



Schützen Sie Datenspeicher und virtuelle Maschinen

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

Inhalt

- Schützen Sie Datenspeicher und virtuelle Maschinen 1
 - Schützen Sie sich mit dem Hostclusterschutz 1
 - Schützen Sie sich mit SRA-Schutz 2
 - Konfigurieren Sie SRA zum Schutz von Datenspeichern 2
 - Konfigurieren von SRA für SAN- und NAS-Umgebungen 2
 - Konfigurieren von SRA für hochskalierte Umgebungen 4
 - Konfigurieren von SRA auf der VMware Live Site Recovery-Appliance 4
 - SRA-Anmeldeinformationen aktualisieren 6
 - Konfigurieren von geschützten Sites und Wiederherstellungssites 6
 - Konfigurieren von geschützten Site- und Wiederherstellungs-Site-Ressourcen 8
 - Überprüfen replizierter Speichersysteme 12
 - Fan-Out-Schutz 12

Schützen Sie Datenspeicher und virtuelle Maschinen

Schützen Sie sich mit dem Hostclusterschutz

ONTAP tools for VMware vSphere verwalten den Schutz von Host-Clustern. Unter einem Hostcluster werden alle Datenspeicher geschützt, die zur ausgewählten SVM gehören und auf einem oder mehreren Hosts des Clusters gemountet sind.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der Hostcluster verfügt nur über Datenspeicher von einer SVM.
- Auf dem Hostcluster gemountete Datenspeicher sollten nicht auf einem Host außerhalb des Clusters gemountet werden.
- Alle auf dem Hostcluster bereitgestellten Datenspeicher müssen VMFS-Datenspeicher mit iSCSI/FC-Protokoll sein. vVols, NFS- oder VMFS-Datenspeicher mit NVMe/FC- und NVMe/TCP-Protokollen werden nicht unterstützt.
- Auf dem Hostcluster gemountete FlexVol/LUN-bildende Datenspeicher sollten nicht Teil einer vorhandenen Konsistenzgruppe (CG) sein.
- Auf dem Hostcluster bereitgestellte FlexVol/LUN-bildende Datenspeicher sollten nicht Teil einer bestehenden SnapMirror -Beziehung sein.
- Der Hostcluster sollte mindestens einen Datenspeicher haben.

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* > **Cluster schützen**.
3. Im Fenster „Cluster schützen“ werden der Datenspeichertyp und die Details der virtuellen Maschine (VM) des Quellspeichers automatisch eingetragen. Wählen Sie den Link „Datenspeicher“ aus, um die geschützten Datenspeicher anzuzeigen.
4. Geben Sie den **Namen der Konsistenzgruppe** ein.
5. Wählen Sie **Beziehung hinzufügen**.
6. Wählen Sie im Fenster * SnapMirror -Beziehung hinzufügen* die **Zielspeicher-VM** und den **Richtlinientyp** aus.

Der Richtlinientyp kann „Asynchron“ oder „AutomatedFailOverDuplex“ sein.

Wenn Sie die SnapMirror -Beziehung als Richtlinie vom Typ „AutomatedFailOverDuplex“ hinzufügen, müssen Sie die Zielspeicher-VM als Speicher-Backend zum selben vCenter hinzufügen, in dem ONTAP tools for VMware vSphere bereitgestellt werden.

Beim Richtlinientyp „AutomatedFailOverDuplex“ gibt es einheitliche und nicht einheitliche Hostkonfigurationen. Wenn Sie die Umschalttaste **einheitliche Hostkonfiguration** auswählen, wird die Konfiguration der Hostinitiatorgruppe implizit auf der Zielsite repliziert. Weitere Einzelheiten finden Sie unter ["Wichtige Konzepte und Begriffe"](#) .

7. Wenn Sie sich für eine nicht einheitliche Hostkonfiguration entscheiden, wählen Sie den Hostzugriff (Quelle/Ziel) für jeden Host innerhalb dieses Clusters aus.
8. Wählen Sie **Hinzufügen**.
9. Im Fenster **Cluster schützen** können Sie den geschützten Cluster während des Erstellungsvorgangs nicht bearbeiten. Sie können den Schutz löschen und erneut hinzufügen. Während des Vorgangs „Hostclusterschutz ändern“ ist die Bearbeitungsoption verfügbar. Sie können die Beziehungen mithilfe der Auslassungspunkte-Menüoptionen bearbeiten oder löschen.
10. Wählen Sie die Schaltfläche **Schützen**.

Eine vCenter-Aufgabe wird mit Job-ID-Details erstellt und ihr Fortschritt wird im Bereich „Letzte Aufgaben“ angezeigt. Dies ist eine asynchrone Aufgabe. Die Benutzeroberfläche zeigt nur den Status der Anforderungsübermittlung an und wartet nicht auf die Fertigstellung der Aufgabe.
11. Um die geschützten Host-Cluster anzuzeigen, navigieren Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**.

