



Datenspeicher und virtuelle Maschinen schützen

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

- Datenspeicher und virtuelle Maschinen schützen 1
 - Schützen Sie einen Hostcluster in ONTAP tools 1
 - Schutz mit SRA-Schutz verwenden 2
 - Konfigurieren Sie SRA in ONTAP tools, um Datastores zu schützen 2
 - Konfigurieren Sie SRA in ONTAP tools for VMware vSphere für SAN- und NAS-Umgebungen 3
 - Konfigurieren Sie SRA in ONTAP tools für hochskalierte Umgebungen 4
 - Konfigurieren Sie SRA auf der VMware Live Site Recovery Appliance mithilfe von ONTAP tools 5
 - Aktualisieren Sie die SRA-Anmeldeinformationen in ONTAP tools 6
 - Konfigurieren von geschützten und Wiederherstellungsstandorten in ONTAP tools 7
 - Konfiguration von Ressourcen für geschützte und Wiederherstellungsstandorte 9
 - Überprüfen Sie replizierte Speichersysteme in ONTAP tools 13
 - Fan-out-Schutz in ONTAP tools 14

Datenspeicher und virtuelle Maschinen schützen

Schützen Sie einen Hostcluster in ONTAP tools

ONTAP tools for VMware vSphere verwaltet den Schutz von Host-Clustern. Alle Datenspeicher, die zur ausgewählten SVM gehören und auf einem oder mehreren Hosts des Clusters eingebunden sind, werden unter einem Host-Cluster geschützt.

Bevor Sie beginnen

Stellen Sie sicher, dass diese Anforderungen erfüllt sind, bevor Sie einen Hostcluster schützen:

- Der Host-Cluster enthält Datenspeicher nur von einer einzigen SVM.
- Datenspeicher auf dem Host-Cluster werden nicht auf Hosts außerhalb des Clusters eingebunden.
- Die auf dem Hostcluster eingebundenen Datenspeicher sind VMFS-Datenspeicher mit iSCSI- oder FC-Protokoll. Die Verwendung von vVols, NFS- oder VMFS-Datenspeichern mit NVMe/FC- und NVMe/TCP-Protokollen ist nicht möglich.
- Datenspeicher, die auf FlexVol/LUN-Volumes basieren und auf einem Host eingebunden sind, sind nicht Teil einer Konsistenzgruppe.
- Datenspeicher, die auf FlexVol/LUN-Volumes basieren und auf einem Host eingebunden sind, sind nicht Teil einer SnapMirror-Beziehung.
- Der Host-Cluster enthält mindestens einen Datenspeicher.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie **NetApp ONTAP tools > Protect Cluster**.
3. Im Fenster „Cluster schützen“ werden der Datentyp und die Details der Storage Virtual Machine (VM) des Quellspeichers automatisch ausgefüllt. Der Link „Datenspeicher“ zeigt die geschützten Datenspeicher an.
4. **Beziehung hinzufügen** auswählen.
5. Im Fenster **SnapMirror Beziehung hinzufügen** werden die **Ziel-Storage-VM** und der **Richtlinientyp** ausgewählt.

Der Richtlinientyp kann asynchron oder AutomatedFailOverDuplex sein.

Wenn Sie die SnapMirror Beziehung als AutomatedFailOverDuplex Typ-Richtlinie hinzufügen, müssen Sie die Ziel-Speicher-VM als Speicher-Backend zu demselben vCenter hinzufügen, auf dem ONTAP tools for VMware vSphere bereitgestellt ist.

Im AutomatedFailOverDuplex-Richtlinientyp gibt es einheitliche und nicht einheitliche Hostkonfigurationen. Wenn Sie die Umschalttaste **Einheitliche Hostkonfiguration** auswählen, wird die Konfiguration der Host-Initiatorgruppe implizit auf dem Zielstandort repliziert. Weitere Informationen finden sich unter ["Schlüsselkonzepte und Begriffe"](#).

6. Wenn Sie eine nicht einheitliche Hostkonfiguration wählen, wählen Sie den Hostzugriff (Quelle/Ziel) für jeden Host innerhalb dieses Clusters aus.
7. Wählen Sie **Add**.

8. Sie können den Hostclusterschutz mit der Operation **Hostclusterschutz ändern** bearbeiten. Sie können die Beziehungen mit den Menüoptionen mit den Auslassungspunkten bearbeiten oder löschen.
9. Die Schaltfläche **Schützen** auswählen.

Das System erstellt eine vCenter Aufgabe mit den Details der Auftrags-ID und zeigt deren Fortschritt im Bereich „Letzte Aufgaben“ an. Dies ist eine asynchrone Aufgabe, die Benutzeroberfläche zeigt nur den Status der Anfrageübermittlung an und wartet nicht auf den Abschluss der Aufgabe.

10. Die geschützten Host-Cluster sind unter **NetApp ONTAP tools > Protection > Host cluster relationships** zu finden. Für eine Konsistenzgruppe werden deren Kapazität, zugehörige Datenspeicher und untergeordnete Konsistenzgruppen angezeigt.



Wenn der Schutz innerhalb einer Stunde nach der Erstellung entfernt werden muss, sollte zuerst die Speichererkennung durchgeführt werden.

Verwandte Informationen

["VMware vSphere Metro Storage Cluster \(vMSC\)"](#)

Schutz mit SRA-Schutz verwenden

Konfigurieren Sie SRA in ONTAP tools, um Datastores zu schützen

ONTAP tools for VMware vSphere bietet die Möglichkeit, die SRA-Funktionalität zu aktivieren, um die Notfallwiederherstellung zu konfigurieren.

Bevor Sie beginnen

- Sie sollten Ihre vCenter Server-Instanz eingerichtet und die ESXi-Hosts konfiguriert haben.
- Sie sollten ONTAP tools for VMware vSphere bereitgestellt haben.
- Sie sollten die SRA Adapter `.tar.gz` Datei von der ["NetApp Support Site"](#) heruntergeladen haben.
- Auf beiden ONTAP-Clustern (Quell- und Zielcluster) sollten die gleichen benutzerdefinierten SnapMirror-Zeitpläne vorhanden sein, bevor die SRA-Workflows ausgeführt werden.
- ["ONTAP tools für VMware vSphere Dienste aktivieren"](#) um die SRA-Funktionalität zu aktivieren.

