



# **VMware Site Recovery Manager mit ONTAP**

## **Enterprise applications**

NetApp  
February 10, 2026

# Inhalt

VMware Site Recovery Manager mit ONTAP .....	1
VMware Live-Site Recovery mit ONTAP .....	1
Vorteile von ONTAP mit VLSR oder SRM .....	1
Wie VLSR ONTAP 9 nutzt .....	2
VLSR mit ONTAP und anderen Anwendungsfällen: Hybrid Cloud und Migration .....	2
Best Practices für die Implementierung .....	3
Verwenden Sie die neueste Version von ONTAP Tools 10 .....	3
SVM-Layout und Segmentierung für SMT .....	3
Best Practices für das Management von ONTAP 9 Systemen .....	3
Best Practices für betriebliche Prozesse .....	4
Datenspeicher und Protokolle .....	4
Allgemeines zu Array-Paaren .....	5
Allgemeines zu Replikationsgruppen .....	6
Allgemeines zu Schutzgruppen .....	6
Recovery-Pläne sprechen .....	7
Testen Sie den Failover .....	7
Überlegungen zum Failover .....	7
Schützen .....	8
Failback .....	8
Wiederherstellung der Originalseite .....	8
Replizierungstopologien .....	9
Unterstützte SnapMirror Layouts .....	9
VMFS-Unterstützung mit SnapMirror Active Sync .....	11
Unterstützte Array Manager-Layouts .....	12
Nicht unterstützte Layouts .....	13
SnapMirror Kaskadierung .....	14
SnapMirror und SnapVault .....	15
Verwendung von Qtrees in Site Recovery Manager-Umgebungen .....	17
Gemischte FC- und iSCSI-Umgebungen .....	17
Fehlerbehebung bei VLSRM/SRM bei Verwendung der VVols-Replikation .....	18
Weitere Informationen .....	19

# VMware Site Recovery Manager mit ONTAP

## VMware Live-Site Recovery mit ONTAP

ONTAP ist seit der Einführung von ESX in modernen Rechenzentren vor mehr als zwei Jahrzehnten eine führende Speicherlösung für VMware vSphere und in jüngerer Zeit für Cloud Foundation. NetApp führt weiterhin innovative Systeme ein, beispielsweise die neueste Generation der ASA A-Serie zusammen mit Funktionen wie SnapMirror Active Sync. Diese Fortschritte vereinfachen die Verwaltung, verbessern die Ausfallsicherheit und senken die Gesamtbetriebskosten (TCO) Ihrer IT-Infrastruktur.

Dieses Dokument stellt die ONTAP -Lösung für VMware Live Site Recovery (VLSR), früher bekannt als Site Recovery Manager (SRM), die branchenführende Disaster Recovery (DR)-Software von VMware, vor, einschließlich der neuesten Produktinformationen und Best Practices zur Optimierung der Bereitstellung, Risikominderung und Vereinfachung der laufenden Verwaltung.



Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4900: VMware Site Recovery Manager mit ONTAP*

Andere Dokumente wie Leitfäden und Kompatibilitäts-Tools werden durch Best Practices ergänzt. Sie werden basierend auf Labortests und umfassenden praktischen Erfahrungen der NetApp Ingenieure und Kunden entwickelt. In einigen Fällen passen empfohlene Best Practices möglicherweise nicht zu Ihrer Umgebung. Sie sind jedoch im Allgemeinen die einfachsten Lösungen, die die Anforderungen der meisten Kunden erfüllen.

Der Schwerpunkt dieses Dokuments liegt auf den Funktionen der neuesten Versionen von ONTAP 9, die in Verbindung mit ONTAP-Tools für VMware vSphere 10.4 (einschließlich NetApp Storage Replication Adapter [SRA] und VASA Provider [VP]) sowie VMware Live Site Recovery 9 verwendet werden.

## Vorteile von ONTAP mit VLSR oder SRM

NetApp Datenverwaltungsplattformen auf Basis von ONTAP gehören zu den am weitesten verbreiteten Speicherlösungen für VLSR. Die Gründe dafür sind vielfältig: Eine sichere, leistungsstarke Datenverwaltungsplattform mit einheitlichem Protokoll (NAS und SAN zusammen), die branchenführende Speichereffizienz, Mandantenfähigkeit, Qualitätskontrollen, Datenschutz mit platzsparenden Snapshots und Replikation mit SnapMirror bietet. Alle nutzen die native Hybrid-Multi-Cloud-Integration zum Schutz von VMware-Workloads und eine Vielzahl von Automatisierungs- und Orchestrierungstools, die Ihnen jederzeit zur Verfügung stehen.

Wenn Sie SnapMirror für die Array-basierte Replikation verwenden, profitieren Sie von einer der bewährtesten und ausgereiftesten Technologien von ONTAP. SnapMirror bietet Ihnen den Vorteil sicherer und hocheffizienter Datenübertragungen, da nur geänderte Dateisystemblöcke kopiert werden, nicht ganze VMs oder Datenspeicher. Sogar diese Blöcke profitieren von Platzeinsparungen wie Deduplizierung, Komprimierung und Verdichtung. Moderne ONTAP -Systeme verwenden jetzt das versionsunabhängige SnapMirror, sodass Sie Ihre Quell- und Zielcluster flexibel auswählen können. SnapMirror hat sich tatsächlich zu einem der leistungstärksten verfügbaren Tools für die Notfallwiederherstellung entwickelt.

Unabhängig davon, ob Sie herkömmliche NFS-, iSCSI- oder Fibre Channel-Datenspeicher verwenden (jetzt mit Unterstützung für vVols Datenspeicher), bietet VLSR ein robustes First-Party-Angebot, das die besten ONTAP Funktionen für die Notfallwiederherstellung oder die Planung und Orchestrierung der Datacenter-Migration nutzt.

## Wie VLSR ONTAP 9 nutzt

VLSR nutzt die erweiterten Datenmanagement-Technologien von ONTAP Systemen. Die Integration mit ONTAP Tools für VMware vSphere, einer virtuellen Appliance mit drei Hauptkomponenten:

- Das vCenter Plug-in der ONTAP Tools, früher als Virtual Storage Console (VSC) bekannt, vereinfacht das Storage Management und die Effizienzfunktionen, erhöht die Verfügbarkeit und senkt die Storage-Kosten und den Betriebsaufwand, sowohl bei SAN als auch bei NAS. Dieses Plug-in nutzt Best Practices für die Bereitstellung von Datastores und optimiert ESXi Hosteinstellungen für NFS- und Block-Storage-Umgebungen. Wegen all dieser Vorteile empfiehlt NetApp bei der Nutzung von vSphere bei Systemen mit ONTAP dieses Plug-in.
- Die ONTAP Tools VASA Provider unterstützen das VMware vStorage APIs for Storage Awareness (VASA) Framework. VASA Provider verbindet vCenter Server mit ONTAP und erleichtert so die Bereitstellung und das Monitoring von VM-Storage. Auf diese Weise wurden VMware Virtual Volumes (VVols) unterstützt und das Management von VM-Storage-Richtlinien sowie die VVols-Performance für einzelne VMs wurde ermöglicht. Außerdem gibt es Alarme zur Überwachung der Kapazität und der Konformität mit den Profilen.
- SRA wird zusammen mit VLSR eingesetzt, um die Replizierung von VM-Daten zwischen Produktions- und Disaster-Recovery-Standorten bei herkömmlichen VMFS- und NFS-Datenspeichern sowie zum unterbrechungsfreien Testen von DR-Replikaten zu managen. Diese Software hilft bei der Automatisierung der Erkennungs-, Recovery- und Sicherungsaufgaben. Es enthält sowohl eine SRA-Server-Appliance als auch SRA-Adapter für den Windows SRM-Server und die VLSR-Appliance.

Nachdem Sie die SRA-Adapter auf dem VLSR-Server zum Schutz von Nicht-vVols-Datenspeichern installiert und konfiguriert haben, können Sie mit der Konfiguration Ihrer vSphere-Umgebung für die Notfallwiederherstellung beginnen.

SRA bietet eine Befehls- und Kontrollschnittstelle für den VLSR-Server zur Verwaltung der ONTAP FlexVol-Volumes, die Ihre virtuellen VMware-Maschinen (VMs) enthalten, sowie zur Sicherung der SnapMirror-Replikation.

VLSR kann Ihren DR-Plan unterbrechungsfrei testen, indem es die proprietäre FlexClone -Technologie von NetApp verwendet, um nahezu sofortige Klone Ihrer geschützten Datenspeicher an Ihrem DR-Standort zu erstellen. VLSR erstellt eine Sandbox zum sicheren Testen, sodass Ihr Unternehmen und Ihre Kunden im Falle einer echten Katastrophe geschützt sind. So können Sie darauf vertrauen, dass Ihr Unternehmen im Katastrophenfall ein Failover durchführen kann.

Bei einem echten Ausfall oder sogar einer geplanten Migration können Sie mit VLSR alle Last-Minute-Änderungen am Datensatz über ein letztes SnapMirror Update senden (sofern Sie dies tun). Dann wird die Spiegelung unterbrochen und der Datenspeicher wird Ihren DR-Hosts gemountet. An diesem Punkt können Ihre VMs automatisch in beliebiger Reihenfolge gemäß Ihrer vorab geplanten Strategie hochgefahren werden.