Schützen Sie sich mit SRA-Schutz

Konfigurieren Sie SRA zum Schutz von Datenspeichern

ONTAP tools for VMware vSphere bieten die Möglichkeit, die SRA-Funktion zur Konfiguration der Notfallwiederherstellung zu aktivieren.

Bevor Sie beginnen

- Sie sollten Ihre vCenter Server-Instanz eingerichtet und den ESXi-Host konfiguriert haben.
- Sie sollten ONTAP tools for VMware vSphere bereitgestellt haben.
- Sie sollten den SRA-Adapter heruntergeladen haben .tar.gz Datei aus dem ["NetApp Support Site"](#) .
- Für Quell- und Ziel- ONTAP Cluster müssen vor der Ausführung der SRA-Workflows dieselben benutzerdefinierten SnapMirror -Zeitpläne erstellt werden.
- ["Aktivieren Sie ONTAP tools for VMware vSphere -Dienste"](#) um die SRA-Funktion zu aktivieren.

Schritte

1. Melden Sie sich mit der folgenden URL bei der Verwaltungsschnittstelle der VMware Live Site Recovery-Appliance an: https://<srm_ip>:5480 und gehen Sie dann zu Storage Replication Adapters in der Verwaltungsschnittstelle der VMware VMware Live Site Recovery-Appliance.
2. Wählen Sie **Neuer Adapter**.
3. Laden Sie das .tar.gz-Installationsprogramm für das SRA-Plug-In auf VMware Live Site Recovery hoch.
4. Scannen Sie die Adapter erneut, um zu überprüfen, ob die Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ aktualisiert sind.

Ähnliche Informationen

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

Konfigurieren von SRA für SAN- und NAS-Umgebungen

Sie sollten die Speichersysteme einrichten, bevor Sie den Storage Replication Adapter (SRA) für VMware Live Site Recovery ausführen.

Konfigurieren von SRA für SAN-Umgebungen

Bevor Sie beginnen

Sie sollten die folgenden Programme auf der geschützten Site und der Wiederherstellungssite installiert haben:

- VMware Live Site Recovery

Dokumentation zur Installation von VMware Live Site Recovery finden Sie auf der VMware-Site.

["Informationen zu VMware Live Site Recovery"](#)

- SRA

Der Adapter ist auf VMware Live Site Recovery installiert.

Schritte

1. Stellen Sie sicher, dass die primären ESXi-Hosts mit den LUNs im primären Speichersystem auf der geschützten Site verbunden sind.
2. Überprüfen Sie, ob die LUNS in igroups sind, die die `ostype` Option auf dem primären Speichersystem auf *VMware* eingestellt.
3. Stellen Sie sicher, dass die ESXi-Hosts am Wiederherstellungsstandort über eine entsprechende iSCSI-Konnektivität zur Storage Virtual Machine (SVM) verfügen. Die ESXi-Hosts des sekundären Standorts sollten Zugriff auf den Speicher des sekundären Standorts haben und die ESXi-Hosts des primären Standorts sollten Zugriff auf den Speicher des primären Standorts haben.

Sie können dies tun, indem Sie entweder überprüfen, ob die ESXi-Hosts lokale LUNs auf der SVM verbunden haben oder die `iscsi show initiators` Befehl auf den SVMs. Überprüfen Sie den LUN-Zugriff für die zugeordneten LUNs im ESXi-Host, um die iSCSI-Konnektivität zu überprüfen.

Konfigurieren von SRA für NAS-Umgebungen

Bevor Sie beginnen

Sie sollten die folgenden Programme auf der geschützten Site und der Wiederherstellungssite installiert haben:

- VMware Live Site Recovery

Dokumentation zur Installation von VMware Live Site Recovery finden Sie auf der VMware-Site.

["Informationen zu VMware Live Site Recovery"](#)

- SRA

Der Adapter wird auf VMware Live Site Recovery und dem SRA-Server installiert.

Schritte

1. Stellen Sie sicher, dass die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die bei vCenter Server registriert sind.
2. Stellen Sie sicher, dass die ESXi-Hosts am geschützten Standort die NFS-Exportvolumes von der Storage Virtual Machine (SVM) gemountet haben.
3. Stellen Sie sicher, dass gültige Adressen wie die IP-Adresse oder der FQDN, unter dem die NFS-Exporte vorliegen, im Feld **NFS-Adressen** angegeben sind, wenn Sie den Array Manager-Assistenten zum

Hinzufügen von Arrays zu VMware Live Site Recovery verwenden. Verwenden Sie im Feld **NFS-Adressen** nicht den NFS-Hostnamen.

4. Verwenden Sie die `ping` auf jedem ESXi-Host am Wiederherstellungsstandort, um zu überprüfen, ob der Host über einen VMkernel-Port verfügt, der auf die IP-Adressen zugreifen kann, die zum Ausführen von NFS-Exporten vom SVM verwendet werden.