Schritte

1. Melden Sie sich an der Managementoberfläche der VMware Live Site Recovery Appliance über die URL `https://<srm_ip>:5480` an und gehen Sie dann zu Storage Replication Adapters in der Managementoberfläche der VMware Live Site Recovery Appliance.
2. **Neuer Adapter** auswählen.
3. Das `.tar.gz` Installationsprogramm für das SRA Plug-in in VMware Live Site Recovery hochladen.
4. Die Adapter werden erneut gescannt, um zu überprüfen, ob die Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ aktualisiert sind.



Nach einem Failover sind Aktionen wie Erweitern, Einbinden und Löschen für Datenspeicher möglicherweise nicht verfügbar. Eine Datenspeichererkennung aktualisiert und zeigt die entsprechenden Kontextmenüaktionen an.



Nach jedem Reprotect Vorgang ist eine Speicherermittlung an beiden Standorten erforderlich.

In einer neuen Konfiguration mit SRA-Schutz wird empfohlen, stets ein Test-Failover durchzuführen. Das Überspringen des Test-Failovers kann dazu führen, dass der Reprotect-Vorgang fehlschlägt.

In einer Fan-Out-Konfiguration, nach einem SnapMirror Active Sync Failover, bei dem die SnapMirror Quelle für Automated Failover Duplex und asynchrones SnapMirror auf Standort B wechselt, sollte ein Test-Failover zwischen den Standorten B und C durchgeführt werden. Das Überspringen dieses Schritts kann zu einem fehlgeschlagenen Reprotect-Vorgang führen.

Verwandte Informationen

["Die Notfallwiederherstellung für NFS-Datenspeicher mit VMware Site Recovery Manager konfigurieren"](#)

Konfigurieren Sie SRA in ONTAP tools for VMware vSphere für SAN- und NAS-Umgebungen

Die Speichersysteme sind vor der Ausführung des Storage Replication Adapter (SRA) für VMware Live Site Recovery einzurichten.

SRA für SAN-Umgebungen konfigurieren



Konsistenzgruppen in SRA-Workflows werden nur mit SAN-Protokollen (iSCSI und Fibre Channel) auf Unified- und ASA r2 Storage-Systemen unterstützt.

Bevor Sie beginnen

Auf dem geschützten Standort und dem Wiederherstellungsstandort sollten die folgenden Programme installiert sein:

- VMware Live Site Recovery: Die VMware Website stellt Installationsdokumentation für VMware Live Site Recovery bereit.

["Über VMware Live Site Recovery"](#)

- SRA: Der Adapter wird auf VMware Live Site Recovery installiert.

Beachten Sie bei der Konfiguration des iSCSI-Protokolls vor dem Ausführen von SRA-Workflows Folgendes:

- **Geschützter Bereich:** iSCSI-Speicheradapter und Daten-LIF-Details werden bei der Bereitstellung von Datenspeichern automatisch konfiguriert. Keine manuelle Konfiguration ist erforderlich.
- **Wiederherstellungsstandort:** iSCSI-Speicheradapter müssen auf jedem ESXi-Host, der in die Ressourcenzuordnung für die Notfallwiederherstellung einbezogen ist, manuell konfiguriert werden. Um die individuelle Konfiguration der Adapter auf jedem Host zu vermeiden, erstellen Sie auf dem Wiederherstellungsstandort mithilfe der SVM, auf der die SRA-Workflows konfiguriert sind, einen Platzhalter-Datenspeicher vom Typ iSCSI. Dadurch werden der iSCSI-Adapter und die erforderlichen Daten-LIF-IP-Adressen automatisch allen zugeordneten ESXi-Hosts hinzugefügt. Weitere Informationen finden Sie unter ["Platzhalterdatenspeicher in ONTAP tools konfigurieren"](#).

Schritte

1. Es wird sichergestellt, dass die primären ESXi Hosts mit den LUNs im primären Storage-System am geschützten Standort verbunden sind.
2. Überprüfen Sie, ob sich die LUNs in igroups befinden, bei denen die `ostype` Option auf *VMware* auf dem primären Storage-System gesetzt ist.
3. Es ist sicherzustellen, dass die ESXi Hosts am Wiederherstellungsstandort über die erforderliche iSCSI-

und Fibre Channel-Konnektivität zur Storage Virtual Machine (SVM) verfügen. Die ESXi Hosts am sekundären Standort sollten Zugriff auf den Speicher des sekundären Standorts haben, und die ESXi Hosts am primären Standort sollten Zugriff auf den Speicher des primären Standorts haben.

Dies kann entweder durch Überprüfung erfolgen, ob die ESXi-Hosts lokale LUNs haben, die auf der SVM verbunden sind, oder durch den `iscsi show initiators` Befehl auf den SVMs. Der LUN-Zugriff für die zugeordneten LUNs im ESXi-Host dient zur Verifizierung der iSCSI-Konnektivität.

SRA für NAS-Umgebungen konfigurieren



Konsistenzgruppen werden für NFS in SRA-Workflows nicht unterstützt. Wenn NFS-Datenspeichervolumen einer Konsistenzgruppe zugeordnet und geschützt werden, schlägt der Vorgang „Geräte ermitteln“ fehl. Verwenden Sie keine Konsistenzgruppen, wenn Sie NFS-Datenspeicher mit SRA schützen.

Bevor Sie beginnen

Auf dem geschützten Standort und dem Wiederherstellungsstandort sollten die folgenden Programme installiert sein:

- VMware Live Site Recovery: Die Installationsdokumentation für VMware Live Site Recovery befindet sich auf der VMware Website "[Über VMware Live Site Recovery](#)"
- SRA: Der Adapter ist auf VMware Live Site Recovery und dem SRA Server zu installieren.

