Replication

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/concepts/snapshot-copies-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Replication 1
Informationen zur ONTAP Snapshot-Technologie 1
Wie ONTAP SnapMirror die Notfallwiederherstellung und den Datentransfer unterstützt 2
Informationen zu ONTAP SnapMirror Cloud-Backups in Objektspeicher 4
Informationen zur ONTAP SnapVault Archivierung 5
Informationen zu ONTAP Cloud Backup und Unterstützung für traditionelle Backups 6
ONTAP MetroCluster kontinuierliche Verfügbarkeit 7

Replication

Informationen zur ONTAP Snapshot-Technologie

Traditionell dienten ONTAP Replikationstechnologien der Notfallwiederherstellung (DR) und der Datenarchivierung. Mit dem Aufkommen von Cloud-Services wurde die ONTAP Replikation an den Datentransfer zwischen Endpunkten im NetApp data fabric angepasst. Die Grundlage für all diese Verwendungen ist die ONTAP Snapshot-Technologie.

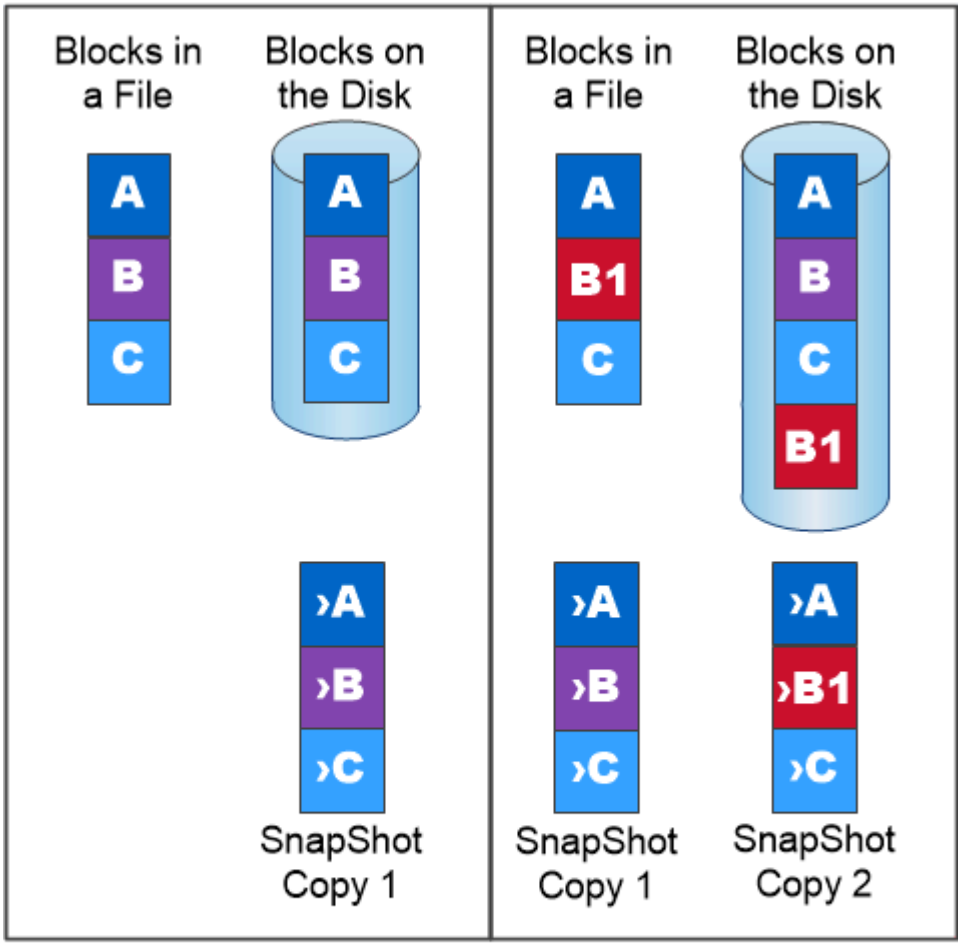
Ein Snapshot (früher Snapshot-Kopie) ist ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes. Nach der Erstellung eines Snapshots verweisen das aktive Dateisystem und der Snapshot auf dieselben Festplattenblöcke, daher benötigt der Snapshot keinen zusätzlichen Speicherplatz. Im Laufe der Zeit verbraucht das Image nur minimalen Speicherplatz und verursacht einen vernachlässigbaren Performance-Overhead, da nur Änderungen an Dateien seit dem letzten Snapshot aufgezeichnet werden.