Mit ONTAP Systemen können Sie SVMs zwecks SnapMirror Replizierung im selben Cluster kombinieren, jedoch wurde dieses Szenario nicht mit VLSR getestet und zertifiziert. Daher wird empfohlen, bei Verwendung von VLSR nur SVMs aus unterschiedlichen Clustern zu verwenden.

## VLSR mit ONTAP und anderen Anwendungsfällen: Hybrid Cloud und Migration

Durch die Integration Ihrer VLSR-Bereitstellung mit den erweiterten Datenverwaltungsfunktionen von ONTAP können Sie im Vergleich zu lokalen Speicheroptionen eine deutlich verbesserte Skalierbarkeit und Leistung erzielen. Darüber hinaus bietet es die Flexibilität der Hybrid Cloud. Mit der Hybrid Cloud können Sie Geld sparen, indem Sie ungenutzte Datenblöcke von Ihrem Hochleistungs-Array mithilfe von FabricPool auf Ihren bevorzugten Hyperscaler auslagern. Dabei kann es sich um einen lokalen S3-Speicher wie NetApp StorageGRID handeln. Sie können SnapMirror auch für Edge-basierte Systeme mit softwaredefiniertem

ONTAP Select oder Cloud-basierter DR verwenden, indem Sie ["NetApp Storage auf Equinix Metal"](#) oder andere gehostete ONTAP -Dienste.

Anschließend könnten Sie dank FlexClone ein Test-Failover innerhalb des Datacenters eines Cloud-Service-Providers durchführen, bei einem Storage-Platzbedarf von nahezu null. Der Schutz Ihres Unternehmens ist jetzt günstiger als je zuvor.

Mit VLSR können auch geplante Migrationen durchgeführt werden, indem VMs mit SnapMirror effizient von einem Datacenter in ein anderes oder sogar innerhalb desselben Datacenters übertragen werden, unabhängig davon, ob es sich um Ihr eigenes Datacenter oder über eine beliebige Anzahl an Service Providern von NetApp Partnern handelt.

## Best Practices für die Implementierung

In den folgenden Abschnitten werden die Best Practices für die Implementierung mit ONTAP und VMware SRM beschrieben.

### Verwenden Sie die neueste Version von ONTAP Tools 10

Die ONTAP Tools 10 bieten im Vergleich zu den Vorgängerversionen erhebliche Verbesserungen, darunter:

- 8-mal schnelleres Test-Failover\*
- 2x schnellere Bereinigung und erneuer Schutz\*
- 32 % schnellerer Failover\*
- Besser skalieren
- Native Unterstützung für gemeinsam genutzte Site-Layouts

\*Diese Verbesserungen basieren auf internen Tests und können je nach Umgebung variieren.

### SVM-Layout und Segmentierung für SMT

Mit ONTAP sorgt das Konzept der Storage Virtual Machine (SVM) für eine strenge Segmentierung in sicheren mandantenfähigen Umgebungen. SVM-Benutzer auf einer SVM können nicht auf Ressourcen einer anderen SVM zugreifen bzw. diese managen. Auf diese Weise können Sie die ONTAP Technologie nutzen, indem Sie separate SVMs für verschiedene Geschäftseinheiten erstellen, die ihre eigenen SRM Workflows im selben Cluster managen, um eine größere Storage-Effizienz zu erzielen.

Erwägen Sie die Verwaltung von ONTAP mit SVM-Scoped-Konten und SVM-Management-LIFs, um nicht nur die Sicherheitskontrolle zu verbessern, sondern auch die Performance zu verbessern. Die Performance ist bei der Nutzung von Verbindungen mit SVM-Umfang höher, da der SRA nicht erforderlich ist, alle Ressourcen eines gesamten Clusters – einschließlich physischer Ressourcen – zu verarbeiten. Stattdessen müssen sie nur die logischen Ressourcen verstehen, die zu der jeweiligen SVM abstrahiert sind.

### Best Practices für das Management von ONTAP 9 Systemen

Wie bereits erwähnt, können Sie ONTAP Cluster mit Anmeldedaten im Cluster oder SVM-Umfang und Management-LIFs managen. Um die optimale Performance zu erzielen, sollten Sie immer dann die Verwendung von VVols in Betracht ziehen, wenn Sie über den SVM-Umfang verfügen. Dabei sollten Sie sich jedoch einigen Anforderungen bewusst sein und dass einige Funktionen verloren gehen.

- Das Standard-vsadmin SVM-Konto verfügt nicht über die erforderliche Zugriffsebene, um ONTAP-Tools-

Aufgaben durchzuführen. Daher müssen Sie ein neues SVM-Konto erstellen. "[Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen](#)" Verwenden der enthaltenen JSON-Datei. Diese Option kann für SVM oder Konten mit Cluster-Umfang verwendet werden.

- Da es sich bei dem vCenter UI Plug-in, VASA Provider und SRA Server um vollständig integrierte Microservices handelt, müssen Sie ebenso wie beim Hinzufügen von Storage in der vCenter UI für ONTAP-Tools Storage zum SRA-Adapter in SRM hinzufügen. Andernfalls erkennt der SRA-Server möglicherweise nicht die Anfragen, die von SRM über den SRA-Adapter gesendet werden.
- Die NFS-Pfadprüfung wird bei Verwendung der im SVM-Umfang enthaltenen Anmeldedaten nicht durchgeführt, es sei denn, Sie befinden sich zuerst "[Onboard Cluster](#)" im ONTAP Tools Manager und verknüpfen sie mit den vCenter. Der Grund dafür ist, dass der physische Standort logisch von der SVM abstrahiert ist. Dies stellt jedoch keine Sorge mehr dar, da bei der Verwendung von indirekten Pfaden nicht mehr deutliche Performance-Einbußen bei modernen ONTAP Systemen auftreten.
- Es werden möglicherweise keine Aggregat-Platzeinsparungen aufgrund von Storage-Effizienz gemeldet.
- Wenn unterstützt, können Spiegelungen zur Lastverteilung nicht aktualisiert werden.
- Die EMS-Protokollierung wird möglicherweise nicht auf ONTAP Systemen durchgeführt, die mit den Anmeldedaten im Umfang des SVM-Service gemanagt werden.

## Best Practices für betriebliche Prozesse

In den folgenden Abschnitten werden die betrieblichen Best Practices für VMware SRM und ONTAP Storage beschrieben.

### Datenspeicher und Protokolle

- Wenn möglich, verwenden Sie immer ONTAP Tools, um Datenspeicher und Volumes bereitzustellen. Damit stellen wir sicher, dass Volumes, Verbindungspfade, LUNs, Initiatorgruppen, Exportrichtlinien Und andere Einstellungen sind kompatibel konfiguriert.
- SRM unterstützt iSCSI, Fibre Channel und NFS Version 3 mit ONTAP 9 bei Nutzung der Array-basierten Replizierung über SRA. SRM unterstützt nicht die Array-basierte Replizierung für NFS Version 4.1 mit herkömmlichen oder VVols-Datstores.
- Zur Bestätigung der Konnektivität überprüfen Sie immer, ob Sie einen neuen Testdatenspeicher am DR-Standort vom Ziel-ONTAP-Cluster aus mounten und wieder mounten können. Testen Sie jedes Protokoll, das Sie für die Datastore-Konnektivität verwenden möchten. Eine Best Practice besteht darin, mit ONTAP-Tools Ihren Testdatenspeicher zu erstellen, da dies die gesamte Datastore-Automatisierung gemäß den Anweisungen von SRM erfolgt.
- SAN-Protokolle sollten für jeden Standort homogen sein. Sie können NFS und SAN mixen, aber die SAN-Protokolle sollten nicht innerhalb eines Standorts gemischt werden. Sie können beispielsweise FCP in Standort A und iSCSI in Standort B verwenden. Sie sollten nicht sowohl FCP als auch iSCSI an Standort A verwenden
- In den vorherigen Leitfäden wurde das Erstellen von LIF zur Datenlokalität empfohlen. Das heißt, mounten Sie immer einen Datenspeicher mit einer LIF auf dem Node, der physisch Eigentümer des Volume ist. Das ist zwar immer noch die Best Practice, ist aber in modernen Versionen von ONTAP 9 nicht mehr vorgeschrieben. Wenn möglich und im Cluster-Umfang Zugangsdaten angegeben, entscheiden sich ONTAP Tools weiterhin für den Lastausgleich über lokale LIFs hinweg für die Daten, allerdings sind dies keine Voraussetzungen für Hochverfügbarkeit oder Performance.
- ONTAP 9 kann so konfiguriert werden, dass Snapshots automatisch entfernt werden, um die Uptime aufrechtzuerhalten, falls ein Speicherplatz nicht ausreicht, wenn Autosize nicht in der Lage ist, eine ausreichende Notfallkapazität zur Verfügung zu stellen. In der Standardeinstellung für diese Funktion werden die von SnapMirror erstellten Snapshots nicht automatisch gelöscht. Wenn SnapMirror Snapshots

gelöscht werden, kann NetApp SRA die Replizierung für das betroffene Volume nicht rückgängig machen und erneut synchronisieren. Um zu verhindern, dass ONTAP SnapMirror Snapshots löscht, konfigurieren Sie die Funktion für automatisches Löschen von Snapshots und wählen Sie „versuchen“.

```
snap autodelete modify -volume -commitment try
```

- Die automatische Größenanpassung von Volumes sollte für Volumes, die SAN-Datstores enthalten, und `grow_shrink` für NFS-Datstores auf festgelegt werden `grow`. Erfahren Sie mehr über dieses Thema unter ["Konfigurieren Sie Volumes für die automatische Vergrößerung und Verkleinerung ihrer Größe"](#).
- SRM führt am besten aus, wenn die Anzahl der Datstores und damit die Schutzgruppen in Ihren Recovery-Plänen minimiert wird. Daher sollten Sie die Optimierung für die VM-Dichte in SRM-geschützten Umgebungen in Betracht ziehen, in denen RTO eine zentrale Bedeutung hat.
- Nutzen Sie den Distributed Resource Scheduler (DRS), um die Last auf den geschützten und Recovery ESXi Clustern auszugleichen. Wenn Sie ein Failback planen, werden die zuvor geschützten Cluster beim Ausführen eines Reprotect zu den neuen Recovery-Clustern. DRS hilft dabei, die Platzierung in beide Richtungen auszugleichen.
- Wenn möglich, vermeiden Sie die Verwendung von IP-Anpassung mit SRM, da dies Ihre RTO erhöhen kann.