Schritte

1. Es sollte sichergestellt sein, dass die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die beim vCenter Server registriert sind.
2. Überprüfen Sie, ob die ESXi-Hosts am geschützten Standort die NFS-Exportvolumen der Storage Virtual Machine (SVM) eingebunden haben.
3. Stellen Sie sicher, dass im Feld **NFS Addresses** gültige IP-Adressen angegeben sind, unter denen die NFS-Exporte vorhanden sind, wenn Sie den Array Manager-Assistenten zum Hinzufügen von Arrays zu VMware Live Site Recovery verwenden. Verwenden Sie im Feld **NFS Addresses** nicht den NFS-Hostnamen oder den FQDN.
4. Der `ping` Befehl ist auf jedem ESXi Host am Wiederherstellungsstandort zu verwenden, um zu überprüfen, ob der Host über einen VMkernel Port verfügt, der auf die IP-Adressen zugreifen kann, die zum Bereitstellen von NFS-Exporten von der SVM verwendet werden.

Konfigurieren Sie SRA in ONTAP tools für hochskalierte Umgebungen

Die Zeitüberschreitungsintervalle für den Speicher sollten gemäß den empfohlenen Einstellungen konfiguriert werden, damit der Storage Replication Adapter (SRA) in hochskalierten Umgebungen optimal arbeitet.

Einstellungen des Speicheranbieters

Für skalierte Umgebungen in VMware Live Site Recovery sind die folgenden Zeitüberschreitungswerte festzulegen:

Erweiterte Einstellungen	Timeout-Werte
--------------------------	---------------

<code>StorageProvider.resignatureTimeout</code>	Der Wert der Einstellung wird von 900 Sekunden auf 12000 Sekunden erhöht.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Ein hoher Wert festlegen (zum Beispiel: 99999)

Die Option `StorageProvider.autoResignatureMode` sollte ebenfalls aktiviert werden.

Weitere Informationen zum Ändern der Einstellungen des Speicheranbieters finden Sie unter ["Speicheranbieter-Einstellungen ändern"](#).

Speichereinstellungen

Wenn eine Zeitüberschreitung auftritt, die Werte von `storage.commandTimeout` und `storage.maxConcurrentCommandCnt` auf einen höheren Wert erhöhen.



Das angegebene Zeitüberschreitungsintervall ist der Maximalwert. Sie müssen nicht warten, bis die maximale Zeitüberschreitung erreicht ist. Die meisten Befehle werden innerhalb des festgelegten maximalen Zeitüberschreitungsintervalls abgeschlossen.

Siehe ["Speichereinstellungen ändern"](#) zum Ändern der SAN-Provider-Einstellungen.

Konfigurieren Sie SRA auf der VMware Live Site Recovery Appliance mithilfe von ONTAP tools

Nach der Bereitstellung der VMware Live Site Recovery Appliance wird der Storage Replication Adapter (SRA) konfiguriert, um das Disaster Recovery Management zu ermöglichen.

Die Konfiguration von SRA auf der VMware Live Site Recovery Appliance speichert die ONTAP tools for VMware vSphere Anmeldeinformationen innerhalb der Appliance und ermöglicht so die Kommunikation zwischen VMware Live Site Recovery und SRA.

Bevor Sie beginnen

- Die `.tar.gz`-Datei kann von der ["NetApp Support Site"](#) heruntergeladen werden.
- Aktivieren Sie die SRA-Dienste im ONTAP tools Manager. Weitere Informationen finden Sie im ["Dienste aktivieren"](#) Abschnitt.
- Fügen Sie vCenter Server zur ONTAP tools for VMware vSphere Appliance hinzu. Weitere Informationen finden Sie im ["Fügen Sie vCenter Server hinzu"](#) Abschnitt.
- Fügen Sie Speicher-Backends zu ONTAP tools for VMware vSphere hinzu. Weitere Informationen finden Sie im ["Storage-Backends hinzufügen"](#) Abschnitt.



Wenn der vCenter-Zertifikatspatch von ONTAP tools angewendet wurde, sollte die vCenter-Konfiguration in der VMware Live Site Recovery Appliance über den Port (:5480) aktualisiert werden. Anleitungen finden sich unter ["Die Site Recovery Manager Appliance neu konfigurieren"](#).

Schritte

1. Auf dem Bildschirm der VMware Live Site Recovery Appliance **Storage Replication Adapter > New Adapter** auswählen.
2. Die `.tar.gz`-Datei in VMware Live Site Recovery hochladen.
3. Melden Sie sich mit einem Administratorkonto über einen SSH-Client wie PuTTY bei der VMware Live Site Recovery Appliance an.
4. Zum Root-Benutzer mit folgendem Befehl wechseln: `su root`
5. Führen Sie den Befehl `cd /var/log/vmware/srm` aus, um zum Protokollverzeichnis zu wechseln.
6. Geben Sie am Speicherort des Protokolls den Befehl ein, um die von SRA verwendete docker id zu erhalten: `docker ps -l`
7. Um sich bei der Container-ID anzumelden, den folgenden Befehl eingeben: `docker exec -it -u srm <container id> sh`
8. VMware Live Site Recovery mit ONTAP tools for VMware vSphere IP-Adresse und Passwort wird mit folgendem Befehl konfiguriert: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Das Passwort ist in einfache Anführungszeichen zu setzen, damit das Perl-Skript Sonderzeichen als Teil des Passworts und nicht als Trennzeichen behandelt.
 - Sie können den Benutzernamen und das Kennwort für die Anwendung (VASA Provider/SRA) im ONTAP tools Manager festlegen, wenn diese Dienste zum ersten Mal aktiviert werden. Mit diesen Anmeldeinformationen lässt sich SRA bei VMware Live Site Recovery registrieren.
 - Um die vCenter GUID zu finden, gehen Sie nach dem Hinzufügen Ihrer vCenter Instanz auf die vCenter Serverseite im ONTAP tools Manager. Siehe ["Fügen Sie vCenter Server hinzu"](#) Abschnitt.
9. Die Adapter werden erneut gescannt, sodass die aktualisierten Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ angezeigt werden.

Ergebnis Es erscheint eine Bestätigungsmeldung, die anzeigt, dass die Speicherzugangsdaten gespeichert wurden. Sie können SRA nun verwenden, um mit dem SRA Server über die angegebene IP-Adresse, den Port und die Zugangsdaten zu kommunizieren.