Konfigurieren von SRA für hochskalierte Umgebungen

Sie sollten die Speicher-Timeout-Intervalle gemäß den empfohlenen Einstellungen für den Storage Replication Adapter (SRA) konfigurieren, um in stark skalierten Umgebungen eine optimale Leistung zu erzielen.

Speicheranbieterereinstellungen

Sie sollten die folgenden Timeout-Werte für VMware Live Site Recovery für eine skalierte Umgebung festlegen:

Erweiterte Einstellungen	Timeout-Werte
<code>StorageProvider.resignatureTimeout</code>	Erhöhen Sie den Wert der Einstellung von 900 Sekunden auf 12.000 Sekunden.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Stellen Sie einen hohen Wert ein (Beispiel: 99999)

Aktivieren Sie außerdem die `StorageProvider.autoResignatureMode` Option.

Siehe "[Speicheranbieterereinstellungen ändern](#)" Weitere Informationen zum Ändern der Speicheranbieterereinstellungen.

Speichereinstellungen

Wenn Sie ein Timeout erreichen, erhöhen Sie die Werte von `storage.commandTimeout` Und `storage.maxConcurrentCommandCnt` auf einen höheren Wert.



Das angegebene Timeout-Intervall ist der Maximalwert. Sie müssen nicht warten, bis das maximale Timeout erreicht ist. Die meisten Befehle werden innerhalb des festgelegten maximalen Timeout-Intervalls abgeschlossen.

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

Konfigurieren von SRA auf der VMware Live Site Recovery-Appliance

Konfigurieren Sie nach der Bereitstellung der VMware Live Site Recovery-Appliance den Storage Replication Adapter (SRA), um die Notfallwiederherstellungsverwaltung zu aktivieren.

Durch die Konfiguration von SRA auf der VMware Live Site Recovery-Appliance werden die ONTAP tools for VMware vSphere -Anmeldeinformationen innerhalb der Appliance gespeichert, wodurch die Kommunikation zwischen VMware Live Site Recovery und SRA ermöglicht wird.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie auf dem Bildschirm der VMware Live Site Recovery-Appliance **Storage Replication Adapter > New Adapter**.
2. Laden Sie die Datei `.tar.gz` in VMware Live Site Recovery hoch.
3. Melden Sie sich mit einem Administratorkonto über einen SSH-Client wie PuTTY bei der VMware Live Site Recovery-Appliance an.
4. Wechseln Sie mit dem folgenden Befehl zum Root-Benutzer: `su root`
5. Führen Sie den Befehl aus `cd /var/log/vmware/srm`, um zum Protokollverzeichnis zu navigieren.
6. Geben Sie am Protokollspeicherort den Befehl ein, um die von SRA verwendete Docker-ID abzurufen:
`docker ps -l`
7. Um sich bei der Container-ID anzumelden, geben Sie den folgenden Befehl ein: `docker exec -it -u srm <container id> sh`
8. Konfigurieren Sie VMware Live Site Recovery mit ONTAP tools for VMware vSphere IP-Adresse und das Kennwort mithilfe des folgenden Befehls: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv -username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Geben Sie das Kennwort in einfachen Anführungszeichen ein, damit das Perl-Skript Sonderzeichen als Teil des Kennworts und nicht als Trennzeichen behandelt.
 - Sie können den Benutzernamen und das Kennwort der Anwendung (VASA Provider/SRA) im ONTAP Tools Manager festlegen, wenn Sie diese Dienste zum ersten Mal aktivieren. Verwenden Sie diese Anmeldeinformationen, um SRA bei VMware Live Site Recovery zu registrieren.
 - Um die vCenter-GUID zu finden, gehen Sie nach dem Hinzufügen Ihrer vCenter-Instanz zur vCenter-Server-Seite im ONTAP Tools Manager. Siehe ["vCenter-Server hinzufügen"](#) Abschnitt.
9. Scannen Sie die Adapter erneut, um zu bestätigen, dass die aktualisierten Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ angezeigt werden.

Ergebnisse

Eine Bestätigungsmeldung zeigt an, dass die Speicheranmeldeinformationen gespeichert wurden. SRA kann nun über die angegebene IP-Adresse, den Port und die Anmeldeinformationen mit dem SRA-Server kommunizieren.

SRA-Anmeldeinformationen aktualisieren

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

Bevor Sie beginnen

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

Schritte

1. Führen Sie die folgenden Befehle aus, um den im Ordner „VMware Live Site Recovery“ zwischengespeicherten Benutzernamen und das Kennwort für die ONTAP -Tools 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>`` Der Kennwortwert muss in einfache Anführungszeichen gesetzt werden.

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

Konfigurieren von geschützten Sites und Wiederherstellungssites

Sie sollten Schutzgruppen erstellen, um eine Gruppe virtueller Maschinen auf der geschützten Site zu schützen.