## Allgemeines zu Array-Paaren

Für jedes Array-Paar wird ein Array-Manager erstellt. Zusammen mit SRM und ONTAP Tools erfolgt die Kopplung jedes Arrays mit dem Umfang einer SVM, auch wenn Cluster-Anmeldedaten verwendet werden. So können Sie DR-Workflows zwischen Mandanten segmentieren, basierend auf den ihnen zugewiesenen SVMs. Sie können mehrere Array-Manager für ein bestimmtes Cluster erstellen und diese asymmetrisch sein. Sie können Fan-out oder Fan-in zwischen verschiedenen ONTAP 9 Clustern. So können beispielsweise SVM-A und SVM-B auf Cluster-1 und damit auf SVM-C auf Cluster-2, SVM-D auf Cluster-3 oder umgekehrt genutzt werden.

Wenn Sie Array-Paare in SRM konfigurieren, sollten Sie sie immer in SRM auf die gleiche Weise hinzufügen, wie Sie sie den ONTAP Tools hinzugefügt haben. Das bedeutet, dass sie denselben Benutzernamen, dasselbe Passwort und dieselbe Management-LIF verwenden müssen. Diese Anforderung stellt sicher, dass SRA ordnungsgemäß mit dem Array kommuniziert. Der folgende Screenshot veranschaulicht, wie ein Cluster in ONTAP-Tools angezeigt wird und wie es zu einem Array Manager hinzugefügt werden kann.



## Allgemeines zu Replikationsgruppen

Replikationsgruppen enthalten logische Sammlungen von virtuellen Maschinen, die zusammen wiederhergestellt werden. Da die ONTAP SnapMirror Replizierung auf Volume-Ebene stattfindet, befinden sich alle VMs in einem Volume in derselben Replizierungsgruppe.

Es gibt mehrere Faktoren, die bei Replizierungsgruppen berücksichtigt werden müssen und die Art und Weise, wie VMs über FlexVol Volumes verteilt werden. Das Gruppieren ähnlicher VMs im selben Volume kann die Storage-Effizienz in älteren ONTAP Systemen steigern, bei denen Deduplizierung auf Aggregatebene fehlt. Beim Gruppieren wird jedoch die Größe des Volumes vergrößert und die Volume-I/O-Parallelität verringert. Moderne ONTAP Systeme bieten ein optimales Verhältnis zwischen Performance und Storage-Effizienz, indem VMs über FlexVol Volumes im selben Aggregat verteilt werden. Dadurch wird die Deduplizierung auf Aggregatebene genutzt und die I/O-Parallelisierung über mehrere Volumes hinweg wird gesteigert. Sie können VMs in den Volumes zusammen wiederherstellen, da eine (nachfolgend erläutert) Sicherungsgruppe mehrere Replizierungsgruppen enthalten kann. Der Nachteil dieses Layouts besteht darin, dass Blöcke mehrmals über das Netzwerk übertragen werden können, da bei SnapMirror die Aggregatdeduplizierung nicht berücksichtigt wird.

Eine letzte Überlegung für Replikationsgruppen besteht darin, dass jede von Natur aus eine logische Konsistenzgruppe ist (nicht zu verwechseln mit SRM-Konsistenzgruppen). Das liegt daran, dass alle VMs im Volume mithilfe desselben Snapshots zusammen übertragen werden. Wenn Sie also VMs haben, die stets konsistent sein müssen, sollten Sie sie in der gleichen FlexVol speichern.

## Allgemeines zu Schutzgruppen

Sicherungsgruppen definieren VMs und Datastores in Gruppen, die am geschützten Standort zusammen wiederhergestellt werden. Am geschützten Standort befinden sich die VMs, die in einer Schutzgruppe konfiguriert sind, im normalen Steady-State-Betrieb. Es ist wichtig zu beachten, dass eine Schutzgruppe nicht mehrere Array-Manager umfassen kann, obwohl SRM möglicherweise mehrere Array-Manager für eine Schutzgruppe anzeigt. Aus diesem Grund sollten Sie VM-Dateien nicht über Datastores auf unterschiedlichen SVMs verteilen.



## Recovery-Pläne sprechen

Recovery-Pläne legen fest, welche Schutzgruppen im gleichen Prozess wiederhergestellt werden. Mehrere Sicherungsgruppen können im selben Recovery-Plan konfiguriert werden. Um darüber hinaus mehr Optionen für die Ausführung von Recovery-Plänen zu aktivieren, kann eine einzige Sicherungsgruppe in mehreren Recovery-Plänen enthalten sein.

Durch Recovery-Pläne können SRM-Administratoren Recovery-Workflows definieren, indem VMs einer Prioritätsgruppe von 1 (hoch) bis 5 (niedrig) zugewiesen werden, wobei 3 (mittel) standardmäßig verwendet wird. Innerhalb einer Prioritätsgruppe können VMs für Abhängigkeiten konfiguriert werden.

So könnte Ihr Unternehmen beispielsweise eine geschäftskritische Tier-1-Applikation nutzen, die für seine Datenbank auf einen Microsoft SQL Server aufbaut. Sie entscheiden also, Ihre VMs in Prioritätsgruppe 1 einzufügen. Innerhalb der Prioritätsgruppe 1 beginnen Sie mit der Planung des Auftrages der Dienste. Wahrscheinlich möchten Sie, dass Ihr Microsoft Windows Domänencontroller vor Ihrem Microsoft SQL Server gebootet wird, der vor Ihrem Anwendungsserver online sein müsste usw. Sie würden alle diese VMs der Prioritätsgruppe hinzufügen und dann die Abhängigkeiten festlegen, da Abhängigkeiten nur innerhalb einer bestimmten Prioritätsgruppe gelten.

NetApp empfiehlt besonders, mit Ihren Applikationsteams zusammenarbeiten zu müssen, um die Reihenfolge der für ein Failover-Szenario erforderlichen Operationen zu ermitteln und die Recovery-Pläne entsprechend zu erstellen.

## Testen Sie den Failover

Als Best Practice empfiehlt es sich, immer dann ein Test-Failover durchzuführen, wenn an der Konfiguration des geschützten VM-Storage Änderungen vorgenommen werden. Dadurch wird sichergestellt, dass Sie bei einem Notfall darauf vertrauen können, dass Site Recovery Manager Services innerhalb des erwarteten RTO-Ziels wiederherstellen kann.

NetApp empfiehlt zudem, die Funktion der in Gast-Applikationen gelegentlich zu bestätigen, insbesondere nach der Neukonfiguration von VM-Storage.

Wenn ein Test-Recovery-Vorgang ausgeführt wird, wird auf dem ESXi Host für die VMs ein privates Test-Bubble-Netzwerk erstellt. Dieses Netzwerk wird jedoch nicht automatisch mit physischen Netzwerkadaptern verbunden und bietet daher keine Verbindung zwischen den ESXi Hosts. Um die Kommunikation zwischen VMs zu ermöglichen, die während des DR-Tests auf verschiedenen ESXi Hosts ausgeführt werden, wird ein physisches privates Netzwerk zwischen den ESXi Hosts am DR-Standort erstellt. Um zu überprüfen, ob das Testnetzwerk privat ist, kann das Testblasennetzwerk physisch oder mittels VLANs oder VLAN-Tagging getrennt werden. Dieses Netzwerk muss von dem Produktionsnetzwerk getrennt werden, da die VMs wiederhergestellt werden und nicht mit IP-Adressen im Produktionsnetzwerk platziert werden können, die mit den tatsächlichen Produktionssystemen kollidieren können. Nach dem Erstellen eines Recovery-Plans in SRM kann das erstellte Testnetzwerk als privates Netzwerk ausgewählt werden, um die VMs mit während des Tests zu verbinden.

Nachdem der Test validiert und nicht mehr erforderlich ist, führen Sie eine Bereinigung durch. Bei der Durchführung der Bereinigung werden die geschützten VMs in ihren Ausgangszustand zurückversetzt und der Recovery-Plan wird auf den Status „bereit“ zurückgesetzt.

## Überlegungen zum Failover

Wenn es um Failover an einem Standort zusätzlich zur in diesem Leitfaden beschriebenen Reihenfolge geht, müssen noch einige weitere Aspekte berücksichtigt werden.