Aktualisieren Sie die SRA-Anmeldeinformationen in ONTAP tools

Damit VMware Live Site Recovery mit SRA kommunizieren kann, sollten Sie die SRA-Anmeldeinformationen auf dem VMware Live Site Recovery Server aktualisieren, falls Sie die Anmeldeinformationen geändert haben.

Bevor Sie beginnen

Sie sollten die im Thema genannten Schritte ["Konfiguration von SRA auf der VMware Live Site Recovery Appliance"](#) ausgeführt haben.

Schritte

1. Führen Sie die folgenden Befehle aus, um die zwischengespeicherten ONTAP tools-Anmeldeinformationen von der VMware Live Site Recovery-Maschine zu löschen:

- a. `sudo su <enter root password>`
- b. `docker ps`
- c. `docker exec -it <container_id> sh`
- d. `cd conf/`
- e. `rm -rf *`

2. Führen Sie den Perl-Befehl aus, um SRA mit den neuen Anmeldeinformationen zu konfigurieren:

- a. `cd ..`
- b. ``perl command.pl -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`` Es muss ein einfaches Anführungszeichen um den Passwortwert gesetzt werden.

Es wird eine Erfolgsmeldung angezeigt, die bestätigt, dass die Speicherzugangsdaten gespeichert wurden. SRA kann über die angegebene IP-Adresse, den Port und die Zugangsdaten mit dem SRA-Server kommunizieren.

Konfigurieren Sie vCenter in der VMware Live Site Recovery Appliance nach einer Zertifikatsänderung neu

Wenn sich das vCenter-Zertifikat ändert, beispielsweise nach einem vCenter-Upgrade, kann bei der Site Recovery-Erweiterung ein Fehler aufgrund eines nicht übereinstimmenden Fingerabdrucks auftreten. Führen Sie die folgenden Schritte aus, um das Problem zu beheben.

Schritte

1. Neukonfiguration vCenter in der VMware Live Site Recovery Appliance

- a. Öffnen Sie die VMware Live Site Recovery Appliance Managementoberfläche in einem Browser:
`https://<SRM_IP>:5480`
- b. Wählen Sie die Registerkarte **Zusammenfassung**.
- c. Wählen Sie **Neu konfigurieren** für die vCenter Serververbindung.

Dies ruft den neuesten Zertifikatfingerabdruck von vCenter ab und akzeptiert ihn.

2. Stellen Sie die Standortkopplung erneut her (falls der Fehler weiterhin besteht)

Wenn der Fehler mit der Fingerabdruckabweichung auch nach der Neukonfiguration weiterhin besteht:

- a. Melden Sie sich bei der vCenter Benutzeroberfläche an.
- b. Navigieren Sie zur Erweiterung **Site Recovery**.
- c. Suchen Sie den Abschnitt **Site Pairing**.
- d. Wählen Sie **Neu verbinden**, um die Standortkopplung mit dem aktualisierten Zertifikat wiederherzustellen.

Konfigurieren von geschützten und Wiederherstellungsstandorten in ONTAP tools

Es empfiehlt sich, Schutzgruppen zu erstellen, um eine Gruppe virtueller Maschinen auf

der geschützten Site zu schützen.

Beim Hinzufügen eines neuen Datenspeichers kann dieser in die bestehende Datenspeichergruppe aufgenommen oder ein neuer Datenspeicher hinzugefügt und ein neues Volume oder eine neue Konsistenzgruppe zum Schutz erstellt werden. Nach dem Hinzufügen eines neuen Datenspeichers zu einer geschützten Konsistenzgruppe oder einem geschützten Volume sollten SnapMirror aktualisiert und die Speichererkennung sowohl am geschützten als auch am Wiederherstellungsstandort durchgeführt werden. Die Erkennung kann manuell oder nach einem Zeitplan ausgeführt werden, um sicherzustellen, dass der neue Datenspeicher erkannt und geschützt ist.

Geschützte und Wiederherstellungsstandorte paaren

Sie sollten die mit Ihrem vSphere Client erstellten geschützten und Wiederherstellungsstandorte koppeln, damit der Storage Replication Adapter (SRA) die Speichersysteme erkennen kann.



Der Storage Replication Adapter (SRA) unterstützt Fan-Out mit einer synchronen Beziehung vom Typ Automated Failover Duplex und einer asynchronen SnapMirror-Beziehung in einer Konsistenzgruppe. Fan-Out mit zwei asynchronen SnapMirror-Beziehungen in Konsistenzgruppen oder Fan-Out SnapMirror-Beziehungen auf Volumes wird jedoch nicht unterstützt. Vault-Typ SnapMirror-Beziehungen werden bei diesen Fan-Out-Beschränkungen nicht berücksichtigt. Die Unterstützung von Konsistenzgruppen im SRA ist auf SAN-Protokolle (iSCSI und Fibre Channel) auf Unified- und ASA r2-Speichersystemen beschränkt. Konsistenzgruppen werden für NFS nicht unterstützt. Wenn NFS-Datenspeichervolumen einer Konsistenzgruppe zugeordnet werden, schlägt die Geräteerkennung fehl.

Bevor Sie beginnen

- VMware Live Site Recovery sollte auf den geschützten und den Wiederherstellungsstandorten installiert sein.
- SRA sollte auf den geschützten und Wiederherstellungsstandorten installiert sein.

Schritte

1. Auf der Startseite des vSphere Clients auf das Symbol **Site Recovery** doppelklicken und anschließend **Sites** auswählen.
2. **Objekte > Aktionen > Standorte koppeln** auswählen.
3. Im Dialogfeld **Pair Site Recovery Manager Servers** die Adresse des Platform Services Controllers der geschützten Site eingeben und anschließend **Weiter** auswählen.
4. Führen Sie im Abschnitt vCenter Server auswählen die folgenden Schritte aus:
 - a. Es sollte überprüft werden, ob der vCenter Server der geschützten Site als passender Kandidat für die Kopplung angezeigt wird.
 - b. Geben Sie die SSO-Administratoranmeldeinformationen ein und wählen Sie anschließend **Fertigstellen** aus.
5. Falls Sie dazu aufgefordert werden, **Ja** auswählen, um die Sicherheitszertifikate zu akzeptieren.

Ergebnis

Im Dialogfeld **Objekte** werden sowohl die geschützten als auch die Wiederherstellungs-Sites angezeigt.