Wenn Sie einen neuen Datenspeicher hinzufügen, können Sie ihn in die bestehende Datenspeichergruppe aufnehmen oder einen neuen Datenspeicher hinzufügen und ein neues Volume oder eine neue Konsistenzgruppe zum Schutz erstellen. Nachdem Sie einen neuen Datenspeicher zu einer geschützten Konsistenzgruppe oder einem geschützten Volume hinzugefügt haben, aktualisieren Sie SnapMirror und führen Sie die Speichererkennung sowohl auf dem geschützten als auch auf dem Wiederherstellungsstandort durch. Sie können die Erkennung manuell oder nach Zeitplan durchführen, um sicherzustellen, dass der neue Datenspeicher erkannt und geschützt wird.

Koppeln Sie geschützte Sites und Wiederherstellungssites

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



Storage Replication Adapter (SRA) unterstützt Fan-Out mit einer Synchronisierungsbeziehung vom Typ „Automated Failover Duplex“ und der asynchronen Beziehung SnapMirror auf der Konsistenzgruppe. Allerdings wird Fan-Out mit zwei asynchronen SnapMirror auf einer Konsistenzgruppe oder Fan-Out-SnapMirrors auf einem Volume nicht unterstützt.

Bevor Sie beginnen

- Sie sollten VMware Live Site Recovery auf den geschützten Sites und Wiederherstellungssites installiert haben.
- Sie sollten SRA auf den geschützten Sites und Wiederherstellungssites installiert haben.

Schritte

1. Doppelklicken Sie auf der Startseite des vSphere-Clients auf **Site Recovery** und wählen Sie **Sites** aus.
2. Wählen Sie **Objekte > Aktionen > Sites koppeln**.
3. Geben Sie im Dialogfeld **Site Recovery Manager-Server koppeln** die Adresse des Platform Services Controllers der geschützten Site ein und wählen Sie dann **Weiter**.
4. Führen Sie im Abschnitt „vCenter Server auswählen“ die folgenden Schritte aus:
 - a. Überprüfen Sie, 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 dann **Fertig**.
5. Wählen Sie bei der entsprechenden Aufforderung **Ja** aus, um die Sicherheitszertifikate zu akzeptieren.

Ergebnis

Sowohl die geschützten als auch die Wiederherstellungssites werden im Dialogfeld „Objekte“ angezeigt.

Konfigurieren von Schutzgruppen

Bevor Sie beginnen

Sie sollten sicherstellen, dass sowohl die Quell- als auch die Zielsites für Folgendes konfiguriert sind:

- Dieselbe Version von VMware Live Site Recovery installiert
- Virtuelle Maschinen
- Gepaarte geschützte Sites und Wiederherstellungssites
- Quell- und Zieldatenspeicher sollten auf den jeweiligen Sites gemountet werden

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery > Schutzgruppen**.
2. Wählen Sie im Bereich **Schutzgruppen** die Option **Neu** aus.
3. Geben Sie einen Namen und eine Beschreibung für die Schutzgruppe und die Richtung an und wählen Sie **Weiter**.
4. Wählen Sie im Feld **Typ** die Option **Typfeldoption...** als Datenspeicherguppen (Array-basierte Replikation) für NFS- und VMFS-Datenspeicher aus. Die Fehlerdomäne besteht ausschließlich aus SVMs mit aktivierter Replikation. Es werden die SVMs angezeigt, die nur Peering implementiert haben und keine Probleme aufweisen.
5. Wählen Sie auf der Registerkarte „Replikationsgruppen“ entweder das aktivierte Array-Paar oder die Replikationsgruppen mit der von Ihnen konfigurierten virtuellen Maschine aus und wählen Sie dann **Weiter**.

Alle virtuellen Maschinen in der Replikationsgruppe werden der Schutzgruppe hinzugefügt.

6. Sie können entweder den vorhandenen Wiederherstellungsplan auswählen oder einen neuen erstellen, indem Sie **Zum neuen Wiederherstellungsplan hinzufügen** auswählen.
7. Überprüfen Sie auf der Registerkarte „Bereit zum Abschließen“ die Details der von Ihnen erstellten Schutzgruppe und wählen Sie dann **Fertig stellen** aus.

Konfigurieren von geschützten Site- und Wiederherstellungs-Site-Ressourcen

Konfigurieren von Netzwerkzuordnungen

Sie sollten Ihre Ressourcenzuordnungen wie VM-Netzwerke, ESXi-Hosts und Ordner auf beiden Sites konfigurieren, um die Zuordnung jeder Ressource von der geschützten Site zur entsprechenden Ressource auf der Wiederherstellungssite zu ermöglichen.

