VMware Site Recovery Manager mit ONTAP

Enterprise applications

NetApp
May 09, 2024

Inhalt

VMware Site Recovery Manager mit ONTAP

VMware Site Recovery Manager mit ONTAP

ONTAP ist seit seiner Einführung in das moderne Datacenter im Jahr 2002 eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich um innovative Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen.

Dieses Dokument enthält eine Einführung in die ONTAP Lösung für VMware Site Recovery Manager (SRM), die branchenführende VMware Software für Disaster Recovery (DR), sowie in die neuesten Produktinformationen und Best Practices zur Optimierung der Bereitstellung, Risikominderung und Vereinfachung des fortlaufenden Managements.

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 9.12 (einschließlich NetApp Storage Replication Adapter [SRA] und VASA Provider [VP]) sowie VMware Site Recovery Manager 8.7 verwendet werden.

Vorteile von ONTAP mit SRM

Die NetApp Datenmanagementplattformen auf der Basis von ONTAP Software sind eine der am weitesten verbreiteten Storage-Lösungen für SRM. Die Gründe hierfür sind vielfältig: Eine sichere, hochperformante, einheitliche Protokoll-Datenmanagementplattform (NAS und SAN zusammen), die branchenweit definierte Storage-Effizienz, Mandantenfähigkeit, Quality-of-Service-Kontrollen, Datensicherung mit platzsparenden Snapshots und Replizierung mit SnapMirror bietet. Dabei werden native Hybrid-Multi-Cloud-Integrationen für die Sicherung von VMware Workloads sowie eine Fülle von Automatisierungs- und Orchestrierungs-Tools blitzschnell verfügbar.

Wenn Sie SnapMirror für die Array-basierte Replizierung nutzen, profitieren Sie von einer der bewährten und ausgereiftesten Technologien von ONTAP. Mit SnapMirror profitieren Sie von sicheren und hocheffizienten Datentransfers, wobei nur geänderte Datenblöcke kopiert werden, nicht die gesamten VMs oder Datastores. Selbst diese Blöcke profitieren von Platzeinsparungen wie Deduplizierung, Komprimierung und Data-Compaction. Moderne ONTAP Systeme verwenden jetzt versionsunabhängiges SnapMirror für die flexible Auswahl von Quell- und Ziel-Clustern. SnapMirror hat sich tatsächlich zu einem der leistungsstärksten Tools für Disaster Recovery entwickelt.

Ganz gleich, ob Sie herkömmliche NFS-, iSCSI- oder Fibre Channel-Attached Datastores verwenden (jetzt mit Unterstützung für VVols Datastores) – SRM bietet Ihnen einen robusten Erstanbieter, der die besten ONTAP Funktionen für Disaster Recovery oder Planung der Datacenter-Migration und -Orchestrierung nutzt.

Wie SRM ONTAP 9 nutzt

SRM 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, ehemals Virtual Storage Console (VSC), vereinfacht Storage-Management- und Effizienzfunktionen, verbessert die Verfügbarkeit und senkt die Storage-Kosten und den Betriebsaufwand – sei es bei SAN oder 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 dieses Plug-in bei der Verwendung von vSphere bei Systemen mit ONTAP Software.
- Vasa Provider für ONTAP unterstützt 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. Es unterstützt die Unterstützung von VMware Virtual Volumes (VVols) und das Management von Storage-Funktionsprofilen (einschließlich VVols Replizierungsfunktionen) und der individuellen VM VVols Performance. Außerdem gibt es Alarme zur Überwachung der Kapazität und der Konformität mit den Profilen. In Verbindung mit SRM ermöglicht der VASA Provider for ONTAP Unterstützung für VVols basierte Virtual Machines, ohne dass ein SRA Adapter auf dem SRM Server installiert werden muss.
- SRA wird zusammen mit SRM 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. Sie enthält sowohl eine SRA Server-Appliance als auch SRA Adapter für den Windows SRM Server und die SRM Appliance.

Nachdem Sie die SRA Adapter auf dem SRM-Server zum Schutz von Datastores außerhalb von VVols sowie zur aktivierten VVols-Replizierung in den VASA Provider-Einstellungen installiert und konfiguriert haben, können Sie mit der Aufgabe beginnen, Ihre vSphere Umgebung für die Disaster Recovery zu konfigurieren.

SRA und VASA Provider bieten eine Befehlszeilenschnittstelle für den SRM Server zum Managen der ONTAP FlexVols, die Ihre VMware Virtual Machines (VMs) enthalten, sowie zur SnapMirror Replizierung, die sie sichern.

Ab SRM 8.3 wurde ein neuer SRM VVols Provider-Kontrollpfad in den SRM Server eingeführt, der die IT in die Lage versetzt, mit dem vCenter Server und darüber hinaus ohne SRA mit dem VASA Provider zu kommunizieren. Auf diese Weise konnte der SRM Server eine wesentlich umfassendere Kontrolle über das ONTAP Cluster nutzen als bisher möglich, da VASA eine vollständige API für eine nahtlose Integration bietet.

SRM kann Ihren DR-Plan mithilfe der proprietären NetApp FlexClone Technologie unterbrechungsfrei testen, um nahezu sofortige Klone Ihrer geschützten Datenspeicher an Ihrem DR-Standort zu erstellen. SRM erstellt eine Sandbox-Umgebung für sichere Tests, damit sowohl Ihre Organisation als auch Ihre Kunden bei einem echten Ausfall geschützt sind. So können Ihre Unternehmen sicher sein, dass bei einem Ausfall ein Failover ausgeführt werden kann.

Bei einem echten Ausfall oder sogar einer geplanten Migration können Sie mit SRM 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.

SRM mit ONTAP und anderen Anwendungsfällen: Hybrid Cloud und Migration

Durch Integration Ihrer SRM-Implementierung mit erweiterten Datenmanagement-Funktionen von ONTAP lassen sich im Vergleich zu lokalen Storage-Optionen deutlich bessere Skalierungs- und Performance-Möglichkeiten erzielen. Darüber hinaus bringt sie jedoch noch mehr die Flexibilität der Hybrid Cloud. Mit der Hybrid Cloud können Sie Geld sparen, indem Sie ungenutzte Datenblöcke des High-Performance-Arrays mittels FabricPool in den bevorzugten Hyperscaler verschieben, was ein lokaler S3-Speicher wie NetApp StorageGRID sein könnte. Außerdem können Edge-basierte Systeme mit softwaredefiniertem ONTAP Select oder Cloud-basierter DR mithilfe von Cloud Volumes ONTAP (CVO) oder verwendet werden "NetApp Private

Storage in Equinix" Um einen vollständig integrierten Storage-, Networking- und Computing-Service-Stack in der Cloud zu erstellen, führt Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) zum Vorteil.

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 SRM 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.

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.

Nur bei der Verwendung von NAS-Protokollen (kein SAN-Zugriff) können Sie sogar den neuen NAS-optimierten Modus nutzen, indem Sie den folgenden Parameter einstellen (beachten Sie, dass der Name so ist, da SRA und VASA dieselben Backend-Services in der Appliance nutzen):

1. Melden Sie sich am Bedienfeld unter an `https://<IP address>:9083` Und klicken Sie auf webbasierte CLI-Schnittstelle.
2. Führen Sie den Befehl aus `vp updateconfig -key=enable.qtree.discovery -value=true`.
3. Führen Sie den Befehl aus `vp updateconfig -key=enable.optimised.sra -value=true`.
4. Führen Sie den Befehl aus `vp reloadconfig`.

