Richten Sie die synchrone Replikation mit NetApp SnapMirror Active Sync und Microsoft Stretch-Clustern ein

NetApp virtualization solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-virtualization/hyperv/hyperv-smas.html on August 18, 2025. Always check docs.netapp.com for the latest.

Inhalt

Richten Sie die synchrone Replikation mit NetApp SnapMirror Active Sync und Microsoft Stretch-Clustern ein . . . 1
Einführung . . . 1
Anwendungsfälle . . . 1
Lösungsarchitektur . . . 2
Installieren eines Microsoft Stretch Failoverclusters . . . 3
Intercluster-Peering erstellen . . . 5
Mediator mit ONTAP konfigurieren . . . 6
Konfigurieren Sie den symmetrischen Aktiv/Aktiv-Schutz . . . 8
Durchführen eines Cluster-Failover-Validierungstests . . . 9
Zusammenfassung . . . 11

Richten Sie die synchrone Replikation mit NetApp SnapMirror Active Sync und Microsoft Stretch-Clustern ein

Verwenden Sie SnapMirror Active Sync, um eine synchrone, bidirektionale Replikation zwischen Microsoft Stretch-Failover-Clustern zu konfigurieren. Dieses Verfahren umfasst die Installation eines Stretch-Failover-Clusters, die Erstellung eines Intercluster-Peerings, die Konfiguration eines Mediators mit ONTAP, die Aktivierung des symmetrischen Aktiv/Aktiv-Schutzes und die Durchführung von Cluster-Failover-Validierungstests.

Einführung

Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync symmetrische Active/Active-Bereitstellungen und ermöglicht Lese- und Schreib-E/A-Vorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replikation. Ein Windows Stretch Cluster ist eine Erweiterung der Windows Failover Cluster-Funktion, die sich über mehrere geografische Standorte erstreckt, um hohe Verfügbarkeit und Notfallwiederherstellung zu gewährleisten. Mit SnapMirror Active Sync Symmetric Active/Active und Cluster-Anwendungen wie Windows Failover Clustering können wir eine kontinuierliche Verfügbarkeit für geschäftskritische Microsoft Hyper-V-Anwendungen erreichen, um bei unerwarteten Vorfällen RTO und RPO von Null zu erreichen. Diese Lösung bietet die folgenden Vorteile:

- Kein Datenverlust: Stellt sicher, dass Daten synchron repliziert werden, wodurch ein Recovery Point Objective (RPO) von Null erreicht wird.
- Hohe Verfügbarkeit und Lastausgleich: Beide Sites können Anfragen aktiv verarbeiten und so für Lastausgleich und hohe Verfügbarkeit sorgen.
- Geschäftskontinuität: Implementieren Sie eine symmetrische Aktiv/Aktiv-Konfiguration, um sicherzustellen, dass beide Rechenzentren aktiv Anwendungen bereitstellen und im Falle eines Ausfalls nahtlos übernehmen können.
- Verbessern Sie die Leistung: Verwenden Sie eine symmetrische Aktiv/Aktiv-Konfiguration, um die Last auf mehrere Speichersysteme zu verteilen und so die Reaktionszeiten und die Gesamtsystemleistung zu verbessern.

Dieses Dokument dokumentiert die synchrone bidirektionale Replikation der SnapMirror Active Sync-Technologie zwischen Microsoft Stretch Failover-Clustern, wodurch Anwendungsdaten mehrerer Standorte, beispielsweise MSSQL und Oracle, aktiv zugänglich und an beiden Standorten synchronisiert sind. Wenn ein Fehler auftritt, werden Anwendungen sofort auf die verbleibende aktive Site umgeleitet, ohne dass Daten oder Zugriff verloren gehen. Dies gewährleistet hohe Verfügbarkeit, Notfallwiederherstellung und geografische Redundanz.

Anwendungsfälle

Im Falle einer Störung wie beispielsweise eines Cyberangriffs, eines Stromausfalls oder einer Naturkatastrophe erfordert eine global vernetzte Geschäftsumgebung eine schnelle Wiederherstellung geschäftskritischer Anwendungsdaten ohne Datenverlust. Diese Anforderungen sind in Bereichen wie dem Finanzwesen und der Einhaltung gesetzlicher Vorschriften wie der Datenschutz-Grundverordnung (DSGVO) noch höher. Setzen Sie eine symmetrische Aktiv/Aktiv-Konfiguration ein, um Daten zwischen geografisch verteilten Standorten zu replizieren, lokalen Zugriff auf Daten zu ermöglichen und die Kontinuität bei regionalen Ausfällen sicherzustellen.

SnapMirror Active Sync bietet die folgenden Anwendungsfälle:

Anwendungsbereitstellung für Zero Recovery Time Object (RTO)

Bei einer SnapMirror Active Sync-Bereitstellung verfügen Sie über einen primären und einen Spiegelcluster. Ein LUN im primären Cluster (L1P) verfügt über ein Spiegelbild (L1S) auf dem sekundären Cluster. Lese- und Schreibvorgänge werden basierend auf den Hot Proximity-Einstellungen von der lokalen Site der Hosts ausgeführt.