Sie sollten die folgenden Ressourcenkonfigurationen durchführen:

- Netzwerkzuordnungen
- Ordnerzuordnungen
- Ressourcenzuordnungen
- Platzhalter-Datenspeicher

Bevor Sie beginnen

Sie sollten die geschützten und Wiederherstellungssites verbunden haben.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte „Verwalten“ **Netzwerkzuordnungen > Neu**, um eine neue Netzwerkzuordnung zu erstellen.
4. Führen Sie im Assistenten „Netzwerkzuordnung erstellen“ die folgenden Schritte aus:
 - a. Wählen Sie **Zuordnungen für Netzwerke mit übereinstimmenden Namen automatisch vorbereiten** und wählen Sie **Weiter**.
 - b. Wählen Sie die erforderlichen Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. Wählen Sie **Weiter**, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das zuvor zum Erstellen der Rückwärtszuordnung verwendete Objekt aus und wählen Sie dann **Fertig**.

Ergebnis

Auf der Seite „Netzwerkzuordnungen“ werden die Ressourcen der geschützten Site und der Wiederherstellungssite angezeigt. Sie können dieselben Schritte für andere Netzwerke in Ihrer Umgebung ausführen.

Konfigurieren von Ordnerzuordnungen

Sie sollten Ihre Ordner auf der geschützten Site und der Wiederherstellungssite zuordnen, um die Kommunikation zwischen ihnen zu ermöglichen.

Bevor Sie beginnen

Sie sollten die geschützten und Wiederherstellungssites verbunden haben.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte „Verwalten“ das Symbol „**Ordnerzuordnungen > Ordner**“, um eine neue Ordnerzuordnung zu erstellen.
4. Führen Sie im Assistenten „Ordnerzuordnung erstellen“ die folgenden Schritte aus:
 - a. Wählen Sie **Zuordnungen für Ordner mit übereinstimmenden Namen automatisch vorbereiten** und wählen Sie **Weiter**.
 - b. Wählen Sie die erforderlichen Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. Wählen Sie **Weiter**, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das zuvor zum Erstellen der Rückwärtszuordnung verwendete Objekt aus und wählen Sie dann **Fertig**.

Ergebnis

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

Konfigurieren von Ressourcenzuordnungen

Sie sollten Ihre Ressourcen auf der geschützten Site und der Wiederherstellungssite so zuordnen, dass virtuelle Maschinen für ein Failover in die eine oder andere Hostgruppe konfiguriert sind.

Bevor Sie beginnen

Sie sollten die geschützten und Wiederherstellungssites verbunden haben.



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

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte „Verwalten“ **Ressourcenzuordnungen > Neu** aus, um eine neue Ressourcenzuordnung zu erstellen.
4. Führen Sie im Assistenten „Ressourcenzuordnung erstellen“ die folgenden Schritte aus:
 - a. Wählen Sie **Zuordnungen für Ressourcen mit übereinstimmenden Namen automatisch vorbereiten** und klicken Sie auf **Weiter**.
 - b. Wählen Sie die erforderlichen Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. Wählen Sie **Weiter**, nachdem die Zuordnungen erfolgreich erstellt wurden.

- d. Wählen Sie das zuvor zum Erstellen der Rückwärtszuordnung verwendete Objekt aus und wählen Sie dann **Fertig**.

Ergebnis

Auf der Seite „Ressourcenzuordnungen“ werden die Ressourcen der geschützten Site und der Wiederherstellungssite angezeigt. Sie können dieselben Schritte für andere Netzwerke in Ihrer Umgebung ausführen.

Platzhalter-Datenspeicher konfigurieren

Sie sollten einen Platzhalterdatenspeicher konfigurieren, der im vCenter-Inventar am Wiederherstellungsstandort Platz für die geschützte virtuelle Maschine (VM) reserviert. Der Platzhalterdatenspeicher muss nicht groß sein, da die Platzhalter-VMs klein sind und nur wenige hundert Kilobyte oder weniger belegen.

Bevor Sie beginnen

- Sie sollten die geschützten und Wiederherstellungssites verbunden haben.
- Sie sollten Ihre Ressourcenzuordnungen konfiguriert haben.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte „Verwalten“ **Platzhalter-Datenspeicher > Neu**, um einen neuen Platzhalter-Datenspeicher zu erstellen.
4. Wählen Sie den entsprechenden Datenspeicher aus und klicken Sie auf **OK**.



Platzhalter-Datenspeicher können lokal oder remote sein und sollten nicht repliziert werden.

5. Wiederholen Sie die Schritte 3 bis 5, um einen Platzhalterdatenspeicher für die Wiederherstellungssite zu konfigurieren.

Konfigurieren Sie SRA mit dem Array-Manager

Sie können den Storage Replication Adapter (SRA) mithilfe des Array Manager-Assistenten von VMware Live Site Recovery konfigurieren, um Interaktionen zwischen VMware Live Site Recovery und virtuellen Speichermaschinen (SVMs) zu ermöglichen.