Implementieren von ONTAP-Tools und Überlegungen für VVols

Falls Sie SRM mit VVols verwenden möchten, müssen Sie den Storage mit Anmeldedaten für den Cluster-Umfang und einer Cluster-Management-LIF managen. Der Grund dafür ist, dass VASA Provider die zugrunde liegende physische Architektur verstehen muss, um die für VM Storage-Richtlinien erforderlichen Richtlinien erfüllen zu können. Wenn Sie beispielsweise eine Richtlinie haben, die All-Flash-Storage erfordert, muss der VASA Provider in der Lage sein, zu sehen, welche All-Flash-Systeme sind.

Eine weitere Best Practice bei der Implementierung besteht darin, Ihre ONTAP Tools Appliance niemals auf

einem VVols Datastore zu speichern, den sie managen. Dies kann dazu führen, dass Sie den VASA Provider nicht einschalten können, da Sie die Swap-vVol für die Appliance nicht erstellen können, da die Appliance offline ist.

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.
- Wenn Sie ONTAP 9.8 oder höher verwenden, empfiehlt NetApp die Erstellung eines RBAC-Kontos mit den geringsten Berechtigungen über das Benutzermenü von ONTAP System Manager sowie die JSON-Datei, die auf der ONTAP Tools-Appliance unter verfügbar ist `https://<IP address>:9083/vsc/config/`. Verwenden Sie Ihr Administratorpasswort, um die JSON-Datei herunterzuladen. Diese Option kann für SVM oder Konten mit Cluster-Umfang verwendet werden.

  Wenn Sie ONTAP 9.6 oder eine frühere Version verwenden, sollten Sie das RUC-Tool (RBAC User Creator) verwenden, das im verfügbar ist "NetApp Support Site Tool".

- Da die vCenter UI Plug-in, VASA Provider und SRA Server vollständig integrierte Services sind, müssen Sie den SRA-Adapter in SRM um Storage ebenso ergänzen wie in der vCenter UI für ONTAP-Tools. Andernfalls erkennt der SRA-Server möglicherweise nicht die Anfragen, die von SRM über den SRA-Adapter gesendet werden.
- Die NFS-Pfadprüfung wird bei der Verwendung der SVM-Scoped-Anmeldedaten nicht durchgeführt. 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-Datastores.
- 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. Beispielsweise können Sie FCP in Seite A und iSCSI in Standort B verwenden Sie sollten FCP und iSCSI nicht an Standort A verwenden Der Grund hierfür: Der SRA erstellt nicht gemischte Initiatorgruppen am Recovery-Standort, und SRM filtert nicht die Initiatorliste, die den SRA gegeben wurde.
- 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. In modernen Versionen von ONTAP 9 ist das nicht mehr erforderlich. 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 für den Versuch.

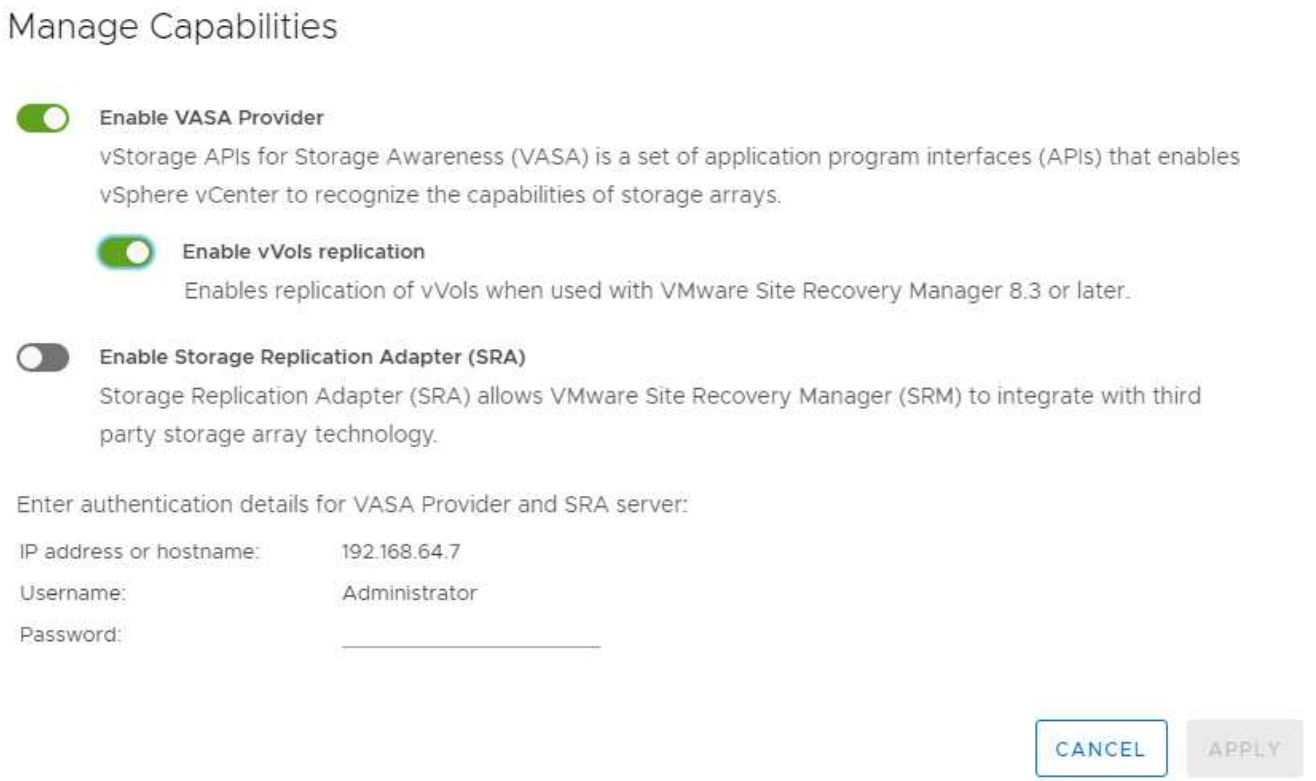
```
snap autodelete modify -volume -commitment try
```

- Die automatische Volume-Größe sollte auf festgelegt werden `grow` Für Volumes mit SAN-Datastores und `grow_shrink` Für NFS-Datastores. Weitere Informationen zu "Automatisches Vergrößern oder Verkleinern von Volumes".
- SRM führt am besten aus, wenn die Anzahl der Datastores 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.