Ein Problem, mit dem Sie möglicherweise zu kämpfen haben, ist die Netzwerkunterschiede zwischen den Standorten. In einigen Umgebungen können am primären Standort und am DR-Standort dieselben Netzwerk-IP-Adressen verwendet werden. Diese Fähigkeit wird als Stretched Virtual LAN (VLAN) oder Stretched Network Setup bezeichnet. Andere Umgebungen müssen möglicherweise unterschiedliche Netzwerk-IP-Adressen (z. B. in unterschiedlichen VLANs) am primären Standort relativ zum DR-Standort verwenden.

VMware bietet verschiedene Möglichkeiten zur Lösung dieses Problems. Netzwerkvirtualisierungstechnologien wie VMware NSX-T Data Center abstrahieren den gesamten Netzwerk-Stack von Ebene 2 bis 7 von der Betriebsumgebung und ermöglichen so portablere Lösungen. Weitere Informationen zu ["NSX-T-Optionen mit SRM"](#).

SRM ermöglicht es Ihnen auch, die Netzwerkkonfiguration einer VM wie das Recovery zu ändern. Diese Neukonfiguration umfasst Einstellungen wie IP-Adressen, Gateway-Adressen und DNS-Servereinstellungen. Verschiedene Netzwerkeinstellungen, die bei der Wiederherstellung auf einzelne VMs angewendet werden, können in den Einstellungen einer VM der Eigenschaft im Recovery-Plan angegeben werden.

Um SRM so zu konfigurieren, dass verschiedene Netzwerkeinstellungen auf mehrere VMs angewendet werden können, ohne die Eigenschaften der einzelnen im Recovery-Plan bearbeiten zu müssen, stellt VMware ein Tool namens dr-ip-Customizer bereit. Informationen zur Verwendung dieses Dienstprogramms finden Sie unter ["VMware Dokumentation"](#).

## Schützen

Nach einem Recovery wird der Recovery-Standort zum neuen Produktionsstandort. Da der Recovery-Vorgang die SnapMirror Replizierung ausbrach, ist der neue Produktionsstandort nicht vor zukünftigen Ausfällen geschützt. Als Best Practice wird empfohlen, den neuen Produktionsstandort unmittelbar nach dem Recovery auf einen anderen Standort zu schützen. Wenn der ursprüngliche Produktionsstandort betriebsbereit ist, kann der VMware Administrator den ursprünglichen Produktionsstandort als neuen Recovery-Standort zum Schutz des neuen Produktionsstandorts verwenden und damit die Richtung des Schutzes umkehren. Repschutz ist nur bei nicht-katastrophalen Ausfällen verfügbar. Daher müssen die ursprünglichen vCenter Server, ESXi Server, SRM Server und entsprechenden Datenbanken irgendwann wiederhergestellt werden können. Falls diese nicht verfügbar sind, müssen eine neue Schutzgruppe und ein neuer Recovery-Plan erstellt werden.

## Failback

Ein Failback-Vorgang ist im Grunde ein Failover in eine andere Richtung als zuvor. Als Best Practice überprüfen Sie, ob der ursprüngliche Standort wieder zu akzeptablen Funktionsstufen zurückkehrt, bevor Sie ein Failback durchführen, oder, anders ausgedrückt, ein Failover zum ursprünglichen Standort durchführen. Falls der ursprüngliche Standort weiterhin kompromittiert wird, sollten Sie ein Failback verzögern, bis der Ausfall ausreichend behoben ist.

Eine weitere Failback Best Practice besteht darin, immer einen Test-Failover auszuführen, nachdem der erneute Schutz abgeschlossen und bevor das endgültige Failback durchgeführt wurde. Dadurch wird sichergestellt, dass die vorhandenen Systeme am ursprünglichen Standort den Betrieb abschließen können.

## Wiederherstellung der Originalseite

Nach dem Failback sollten Sie mit allen Stakeholdern bestätigen, dass ihre Dienste wieder in den Normalzustand gebracht wurden, bevor Sie erneut den Schutz erneut ausführen,

Wenn eine erneute Sicherung nach dem Failback ausgeführt wird, befindet sich die Umgebung im Wesentlichen in dem Zustand, in dem sie sich zu Beginn befand. Die SnapMirror Replizierung wird erneut vom Produktionsstandort zum Recovery-Standort ausgeführt.

# Replizierungstopologien

In ONTAP 9 sind die physischen Komponenten eines Clusters für Cluster-Administratoren sichtbar, sind aber für die Applikationen und Hosts, die das Cluster nutzen, nicht direkt sichtbar. Die physischen Komponenten stellen einen Pool mit gemeinsam genutzten Ressourcen bereit, anhand dessen die logischen Clusterressourcen erstellt werden. Applikationen und Hosts greifen ausschließlich über SVMs auf Daten zu, die Volumes und LIFs enthalten.

Jede NetApp SVM wird in Site Recovery Manager als eindeutiges Array behandelt. VLSR unterstützt bestimmte Array-zu-Array- (oder SVM-zu-SVM-) Replikationslayouts.

Eine einzelne VM kann aus den folgenden Gründen keine Daten besitzen – Virtual Machine Disk (VMDK) oder RDM – auf mehr als einem VLSR Array:

- VLSR sieht nur die SVM, nicht einen individuellen physischen Controller.
- Eine SVM kann LUNs und Volumes steuern, die mehrere Nodes in einem Cluster umfassen.

## Best Practices In Sich

Bedenken Sie bei der Ermittlung von Supportmöglichkeiten diese Regel: Um eine VM mithilfe von VLSR und der NetApp SRA zu schützen, müssen alle Bestandteile der VM nur auf einer SVM vorhanden sein. Diese Regel gilt sowohl für den geschützten Standort als auch für den Recovery-Standort.

## Unterstützte SnapMirror Layouts

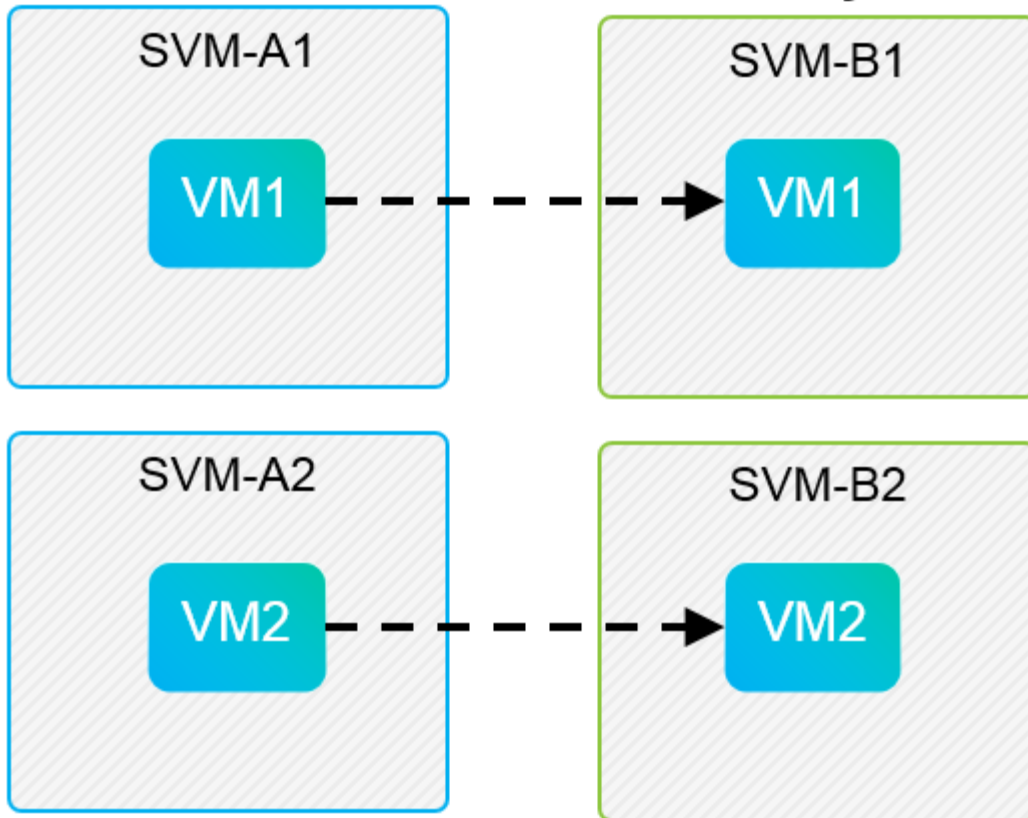
Die folgenden Abbildungen zeigen die Szenarien des SnapMirror Beziehungs-Layouts, die von VLSR und SRA unterstützt werden. Jede VM in den replizierten Volumes besitzt die Daten auf nur einem VLSR Array (SVM) an jedem Standort.

