- Stellen Sie `storageProvider.autoResignatureMode` auf 1 ein (erforderlich).
- Stellen Sie `storageProvider.hostRescanRepeatCnt` auf 2 ein (erforderlich).
- Stellen Sie `Storage.commandTimeout` auf 1200 Sekunden ein (erforderlich).

# Verwenden von SRM für die Disaster Recovery

Nach der Konfiguration der Software für die Speichersystemreplikation und VMware SRM an lokalen und Remotestandorten und der Konfiguration von mindestens einem Replikationssatz verwenden Sie MESM zum Planen von Replikationen. Verwenden Sie dann SRM zum Erstellen und Testen von einem oder mehreren Recovery-Plänen. Zu diesem Zeitpunkt kann SRM Disaster Recovery, Failover und Failback sowie Vorgänge zur erneuten Sicherung bereitstellen.

Das Handbuch für VMware *Site Recovery Manager Administration* enthält detaillierte Anweisungen und Informationen hinsichtlich dieser Vorgänge. Das Handbuch steht auf der [VMware-Supportwebsite](#) zur Verfügung.

Themen:

- [Volume-Erkennung](#)
- [Erstellen eines Recovery-Plans](#)
- [Testen eines Recovery-Plans](#)
- [Failover und Failback](#)
- [Automatisches Failover](#)
- [Erneute Sicherung](#)
- [Automatisches Failback](#)

## Volume-Erkennung

SRM erfasst Informationen vom SRA darüber, welche Volumes repliziert werden. SRM vergleicht dann diese Liste mit den Volumes, die er in einer VMware-Umgebung erkennt.

Für SRM-geplante Migrationen in Situationen, bei denen es sich nicht um einen Notfall handelt, kann SRM eine Replikation initiieren, um sicherzustellen, dass die replizierten Daten aktuell sind.

In Disaster-Recovery-Situationen versucht SRM, eine aktuelle Replikation zu erstellen. Sollte dies nicht möglich sein, da beispielsweise der gesicherte Standort offline ist, verwendet SRM die neueste am Remotestandort verfügbare Replikation.

Verwenden Sie den Replikationszeitplaner, um regelmäßig Replikationen durchzuführen und dadurch Datenverlust in einem Notfall zu minimieren oder regelmäßig SRM-geplante Migrationen zu erstellen. Stellen Sie aber in jedem Fall sicher, dass die zu replizierenden Volumes aus dem gesicherten Standort einen gültigen Status aufweisen, sodass die neueste Replikation am Remotestandort in der Produktion verwendet werden kann.

Anweisungen zur Konfiguration von Replikationszeitplänen finden Sie im Kapitel zum Verwenden der Replikation im *Dell EMC ME4-Serie der Dell EMC ME4-Serie*.

## Erstellen eines Recovery-Plans

Erstellen Sie einen Recovery-Plan, um festzulegen, wie virtuelle Maschinen wiederhergestellt werden. Ein grundlegender Recovery-Plan umfasst Schritte, in denen Standardwerte verwendet werden, die steuern, wie virtuelle Maschinen in einer Sicherungsgruppe am Recovery-Standort wiederhergestellt werden. Sie können den Plan auf Ihre Anforderungen abstimmen. Recovery-Pläne unterscheiden sich von Sicherungsgruppen. Recovery-Pläne geben an, wie virtuelle Maschinen in einer oder mehreren Sicherungsgruppen am Recovery-Standort wiederhergestellt werden.

Die Registerkarte **Recovery** des SRM-Hauptfensters führt Sie durch die erforderlichen Schritte zum Erstellen, Testen und Ausführen eines Recovery-Plans. Ausführliche Anweisungen finden Sie im VMware-Handbuch für *Site Recovery Manager Administration*.

## Testen eines Recovery-Plans

Sie können automatisch eine unterbrechungsfreie, isolierte Testumgebung am Recovery-Standort durch Verwendung von Replikation und die Verbindung von virtuellen Maschinen mit Ihrem isolierten Testnetzwerk erstellen. Sie können Testergebnisse auch speichern, um sie zu einem beliebigen Zeitpunkt anzuzeigen und zu exportieren.