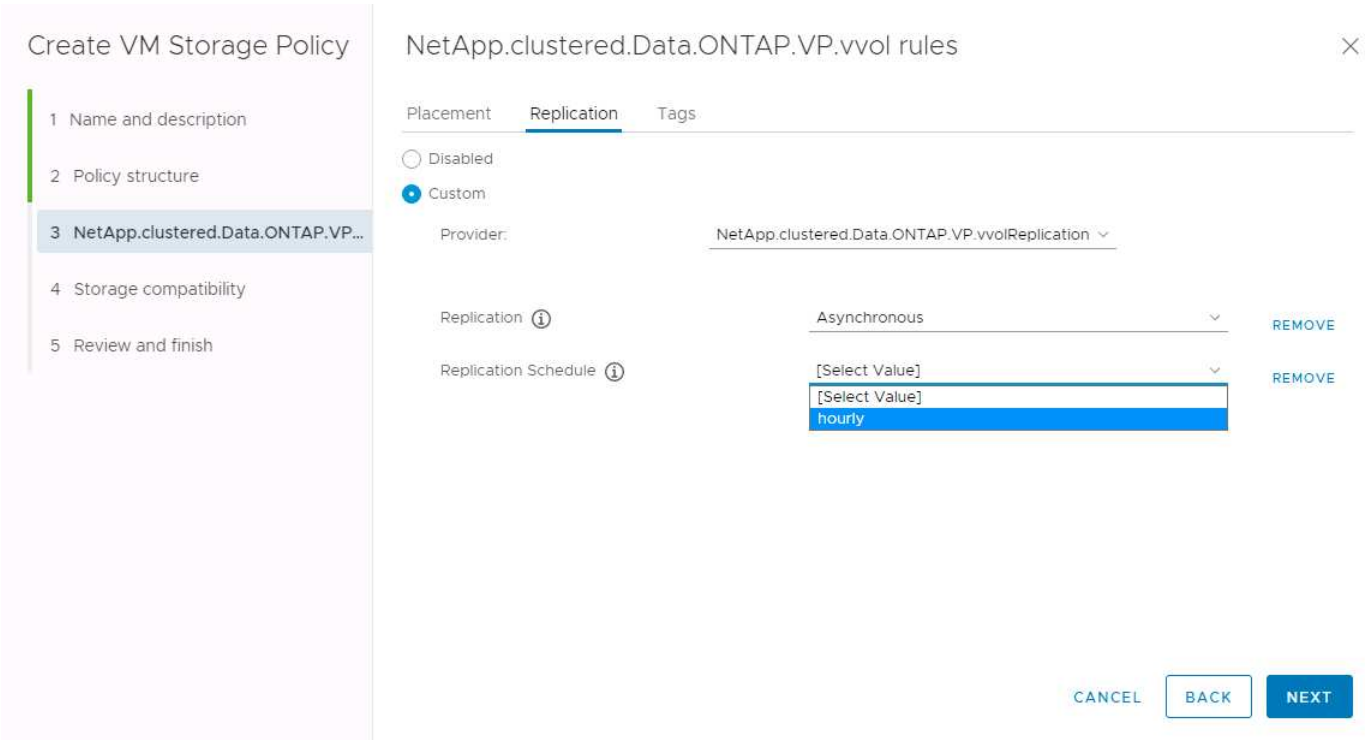
Storage Policy Based Management (SPBM) und VVols

Ab SRM 8.3 wird die Sicherung von VMs mit VVols Datastores unterstützt. SnapMirror Zeitpläne werden über den VASA Provider VM-Storage-Richtlinien ausgesetzt, wenn die VVols Replizierung im Einstellungsmenü der ONTAP Tools aktiviert ist, wie in den folgenden Screenshots dargestellt.

Im folgenden Beispiel wird die Aktivierung der VVols-Replizierung gezeigt.

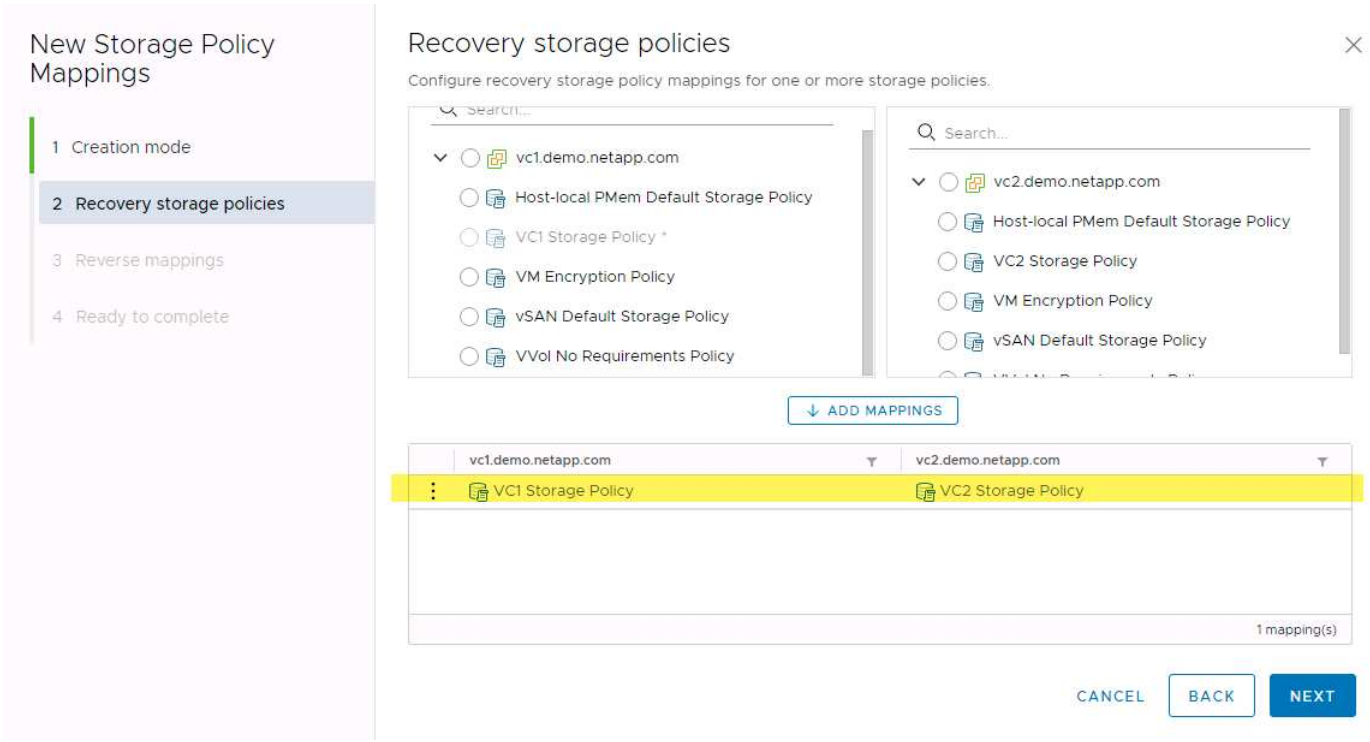


Der folgende Screenshot zeigt ein Beispiel zu SnapMirror Zeitplänen, die im Assistenten zur Erstellung von VM-Storage-Richtlinien angezeigt werden.



Der ONTAP VASA Provider unterstützt den Failover auf unterschiedlichen Storage. So kann beispielsweise ein Failover des Systems von ONTAP Select an einem Edge-Standort auf ein AFF System im Core-Datacenter durchgeführt werden. Unabhängig von Ähnlichkeit zum Storage müssen Sie für VM Storage-Richtlinien immer Storage-Richtlinien-Zuordnungen und Reverse-Mappings konfigurieren, damit die Services am Recovery-

Standort die Erwartungen und Anforderungen erfüllen. Der folgende Screenshot zeigt ein Beispiel für eine Richtlinienzuordnung.