Bevor Sie beginnen

- Sie sollten die geschützten Sites und Wiederherstellungssites in VMware Live Site Recovery gekoppelt haben.
- Sie sollten Ihren integrierten Speicher konfiguriert haben, bevor Sie den Array-Manager konfigurieren.
- Sie sollten die SnapMirror -Beziehungen zwischen den geschützten Sites und den Wiederherstellungssites konfiguriert und repliziert haben.
- Sie sollten die SVM-Verwaltungs-LIFs aktiviert haben, um Multitenancy zu ermöglichen.

SRA unterstützt die Verwaltung auf Cluster- und SVM-Ebene. Wenn Sie Speicher auf Clusterebene hinzufügen, können Sie alle SVMs im Cluster erkennen und Vorgänge darauf ausführen. Wenn Sie Speicher auf SVM-Ebene hinzufügen, können Sie nur dieses bestimmte SVM verwalten.

Schritte

1. Wählen Sie in VMware Live Site Recovery **Array-Manager** > **Array-Manager hinzufügen**.
2. Geben Sie die folgenden Informationen ein, um das Array in VMware Live Site Recovery zu beschreiben:
 - a. Geben Sie im Feld **Anzeigename** einen Namen zur Identifizierung des Array-Managers ein.
 - b. Wählen Sie im Feld **SRA-Typ** * NetApp Storage Replication Adapter für ONTAP* aus.
 - c. Geben Sie die Informationen zum Herstellen einer Verbindung mit dem Cluster oder der SVM ein:
 - Wenn Sie eine Verbindung zu einem Cluster herstellen, sollten Sie das Cluster-Management-LIF eingeben.
 - Wenn Sie eine direkte Verbindung zu einer SVM herstellen, sollten Sie die IP-Adresse des SVM-Verwaltungs-LIF eingeben.



Beim Konfigurieren des Array-Managers sollten Sie für das Speichersystem dieselbe Verbindung (IP-Adresse) verwenden, die zum Onboarding des Speichersystems in den ONTAP tools for VMware vSphere verwendet wurde. Wenn die Array-Manager-Konfiguration beispielsweise auf SVM beschränkt ist, sollte der Speicher unter ONTAP tools for VMware vSphere auf SVM-Ebene hinzugefügt werden.

- d. Wenn Sie eine Verbindung zu einem Cluster herstellen, geben Sie den SVM-Namen im Feld **SVM-Name** an oder lassen Sie es leer, um alle SVMs im Cluster zu verwalten.
- e. Geben Sie die zu ermittelnden Volumes in das Feld **Volume-Einschlussliste** ein.

Sie können das Quellvolume am geschützten Standort und das replizierte Zielvolume am Wiederherstellungsstandort eingeben.

Wenn Sie beispielsweise das Volume `src_vol1` ermitteln möchten, das in einer SnapMirror -Beziehung mit dem Volume `dst_vol1` steht, sollten Sie `src_vol1` im Feld „geschützte Site“ und `dst_vol1` im Feld „Wiederherstellungsstelle“ angeben.

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

Sie können das Quellvolume am geschützten Standort und das replizierte Zielvolume am Wiederherstellungsstandort eingeben.

Wenn Sie beispielsweise das Volume `src_vol1` ausschließen möchten, das in einer SnapMirror -Beziehung mit dem Volume `dst_vol1` steht, sollten Sie `src_vol1` im Feld „Geschützter Standort“ und `dst_vol1` im Feld „Wiederherstellungsstandort“ angeben.

3. Wählen Sie **Weiter**.
4. Überprüfen Sie, ob das Array erkannt und unten im Fenster „Array-Manager hinzufügen“ angezeigt wird, und wählen Sie „Fertig stellen“ aus.

Sie können dieselben Schritte für die Wiederherstellungsstelle ausführen, indem Sie die entsprechenden SVM-Verwaltungs-IP-Adressen und Anmeldeinformationen verwenden. Überprüfen Sie auf dem Bildschirm „Array-Paare aktivieren“ des Assistenten „Array-Manager hinzufügen“, ob das richtige Array-Paar ausgewählt ist und als zur Aktivierung bereit angezeigt wird.

Überprüfen replizierter Speichersysteme

Sie sollten überprüfen, ob die geschützte Site und die Wiederherstellungssite nach der Konfiguration des Storage Replication Adapter (SRA) erfolgreich gekoppelt wurden. Das replizierte Speichersystem sollte sowohl vom geschützten Standort als auch vom Wiederherstellungsstandort erkennbar sein.

Bevor Sie beginnen

- Sie sollten Ihr Speichersystem konfiguriert haben.
- Sie sollten die geschützte Site und die Wiederherstellungssite mithilfe des VMware Live Site Recovery-Array-Managers gekoppelt haben.
- Sie sollten die FlexClone -Lizenz und die SnapMirror -Lizenz aktiviert haben, bevor Sie den Test-Failover-Vorgang und den Failover-Vorgang für SRA durchführen.
- Sie sollten auf Quell- und Zielsites dieselben SnapMirror -Richtlinien und -Zeitpläne haben.