Schutzgruppen konfigurieren

Bevor Sie beginnen

Es sollte sichergestellt sein, dass sowohl die Quell- als auch die Zielseite für Folgendes konfiguriert sind:

- Dieselbe Version von VMware Live Site Recovery ist installiert
- Virtuelle Maschinen
- Gepaarte geschützte und Wiederherstellungsstandorte
- Quell- und Zieldatenspeicher sollten an den jeweiligen Standorten eingebunden sein.

Schritte

1. Melden Sie sich beim vCenter Server an und wählen Sie **Site Recovery > Protection Groups**.
2. Im Bereich **Schutzgruppen** auf **Neu** auswählen.
3. Einen Namen und eine Beschreibung für die Schutzgruppe sowie die Richtung angeben und **Weiter** auswählen.
4. Wählen Sie im Feld **Typ** die Option **Typfeld...** als Datenspeichergruppen (Array-basierte Replikation) für NFS- und VMFS-Datenspeicher aus. Die Fehlerdomäne besteht aus SVMs mit aktivierter Replikation. Die SVMs, die ausschließlich Peering implementiert haben und keine Probleme aufweisen, werden angezeigt.
5. Auf der Registerkarte Replikationsgruppen entweder das aktivierte Array-Paar oder die Replikationsgruppen auswählen, die die konfigurierte virtuelle Maschine enthalten, und anschließend **Weiter** auswählen.

Alle virtuellen Maschinen der Replikationsgruppe werden der Schutzgruppe hinzugefügt.

6. Sie können entweder den bestehenden Wiederherstellungsplan auswählen oder einen neuen erstellen, indem Sie **Zu neuem Wiederherstellungsplan hinzufügen** auswählen.
7. Auf der Registerkarte „Bereit zum Abschließen“ werden die Details der erstellten Schutzgruppe angezeigt, anschließend kann **Fertigstellen** ausgewählt werden.

Konfiguration von Ressourcen für geschützte und Wiederherstellungsstandorte

Netzwerkzuordnungen in ONTAP tools konfigurieren

Ihre Ressourcenzuordnungen wie VM-Netzwerke, ESXi Hosts und Ordner an beiden Standorten sind so zu konfigurieren, dass die Zuordnung jeder Ressource vom geschützten Standort zur entsprechenden Ressource am Wiederherstellungsstandort möglich ist.

Die folgenden Ressourcenkonfigurationen sollten abgeschlossen werden:

- Netzwerkzuordnungen
- Ordnerzuordnungen
- Ressourcenzuordnungen
- Platzhalter Datenspeicher

Bevor Sie beginnen

Die geschützten und die Wiederherstellungsstandorte sollten verbunden sein.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.

3. Im Tab „Verwalten“ unter **Netzwerkzuordnungen** > **Neu** kann eine neue Netzwerkzuordnung erstellt werden.
4. Im Assistenten zum Erstellen einer Netzwerkzuordnung sind folgende Schritte auszuführen:
 - a. **Automatisch Zuordnungen für Netzwerke mit übereinstimmenden Namen vorbereiten** auswählen und **Weiter** auswählen.
 - b. Wählen Sie die benötigten Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. **Weiter** auswählen, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das Objekt aus, das zuvor zum Erstellen der umgekehrten Zuordnung verwendet wurde, und dann **Fertigstellen**.

Ergebnis

Auf der Seite „Netzwerkzuordnungen“ werden die Ressourcen des geschützten Standorts und die Ressourcen des Wiederherstellungsstandorts angezeigt. Für andere Netzwerke in Ihrer Umgebung sind die gleichen Schritte möglich.

Ordnerzuordnungen in ONTAP tools konfigurieren

Ihre Ordner auf der geschützten Site und der Wiederherstellungs-Site sollten einander zugeordnet werden, damit die Kommunikation zwischen ihnen möglich ist.

Bevor Sie beginnen

Die geschützten und die Wiederherstellungsstandorte sollten verbunden sein.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.
3. **Ordnerzuordnungen** > **Ordner**-Symbol in der Registerkarte „Verwalten“ auswählen, um eine neue Ordnerzuordnung zu erstellen.
4. Im Assistenten zum Erstellen von Ordnerzuordnungen sind die folgenden Schritte auszuführen:
 - a. **Automatische Zuordnung für Ordner mit übereinstimmenden Namen vorbereiten** auswählen und **Weiter** auswählen.
 - b. Wählen Sie die benötigten Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. **Weiter** auswählen, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das Objekt aus, das zuvor zum Erstellen der umgekehrten Zuordnung verwendet wurde, und dann **Fertigstellen**.

Ergebnis

Auf der Seite „Ordnerzuordnungen“ werden die geschützten Site-Ressourcen und die Ressourcen der Wiederherstellungssite angezeigt. Sie können die gleichen Schritte für andere Ordner in Ihrer Umgebung ausführen.

Ressourcenzuordnungen in ONTAP tools konfigurieren

Ihre Ressourcen auf dem geschützten Standort und dem Wiederherstellungsstandort sollten so zugeordnet werden, dass virtuelle Maschinen so konfiguriert sind, dass sie bei

einem Failover in die eine oder andere Gruppe von Hosts wechseln.

Bevor Sie beginnen

Die geschützten und die Wiederherstellungsstandorte sollten verbunden sein.



In VMware Live Site Recovery können Ressourcen Ressourcenpools, ESXi Hosts oder vSphere Clustern sein.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.
3. Im Tab „Verwalten“ **Ressourcenzuordnungen > Neu** auswählen, um eine neue Ressourcenzuordnung zu erstellen.
4. Im Assistenten zum Erstellen von Ressourcenzuordnungen sind die folgenden Schritte auszuführen:
 - a. Wählen Sie **Automatisch Zuordnungen für Ressourcen mit übereinstimmenden Namen vorbereiten** und wählen Sie **Weiter**.
 - b. Wählen Sie die benötigten Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. **Weiter** auswählen, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das Objekt aus, das zuvor zum Erstellen der umgekehrten Zuordnung verwendet wurde, und dann **Fertigstellen**.