Erstellung replizierter Volumes für VVols-Datastores

Im Gegensatz zu älteren VVols-Datastores müssen replizierte VVols Datastores von Anfang an bei aktivierter Replizierung erstellt werden. Dabei müssen sie Volumes verwenden, die vorab auf den ONTAP Systemen mit SnapMirror Beziehungen erstellt wurden. Hierfür sind vorab-Konfigurationen wie Cluster-Peering und SVM-Peering erforderlich. Diese Aktivitäten sollten von Ihrem ONTAP Administrator durchgeführt werden, da hierdurch die Zuständigkeiten zwischen denjenigen, die ONTAP Systeme an mehreren Standorten managen, und denjenigen, die hauptsächlich für vSphere Vorgänge verantwortlich sind, strikt getrennt werden können.

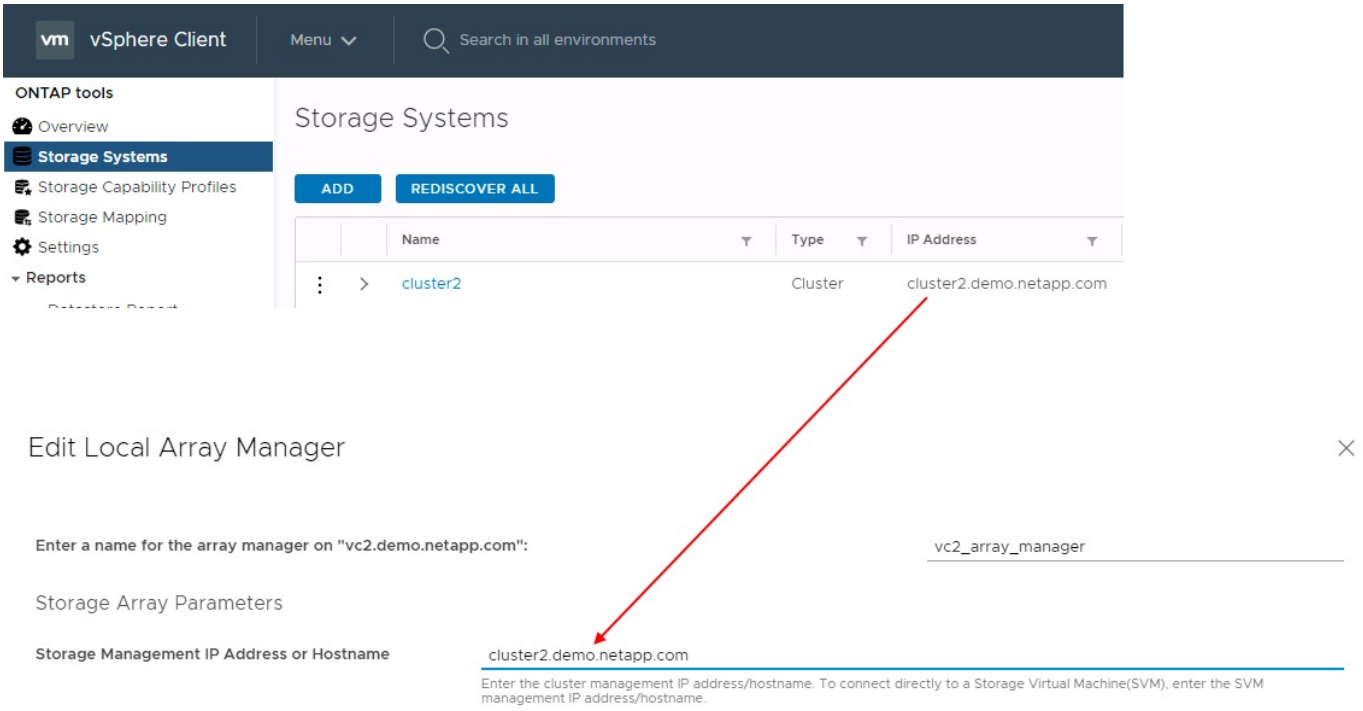
Dafür muss der vSphere Administrator eine neue Anforderung erfüllen. Da Volumes außerhalb der ONTAP Tools erstellt werden, ist es nicht bekannt, dass die Änderungen, die Ihr ONTAP-Administrator bis zur regelmäßigen planmäßigen Neuerfassungszeit vorgenommen hat. Daher ist es eine Best Practice, immer wieder neu zu ermitteln, wenn Sie eine Volume- oder SnapMirror Beziehung erstellen, die mit VVols verwendet werden soll. Klicken Sie einfach mit der rechten Maustaste auf den Host oder den Cluster und wählen Sie ONTAP Tools > Host- und Speicherdaten aktualisieren aus, wie im folgenden Screenshot dargestellt.

Bei VVols und SRM ist Vorsicht geboten. Niemals geschützte und ungesicherte VMs in demselben VVols Datastore zusammen Der Grund dafür: Wenn Sie SRM für das Failover an Ihrem DR-Standort verwenden, werden nur die VMs, die Teil der Sicherungsgruppe sind, in die DR online geschaltet. Wenn Sie die Sicherung rückgängig machen (das SnapMirror aus der DR wieder in die Produktionsumgebung verschieben), können die VMs, die nicht Failover waren, überschrieben werden und wertvolle Daten enthalten.

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. Mit den ONTAP Tools VASA Provider werden automatisch Replikationsgruppen für Sie erstellt. 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 die Aggregat-Deduplizierung bei Volume SnapMirror 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. Sie möchten wahrscheinlich, dass Ihr Microsoft Windows Domain Controller vor Ihrem Microsoft SQL Server hochgefahren wird, was 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 einen Test-Failover durchzuführen, wenn die Konfiguration eines geschützten VM Storage geändert wird. 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 im VMware vCenter Site Recovery Manager als Array behandelt. SRM unterstützt bestimmte Array-to-Array (oder SVM-zu-SVM) Replizierungslayouts.