Beim Testen eines Recovery-Plans wird fast jeder Aspekt des Plans durchgespielt, wobei mehrere Zugeständnisse gemacht werden, um die Unterbrechung des laufenden Betriebs zu vermeiden. Während das Testen eines Recovery-Plans keine dauerhaften Auswirkungen auf die Standorte hat, hat das Ausführen eines Recovery-Plans bedeutende Auswirkungen auf beide Standorte.

Sie sollten Test-Recoverys so oft wie nötig durchführen. Das Testen eines Recovery-Plans hat keinen Einfluss auf die Replikation oder den laufenden Betrieb an beiden Standorten (obwohl die ausgewählten lokalen virtuellen Maschinen am Recovery-Standort unter Umständen vorübergehend ausgesetzt werden, wenn die Recoverys dazu konfiguriert sind). Sie können den Test eines Recovery-Plans jederzeit abbrechen.

Im Falle geplanter Migrationen stoppt eine Recovery die Replikation nach einer abschließenden Synchronisierung der Quelle und des Ziels. Beachten Sie, dass virtuelle Maschinen bei Disaster Recoverys auf den neuesten verfügbaren Status wiederhergestellt werden (festgelegt durch Recovery Point Objective, RPO). Nach Abschluss der letzten Replikation nimmt SRM Änderungen an beiden Standorten vor. Das Rückgängigmachen dieser Änderungen erfordert viel Zeit und Mühe. Deshalb müssen die Berechtigung zum Testen eines Recovery-Plans und die Berechtigung zum Ausführen eines Recovery-Plans separat zugewiesen werden.

Wenn SRM-Test-Failover an den Recovery-Standort angefordert werden, führt SRM die folgenden Schritte durch:

- 1 Bestimmt den neuesten Recovery-Punkt für jedes replizierte Volume.
  - 2 Erstellt einen beschreibbaren Test-Snapshot für jeden Recovery-Punkt mit einem Namen in der Form **sra***nnnnnn*, wobei *nnnnnn* eine monoton steigende Zahl ist.
  - 3 Ordnet die Test-Snapshots den entsprechenden ESXi-Hosts am Recovery-Standort zu.
- Wenn der Test beendet wird, wird die Zuweisung der Test-Snapshots aufgehoben und sie werden gelöscht.

## Failover und Failback

Failback bezeichnet das Zurücksetzen der Replikationsumgebung auf den ursprünglichen Zustand am gesicherten Standort vor dem Failover. Failback mit SRM ist ein automatisiertes Verfahren, das nach der Recovery erfolgt. Dies macht den Failback-Vorgang der gesicherten virtuellen Maschinen im Falle einer geplanten Migration relativ einfach. Wenn die gesamte SRM-Umgebung nach der Recovery intakt bleibt, erfolgt das Failback durch die Ausführung der Recovery-Schritte für die erneute Sicherung mit SRM, gefolgt von der erneuten Ausführung des Recovery-Plans. Dadurch werden die in ihren Sicherungsgruppen konfigurierten virtuellen Maschinen zurück zum ursprünglichen gesicherten SRM-Standort verschoben.

In Notfallszenarien variieren Failback-Schritte im Bezug auf den Ausfallumfang am gesicherten Standort. Zum Beispiel kann das Failover aufgrund eines Speichersystemfehlers oder aufgrund des Verlusts des gesamten Rechenzentrums durchgeführt worden sein. Die manuelle Konfiguration des Failbacks ist wichtig, weil der gesicherte Standort nach einem Notfall möglicherweise eine andere Hardware- oder SAN-Konfiguration hat. Unter Verwendung von SRM kann er nach der Konfiguration des Failbacks wie jedes geplante SRM-Failover verwaltet und automatisiert werden. Die Recovery-Schritte können sich abhängig von den Bedingungen des letzten Failovers unterscheiden. Wenn das Failback einem ungeplanten Failover folgt, ist unter Umständen ein vollständiges Re-Mirroring zwischen den beiden Standorten erforderlich. Dieser Schritt dauert normalerweise in einem Failback-Szenario am längsten.