## SnapMirror Replication



### Protected Site

### Recovery Site

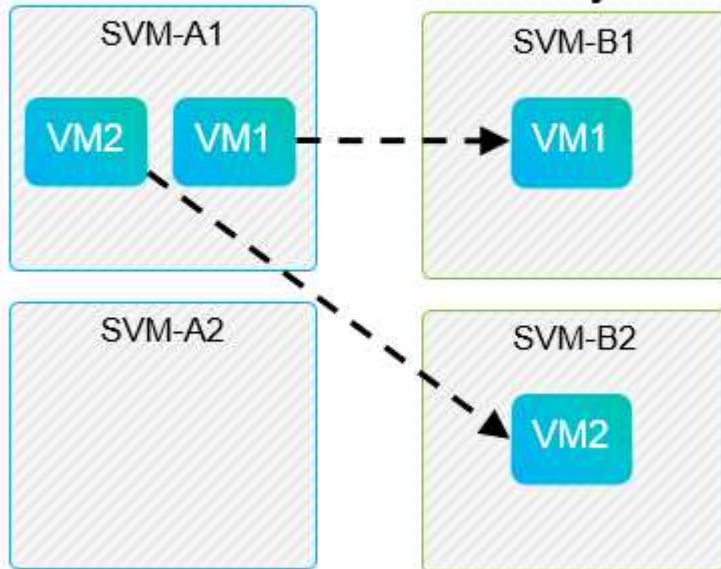


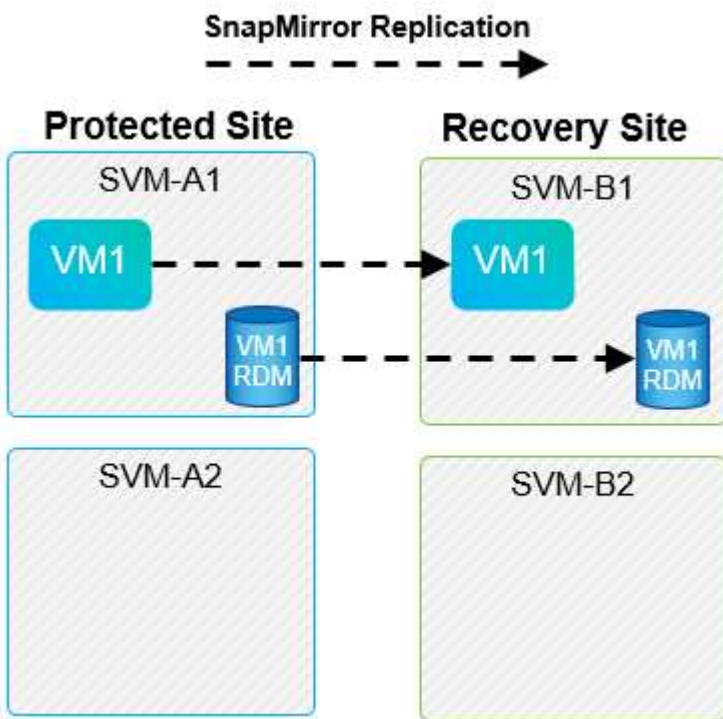
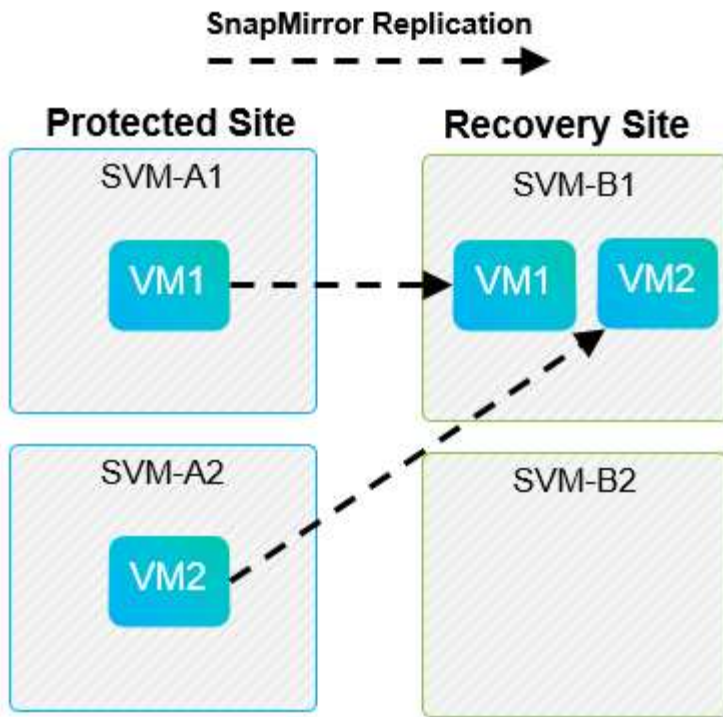
## SnapMirror Replication



### Protected Site

### Recovery Site





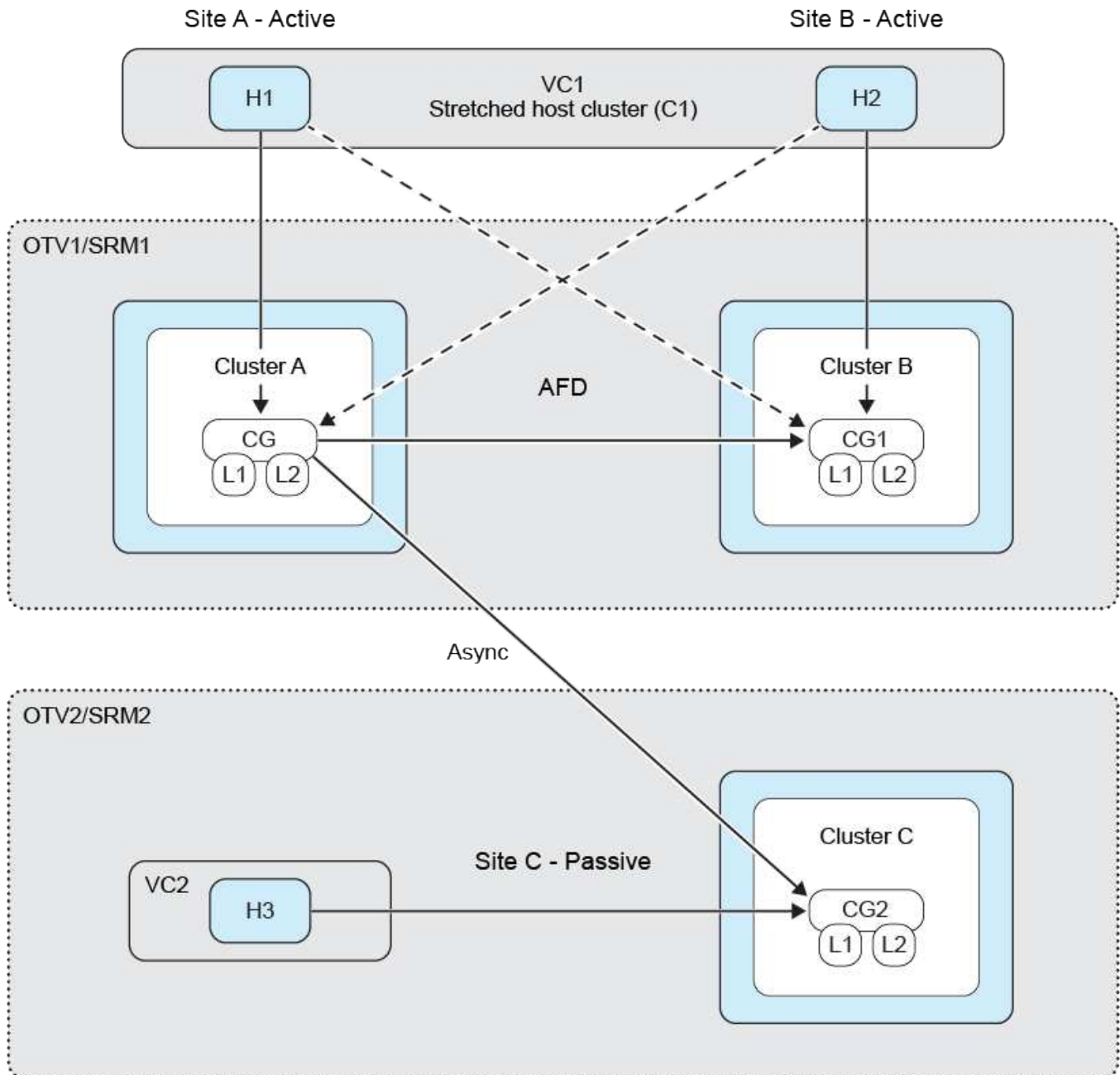
## VMFS-Unterstützung mit SnapMirror Active Sync

ONTAP Tools 10.3 und höher unterstützen auch den Schutz Ihrer VMFS-Datenspeicher mit SnapMirror Active Sync (SMas). Dies ermöglicht ein transparentes Failover zur Gewährleistung der Geschäftskontinuität zwischen zwei Rechenzentren (als Fehlerdomänen bezeichnet), die relativ nahe beieinander liegen. Die Notfallwiederherstellung über große Entfernungen kann dann mithilfe von SnapMirror asynchron über die ONTAP -Tools SRA mit VLSR orchestriert werden.

["Erfahren Sie mehr über ONTAP SnapMirror Active Sync"](#)

Datenspeicher werden in einer Konsistenzgruppe (CG) zusammengefasst und die VMs aller Datenspeicher bleiben als Mitglieder derselben CG hinsichtlich der Schreibreihenfolge konsistent.

Einige Beispiele könnten sein, dass Standorte in Berlin und Hamburg durch SMas geschützt sind und dass eine dritte Standortreplik SnapMirror asynchron verwendet und durch VLSR geschützt ist. Ein weiteres Beispiel wäre der Schutz von Standorten in New York und New Jersey durch SMas sowie eines dritten Standorts in Chicago.



## Unterstützte Array Manager-Layouts

Wenn Sie in VLSR Array-basierte Replizierung (ABR) verwenden, werden Schutzgruppen auf ein einzelnes Array-Paar isoliert, wie im folgenden Screenshot dargestellt. In diesem Szenario **SVM1** und **SVM2** werden mit und **SVM4** am Recovery-Standort gesteuert **SVM3**. Sie können jedoch nur eines der beiden Array-Paare

auswählen, wenn Sie eine Schutzgruppe erstellen.