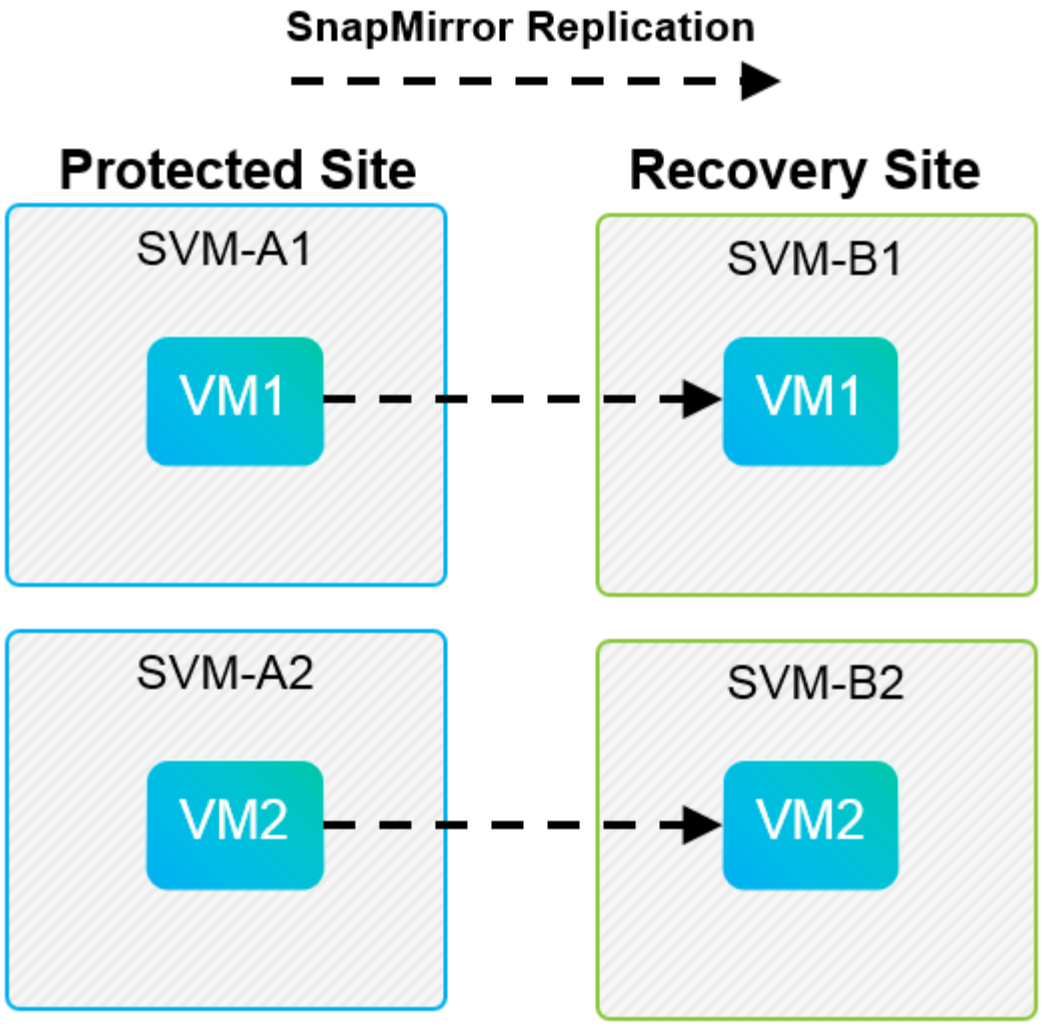
Eine einzelne VM kann aus den folgenden Gründen keine Daten besitzen – Virtual Machine Disk (VMDK) oder RDM – auf mehr als einem SRM Array:

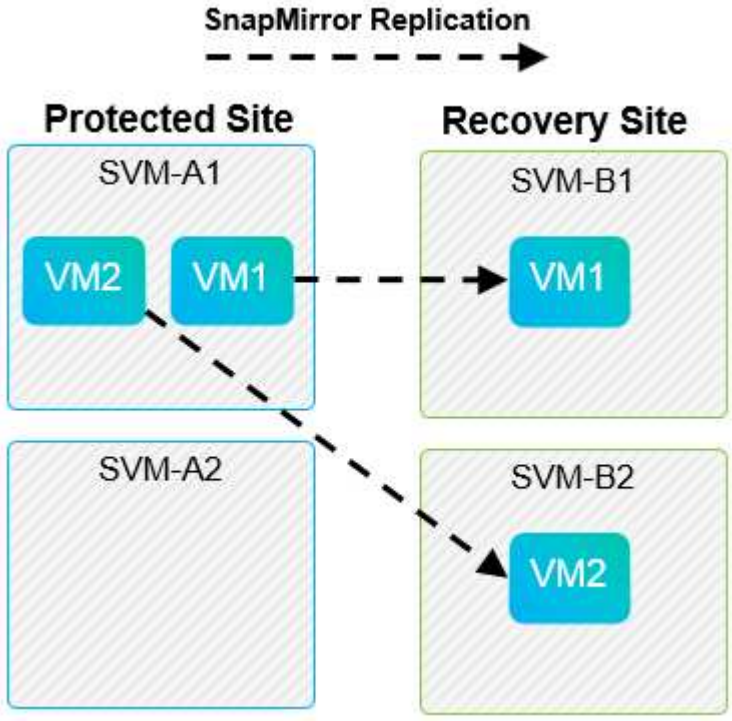
- SRM sieht nur die SVM, nicht einen individuellen physischen Controller.
- Eine SVM kann LUNs und Volumes steuern, die mehrere Nodes in einem Cluster umfassen.

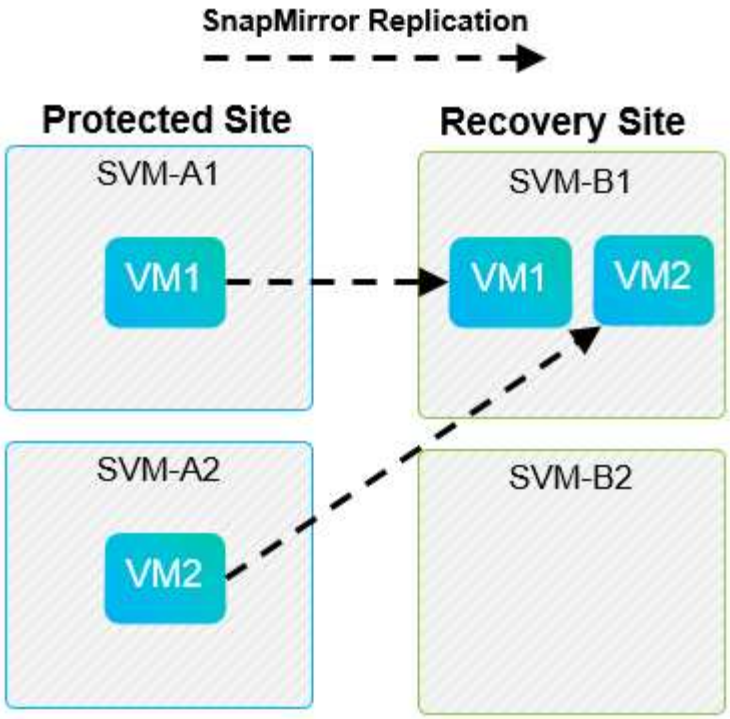
Best Practices In Sich
Bedenken Sie bei der Ermittlung von Supportmöglichkeiten diese Regel: Um eine VM mithilfe von SRM und der NetApp SRA zu schützen, müssen alle Bestandteile der VM nur auf einer SVM vorhanden sein. Diese Regel gilt sowohl für den geschützten Standort als auch für den Recovery-Standort.