Anwendungsbereitstellung für null RTO oder TAF

Transparent Application Failover (TAF) basiert auf einem softwarebasierten Pfad-Failover des Host-MPIO, um einen unterbrechungsfreien Zugriff auf den Speicher zu erreichen. Beide LUN-Kopien – beispielsweise die primäre (L1P) und die Spiegelkopie (L1S) – haben dieselbe Identität (Seriennummer) und werden dem Host als lesbar und schreibbar gemeldet.

Clusteranwendungen

Clusteranwendungen, darunter VMware vSphere Metro Storage Cluster (vMSC), Oracle RAC und Windows Failover Clustering mit SQL, erfordern gleichzeitigen Zugriff, damit die VMs ohne Leistungseinbußen auf die andere Site umgeschaltet werden können. SnapMirror Active Sync Symmetric Active/Active bedient IO lokal mit bidirektionaler Replikation, um die Anforderungen von Clusteranwendungen zu erfüllen.

Katastrophenszenario

Replizieren Sie synchron mehrere Volumes für eine Anwendung zwischen Standorten an geografisch verteilten Standorten. Sie können im Falle einer Störung auf der primären Kopie automatisch ein Failover auf die sekundäre Kopie durchführen und so die Geschäftskontinuität für Tier-1-Anwendungen gewährleisten.

Windows-Failover

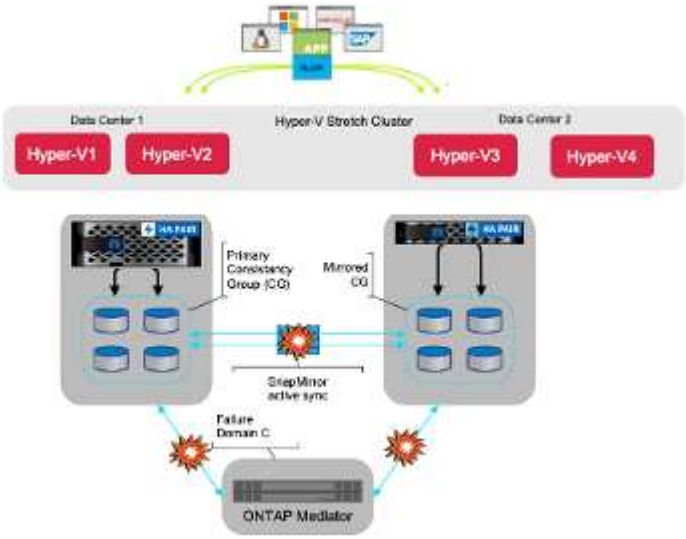
SnapMirror Active Sync bietet Flexibilität mit benutzerfreundlicher Granularität auf Anwendungsebene und automatischem Failover, um eine hohe Datenverfügbarkeit und schnelle Datenreplikation für Ihre geschäftskritischen Anwendungen wie Oracle, Microsoft SQL Server usw. sowohl in virtuellen als auch in physischen Umgebungen zu erreichen.

Lösungsarchitektur

Der Microsoft Stretch-Cluster verfügt an jedem Standort über zwei Hyper-V-Knoten. Diese beiden Knoten teilen sich den NetApp -Speicher und verwenden SnapMirror Active Sync Symmetric Active-Active, um die Volumes zwischen den beiden Standorten zu replizieren. Eine Konsistenzgruppe stellt sicher, dass alle Volumes eines Datensatzes stillgelegt und zum exakt gleichen Zeitpunkt erneut gesichert werden. Dies bietet einen datenkonsistenten Wiederherstellungspunkt über alle Volumes hinweg, die den Datensatz unterstützen. Der ONTAP Mediator empfängt Integritätsinformationen zu verbundenen ONTAP Clustern und -Knoten, koordiniert die Kommunikation zwischen beiden und ermittelt, ob jeder Knoten/Cluster fehlerfrei und betriebsbereit ist.

Lösungskomponenten:

- Zwei NetApp Storage Systeme ONTAP 9.15.1: erste und zweite Fehlerdomäne
- Eine Redhat 8.7 VM für ONTAP Mediator
- Drei Hyper-V-Failovercluster unter Windows 2022:
  - Site1, Site 2 für die Anwendungen
  - Site 3 für Mediator
- VM auf Hyper-V: Microsoft Domänencontroller, MSSQL Always On Failoverclusterinstanz, ONTAP Mediator



Installieren eines Microsoft Stretch Failoverclusters

Sie können Windows Admin Center, PowerShell oder die Server Manager-Konsole verwenden, um die Failoverclustering-Funktion und die zugehörigen PowerShell-Cmdlets zu installieren. Ausführliche Informationen zu Voraussetzungen und Schritten finden Sie unter „Erstellen eines Failoverclusters“.