Schritte

1. Melden Sie sich bei Ihrem vCenter Server an.
2. Navigieren Sie zu **Site Recovery > Array-basierte Replikation**.
3. Wählen Sie das gewünschte Array-Paar aus und überprüfen Sie die entsprechenden Angaben.

Die Speichersysteme sollten am geschützten Standort und am Wiederherstellungsstandort mit dem Status „Aktiviert“ erkannt werden.

Fan-Out-Schutz

Bei einem Fan-Out-Schutz ist die Konsistenzgruppe doppelt geschützt, mit einer synchronen Beziehung auf dem ersten Ziel ONTAP Cluster und mit einer asynchronen Beziehung auf dem zweiten Ziel ONTAP Cluster. Die Workflows zum Erstellen, Bearbeiten und Löschen des SnapMirror Active Sync-Schutzes gewährleisten den synchronen Schutz. SRM-Failover- und Reprotect-Workflows erhalten den asynchronen Schutz aufrecht.

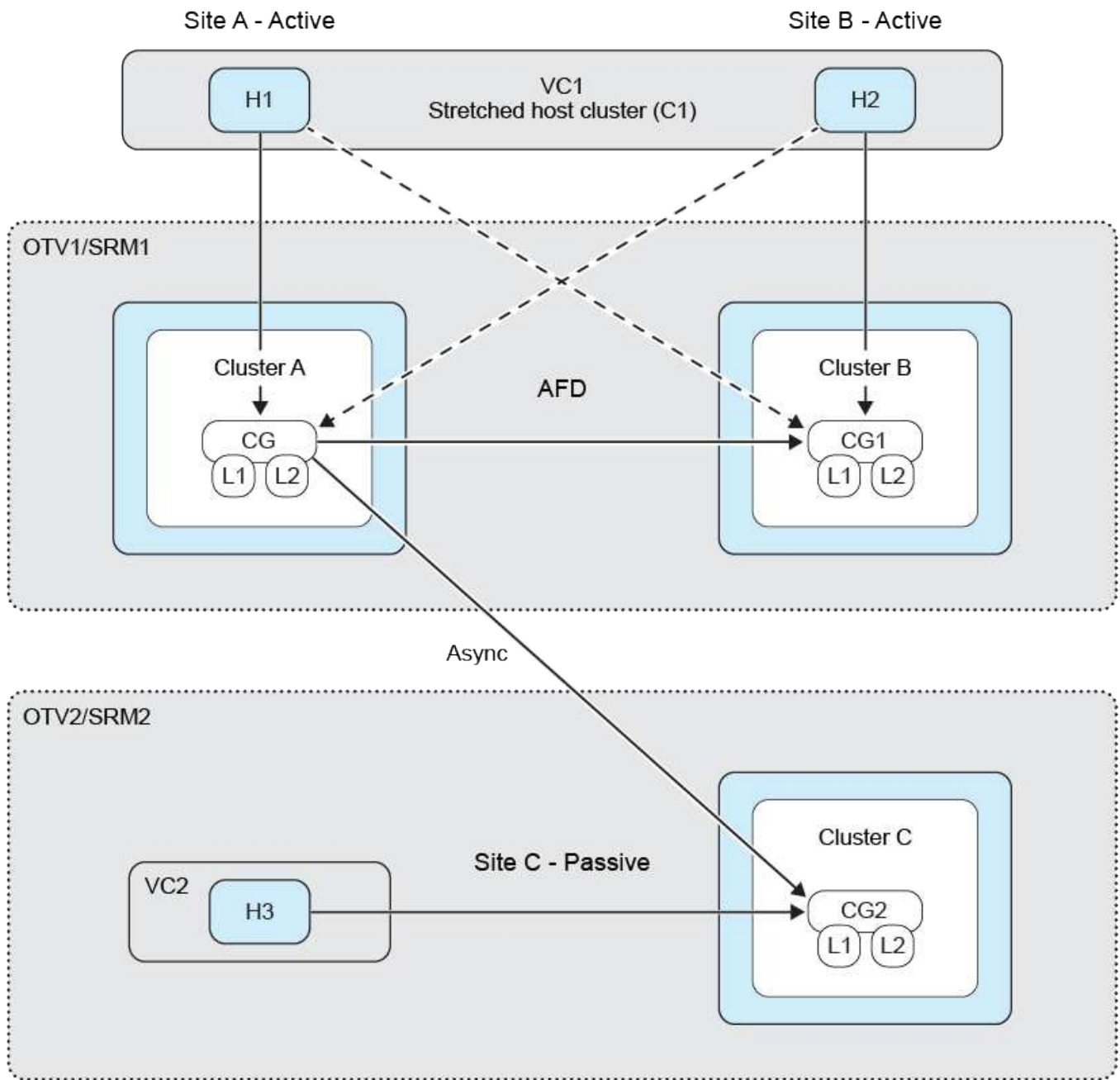
Um einen Fan-Out-Schutz einzurichten, müssen Sie drei Site-Cluster und SVMs miteinander verbinden.