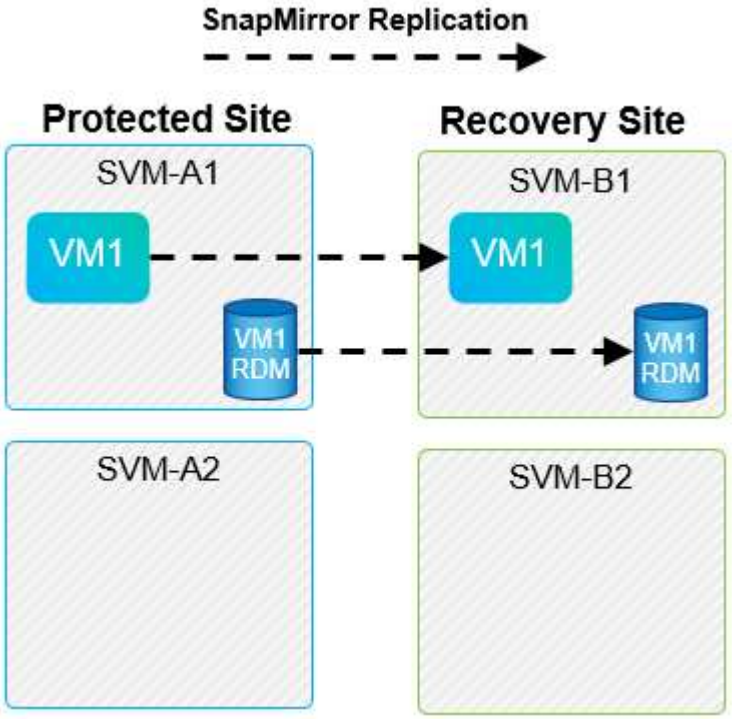
Unterstützte SnapMirror Layouts

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


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2

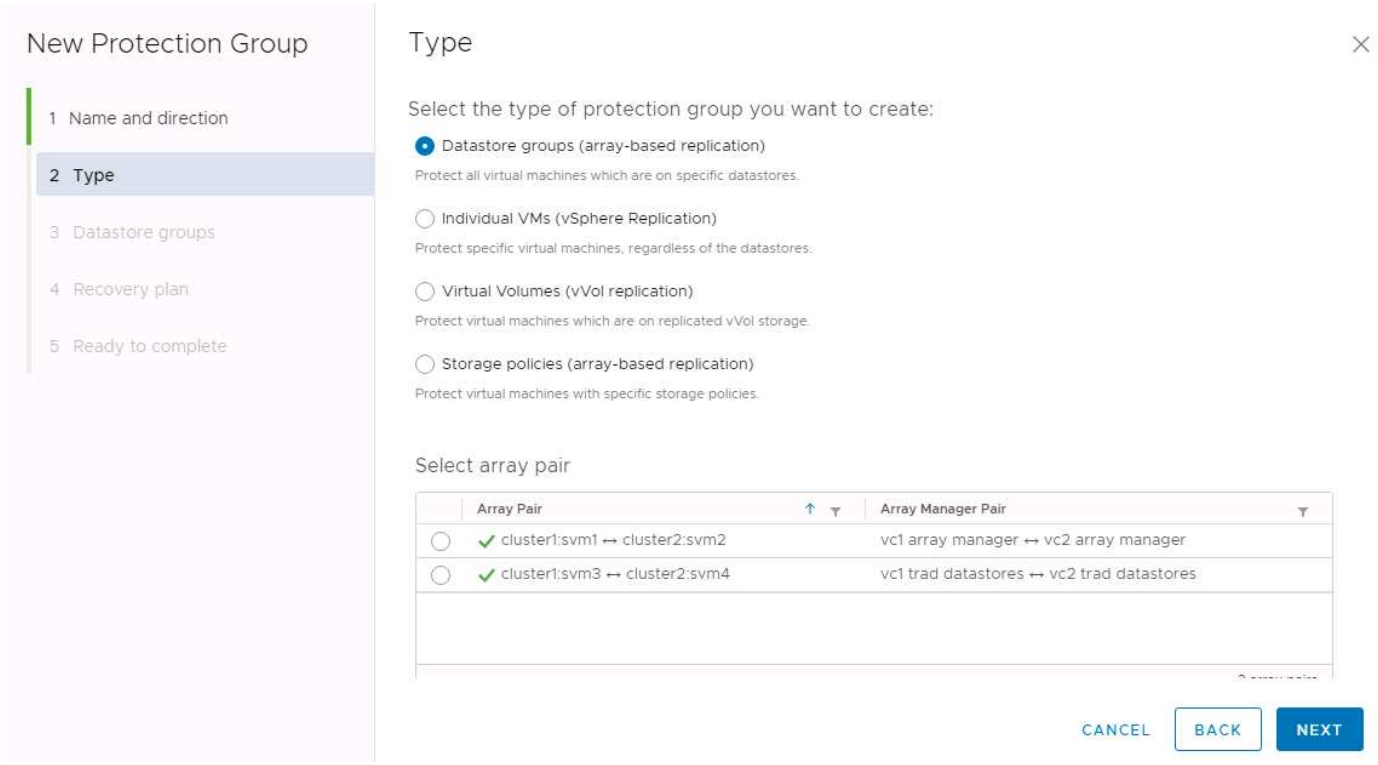

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2





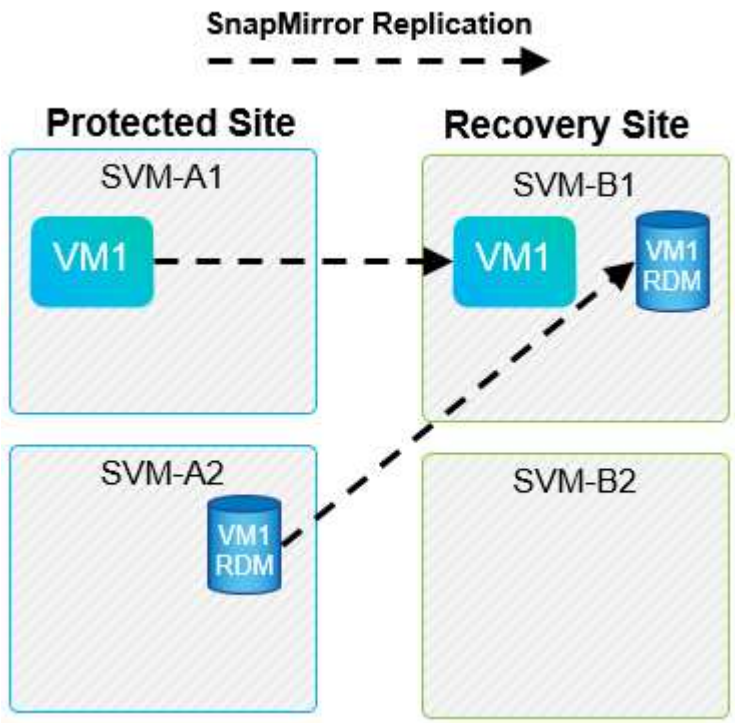
Unterstützte Array Manager-Layouts

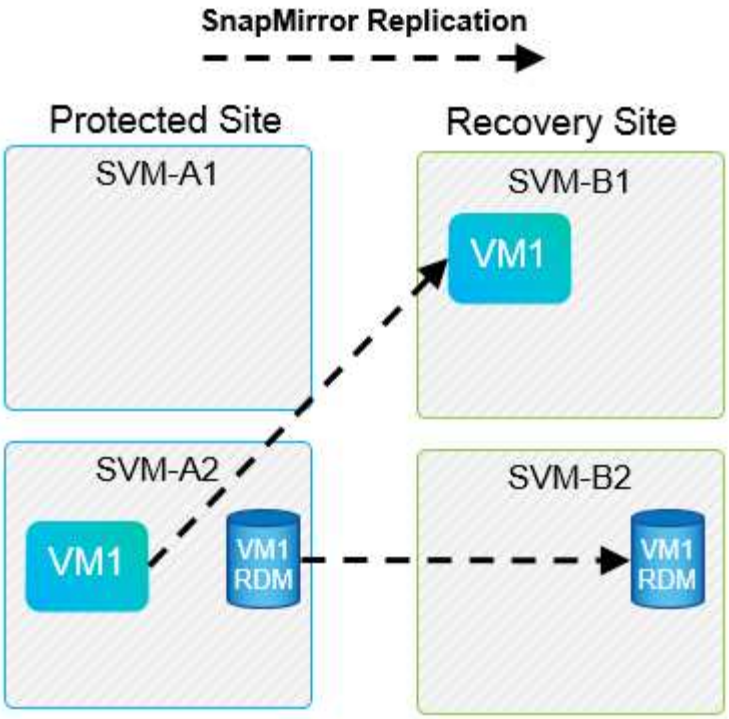
Wenn Sie in SRM Array-basierte Replizierung (ABR) verwenden, werden Schutzgruppen auf ein einzelnes Array-Paar isoliert, wie im folgenden Screenshot dargestellt. In diesem Szenario `SVM1` Und `SVM2` Werden mit Peering durchgeführt `SVM3` Und `SVM4` Am Recovery-Standort. Sie können jedoch nur eines der beiden Array-Paare auswählen, wenn Sie eine Schutzgruppe erstellen.