Hier ist eine Schritt-für-Schritt-Anleitung zum Einrichten eines Windows Stretch Clusters:

1. Installieren Sie Windows 2022 auf allen vier Servern Hyperv1, Hyperv2, Hyperv3 und Hyperv4
2. Fügen Sie alle vier Server derselben Active Directory-Domäne hinzu: hyperv.local.
3. Installieren Sie die Windows-Funktionen Failover-Clustering, Hyper-V, Hyper-V_Powershell und MPIO auf jedem Server.

```
Install-WindowsFeature -Name "Failover-Clustering", "Hyper-V", "Hyper-V-Powershell", "MPIO" -IncludeManagementTools
```

4. Konfigurieren Sie MPIO und fügen Sie Unterstützung für iSCSI-Geräte hinzu.

5. Erstellen Sie auf dem ONTAP -Speicher von Site 1 und Site 2 zwei iSCSI-LUNs (SQLdata und SQLlog) und ordnen Sie sie der IQN-Gruppe der Windows-Server zu. Verwenden Sie den Microsoft iSCSI-

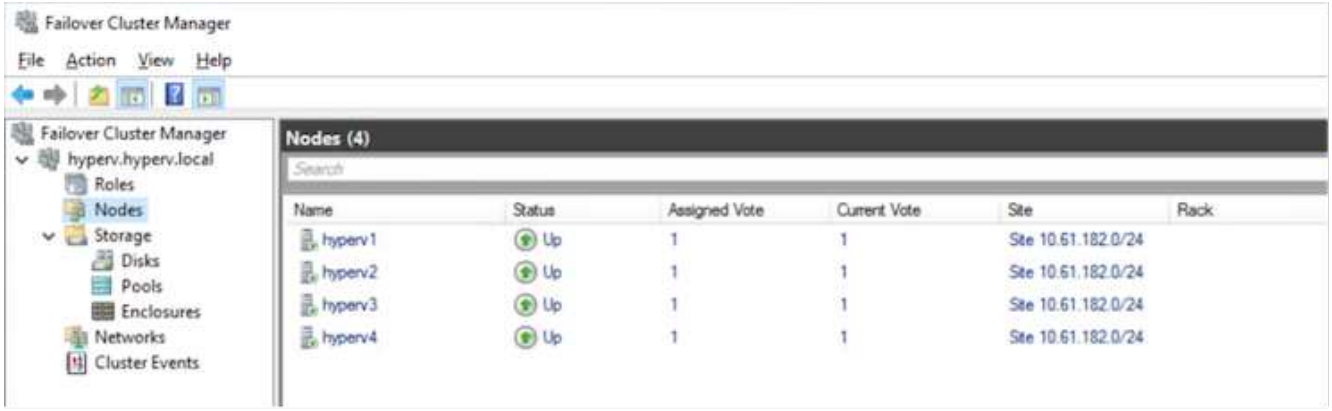
Softwareinitiator, um die LUNs zu verbinden. Weitere Einzelheiten finden Sie unter"iSCSI-Konfiguration für Windows" .

6. Führen Sie den Clustervalidierungsbericht aus, um Fehler oder Warnungen zu ermitteln.

```
Test-Cluster -Node hyperv1, hyperv2, hyperv3, hyperv4
```

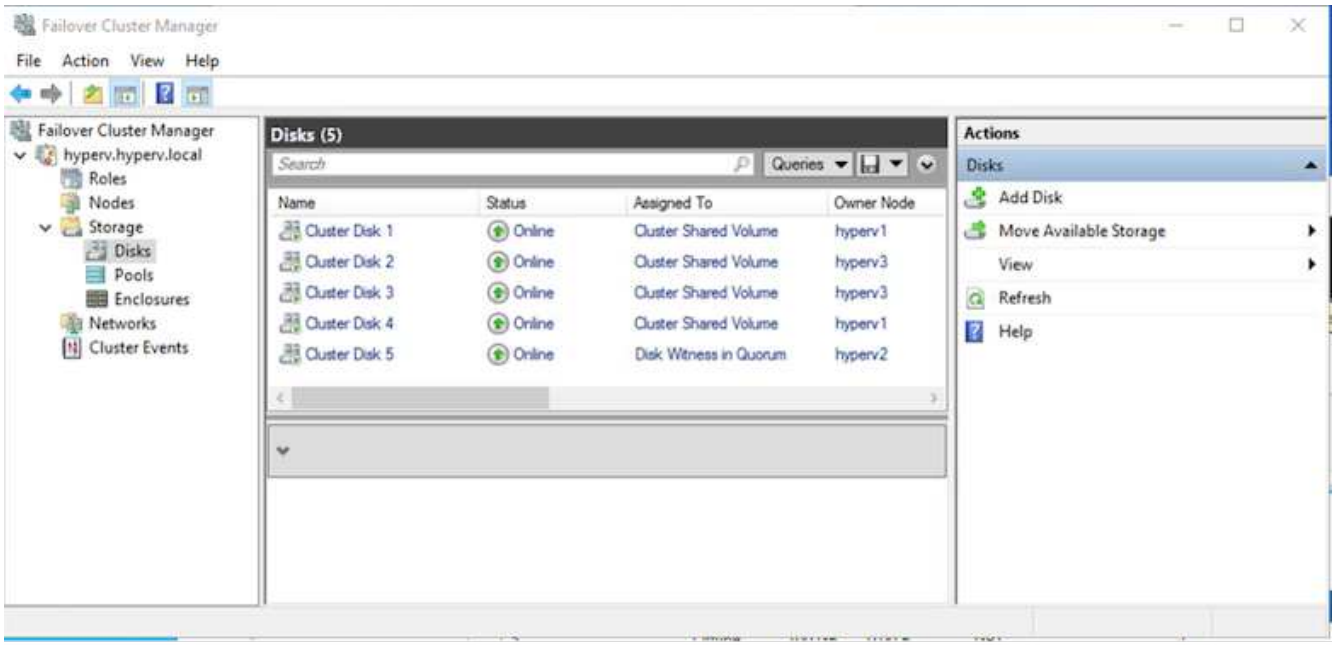
7. Erstellen Sie einen Failover-Cluster, weisen Sie eine statische IP-Adresse zu,

```
New-Cluster -Name <clustername> -Node hyperv1, hyperv2, hyperv3,
hyperv4, StaticAddress <IPaddress>
```