Ergebnis

Auf der Seite „Ressourcenzuordnungen“ werden die geschützten Standortressourcen und die Ressourcen des Wiederherstellungsstandorts angezeigt. Sie können die gleichen Schritte für andere Ressourcen in Ihrer Umgebung ausführen.

Platzhalterdatenspeicher in ONTAP tools konfigurieren

Ein Platzhalterdatenspeicher wird konfiguriert, um Speicherplatz im vCenter-Inventar am Wiederherstellungsstandort für geschützte virtuelle Maschinen (VMs) zu reservieren. Platzhalterdatenspeicher benötigen nur minimale Kapazität, da Platzhalter-VMs klein sind und typischerweise nur wenige hundert Kilobyte belegen.

Bevor Sie beginnen

- Es ist sicherzustellen, dass die geschützten Standorte und die Wiederherstellungsstandorte miteinander verbunden sind.
- Es sollte überprüft werden, ob die Ressourcenzuordnungen konfiguriert wurden.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.
3. Im Tab „Verwalten“ **Placeholder Datastores > Neu** auswählen, um einen neuen Platzhalter-Datenspeicher zu erstellen.
4. Den entsprechenden Datenspeicher auswählen und **OK** wählen.



Platzhalterdatenspeicher können sich auf lokalem oder entferntem Speicher befinden, erfordern jedoch keine Replikation.

5. Schritte 3 bis 5 werden wiederholt, um einen Platzhalter-Datenspeicher für den Wiederherstellungsstandort zu konfigurieren.

Konfigurieren Sie SRA mithilfe des Array-Managers in ONTAP tools

Sie können den Storage Replication Adapter (SRA) mithilfe des Array Manager Assistenten von VMware Live Site Recovery konfigurieren, um die Interaktion zwischen VMware Live Site Recovery und Storage Virtual Machines (SVMs) zu ermöglichen.

Bevor Sie beginnen

- Die geschützten Standorte und die Wiederherstellungsstandorte sollten in VMware Live Site Recovery gekoppelt sein.
- Der integrierte Speicher sollte vor der Konfiguration des Array-Managers konfiguriert worden sein.
- Die SnapMirror Beziehungen zwischen den geschützten Standorten und den Wiederherstellungsstandorten sollten konfiguriert und repliziert sein.
- Die SVM Management-LIFs sollten aktiviert sein, um Mandantenfähigkeit zu ermöglichen.

SRA unterstützt die Verwaltung auf Cluster-Ebene und SVM-Ebene. Wenn Speicher auf Cluster-Ebene hinzugefügt wird, können alle SVMs im Cluster erkannt und Operationen an ihnen durchgeführt werden. Wenn Speicher auf SVM-Ebene hinzugefügt wird, kann nur diese spezifische SVM verwaltet werden.

Schritte

1. In VMware Live Site Recovery **Array Manager > Array Manager hinzufügen** auswählen.
2. Folgende Informationen beschreiben das Array in VMware Live Site Recovery:
 - a. Im Feld **Anzeigename** einen Namen zur Identifizierung des Array Managers eingeben.
 - b. Im Feld **SRA-Typ** ist **NetApp Storage Replication Adapter für ONTAP** auszuwählen.
 - c. Geben Sie die Informationen ein, um eine Verbindung zum Cluster oder zur SVM herzustellen:
 - Wenn Sie eine Verbindung zu einem Cluster herstellen, sollte die Cluster-Management-LIF eingegeben werden.
 - Wenn Sie eine direkte Verbindung zu einer SVM herstellen, sollte die IP-Adresse des SVM Management-LIF eingegeben werden.



Bei der Konfiguration des Array-Managers sollte dieselbe Verbindung (IP-Adresse) für das Speichersystem verwendet werden, die auch für das Onboarding des Speichersystems in ONTAP tools for VMware vSphere verwendet wurde. Wenn die Konfiguration des Array-Managers beispielsweise auf SVM-Ebene erfolgt, sollte der Speicher unter ONTAP tools for VMware vSphere auf SVM-Ebene hinzugefügt werden.

- d. Wenn eine Verbindung zu einem Cluster hergestellt wird, ist der SVM-Name im Feld **SVM-Name** anzugeben oder das Feld bleibt leer, um alle SVMs im Cluster zu verwalten.
- e. Geben Sie die zu ermittelnden Volumes im Feld **Volume-Einschlussliste** ein.

Am geschützten Standort kann das Quellvolume und am Wiederherstellungsstandort das replizierte

Zielvolume eingegeben werden.

Wenn beispielsweise das Volume `src_vol1` ermittelt werden soll, das sich in einer SnapMirror Beziehung mit dem Volume `dst_vol1` befindet, ist `src_vol1` im Feld „geschützter Standort“ und `dst_vol1` im Feld „Wiederherstellungsstandort“ anzugeben.

- f. **(Optional)** Geben Sie die Volumes, die von der Erkennung ausgeschlossen werden sollen, im Feld **Volume exclude list** ein.

Am geschützten Standort kann das Quellvolume und am Wiederherstellungsstandort das replizierte Zielvolume eingegeben werden.

Wenn beispielsweise das Volume `src_vol1` ausgeschlossen werden soll, das sich in einer SnapMirror Beziehung mit dem Volume `dst_vol1` befindet, ist `src_vol1` im Feld „geschützter Standort“ und `dst_vol1` im Feld „Wiederherstellungsstandort“ anzugeben.

3. **Weiter** auswählen.

4. Es sollte überprüft werden, ob das Array erkannt und unten im Fenster „Add Array Manager“ angezeigt wird, und anschließend **Finish** ausgewählt werden.

Die gleichen Schritte können für den Wiederherstellungsstandort unter Verwendung der entsprechenden SVM-Management-IP-Adressen und Anmeldedaten durchgeführt werden. Auf dem Bildschirm „Array-Paare aktivieren“ des Assistenten zum Hinzufügen eines Array-Managers sollte überprüft werden, ob das richtige Array-Paar ausgewählt ist und als aktivierungsbereit angezeigt wird.

Überprüfen Sie replizierte Speichersysteme in ONTAP tools

Nach der Konfiguration des Storage Replication Adapter (SRA) sollte überprüft werden, ob der geschützte Standort und der Wiederherstellungsstandort erfolgreich gekoppelt sind. Das replizierte Storage-System sollte sowohl vom geschützten Standort als auch vom Wiederherstellungsstandort aus auffindbar sein.