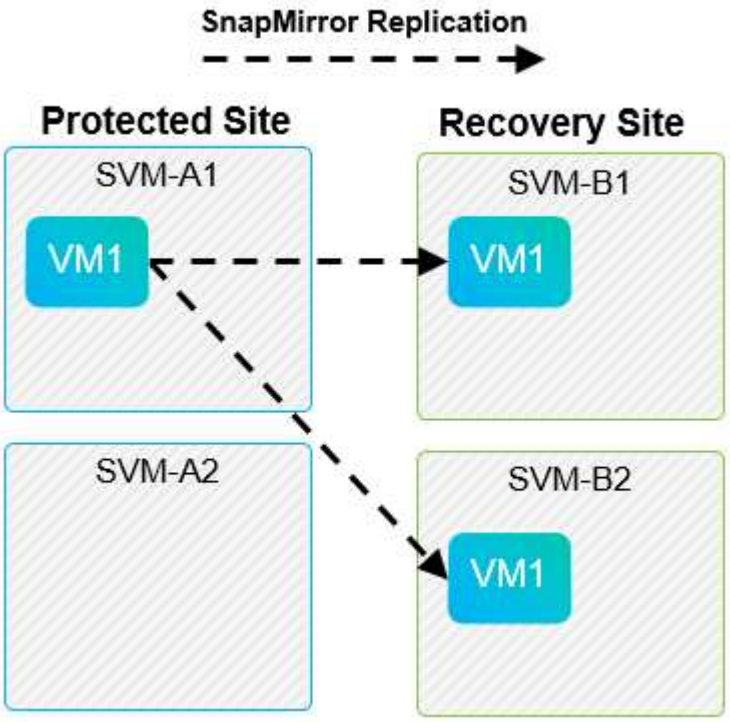
Nicht unterstützte Layouts

Nicht unterstützte Konfigurationen beinhalten Daten (VMDK oder RDM) auf mehreren SVMs, die sich im Besitz einer individuellen VM befinden. In den folgenden Abbildungen sind `VM1` Kann aus dem Grund nicht für den Schutz mit SRM konfiguriert werden `VM1` Verfügt über Daten auf zwei SVMs.





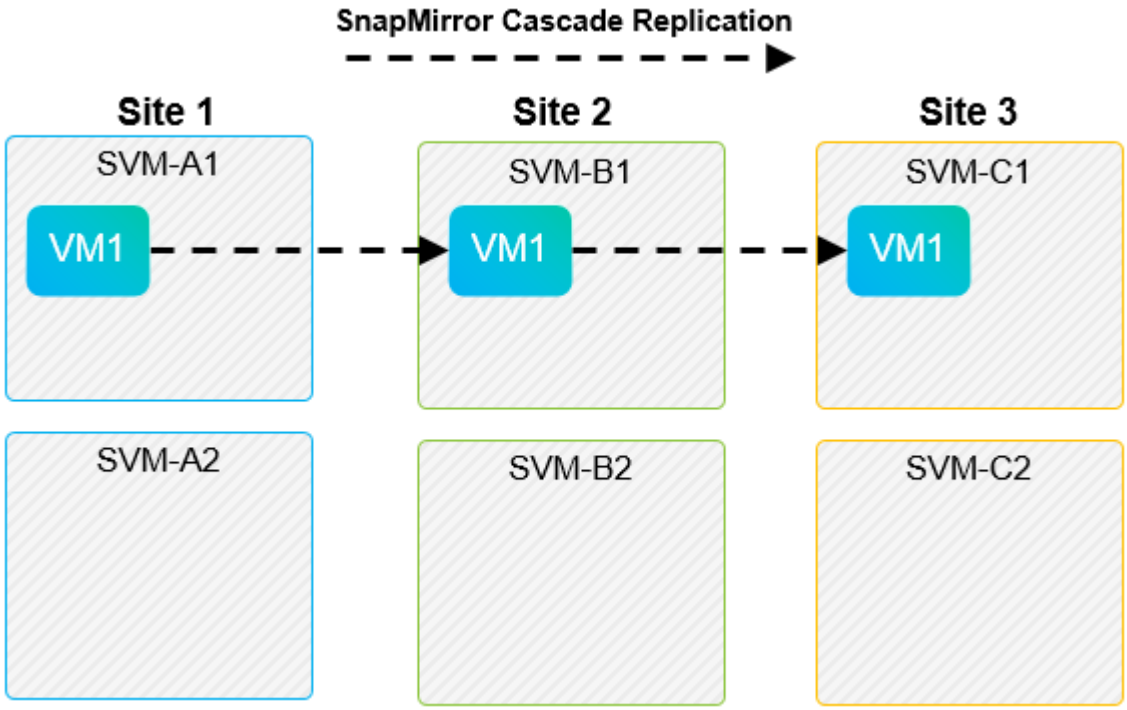
Jegliche Replizierungsbeziehungen, bei denen ein einzelnes NetApp Volume von einer Quell-SVM auf mehrere Ziele in derselben SVM oder in verschiedenen SVMs repliziert wird, werden als SnapMirror Fan-out bezeichnet. Fan-out wird mit SRM nicht unterstützt. In der folgenden Abbildung ist das Beispiel dargestellt.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



SnapMirror Kaskadierung

SRM 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 SRM 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. SRM unterstützt jedoch nur das Failover der SnapMirror Beziehungen.