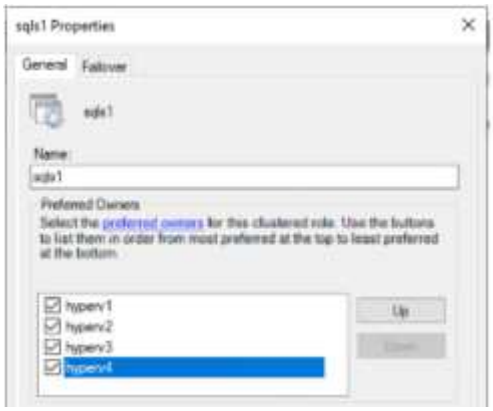
8. Fügen Sie die zugeordneten iSCSI-Speicher zum Failovercluster hinzu.
9. Konfigurieren Sie einen Zeugen für das Quorum, klicken Sie mit der rechten Maustaste auf den Cluster → Weitere Aktionen → Cluster-Quorum-Einstellungen konfigurieren, wählen Sie Datenträgerzeugen.

   Das folgende Diagramm zeigt vier geclusterte gemeinsam genutzte LUNs – zwei Sites „sqldata“ und „sqllog“ und einen Datenträgerzeugen im Quorum.



Always On-Failoverclusterinstanz

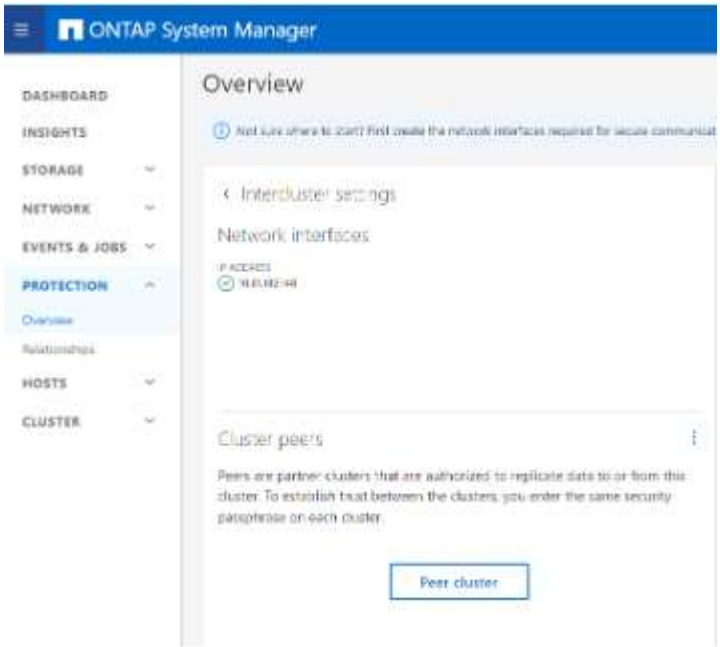
Eine Always On Failover Cluster Instance (FCI) ist eine SQL Server-Instanz, die über Knoten mit gemeinsam genutztem SAN-Datenträgerspeicher in einem WSFC installiert wird. Während eines Failovers überträgt der WSFC-Dienst den Besitz der Ressourcen der Instanz auf einen bestimmten Failover-Knoten. Anschließend wird die SQL Server-Instanz auf dem Failover-Knoten neu gestartet und die Datenbanken werden wie gewohnt wiederhergestellt. Weitere Einzelheiten zur Einrichtung finden Sie unter Windows Failover Clustering mit SQL. Erstellen Sie an jedem Standort zwei Hyper-V SQL FCI-VMs und legen Sie die Priorität fest. Verwenden Sie Hyperv1 und Hyperv2 als bevorzugte Besitzer für die VMs von Site 1 und Hyperv3 und Hyperv4 als bevorzugte Besitzer für die VMs von Site 2.