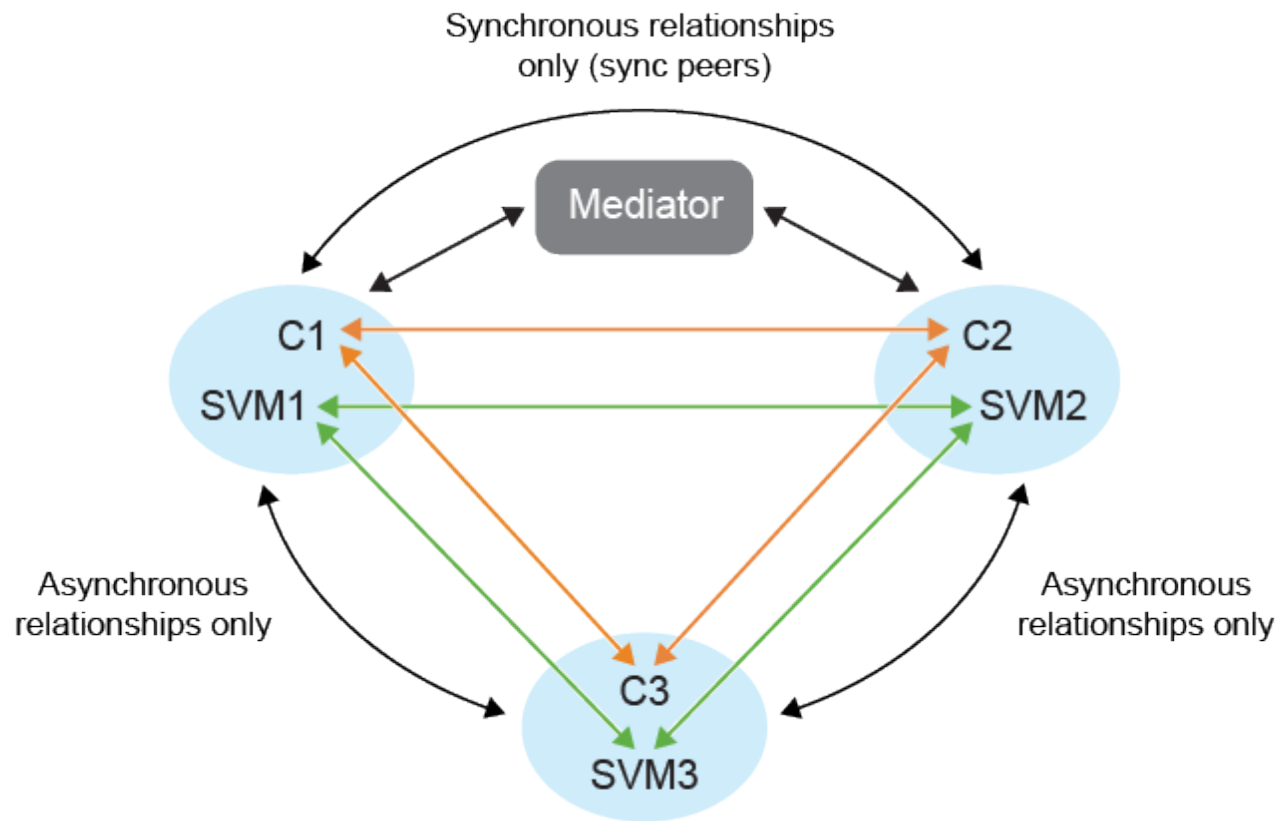
Beispiel:

Wenn	Dann
------	------

• Die Quellkonsistenzgruppe befindet sich auf Cluster c1 und SVM svm1 • Die erste Zielkonsistenzgruppe befindet sich auf Cluster c2 und SVM svm2 und • Die zweite Zielkonsistenzgruppe 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 wird (C2, C1) und (C2, C3) sein und • Das Cluster-Peering auf dem zweiten Ziel ONTAP Cluster wird (C3, C1) und (C3, C2) sein. • SVM-Peering auf Quell-SVM wird (svm1, svm2) und (svm1, svm3) sein. • SVM-Peering auf dem ersten Ziel-SVM wird (svm2, svm1) und (svm2, svm3) sein und • Das SVM-Peering auf dem zweiten Ziel-SVM erfolgt (svm3, svm1) und (svm3, svm2).
--	---

Das folgende Diagramm zeigt die Fan-Out-Schutzkonfiguration:





Schritte

1. Erstellen Sie einen neuen Platzhalter-Datenspeicher. Verweisen ["Wählen Sie einen Platzhalter-Datenspeicher aus"](#)
2. Fügen Sie dem Hostclusterschutz einen Datenspeicher hinzu ["Geschützten Hostcluster ändern"](#) . Sie müssen sowohl asynchrone als auch synchrone Richtlinientypen hinzufügen.

Copyright-Informationen

Copyright © 2025 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.