Snapshots verdanken ihre Effizienz der Kerntechnologie von ONTAP zur Virtualisierung, dem Write Anywhere File Layout (WAFL). Wie eine Datenbank verwendet WAFL Metadaten, um auf die tatsächlichen Datenblöcke auf der Festplatte zu verweisen. Im Gegensatz zu einer Datenbank überschreibt WAFL jedoch keine vorhandenen Blöcke. WAFL schreibt aktualisierte Daten in einen neuen Block und passt die Metadaten an.

Snapshots sind effizient, da ONTAP beim Erstellen eines Snapshots anstelle des Kopierens von Datenblöcken auf Metadaten verweist. Dadurch entfallen sowohl die „Suchzeit“, die bei anderen Systemen beim Auffinden der zu kopierenden Blöcke anfällt, als auch die Kosten für das Erstellen der Kopie selbst.

Mithilfe eines Snapshots können einzelne Dateien oder LUNs wiederhergestellt oder der gesamte Inhalt eines Volumes zurückgespielt werden. ONTAP vergleicht Zeigerinformationen im Snapshot mit den Daten auf der Festplatte, um das fehlende oder beschädigte Objekt ohne Ausfallzeiten oder nennenswerte Leistungseinbußen zu rekonstruieren.

Eine *Snapshot-Richtlinie* definiert, wie das System Snapshots von Volumes erstellt. Die Richtlinie legt fest, wann die Snapshots erstellt werden, wie viele Kopien aufzubewahren sind, wie sie benannt und wie sie für die Replikation gekennzeichnet werden. Beispielsweise kann ein System täglich um 00:10 Uhr einen Snapshot erstellen, die zwei neuesten Kopien aufbewahren, sie “daily” nennen (ergänzt um einen Zeitstempel) und sie für die Replikation mit “daily” kennzeichnen.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Wie ONTAP SnapMirror die Notfallwiederherstellung und den Datentransfer unterstützt

SnapMirror ist eine Technologie zur Notfallwiederherstellung, die für die Ausfallsicherung von primärem Speicher auf sekundären Speicher an einem geografisch entfernten Standort entwickelt wurde. Wie der Name schon sagt, erstellt SnapMirror eine Replik, also einen Spiegel, Ihrer Arbeitsdaten im sekundären Speicher, von dem aus im Katastrophenfall am primären Standort weiterhin Daten bereitgestellt werden können.

Die Daten werden auf Volume-Ebene gespiegelt. Die Beziehung zwischen dem Quell-Volume im Primärspeicher und dem Ziel-Volume im Sekundärspeicher wird als *Datenschutzbeziehung* bezeichnet. Die Cluster, in denen sich die Volumes befinden, und die SVMs, die Daten von den Volumes bereitstellen, müssen *gepeert* sein. Eine Peer-Beziehung ermöglicht Clustern und SVMs den sicheren Austausch von Daten.

Sie können auch eine Datenschutzbeziehung zwischen SVMs erstellen. Bei dieser Art von Beziehung werden die gesamte oder ein Teil der SVM-Konfiguration, von NFS-Exporten und SMB-Freigaben bis hin zu RBAC, sowie die Daten in den Volumes, die der SVM gehören, repliziert.

Ab ONTAP 9.10.1 ist es möglich, Datensicherungsbeziehungen zwischen S3-Buckets mithilfe von SnapMirror S3 zu erstellen. Ziel-Buckets können sich auf lokalen oder entfernten ONTAP Systemen oder auf Nicht-ONTAP Systemen wie StorageGRID und AWS befinden.

Beim ersten Aufruf von SnapMirror erfolgt ein *Basistransfer* vom Quell-Volume zum Ziel-Volume. Der Basistransfer umfasst typischerweise die folgenden Schritte:

- Eine Momentaufnahme des Quellvolumes erstellen.
- Der Snapshot und alle von ihm referenzierten Datenblöcke werden auf das Zielvolume übertragen.
- Die verbleibenden, weniger aktuellen Snapshots auf dem Quellvolume werden auf das Zielvolume übertragen, damit sie im Falle einer Beschädigung des “aktiven” Spiegels verwendet werden können.