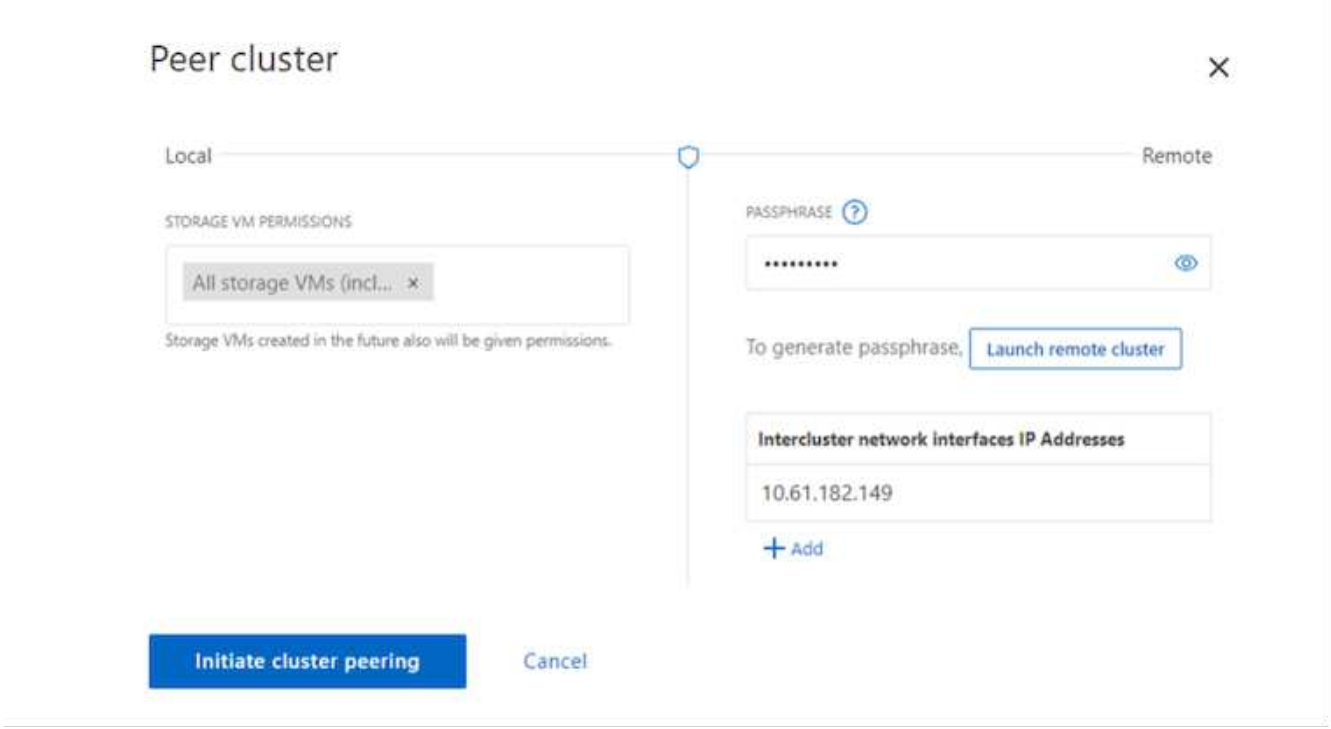
Intercluster-Peering erstellen

Sie müssen Peer-Beziehungen zwischen Quell- und Zielclustern erstellen, bevor Sie Snapshot-Kopien mit SnapMirror replizieren können.

1. Fügen Sie auf beiden Clustern Intercluster-Netzwerkschnittstellen hinzu



2. Mit dem Befehl „Cluster Peer Create“ können Sie eine Peer-Beziehung zwischen einem lokalen und einem Remote-Cluster erstellen. Nachdem die Peer-Beziehung erstellt wurde, können Sie „Cluster Peer Create“ auf dem Remote-Cluster ausführen, um ihn beim lokalen Cluster zu authentifizieren.



Mediator mit ONTAP konfigurieren

Der ONTAP Mediator empfängt Integritätsinformationen zu verbundenen ONTAP Clustern und -Knoten, koordiniert die Kommunikation zwischen beiden und ermittelt, ob jeder Knoten/Cluster fehlerfrei und betriebsbereit ist. SM-as ermöglicht die Replikation von Daten auf das Ziel, sobald sie auf das Quellvolume geschrieben werden. Der Mediator muss in der dritten Fehlerdomäne eingesetzt werden. Voraussetzungen

- HW-Spezifikationen: 8 GB RAM, 2 x 2 GHz CPU, 1 GB Netzwerk (<125 ms RTT)
- Installiertes Red Hat 8.7 OS, überprüfen"ONTAP Mediator-Version und unterstützte Linux-Version" .
- Konfigurieren Sie den Mediator Linux-Host: Netzwerk-Setup und Firewall-Ports 31784 und 3260
- Installieren Sie das yum-utils-Paket
- "Registrieren Sie einen Sicherheitsschlüssel, wenn UEFI Secure Boot aktiviert ist"

Schritte

1. Laden Sie das Mediator-Installationspaket von der"ONTAP Mediator-Downloadseite" .
2. Überprüfen Sie die Code-Signatur des ONTAP Mediators.
3. Führen Sie das Installationsprogramm aus und reagieren Sie wie erforderlich auf die Eingabeaufforderungen:

```
./ontap-mediator-1.8.0/ontap-mediator-1.8.0 -y
```