Alle Recovery-Pläne in SRM umfassen einen ersten Versuch zum Synchronisieren von Daten zwischen den Sicherungs- und Recovery-Standorten, selbst bei einem Disaster-Recovery-Szenario.

Während der Disaster Recovery wird ein erster Versuch zum Herunterfahren der virtuellen Maschinen der Sicherungsgruppe und Herstellen einer endgültigen Synchronisierung zwischen den Standorten unternommen. Dadurch soll sichergestellt werden, dass virtuelle Maschinen statisch sind und stillgelegt wurden, bevor der Recovery-Plan ausgeführt wird, um Datenverlust nach Möglichkeit zu minimieren. Wenn der

gesicherte Standort nicht mehr verfügbar ist, wird der Recovery-Plan weiterhin ausgeführt und zum Abschluss gebracht, selbst wenn Fehler auftreten.

Dieses neue Attribut minimiert die Wahrscheinlichkeit von Datenverlust während einer Disaster Recovery und gleicht so die Anforderung an Konsistenz von virtuellen Maschinen mit der Fähigkeit zur Erzielung von strikten Recovery Point Objectives aus.

## Automatisches Failover

SRM automatisiert die Ausführung von Recovery-Plänen und stellt so eine präzise und konsistente Durchführung sicher. Über den vCenter Server erhalten Sie einen vollständigen Überblick und vollständige Steuerungsmöglichkeiten im Hinblick auf Prozesse, einschließlich des Status der einzelnen Schritte, Fortschrittanzeigen und ausführlicher Beschreibungen der Fehler, die eventuell auftreten.

Wenn es zu einem Notfall kommt und ein tatsächlicher SRM-Failover angefordert wird, führt der SRA die folgenden Schritte durch:

- 1 Auswählen der replizierten Volumes.
- 2 Identifizieren und Entfernen aller unvollständigen Remotekopien, die gerade ausgeführt werden, und Darstellen der zuletzt abgeschlossenen Remotekopie als primäres Volume.
- 3 Konvertieren von Remote-Volumes in primäre Volumes und Konfigurieren von Authentifizierung für ESXi-Hosts zum Mounten.

Wenn ein tatsächliches Failover aus irgendeinem Grund nicht vollständig ausgeführt wird, kann das Failover beliebig oft aufgerufen werden, um einen Abschluss der Ausführung zu versuchen. Wenn zum Beispiel nur ein Volume aufgrund eines vorhandenen normalen Snapshots nicht wiederhergestellt werden konnte, könnten Sie den Snapshot manuell löschen und das Failover erneut anfordern.

## Erneute Sicherung

Nachdem ein Recovery-Plan oder eine geplante Migration ausgeführt wurde, gibt es häufig Fälle, in denen die Umgebung weiterhin gegen einen Ausfall geschützt werden muss, um ihre Ausfallsicherheit zu gewährleisten und Disaster-Recovery-Ziele zu erfüllen.

Die erneute Sicherung ist eine SRM-Erweiterung für Recovery-Pläne, die nur zur Verwendung mit Speichersystemreplikation vorgesehen ist. Sie ermöglicht es der Umgebung am Recovery-Standort, Replikation und Sicherung der ursprünglichen Umgebung synchron durchzuführen.

Nach einem Failover des Recovery-Standorts wird durch die erneute Sicherung der Umgebung eine Synchronisierung vorgenommen und ein Versuch zur Replikation der Daten zwischen den Sicherungsgruppen unternommen, die am Recovery-Standort und am zuvor gesicherten primären Standort ausgeführt werden.

Durch diese Fähigkeit zur erneuten Sicherung einer Umgebung wird sichergestellt, dass Umgebungen sogar nach einem Standort-Recovery-Szenario gegen Ausfall gesichert werden. Darüber hinaus ermöglicht sie das automatisierte Failback zu einem primären Standort nach einer Migration oder einem Failover.

## Automatisches Failback

Sie können einen automatisierten Failback-Workflow einrichten, um die gesamte Umgebung vom Recovery-Standort wieder zurück zum primären Standort zu übertragen.

Das Failback erfolgt, nachdem die erneute Sicherung sichergestellt hat, dass die Datenreplikation und -synchronisierung am ursprünglichen primären Standort implementiert wurden.