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

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

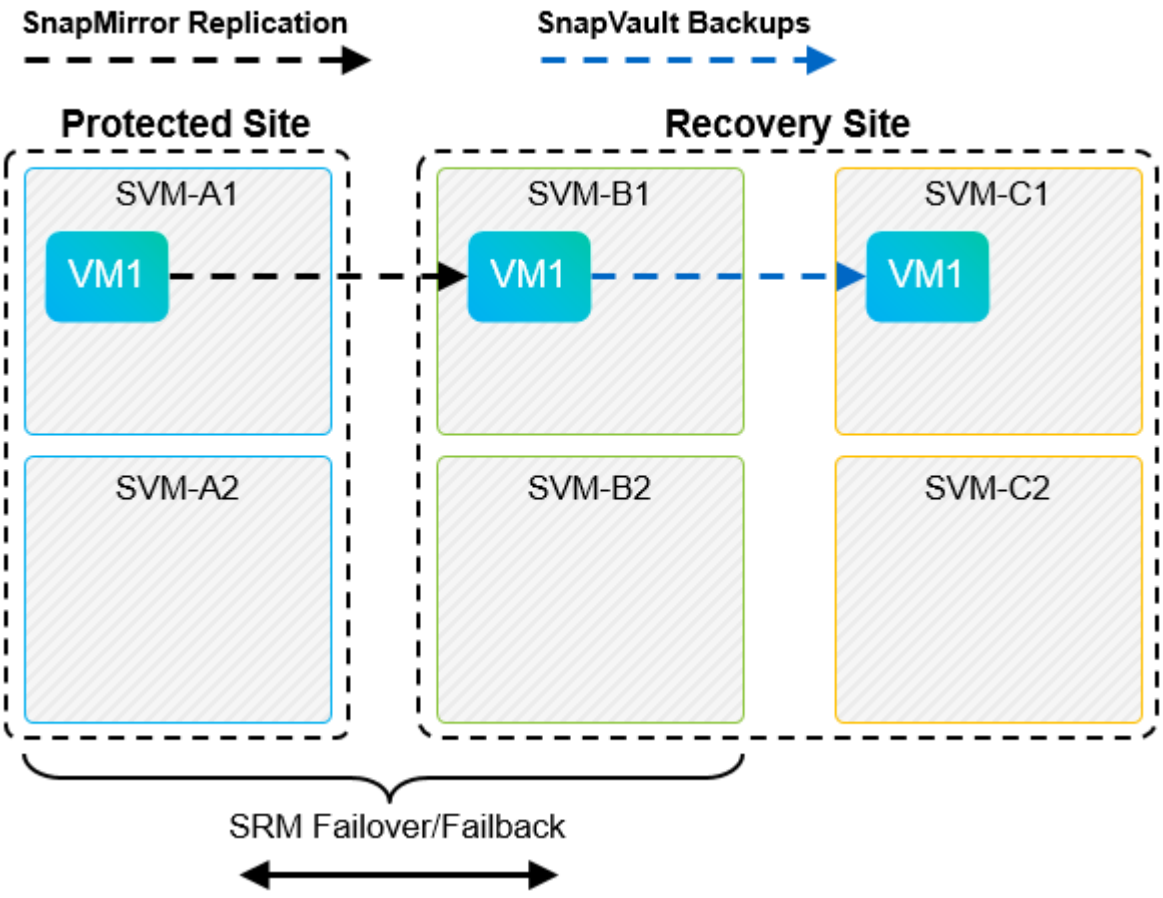
SnapMirror Ziel-Volume als Quelle für den Vault zu verwenden, wenn das SRM Failover oder eine Umkehrung der Replizierung stattfindet.

Aktuelle Informationen zu SnapMirror und SnapVault für ONTAP 9 finden Sie unter "TR-4015 SnapMirror Configuration Best Practice Guide für ONTAP 9."

Best Practices In Sich
Wenn in derselben Umgebung SnapVault und SRM 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.

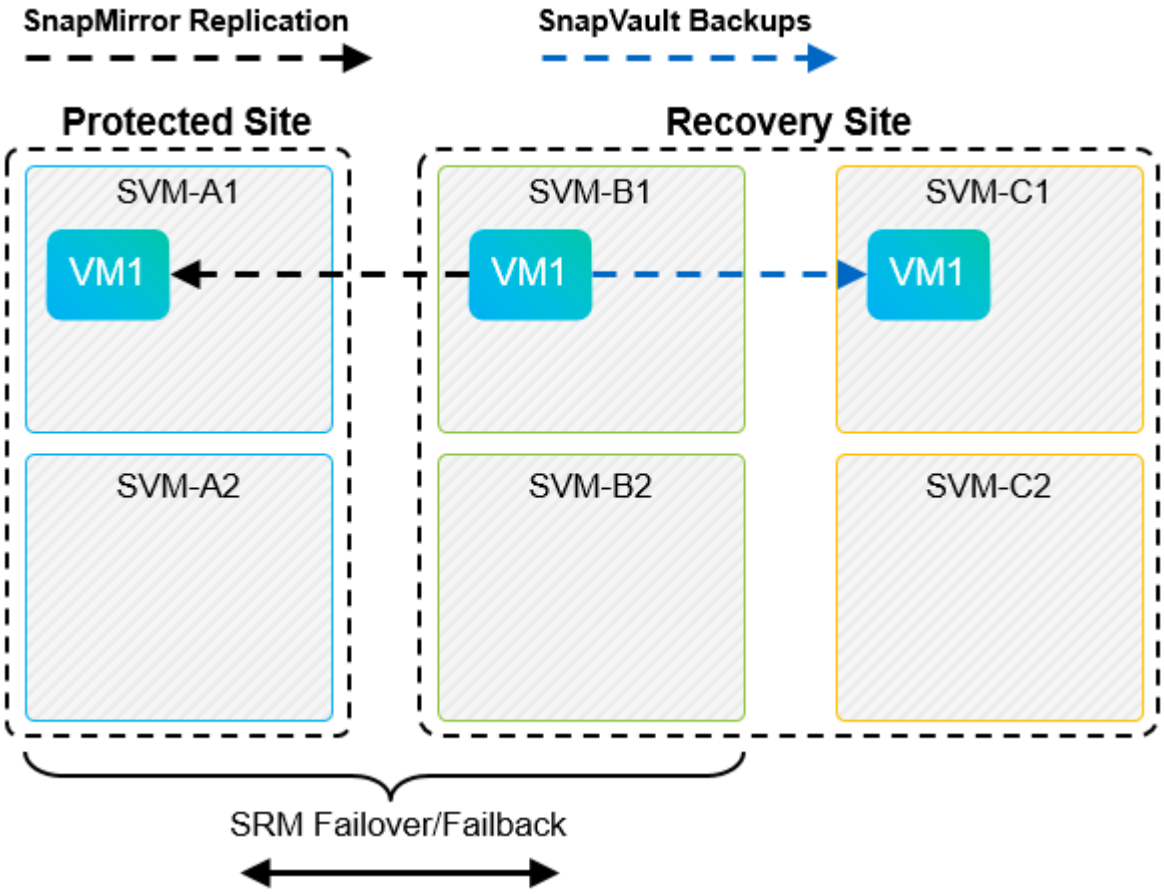
In einer VMware Umgebung verfügt jeder Datenspeicher über eine universelle eindeutige Kennung (Universal Unique Identifier, UUID) und jede VM über eine eindeutige Managed Object ID (MOID). Diese IDs werden während Failover oder Failback durch SRM nicht gepflegt. Da Datastore-UIDs und VM-MOIDs beim Failover durch SRM nicht gepflegt werden, müssen nach dem SRM 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 SRM 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 SRM ein Failback und eine zweite Umkehrung 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 SRM 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 angebundenen 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 SRM 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 SRM nicht unterstützt, da SRM während des SRM Failover oder des Test-Failovers alle FC- und iSCSI-Initiatoren in den ESXi-Hosts in der Anforderung enthält.

Best Practices In Sich
SRM 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 SRM-Ressourcenzuordnung, damit die VMs für das Failover in eine Gruppe von Hosts oder die andere konfiguriert werden.

Fehlerbehebung bei SRM bei Nutzung der VVols-Replizierung

Der Workflow in SRM unterscheidet sich deutlich, wenn VVols Replizierung mit dem verwendet wird, 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. PreparreFailoverReplicationGroup: 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:

- TR-4597: VMware vSphere für ONTAP
  "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"
- TR-4015 SnapMirror Configuration Best Practice Guide für ONTAP 9
  https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- RBAC Benutzer-Creator für ONTAP
  "https://mysupport.netapp.com/site/tools/tool-eula/rbac"
- ONTAP Tools für VMware vSphere Ressourcen
  "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- VMware Site Recovery Manager - Dokumentation
  "https://docs.vmware.com/en/Site-Recovery-Manager/index.html"

Siehe "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.