New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Type

Select the type of protection group you want to create:

☒ Datastore groups (array-based replication)  
Protect all virtual machines which are on specific datastores.

☐ Individual VMs (vSphere Replication)  
Protect specific virtual machines, regardless of the datastores.

☐ Virtual Volumes (vVol replication)  
Protect virtual machines which are on replicated vVol storage.

☐ Storage policies (array-based replication)  
Protect virtual machines with specific storage policies.

Select array pair

Array Pair	Array Manager Pair
<input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

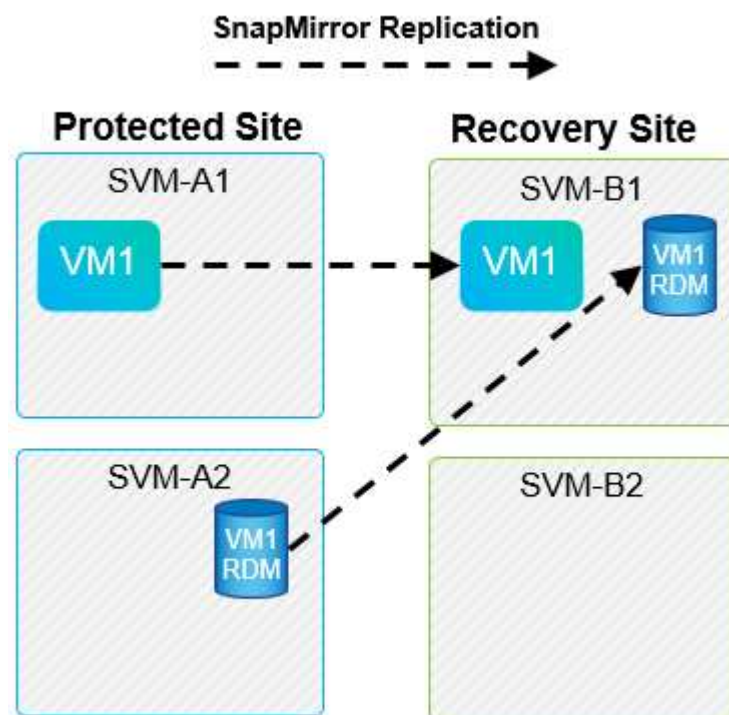
CANCEL

BACK

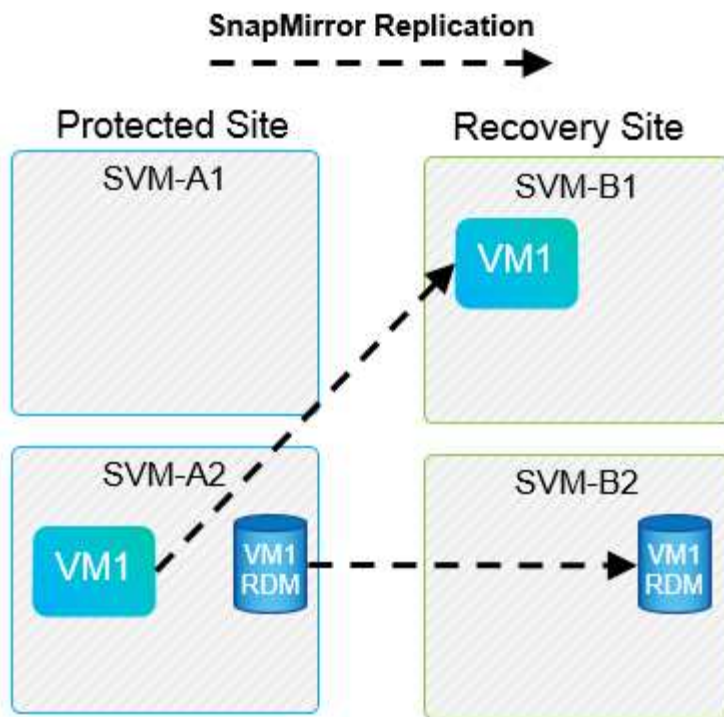
NEXT

## Nicht unterstützte Layouts

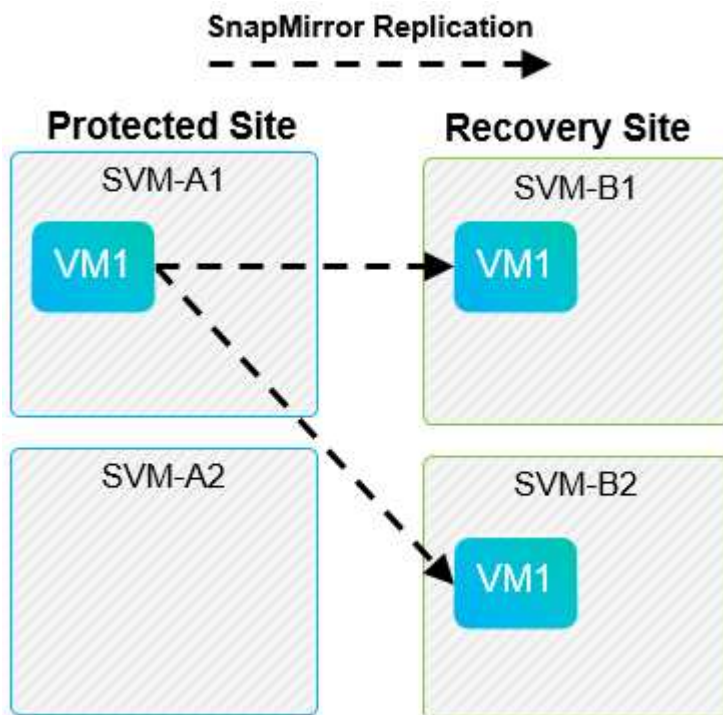
Nicht unterstützte Konfigurationen beinhalten Daten (VMDK oder RDM) auf mehreren SVMs, die sich im Besitz einer individuellen VM befinden. In den Beispielen in den folgenden Abbildungen VM1 kann nicht für den Schutz mit VLSR konfiguriert werden, da VM1 Daten auf zwei SVMs vorhanden sind.







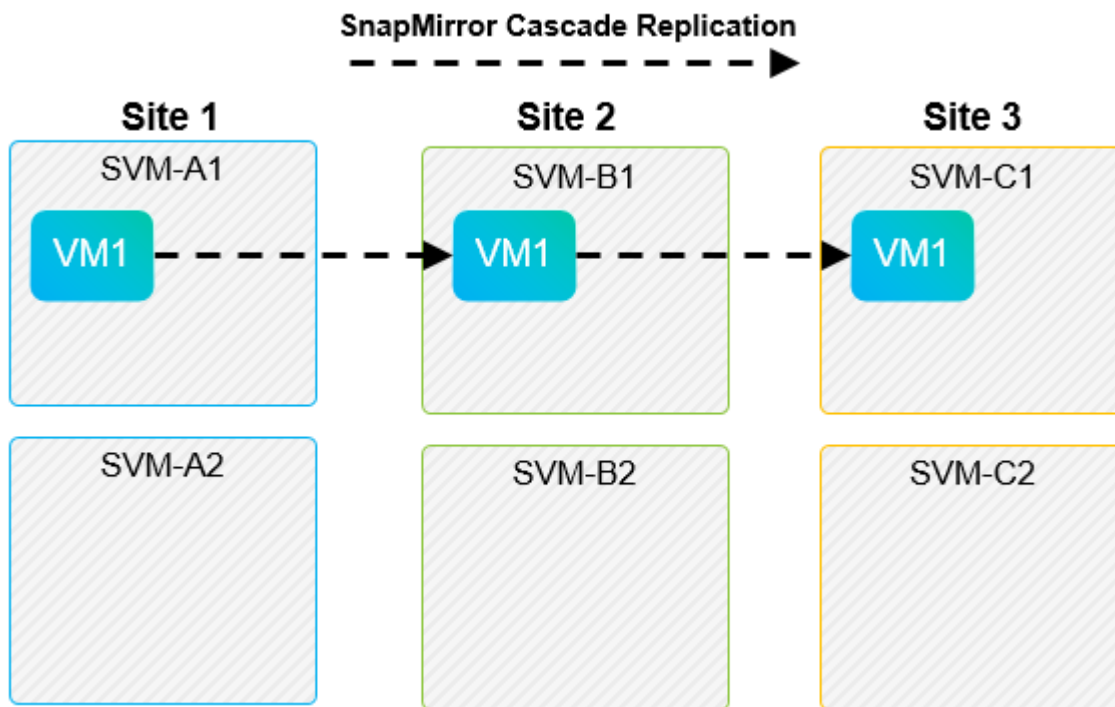
Jegliche Replizierungsbeziehungen, bei denen ein einzelnes NetApp Volume von einer Quell-SVM auf mehrere Ziele in derselben SVM oder in verschiedenen SVMs repliziert wird, werden als SnapMirror Fan-out bezeichnet. Fan-out wird mit VLSR nicht unterstützt. In dem in der folgenden Abbildung gezeigten Beispiel VM1 kann nicht für den Schutz in VLSR konfiguriert werden, da es mit SnapMirror an zwei verschiedenen Standorten repliziert wird.