Beim automatischen Failback wird der gleiche Workflow ausgeführt, der auch für die Migration der Umgebung zum gesicherten Standort verwendet wurde. Dadurch wird sichergestellt, dass die geschäftskritischen Systeme, die durch den Recovery-Plan abgedeckt werden, zurück in ihre ursprüngliche Umgebung übertragen werden. Der Workflow wird nur dann ausgeführt, wenn die erneute Sicherung erfolgreich abgeschlossen wird. Failback ist bei Speichersystemreplikation verfügbar.

Failback stellt Folgendes sicher:

- Alle virtuellen Maschinen, die zunächst zum Recovery-Standort migriert wurden, werden zurück zum primären Standort verschoben.
- Umgebungen, in denen Tests zur Disaster Recovery mit Live-Umgebungen und echten Migrationen durchgeführt werden müssen, können zurück zu ihrem ursprünglichen Standort verschoben werden.
- Vereinfachte Recovery-Prozesse ermöglichen die Rückkehr zum Standardbetrieb nach einem Ausfall.
- Ein Failover kann im Falle eines Notfalls oder im Falle von geplanten Migrationen stattfinden.

# Fehlerbehebung

VMware vCenter Server verwendet den SRA, um jedes Mal eine detaillierte Fehlermeldung anzuzeigen, wenn ein Recovery-Schritt fehlschlägt.

Der SRA erstellt auch eine Protokolldatei mit dem Namen `sra.log`, die jedes SRM-Ereignis und jeden CLI-Befehl auf Speichersystemen der ME4-Serie anzeigt. Durch die Untersuchung der Fehlermeldungen und dieser Protokolldatei haben Sie häufig genügend Informationen, um Fehler zu korrigieren. Wenn Sie weitere Hilfe benötigen, nehmen Sie bitte Kontakt mit VMware auf, um Support zu erhalten.

**Tabelle 1. SRA-Fehlermeldungen und empfohlene Maßnahmen**

Nachrichtennummer	Nachricht	Empfohlene Maßnahme
1002	VMware Site Recovery Manager Version 6.5 wurde nicht auf diesem System gefunden.	Installieren Sie VMware SRM 6.5 oder höher und wiederholen Sie dann das SRA-Installationsverfahren.
1003	XML-Ausgabe zu „{file}“ ist fehlgeschlagen: {error}	Stellen Sie sicher, dass der angegebene Dateispeicherort vorhanden ist, über ausreichend Speicherplatz verfügt und nicht schreibgeschützt ist.
1004	Installationsoption wird auf diesem System nicht unterstützt	Informationen hierzu finden Sie in den SRA-Installationsanweisungen.
1005	Eine native Version von Perl muss beim Aufrufen dieser Option verwendet werden.	Stellen Sie sicher, dass Sie die mit der VMware SRM-Software installierte <code>Perl.exe</code> -Version verwenden.
1006	Zeitüberschreitung beim Warten auf die Anzeige von Volume {volume} auf dem Speichersystem {arrayname} in {file}:{line}.	Stellen Sie sicher, dass das angegebene Volume auf dem Speichersystem erstellt wurde, und wiederholen Sie den Vorgang.
1007	Speichersystem „{systemName}“ ist nicht zur Verwendung mit diesem SRA lizenziert.	Wenden Sie sich an Ihren Speichersystemanbieter, um sicherzustellen, dass dieses System unterstützt wird, und um Replikations- und SRA-Lizenzschlüssel anzufordern.
1008	Kein WWN für Volume „{primary}“ gefunden.	Stellen Sie sicher, dass das angegebene Volume für die Replikation konfiguriert wurde.
1009	discoverDevices: WWN für temporären Snapshot „{serialNumber}“ ({name}) konnte nicht bestimmt werden.	Überprüfen Sie, ob der angegebene Snapshot von einem vorherigen Test übrig war und gelöscht werden kann.
1010	Recovery-Punkt für temporären Snapshot „{serialNumber}“ ({name}) konnte nicht gefunden werden.	Überprüfen Sie, ob der angegebene Snapshot von einem vorherigen Test übrig war und gelöscht werden kann.
1011	discoverDevices: WWN für hochgestuftes Volume „{secondaryName}“ ({secondary}) konnte nicht gefunden werden.	Überprüfen Sie den Status des angegebenen Volumes und die Integrität des Speichersystems und wiederholen Sie den Vorgang.
1013	Kein gültiger Synchronisierungspunkt für {volume} vorhanden.	Verwenden Sie in MESM die Snapshot-Tabelle, um zu überprüfen, ob das angegebene Volume vollständig vom gesicherten Standort repliziert wurde. Weitere Informationen finden Sie im Administratorhandbuch.
1014	Es konnte kein Snapshot für Volume {vol} exportiert werden.	Ein zuvor vom SRA erstellter Snapshot ist bereits für das angegebene Volume vorhanden. Nur ein exportierter Snapshot ist je Replikationsziel-Volume zulässig. Löschen Sie den vorhandenen Snapshot und wiederholen Sie diesen Vorgang.