Bevor Sie beginnen

- Sie sollten Ihr Speichersystem konfiguriert haben.
- Der geschützte Standort und der Wiederherstellungsstandort sollten mithilfe des VMware Live Site Recovery Array Managers gekoppelt worden sein.
- Die FlexClone Lizenz und die SnapMirror Lizenz sollten vor der Durchführung des Test-Failover-Vorgangs und des Failover-Vorgangs für SRA aktiviert worden sein.
- An Quell- und Zielstandorten sollten die gleichen SnapMirror Richtlinien und Zeitpläne vorhanden sein.
- Wenn Sie benutzerdefinierte SnapMirror-Richtlinien mit einem benutzerdefinierten Zeitplan verwenden, müssen Sie denselben Zeitplan und dieselbe Richtlinie sowohl auf dem geschützten als auch auf dem Wiederherstellungsstandort konfigurieren.
- Wenn Sie benutzerdefinierte SnapMirror-Richtlinien verwenden (mit einem Standard- oder benutzerdefinierten Zeitplan), müssen Sie die Speichererkennung von ONTAP tools durchführen, damit die neue Richtlinie erkannt wird. Ohne dies schlagen SRA-Workflows, einschließlich Test-Failover und Failover, fehl. Führen Sie die Speichererkennung an den folgenden Punkten durch:
 - Nach dem Erstellen der benutzerdefinierten Richtlinie auf der Wiederherstellungsseite.
 - Nach einer Reprotect-Operation, bei der die Richtlinie auf der geschützten Site wiederhergestellt wird.

Schritte

1. Melden Sie sich bei Ihrem vCenter Server an.
2. Zu **Site Recovery > Array Based Replication** wechseln.
3. Das erforderliche Array Pair auswählen und die entsprechenden Details überprüfen.

Die Speichersysteme sollten am geschützten Standort und am Wiederherstellungsstandort mit dem Status **Enabled** erkannt werden.

Fan-out-Schutz in ONTAP tools

In einem Fan-Out-Schutzszenario ist die Konsistenzgruppe doppelt geschützt: mit synchroner Beziehung auf dem ersten Ziel-ONTAP Cluster und mit asynchroner Beziehung auf dem zweiten Ziel-ONTAP Cluster. Die Workflows zum Erstellen, Bearbeiten und Löschen von SnapMirror Active Sync-Schutz erhalten den synchronen Schutz. Die Workflows für Failover und Reprotect der VMware Live Site Recovery Appliance erhalten den asynchronen Schutz.



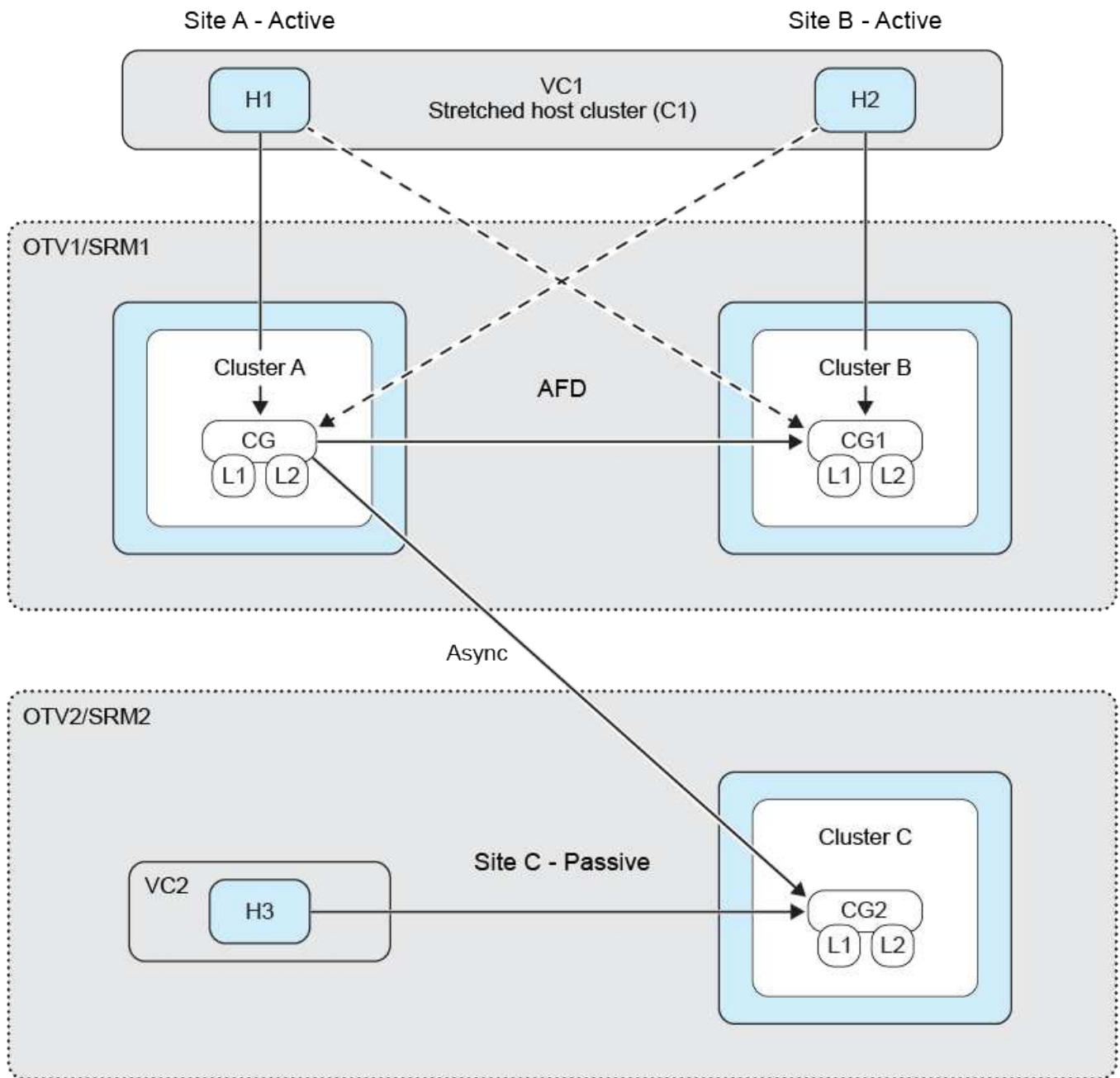
Fan-Out wird für SVM-Benutzer nicht unterstützt.