## SnapMirror Kaskadierung

VLSR unterstützt keine Kaskadierung von SnapMirror Beziehungen, bei denen ein Quell-Volume auf einem

Ziel-Volume repliziert wird und das Ziel-Volume ebenfalls mit SnapMirror auf einem anderen Ziel-Volume repliziert wird. In dem in der folgenden Abbildung gezeigten Szenario kann VLSR nicht für das Failover zwischen mehreren Standorten verwendet werden.



## SnapMirror und SnapVault

Die NetApp SnapVault Software ermöglicht festplattenbasierte Backups von Unternehmensdaten zwischen NetApp Storage-Systemen. SnapVault und SnapMirror können in derselben Umgebung nebeneinander bestehen. VLSR unterstützt jedoch nur das Failover der SnapMirror Beziehungen.



Die NetApp SRA unterstützt das `mirror-vault` Richtlinienentyp.

SnapVault wurde für ONTAP 8.2 von Grund auf neu aufgebaut. Obwohl frühere Benutzer von Data ONTAP 7-Mode Ähnlichkeiten finden sollten, wurden in dieser Version von SnapVault wesentliche Verbesserungen vorgenommen. Eine wichtige Verbesserung ist die Möglichkeit zur Wahrung der Storage-Effizienz von Primärdaten während der SnapVault Transfers.

Eine wichtige Architekturänderung ist, dass SnapVault in ONTAP 9 wie bei 7-Mode SnapVault auf Volume-Ebene repliziert, nicht auf qtree-Ebene. Bei diesem Setup muss die Quelle einer SnapVault Beziehung ein Volume sein, und das Volume muss auf sein eigenes Volume auf dem sekundären SnapVault System repliziert werden.

In einer Umgebung, in der SnapVault verwendet wird, werden auf dem primären Storage-System speziell benannte Snapshots erstellt. Je nach implementierter Konfiguration können die benannten Snapshots auf dem Primärsystem nach einem SnapVault-Zeitplan oder durch eine Anwendung wie NetApp Active IQ Unified Manager erstellt werden. Die benannten Snapshots, die auf dem Primärsystem erstellt werden, werden dann auf das SnapMirror Ziel repliziert und von dort auf das SnapVault Ziel archiviert.

Ein Quell-Volume kann in einer Kaskadenkonfiguration erstellt werden, bei der ein Volume auf ein SnapMirror Ziel am DR-Standort repliziert wird und von dort aus auf ein SnapVault Ziel verlagert wird. Ein Quell-Volume kann auch in einer Fan-out-Beziehung erstellt werden, wobei ein Ziel ein SnapMirror Ziel ist und das andere Ziel eine SnapVault Ziel ist. SRA rekonfiguriert jedoch nicht automatisch die SnapVault-Beziehung neu, um das

SnapMirror Ziel-Volume als Quelle für den Vault zu verwenden, wenn das VLSR Failover oder eine Umkehrung der Replizierung stattfindet.

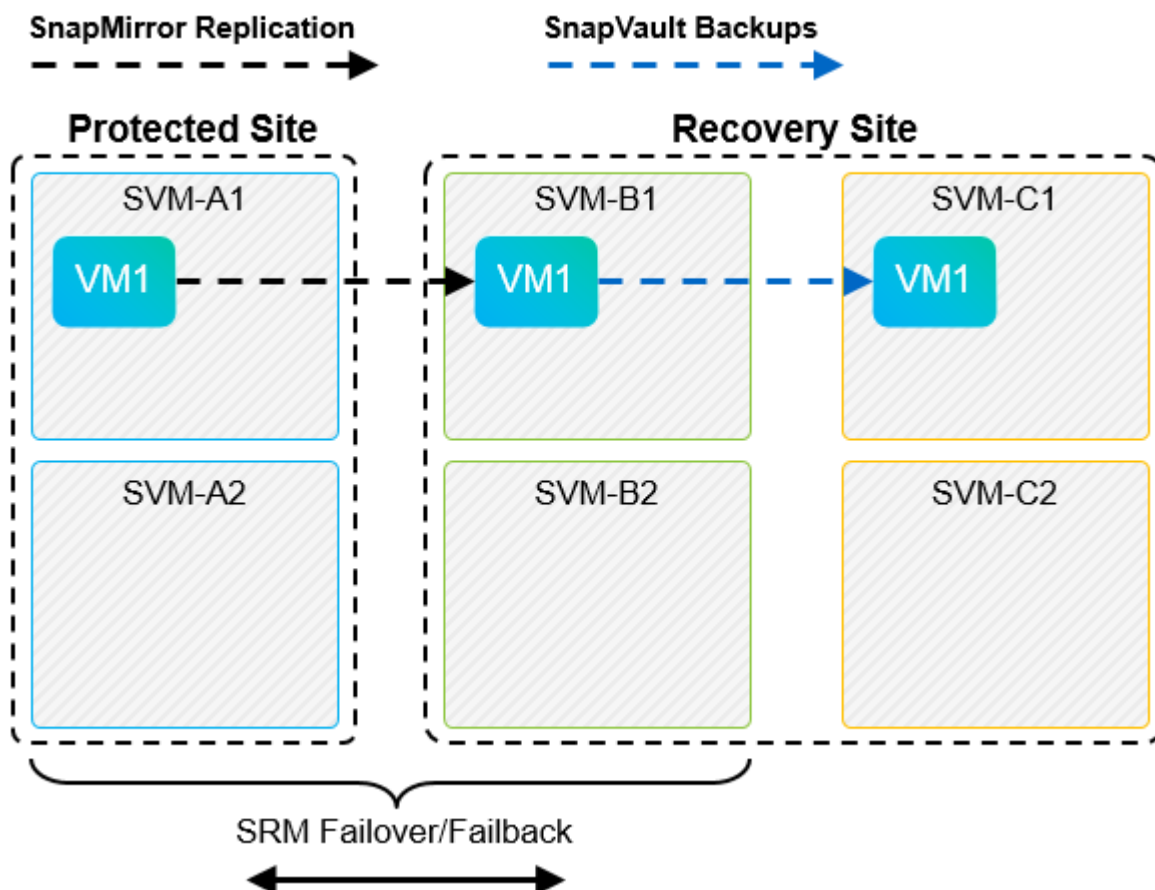
Die neuesten Informationen zu SnapMirror und SnapVault für ONTAP 9 finden Sie hier: ["TR-4015 SnapMirror Configuration Best Practice Guide für ONTAP 9."](#)

#### Best Practices In Sich

Wenn in derselben Umgebung SnapVault und VLSR eingesetzt werden, empfiehlt NetApp, eine Kaskadenkonfiguration von SnapMirror auf SnapVault zu verwenden, bei der SnapVault Backups normalerweise über das SnapMirror Ziel am DR-Standort ausgeführt werden. Bei einem Notfall kann der primäre Standort durch diese Konfiguration nicht mehr zugänglich sein. Indem das SnapVault Ziel am Recovery-Standort gehalten wird, können SnapVault Backups nach dem Failover neu konfiguriert werden, sodass SnapVault Backups weiterhin am Recovery-Standort ausgeführt werden können.

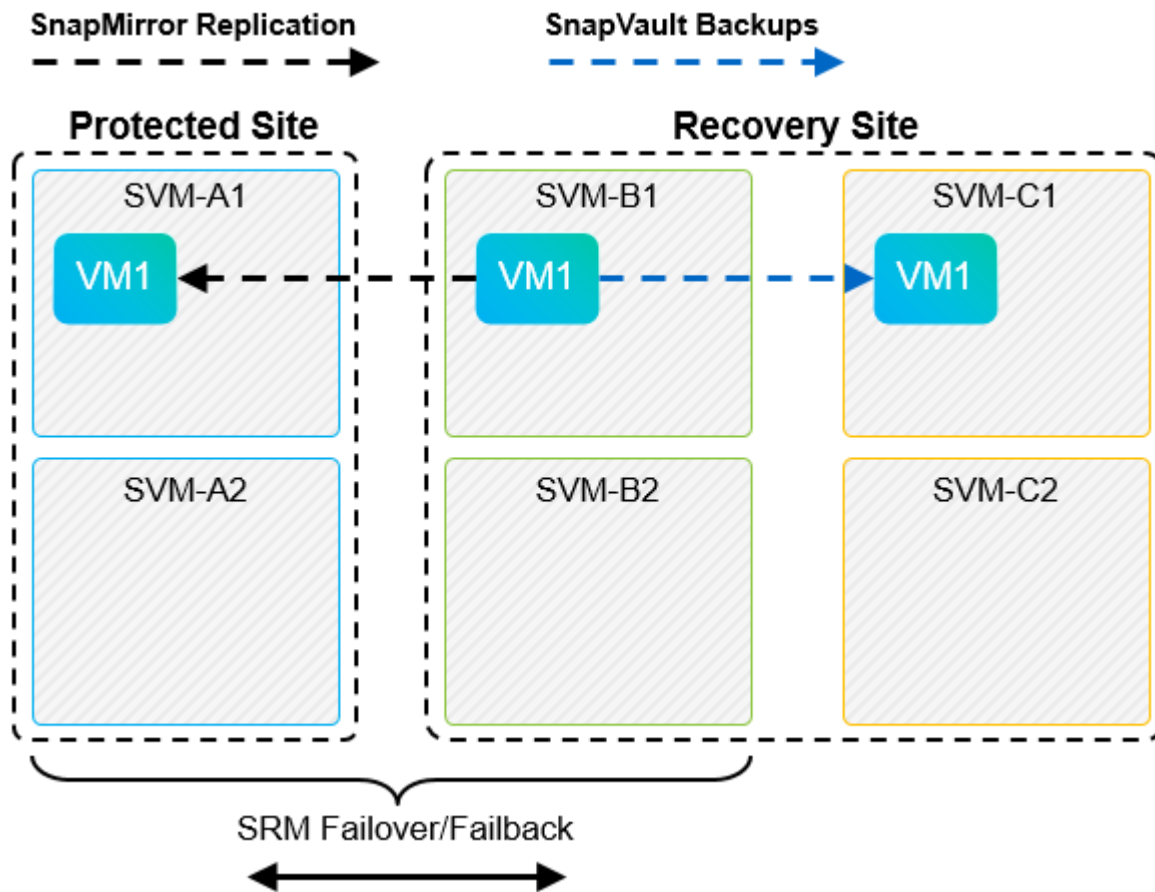
In einer VMware Umgebung verfügt jeder Datenspeicher über eine universelle eindeutige Kennung (Universal Unique Identifier, UUID) und jede VM über eine eindeutige Managed Object ID (MOID). Diese IDs werden während Failover oder Failback durch VLSR nicht gepflegt. Da Datastore-UIDs und VM-MOIDs beim Failover durch VLSR nicht gepflegt werden, müssen nach dem VLSR Failover alle Applikationen, die von diesen IDs abhängen, neu konfiguriert werden. Eine Beispielapplikation ist NetApp Active IQ Unified Manager, wo die SnapVault Replizierung mit der vSphere Umgebung koordiniert wird.