Nachricht nummer	Nachricht	Empfohlene Maßnahme
1018	Unbekannter oder fehlender PeerId-Parameter „{PeerId}“ in {command}-Anforderung.	Stellen Sie sicher, dass jedes Speichersystem den Namen der zugehörigen Replikations-Peers richtig meldet und dass sich die Speichersystemnamen nicht verändert haben, seit SRM konfiguriert wurde. Wenn der Name des Speichersystems geändert wurde, löschen Sie Remotesystemeinträge auf jedem Speichersystem nach Bedarf und erstellen Sie sie neu. Falls das Problem nach dem Neustart des SRM weiterhin auftritt, erstellen Sie die Konfiguration des Speichersystempaars in SRM neu.
1020	Peer-Volume für lokales Volume {localsn} konnte nicht gefunden werden.	Stellen Sie sicher, dass das angegebene Volume als Teil eines Replikationssatzes eingerichtet wurde.
1021	Ungültige oder fehlende Parameter in der „{cmd}“-Anforderung des SRM vom SRA enthalten.	Stellen Sie sicher, dass die Replikationssätze, Remotesysteme und die SRM-Konfiguration korrekt sind.
1022	Ungültige oder unbekannte ArrayId „{ArrayId}“ in {cmd}-Anforderung.	Stellen Sie sicher, dass die Systemnamen und die IP-Adressen des Speicher-Controllers seit der Konfiguration des SRM nicht neu konfiguriert wurden.
1023	Sperrdatei {filename} konnte nicht geöffnet werden.	Überprüfen Sie die Datei- und Verzeichnisberechtigungen für den angegebenen Dateinamen.
1024	Unbekannter oder fehlender DeviceId-Parameter „{DeviceId}“ in {command}-Anforderung.	Stellen Sie sicher, dass SRM und SRA korrekt konfiguriert sind. Prüfen Sie darüber hinaus die Integrität des Speichersystems und der Netzwerkpfade zwischen dem SRM-Host und beiden Speichersystemen.
1025	Kein gültiger Synchronisierungspunkt für Volume {vol} während des {command}-Vorgangs gefunden.	Der Vorgang auf diesem Volume ist fehlgeschlagen, weil für das Volume kein gültiger Synchronisierungspunkt vorhanden ist. Verwenden Sie in MESM die Snapshot-Tabelle, um zu überprüfen, ob das angegebene Volume vollständig vom gesicherten Standort repliziert wurde. Weitere Informationen finden Sie im Administratorhandbuch.
1026	Zeitüberschreitung beim Warten auf die Umstellung von Volume {volume} auf den Konfliktstatus auf dem Speichersystem {arrayname} in {file}:{line}.	Stellen Sie sicher, dass das angegebene Volume auf dem Speichersystem erstellt wurde, und wiederholen Sie den Vorgang.
1027	Zeitüberschreitung des SRA-Befehls „syncOnce“ beim Warten auf Replikationsimages für Volumes [{volumes}] zum Starten auf dem Speichersystem.	Stellen Sie sicher, dass das Speichersystem funktionsfähig ist, und wiederholen Sie den Vorgang bei Bedarf, um sicherzustellen, dass die Volumes repliziert werden.
1028	Kein SRA-Snapshot für Volume „{DeviceID}“ in {command}-Anforderung gefunden.	Der SRA konnte den Snapshot bei einem früheren testFailoverStart-Vorgang nicht exportieren, der Snapshot wurde bereits entfernt oder der Snapshot wurde wegen eines Problems bei der Kommunikation mit dem Managementport auf dem Speichersystem nicht gefunden.
1029	Ein vorhandener SRA-Snapshot {snapshot} muss entfernt werden, bevor die testFailoverStart-Funktion für {volume} ausgeführt werden kann.	Entfernen Sie das Snapshot-Volume {snapshot}, bevor Sie den Test-Failover-Vorgang erneut ausführen.
1030	reverseReplication kann nicht auf Ziel-Volume {volume} ausgeführt werden, da das ursprünglich gesicherte Volume {target} immer noch auf dem Remotespeichersystem {remoteArray} zugewiesen ist	Stellen Sie sicher, dass beide Speichersysteme ({localArray} und {remoteArray}) und die entsprechenden SRM-Server ausgeführt werden und über das Netzwerk verwaltet werden können.