Sobald ein Basistransfer abgeschlossen ist, überträgt SnapMirror nur neue Snapshots auf das Spiegelsystem. Aktualisierungen erfolgen asynchron gemäß dem von Ihnen konfigurierten Zeitplan. Die Aufbewahrung entspricht der Snapshot-Richtlinie auf der Quelle. Im Falle einer Störung am primären Standort lässt sich das Zielvolume mit minimaler Unterbrechung aktivieren, und das Quellvolume kann nach Wiederherstellung des Dienstes wieder aktiviert werden.

Da SnapMirror nach der Erstellung des Basistransfers nur Snapshots überträgt, erfolgt die Replikation schnell und unterbrechungsfrei. Wie der Failover-Anwendungsfall impliziert, sollten die Controller des sekundären Systems den Controllern des primären Systems gleichwertig oder nahezu gleichwertig sein, um Daten effizient vom gespiegelten Speicher bereitzustellen.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

Verwendung von SnapMirror für den Datentransfer

Sie können auch SnapMirror verwenden, um Daten zwischen Endpunkten im NetApp Data Fabric zu replizieren. Es besteht die Wahl zwischen einmaliger Replikation und wiederkehrender Replikation, wenn die SnapMirror Policy erstellt wird.

Informationen zu ONTAP SnapMirror Cloud-Backups in Objektspeicher

SnapMirror Cloud ist eine Backup und Recovery-Technologie für ONTAP Nutzer, die ihre Datensicherungsprozesse in die Cloud oder auf eine lokale Objektspeicherlösung verlagern möchten. Organisationen, die von herkömmlichen Backup-to-Tape-Architekturen abrücken, können Objektspeicher als alternatives Repository für die langfristige Datenaufbewahrung und Archivierung verwenden. SnapMirror Cloud bietet ONTAP zu Objektspeicher Replikation als Teil einer inkrementellen, kontinuierlichen Backup-Strategie.

SnapMirror Cloud Replikation ist eine lizenzpflichtige ONTAP Funktion. SnapMirror Cloud wurde in ONTAP 9.8 als Erweiterung der Familie von SnapMirror Replikationstechnologien eingeführt. Während SnapMirror häufig für ONTAP-zu-ONTAP Backups verwendet wird, nutzt SnapMirror Cloud dieselbe Replikations-Engine, um Snapshots für ONTAP Backups in S3-kompatible Objektspeicher zu übertragen.

Für Backup-Anwendungsfälle konzipiert, unterstützt SnapMirror Cloud sowohl Langzeitaufbewahrung als auch Archivierungs-Workflows. Wie bei SnapMirror führt das initiale SnapMirror Cloud Backup einen Basistransfer eines Volumes durch. Bei nachfolgenden Backups erstellt SnapMirror Cloud einen Snapshot des Quell-Volumes und überträgt den Snapshot mit nur den geänderten Datenblöcken an ein Objektspeicherziel.

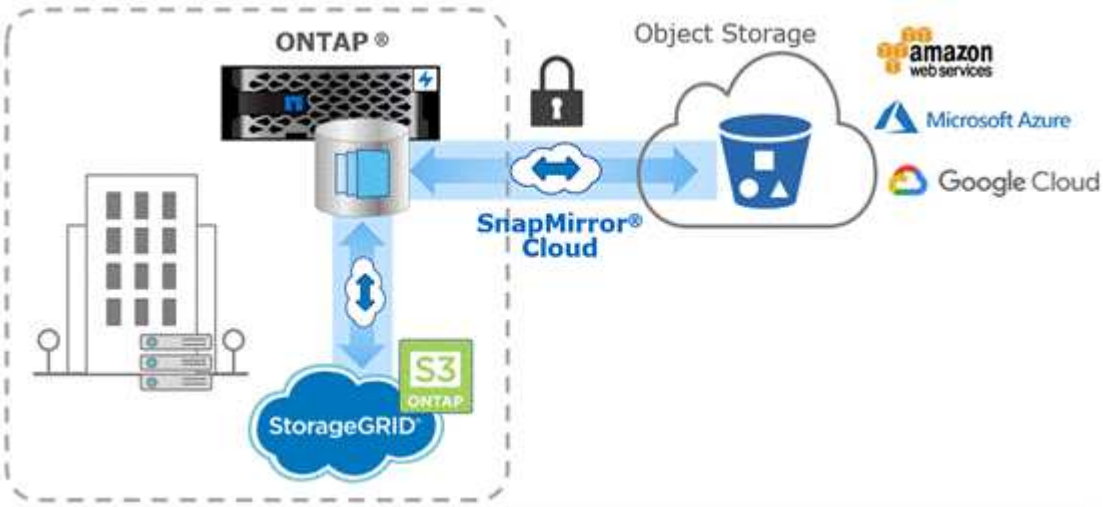
SnapMirror Cloud-Beziehungen können zwischen ONTAP-Systemen und ausgewählten lokalen und öffentlichen Cloud-Objektspeicherzielen konfiguriert werden, einschließlich Amazon S3, Google Cloud Storage und Microsoft Azure Blob Storage. Weitere lokale Objektspeicherziele sind StorageGRID und ONTAP S3.