4. Wenn Secure Boot aktiviert ist, müssen Sie nach der Installation zusätzliche Schritte ausführen, um den Sicherheitsschlüssel zu registrieren:
   a. Befolgen Sie die Anweisungen in der README-Datei, um das SCST-Kernelmodul zu signieren:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.mo
dule-signing
```

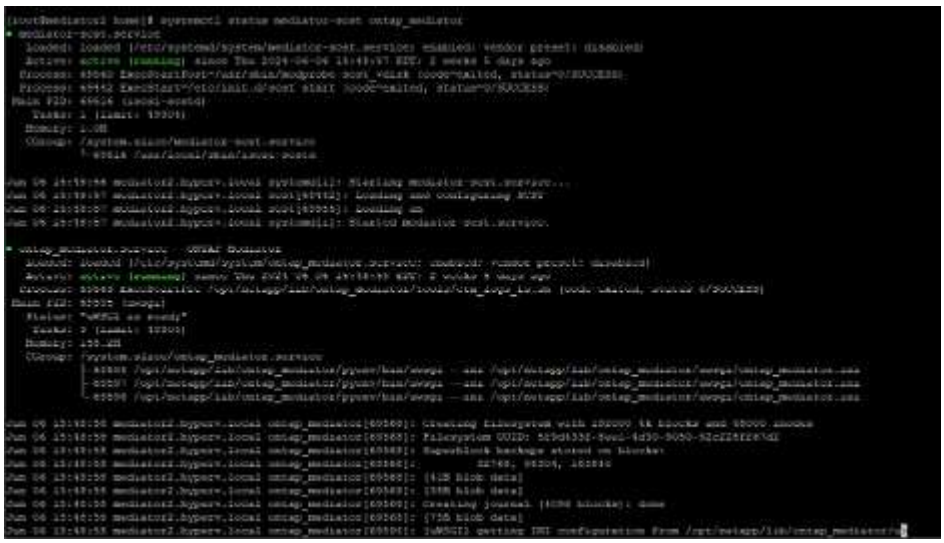
b. Suchen Sie die erforderlichen Schlüssel:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

5. Überprüfen der Installation

a. Bestätigen Sie die Prozesse:

```
systemctl status ontap_mediator mediator-scst
```



b. Bestätigen Sie die vom ONTAP Mediator-Dienst verwendeten Ports:

```
[root@mediator2 server_config]# netstat -anlt | grep -E '3260|31784'
tcp        0      0 0.0.0.0:3260            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:31784           0.0.0.0:*               LISTEN
tcp        0      0 10.61.182.163:31784     10.61.182.148:26429     ESTABLISHED
tcp        0      0 10.61.182.163:31784     10.61.182.148:24546     FIN_WAIT2
tcp6       0      0 :::3260                 :::*                    LISTEN
```

6. Initialisieren Sie den ONTAP Mediator für SnapMirror Active Sync mit selbstsignierten Zertifikaten

a. Suchen Sie das ONTAP Mediator CA-Zertifikat im Installationsverzeichnis der ONTAP Mediator Linux VM/Host-Software: cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config.

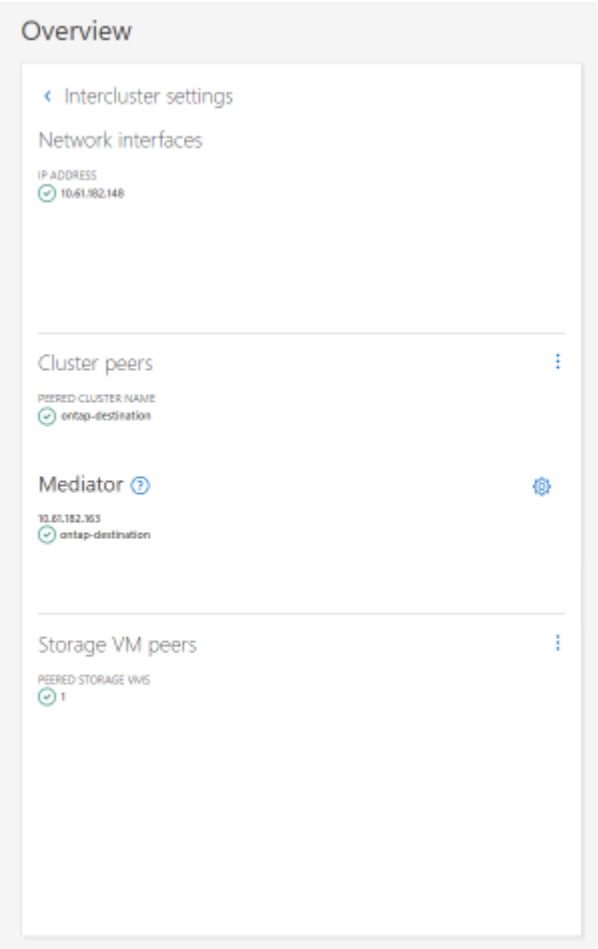
b. Fügen Sie das ONTAP Mediator CA-Zertifikat zu einem ONTAP Cluster hinzu.