Nachrichtennummer	Nachricht	Empfohlene Maßnahme
1101	Anmeldung bei Speichersystem unter {url} ({response}) ist fehlgeschlagen	Stellen Sie sicher, dass die IP-Adressen des Speichersystems korrekt konfiguriert sind und dass das Speichersystem vom SRM-Host erreichbar ist. Wenn sich IP-Adressen des Speichersystems geändert haben, kann es außerdem erforderlich sein, die Remotesystemdefinitionen auf einem oder beiden Speichersystemen zu löschen und neu zu erstellen.
1102	Ausführung des Befehls „{cmd}“ ist auf Speichersystem unter {ipAddr} fehlgeschlagen: {err}	Wenn in der Fehlermeldung kein Grund für den Fehler angegeben wurde, öffnen Sie die angegebene Adresse mit einem Webbrowser, um die Integrität des Speichersystems zu überprüfen.
1103	Keine IP-Adressen für MC für den Befehl „{cmd}“ angegeben	Stellen Sie sicher, dass die IP-Adressen für das Speichersystem auf dem Speichersystem und auf dem Host korrekt konfiguriert sind.
1104	Antwort vom Speichersystem unter {ipaddr} enthielt keine Statusanzeige.	Überprüfen Sie die Integrität des Speichersystems und starten Sie den Management-Controller bei Bedarf neu.
1105	Befehl „{cmd}“ konnte auf dem Speichersystem unter {system} nicht ausgeführt werden: {err}	Überprüfen Sie die Konfiguration der IP-Adresse auf dem Speichersystem und auf dem Host und prüfen Sie die Netzwerkverbindung.
2001	Zuweisung von Volume {volume}({name}) wurde bereits aufgehoben.	SRM hat angefordert, dass ein Volume für das Failover vorbereitet wird, aber das Volume ist bereits vorbereitet.
2002	Keine Daten gefunden für {volume} Replikationsimage {imageSn} ({err})	Überprüfen Sie, ob die Replikation für Volume {volume} begonnen wurde.
2003	querySyncStatus: Keine Daten für Replikationsimage {imageSn} für Volume {vol} gefunden ({err}).	Überprüfen Sie, ob die Replikation für das angegebene Volume begonnen wurde.

**ANMERKUNG:** Erwartungsgemäß werden bestimmte Fehler in der Protokolldatei angezeigt, wenn Befehle ausgeführt werden, um sicherzustellen, dass Volumes sich in einem bestimmten Zustand befinden, und sie sich tatsächlich bereits in diesem Zustand befinden. Diese Fehler sind **-3395** (Replication is not active on this secondary volume) und **-10306** (Unable to set the specified volume as the primary volume because the specified volume is already a primary volume). Sie können diese Fehlermeldungen einfach ignorieren, wenn sie unter diesen Bedingungen auftreten.