Zusätzlich zur Verwendung von ONTAP System Manager zur Verwaltung von SnapMirror Cloud-Konfigurationen stehen verschiedene Orchestrierungsoptionen für die Verwaltung von SnapMirror Cloud-Backups zur Verfügung:

- Mehrere Drittanbieter-Partner für Backup bieten Unterstützung für SnapMirror Cloud-Replikation. Teilnehmende Anbieter sind auf der "NetApp Blog" verfügbar.
- NetApp Backup und Wiederherstellung für eine NetApp native Lösung für ONTAP Umgebungen
- APIs zur Entwicklung kundenspezifischer Software für Data-Protection-Workflows oder zur Nutzung von Automatisierungstools

> SnapMirror Cloud-Replikation, die von System Manager verwaltet wird, unterstützt ausschließlich StorageGrid und ONTAP S3 als Objektspeicherziel. Andere Anbieter werden nicht unterstützt.

> Die Nutzung der SnapMirror Cloud-APIs ist grundsätzlich auf Backup-Partner beschränkt. Kunden, die eigene API-basierte Lösungen entwickeln möchten, erhalten Informationen zu den Lizenzbedingungen über ihr NetApp Account-Team.



Informationen zur ONTAP SnapVault Archivierung

Die SnapMirror Lizenz wird sowohl zur Unterstützung von SnapVault Beziehungen für Backup als auch von SnapMirror Beziehungen für Disaster Recovery verwendet. Ab ONTAP 9.3 sind SnapVault Lizenzen veraltet, und SnapMirror Lizenzen können zur Konfiguration von Vault-, Mirror- und Mirror-and-Vault-Beziehungen verwendet werden. SnapMirror Replikation wird für ONTAP-to-ONTAP Replikation von Snapshots verwendet und unterstützt sowohl Backup- als auch Disaster-Recovery-Anwendungsfälle.

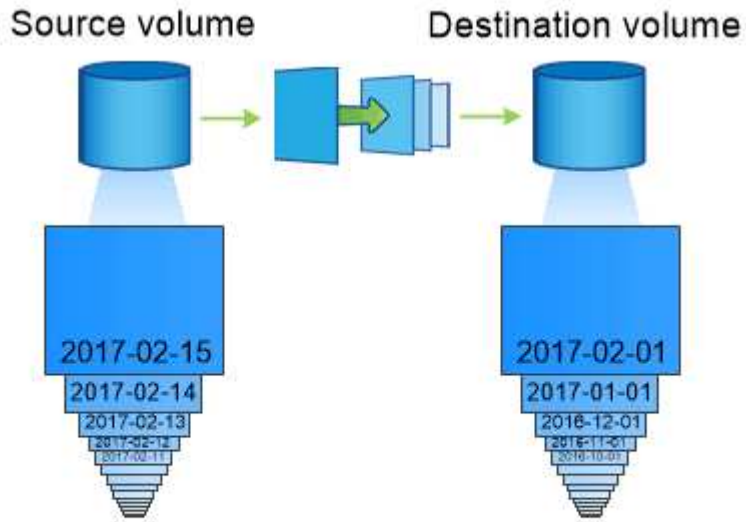
SnapVault ist eine Archivierungstechnologie, die für die Festplatten-zu-Festplatten-Snapshot-Replikation zur Einhaltung von Standards und für andere Governance-bezogene Zwecke entwickelt wurde. Im Gegensatz zu einer SnapMirror Beziehung, bei der das Ziel in der Regel nur die aktuell im Quell-Volume vorhandenen Snapshots enthält, bewahrt ein SnapVault Ziel typischerweise zeitpunktgenaue Snapshots auf, die über einen deutlich längeren Zeitraum erstellt wurden.