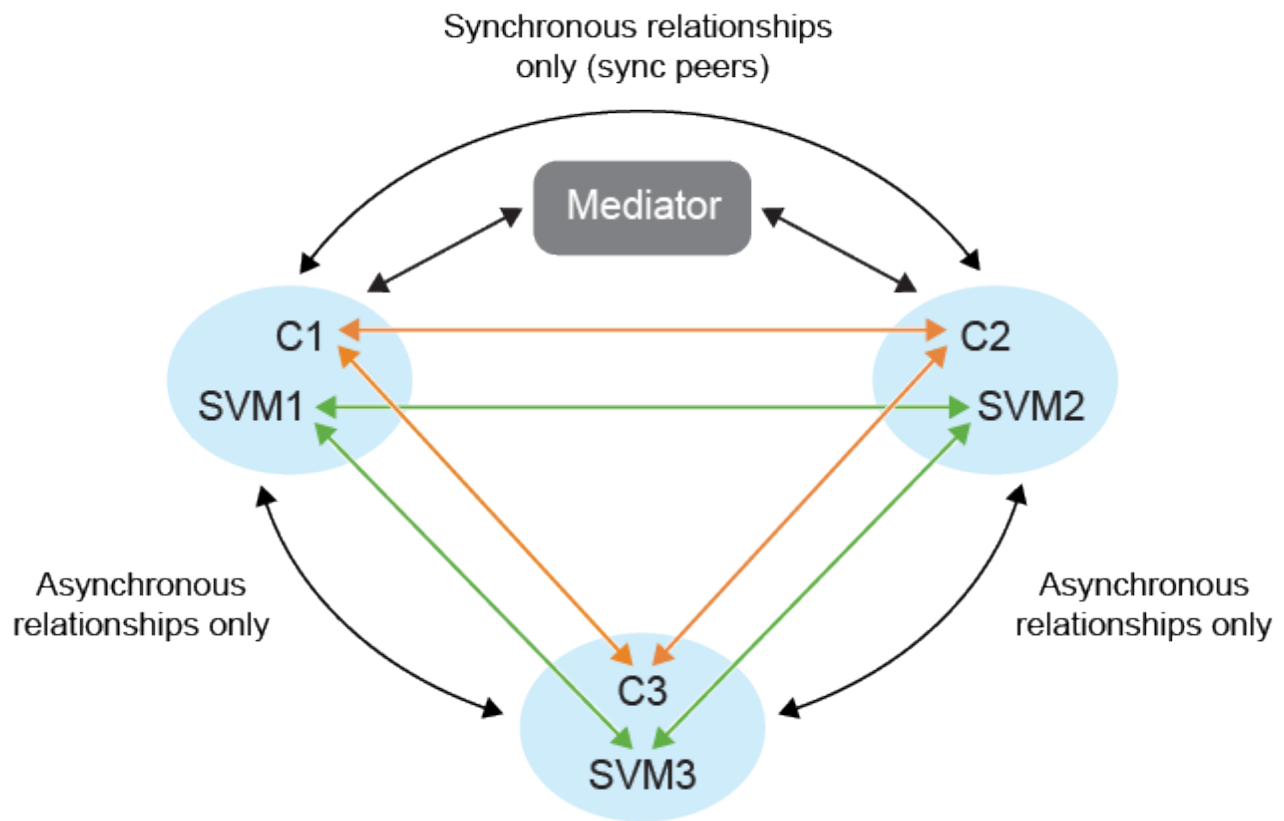
Zum Einrichten des Fan-Out-Schutzes werden die drei Standort-Cluster und SVMs miteinander gekoppelt.

Beispiel:

Wenn	Dann
• Die Konsistenzgruppe der Quelle befindet sich auf Cluster c1 und SVM svm1 • Die erste Konsistenzgruppe befindet sich auf Cluster c2 und SVM svm2 und • Die zweite Konsistenzgruppe befindet sich auf Cluster c3 und SVM svm3	• Das Cluster-Peering auf dem Quell-ONTAP Cluster wird (C1, C2) und (C1, C3) sein. • Das Cluster-Peering auf dem ersten Ziel ONTAP Cluster ist (C2, C1) und (C2, C3) sowie • Das Cluster-Peering auf dem zweiten ONTAP Zielcluster wird (C3, C1) und (C3, C2) sein. • Das SVM-Peering auf der Quell-SVM ist (svm1, svm2) und (svm1, svm3). • Das SVM-Peering auf dem ersten Ziel-SVM ist (svm2, svm1) und (svm2, svm3) sowie • Das SVM-Peering auf dem zweiten Ziel-SVM ist (svm3, svm1) und (svm3, svm2).

Das folgende Diagramm zeigt die Fan-Out-Schutzkonfiguration:





Schritte

1. Wählen Sie einen neuen Platzhalterdatenspeicher aus. Die Auswahlkriterien für den Platzhalterdatenspeicher im Rahmen des phasenweisen Schutzes lauten:
 - Der Platzhalterdatenspeicher sollte nicht im Hostcluster platziert werden, den Sie schützen.
 - Wenn Sie den Platzhalterdatenspeicher in den Hostcluster einbinden müssen, fügen Sie ihn der VMware Live Site Recovery Appliance hinzu, bevor Sie SnapMirror active sync-Schutz einrichten. Mit dieser Konfiguration können Sie den Platzhalterdatenspeicher vom Schutz ausnehmen.

Weitere Informationen finden Sie unter ["Einen Platzhalter-Datenspeicher auswählen"](#)
2. Fügen Sie Datenspeicher zum Hostclusterschutz hinzu, indem Sie ["Geschützten Host-Cluster modifizieren"](#) folgen. Fügen Sie sowohl asynchrone als auch synchrone Richtlinientypen hinzu.

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.