```
security certificate install -type server-ca -vserver <vserver_name>
```

7. Fügen Sie den Mediator hinzu, gehen Sie zu System Manager, Schützen > Übersicht > Mediator, geben

Sie die IP-Adresse, den Benutzernamen (API-Benutzerstandard ist mediatoradmin), das Passwort und den Port 31784 des Mediators ein.

Das folgende Diagramm zeigt die Einrichtung der Intercluster-Netzwerkschnittstelle, der Cluster-Peers, des Mediators und des SVM-Peers.

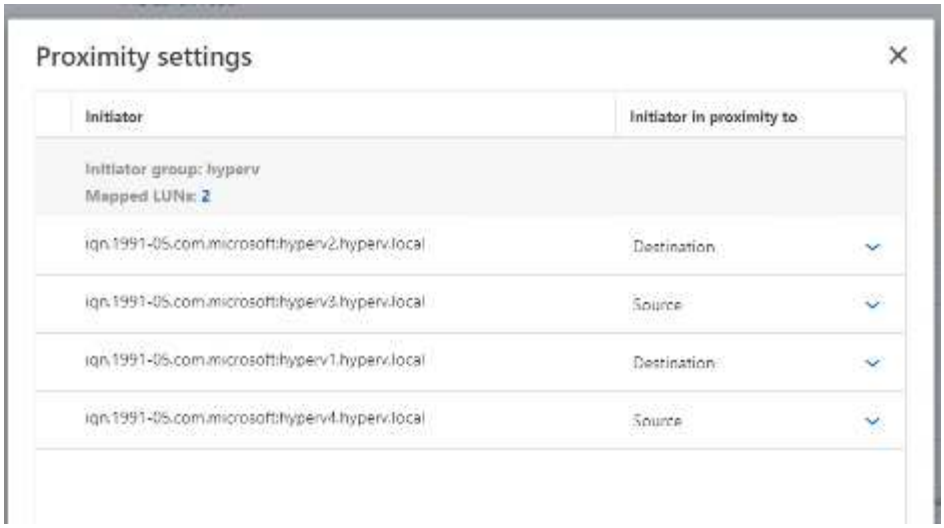


Konfigurieren Sie den symmetrischen Aktiv/Aktiv-Schutz

Konsistenzgruppen erleichtern die Verwaltung der Anwendungsarbeitslast, indem sie einfach zu konfigurierende lokale und Remote-Schutzrichtlinien sowie gleichzeitige absturz- oder anwendungskonsistente Snapshot-Kopien einer Sammlung von Volumes zu einem bestimmten Zeitpunkt bereitstellen. Weitere Einzelheiten finden Sie unter"Übersicht über Konsistenzgruppen" . Für dieses Setup verwenden wir eine einheitliche Konfiguration.

Schritte zur einheitlichen Konfiguration

1. Geben Sie beim Erstellen der Konsistenzgruppe Hostinitiatoren an, um igroups zu erstellen.
2. Aktivieren Sie das Kontrollkästchen „SnapMirror aktivieren“ und wählen Sie dann die Richtlinie „AutomatedFailoverDuplex“ aus.
3. Aktivieren Sie im angezeigten Dialogfeld das Kontrollkästchen „Initiatorgruppen replizieren“, um igroups zu replizieren. Legen Sie unter „Proximale Einstellungen bearbeiten“ proximale SVMs für Ihre Hosts fest.



4. Wählen Sie Speichern

   Die Schutzbeziehung wird zwischen Quelle und Ziel hergestellt.

Durchführen eines Cluster-Failover-Validierungstests

Wir empfehlen Ihnen, geplante Failover-Tests durchzuführen, um eine Clustervalidierungsprüfung durchzuführen. Die SQL-Datenbanken oder jegliche Clustersoftware auf beiden Sites – die primäre oder gespiegelte Site – sollten während der Tests weiterhin zugänglich sein.

Zu den Anforderungen des Hyper-V-Failoverclusters gehören:

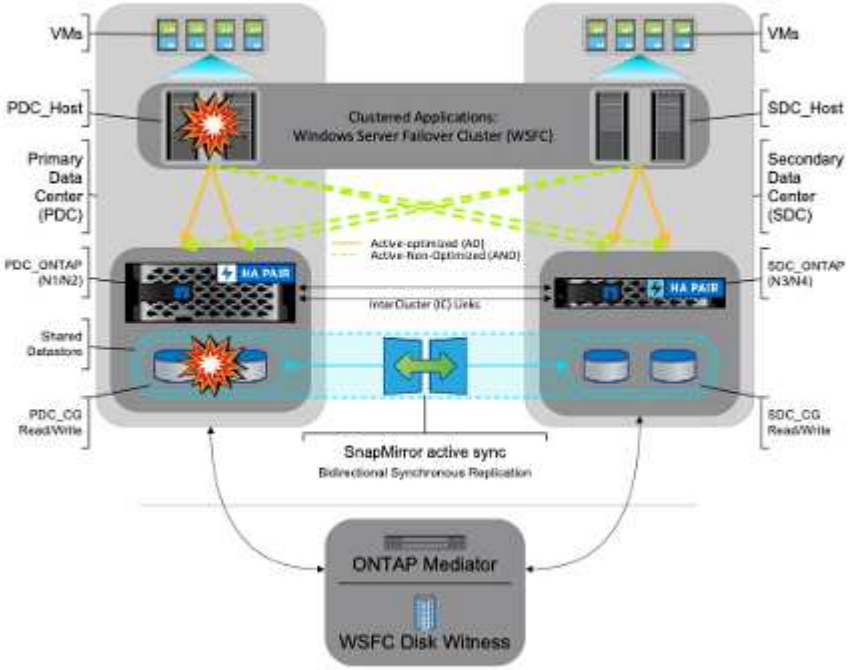
- Die aktive Synchronisierungsbeziehung von SnapMirror muss synchronisiert sein.
- Sie können kein geplantes Failover einleiten, wenn ein unterbrechungsfreier Vorgang ausgeführt wird. Zu den unterbrechungsfreien Vorgängen gehören Volumeverschiebungen, Aggregatverlagerungen und Speicherfailover.
- Der ONTAP Mediator muss konfiguriert, verbunden und im Quorum sein.
- Um den Prozess der VM-Migration zu optimieren, gehören an jedem Standort mindestens zwei Hyper-V-

Clusterknoten mit CPU-Prozessoren zur selben CPU-Familie. Bei den CPUs sollte es sich um CPUs mit Unterstützung für hardwaregestützte Virtualisierung und hardwarebasierte Data Execution Prevention (DEP) handeln.

- Um die Ausfallsicherheit zu gewährleisten, sollten Hyper-V-Clusterknoten dieselben Active Directory-Domänenmitglieder sein.