## Optimale Geschäftsabläufe

Spezifische Richtlinien und Empfehlungen für die Verwendung von SRA und Replikationssoftware in Verbindung mit der VMware SRM-Disaster-Recovery-Lösung umfassen folgende Punkte:

- Bereiten Sie im Voraus einen Plan dazu vor, wie Sie im Falle eines Standort-Failovers erneut Replikationszeitspläne erstellen. Nach dem Ausführen eines Reverse-Replikationsvorgangs müssen Sie Replikationszeitpläne einrichten, um eine regelmäßige Replikation von Daten aus den neuen Quell-Volumes zurück zum ursprünglichen Quellstandort zu gewährleisten. Alternativ können Sie die Replikation gegebenenfalls manuell einleiten.
- Versuchen Sie, virtuelle Maschinen mit ähnlichen Sicherungsanforderungen oder Zeitplänen auf demselben Datenspeicher-Volumen zu gruppieren, da die Replikation pro Volumen erfolgt. Wenn z. B. einige virtuelle Maschinen nicht zu einem Remotestandort repliziert oder weniger häufig repliziert werden müssen, speichern Sie diese nicht auf demselben Datenspeicher-Volumen wie virtuelle Maschinen, die häufig repliziert werden müssen. So verhindern Sie, dass Daten unnötig repliziert werden.
- Der SRA unterstützt nur die Replikation zwischen identischen Hardwaremodellen. Zum Beispiel wird die Replikation zwischen einem vollständig iSCSI-basierten System und einem FC/iSCSI-Hybrid-System nicht unterstützt.
- Vermeiden Sie es, Replikations-Volumen LUN 0 zuzuordnen, damit keine Probleme mit der dynamischen Zuordnung und dem dynamischen Aufheben der Zuordnung von LUNs durch die speziellen Managementfunktionen auftreten, die LUN 0 zugewiesen sind. Sie können Volumen LUN 0 zuweisen, wenn die automatische Zuweisung dieser Volumen und die Aufhebung der Zuweisung nicht auf die gleiche Art und Weise wie bei Replikations-Volumen erfolgen müssen, wie z. B. bei lokalen Datenspeichern, die nicht repliziert werden.
- Replikations-Volumen sollten auf allen Hosts mit derselben LUN-Nummer zugewiesen werden.
- Verwenden Sie nicht dieselbe LUN-Nummer für verschiedene Volumen, die unterschiedlichen Hosts zugewiesen sind.
- Failover-Vorgänge führen dazu, dass Lese-/Schreib-Host-Zuweisungen für Replikations-Volumen in schreibgeschützte Zuweisungen konvertiert werden. Die Recovery der Replikation konvertiert alle schreibgeschützten Zuweisungen für dasselbe Volumen wieder zu Lese-/Schreibzugriff. Erstellen Sie keine schreibgeschützten Zuweisungen für Replikations-Volumen, zum Beispiel für Data-Mining-Zwecke. Wenn eine schreibgeschützte Zuweisung eines Replikations-Volumen erforderlich ist, ziehen Sie die Erstellung eines nicht replizierten Hardware- oder Software-Snapshots des Volumens in Erwägung.
- Der SRA erstellt unter Umständen Host-Einträge auf dem Speichersystem zur Nachverfolgung von Remote-IP- oder FC-Adressen. Löschen Sie keine Host-Einträge, deren Name mit „SRA“ beginnt. Sie können sie jedoch umbenennen, damit ihr Name aussagekräftiger ist.
- Basisnamen von Replikationssätzen für replizierte Volumen (bei der Erstellung des Replikationssatzes zugewiesen) sollte nicht länger als 23 Byte sein, damit Suffixe bei der Erstellung von Replikations-Snapshots angehängt werden können. Bei 23 Byte sind bis zu 23 ASCII-Zeichen zulässig. Bei anderen als ASCII-UTF-8-Zeichen ist jedoch mehr als jeweils ein Byte erforderlich.
- Ändern Sie nicht den Namen von Replikations-Snapshots bzw. ändern Sie Basisnamen von Replikationssätzen nur in Übereinstimmung mit diesen Best Practices. Der SRA hängt von der Konsistenz zwischen den Basisnamen des Replikationssatzes und den Snapshot-Namen ab.