Die folgende Abbildung zeigt die Kaskadenkonfiguration von SnapMirror auf SnapVault. Wenn sich das SnapVault Ziel am DR-Standort oder an einem tertiären Standort befindet, der nicht von einem Ausfall am primären Standort betroffen ist, kann die Umgebung neu konfiguriert werden, sodass Backups nach dem Failover fortgesetzt werden können.



In der folgenden Abbildung wird die Konfiguration dargestellt, nachdem VLSR die SnapMirror Replizierung

zurück auf den primären Standort umgekehrt hat. Die Umgebung wurde außerdem neu konfiguriert, sodass SnapVault Backups von der jetzt SnapMirror Quelle durchgeführt werden. Bei dieser Einrichtung handelt es sich um eine Fan-out-Konfiguration für SnapMirror SnapVault.



Nachdem vsrm ein Failback und eine zweite Umkehr der SnapMirror Beziehungen durchführt, sind die Produktionsdaten am primären Standort zurück. Die Daten werden jetzt auf dieselbe Weise gesichert wie vor dem Failover zum DR-Standort – über SnapMirror und SnapVault Backups.

## Verwendung von Qtrees in Site Recovery Manager-Umgebungen

Qtrees sind spezielle Verzeichnisse, die die Anwendung von Filesystem-Kontingenten für NAS ermöglichen. ONTAP 9 ermöglicht die Erstellung von qtrees und qtrees in Volumes, die mit SnapMirror repliziert werden. SnapMirror ermöglicht jedoch nicht die Replizierung einzelner qtrees oder Qtree-Level-Replikationen. Alle SnapMirror Replikation befindet sich nur auf Volume-Ebene. Aus diesem Grund empfiehlt NetApp die Verwendung von qtrees mit VLSR nicht.

## Gemischte FC- und iSCSI-Umgebungen

Mit den unterstützten SAN-Protokollen (FC, FCoE und iSCSI) bietet ONTAP 9 LUN-Services an, d. h. die Möglichkeit, LUNs zu erstellen und angebotenen Hosts zuzuweisen. Da das Cluster aus mehreren Controllern besteht, gibt es mehrere logische Pfade, die von Multipath I/O zu einer beliebigen einzelnen LUN gemanagt werden. Auf den Hosts wird mithilfe des Asymmetric Logical Unit Access (ALUA) der optimale Pfad zu einer LUN ausgewählt und für den Datentransfer aktiviert. Wenn sich der optimierte Pfad zu einer LUN ändert (z. B. weil das zugehörige Volume verschoben wird), erkennt ONTAP 9 diese Änderung automatisch und passt sich unterbrechungsfrei an. Wenn der optimierte Pfad nicht mehr verfügbar ist, kann ONTAP ohne Unterbrechungen zu einem anderen verfügbaren Pfad wechseln.

VMware VLSR und NetApp SRA unterstützen die Nutzung des FC-Protokolls an einem Standort und das iSCSI-Protokoll am anderen Standort. Eine Kombination aus FC-Attached Datastores und iSCSI-Attached Datastores wird jedoch auf demselben ESXi Host oder auf verschiedenen Hosts im selben Cluster nicht unterstützt. Diese Konfiguration wird mit VLSR nicht unterstützt, da VLSR während des VLSR Failover oder des Test-Failovers alle FC- und iSCSI-Initiatoren in den ESXi-Hosts in der Anforderung enthält.

#### Best Practices In Sich

VLSR und SRA unterstützen gemischte FC- und iSCSI-Protokolle zwischen den geschützten und den Recovery-Standorten. Allerdings sollte jeder Standort nur mit einem Protokoll, entweder FC oder iSCSI, konfiguriert werden, nicht mit beiden Protokollen am selben Standort. Wenn FC- und iSCSI-Protokolle am selben Standort konfiguriert werden müssen, empfiehlt NetApp, dass einige Hosts iSCSI verwenden und andere Hosts FC verwenden. NetApp empfiehlt in diesem Fall außerdem die VLSR-Ressourcenzuordnung, damit die VMs für das Failover in eine Gruppe von Hosts oder die andere konfiguriert werden.

## Fehlerbehebung bei VLSRM/SRM bei Verwendung der VVols-Replikation

Bei Verwendung der ONTAP Tools 9.13P2 unterscheidet sich der Workflow innerhalb von VLSR und SRM bei der VVols-Replizierung erheblich von dem, was mit SRA und herkömmlichen Datastores verwendet wird. Zum Beispiel gibt es kein Konzept für Array-Manager. So `discoverarrays` und `discoverdevices` Befehle werden nie gesehen.

Bei der Fehlerbehebung sind die neuen Workflows zu verstehen, die im Folgenden aufgeführt sind:

1. `QueryReplicationPeer`: Ermittelt die Replikationsvereinbarungen zwischen zwei Fehlerdomänen.
2. `QueryFaultDomain`: Ermittelt die Fehlerdomäne-Hierarchie.
3. `QueryReplicationGroup`: Ermittelt die in den Quell- oder Zieldomänen vorhandenen Replikationsgruppen.
4. `SyncReplicationGroup`: Synchronisiert die Daten zwischen Quelle und Ziel.
5. `QueryPointInTimeReplica`: Ermittelt die Point-in-Time-Replikate auf einem Ziel.
6. `TestFailoverReplicationGroupStart`: Startet Test Failover.
7. `TestFailoverReplicationGroupStop`: Beendet das Test-Failover.
8. `PromoteReplicationGroup`: Fördert eine Gruppe, die sich derzeit in der Produktion befindet.
9. `PreparrreFailoverReplicationGroup`: Bereitet sich auf eine Notfallwiederherstellung vor.
10. `Failover ReplicationGroup`: Durchführung einer Disaster Recovery
11. `ReverseReplicateGroup`: Initiiert Reverse-Replikation.
12. `QueryMatchingContainer`: Sucht Container (zusammen mit Hosts oder Replikationsgruppen), die eine Bereitstellungsanfrage mit einer bestimmten Richtlinie erfüllen können.
13. `QueryResourceMetadaten`: Ermittelt die Metadaten aller Ressourcen des VASA Providers, kann die Ressourcenauslastung als Antwort auf die `queryMatchingContainer`-Funktion zurückgegeben werden.

Der häufigste Fehler bei der Konfiguration der VVols-Replizierung ist das Erkennen der SnapMirror Beziehungen. Dies geschieht, weil die Volumes und SnapMirror Beziehungen außerhalb der ONTAP Tools-Ansicht erstellt werden. Daher empfiehlt es sich, immer sicherzustellen, dass die SnapMirror Beziehung vollständig initialisiert ist und dass Sie an beiden Standorten eine erneute Bestandsaufnahme in ONTAP Tools ausführen, bevor Sie versuchen, einen replizierten VVols Datastore zu erstellen.

## Weitere Informationen

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- ONTAP-Tools für VMware vSphere 10.x-Ressourcen  
["https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"](https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab)
- ONTAP-Tools für VMware vSphere 9.x-Ressourcen  
["https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"](https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab)
- TR-4597: VMware vSphere für ONTAP  
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html)
- TR-4400: VMware vSphere Virtual Volumes with ONTAP  
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html)
- TR-4015 SnapMirror -Konfigurationsleitfaden – Best Practices für ONTAP 9  
<https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf>
- VMware Live Site Recovery-Dokumentation ["https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"](https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html)

**"Interoperabilitäts-Matrix-Tool (IMT)"** Überprüfen Sie auf der NetApp-Support-Website, ob die in diesem Dokument angegebenen Produktversionen und Funktionen in Ihrer IT-Umgebung unterstützt werden. Das NetApp IMT definiert die Produktkomponenten und -Versionen, die für von NetApp unterstützte Konfigurationen verwendet werden können. Die dort angezeigten Ergebnisse basieren auf der spezifischen Infrastruktur des jeweiligen Kunden bzw. auf den technischen Daten der in dieser Infrastruktur enthaltenen Komponenten.

## Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.