- Hyper-V-Clusterknoten und NetApp Speicherknoten sollten über redundante Netzwerke verbunden sein, um einen einzelnen Ausfallpunkt zu vermeiden.
- Gemeinsam genutzter Speicher, auf den alle Clusterknoten über das iSCSI-, Fibre Channel- oder SMB 3.0-Protokoll zugreifen können.

Testszenarien

Es gibt viele Möglichkeiten, ein Failover auf einem Host, Speicher oder Netzwerk auszulösen.



Hyper-V-Knoten oder Site ausgefallen

- Knotenausfall Ein Failover-Clusterknoten kann die Arbeitslast eines ausgefallenen Knotens übernehmen, ein Vorgang, der als Failover bezeichnet wird. Aktion: Schalten Sie einen Hyper-V-Knoten aus. Erwartetes Ergebnis: Der andere Knoten im Cluster übernimmt die Arbeitslast. VMs werden auf den anderen Knoten migriert.
- Ausfall einer Site. Wir können auch die gesamte Site ausfallen lassen und das Failover der primären Site auf die Spiegelsite auslösen: Aktion: Schalten Sie beide Hyper-V-Knoten an einer Site aus. Erwartetes Ergebnis: VMs am primären Standort werden zum Hyper-V-Cluster des Spiegelstandorts migriert, da SnapMirror Active Sync Symmetric Active/Active IO lokal mit bidirektionaler Replikation bedient, ohne Auswirkungen auf die Arbeitslast mit null RPO und null RTO.

Speicherfehler an einem Standort

- Stoppen Sie eine SVM auf der primären Site. Aktion: Stoppen Sie die iSCSI-SVM. Erwartete Ergebnisse: Der primäre Hyper-V-Cluster hat bereits eine Verbindung zur gespiegelten Site hergestellt und mit

SnapMirror Active Sync Symmetric Active/Active gibt es keine Auswirkungen auf die Arbeitslast mit null RPO und null RTO.

Erfolgskriterien

Beachten Sie bei den Tests Folgendes:

- Beobachten Sie das Verhalten des Clusters und stellen Sie sicher, dass die Dienste auf die verbleibenden Knoten übertragen werden.
- Überprüfen Sie, ob Fehler oder Dienstunterbrechungen vorliegen.
- Stellen Sie sicher, dass der Cluster Speicherfehler verarbeiten und den Betrieb fortsetzen kann.
- Stellen Sie sicher, dass auf die Datenbankdaten zugegriffen werden kann und die Dienste weiterhin funktionieren.
- Stellen Sie sicher, dass die Integrität der Datenbankdaten gewahrt bleibt.
- Überprüfen Sie, ob bestimmte Anwendungen ohne Auswirkungen auf den Benutzer auf einen anderen Knoten umgeschaltet werden können.
- Stellen Sie sicher, dass der Cluster die Last ausgleichen und die Leistung während und nach einem Failover aufrechterhalten kann.

Zusammenfassung

SnapMirror Active Sync kann dazu beitragen, dass Anwendungsdaten mehrerer Standorte, beispielsweise MSSQL und Oracle, aktiv zugänglich und auf beiden Standorten synchronisiert sind. Wenn ein Fehler auftritt, werden Anwendungen sofort auf die verbleibende aktive Site umgeleitet, ohne dass Daten oder Zugriff verloren gehen.

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 IRGENDEINER 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.