Beispielsweise könnten Sie monatliche Snapshots Ihrer Daten über einen Zeitraum von 20 Jahren aufbewahren, um die gesetzlichen Buchführungsvorschriften für Ihr Unternehmen einzuhalten. Da keine Anforderung besteht, Daten aus dem Vault-Speicher bereitzustellen, können auf dem Zielsystem langsamere, kostengünstigere Festplatten verwendet werden.

Wie bei SnapMirror, SnapVault führt beim ersten Aufruf einen Basistransfer durch. Es wird ein Snapshot des Quell-Volumes erstellt, anschließend werden die Kopie und die von ihr referenzierten Datenblöcke auf das Ziel-Volume übertragen. Im Gegensatz zu SnapMirror, SnapVault sind ältere Snapshots nicht im Basistransfer enthalten.

Aktualisierungen erfolgen asynchron gemäß dem von Ihnen konfigurierten Zeitplan. Die in der Richtlinie für die SnapMirror Beziehung definierten Regeln legen fest, welche neuen Snapshots in Aktualisierungen einbezogen werden und wie viele Kopien beibehalten werden. Die in der Richtlinie definierten Labels („monthly“ zum Beispiel) müssen mit einem oder mehreren Labels übereinstimmen, die in der Snapshot-Richtlinie auf der Quelle definiert sind. Andernfalls schlägt die Replikation fehl.

SnapMirror und SnapVault teilen sich dieselbe Befehlsinfrastruktur. Die gewünschte Methode wird bei der Erstellung einer Richtlinie festgelegt. Beide Methoden erfordern peered Cluster und peered SVMs.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Informationen zu ONTAP Cloud Backup und Unterstützung für traditionelle Backups

Zusätzlich zu SnapMirror und SnapVault Datensicherungsbeziehungen, die bei ONTAP 9.7 und früheren Versionen nur von Festplatte zu Festplatte möglich waren, gibt es mittlerweile mehrere Backup-Lösungen, die eine kostengünstigere Alternative für die langfristige Datenaufbewahrung bieten.

Zahlreiche Drittanbieter-Datensicherungsanwendungen bieten herkömmliche Backups für ONTAP-verwaltete Daten. Veeam, Veritas und Commvault sowie weitere Anbieter bieten integrierte Backups für ONTAP Systeme.

Ab ONTAP 9.8 bietet SnapMirror cloud asynchrone Replizierung von Snapshots von ONTAP Instanzen zu Objektspeicherendpunkten. Für die SnapMirror cloud Replizierung ist eine lizenzierte Anwendung zur Orchestrierung und Verwaltung von Workflows zum Datenschutz erforderlich. SnapMirror cloud Beziehungen werden von ONTAP Systemen zu ausgewählten lokalen und öffentlichen Cloud-Objektspeicherzielen unterstützt, einschließlich AWS S3, Google Cloud Storage Platform oder Microsoft Azure Blob Storage, was eine höhere Effizienz mit Backup-Software von Anbietern ermöglicht. Eine Liste der unterstützten zertifizierten Anwendungen und Objektspeicheranbieter ist bei Ihrem NetApp Ansprechpartner erhältlich.

Bei Interesse an Cloud-nativem Datenschutz kann die NetApp Console zur Konfiguration von SnapMirror- oder SnapVault-Beziehungen zwischen lokalen Volumes und Cloud Volumes ONTAP Instanzen in der öffentlichen Cloud verwendet werden.

Die Konsole bietet außerdem Backups von Cloud Volumes ONTAP Instanzen mithilfe eines Software as a Service (SaaS) Modells. Benutzer können ihre Cloud Volumes ONTAP Instanzen mithilfe von NetApp Backup and Recovery in S3 und S3-kompatible öffentliche Cloud-Objektspeicher sichern.

"Cloud Volumes ONTAP Dokumentation"

"NetApp Console-Dokumentation"

"NetApp Console"

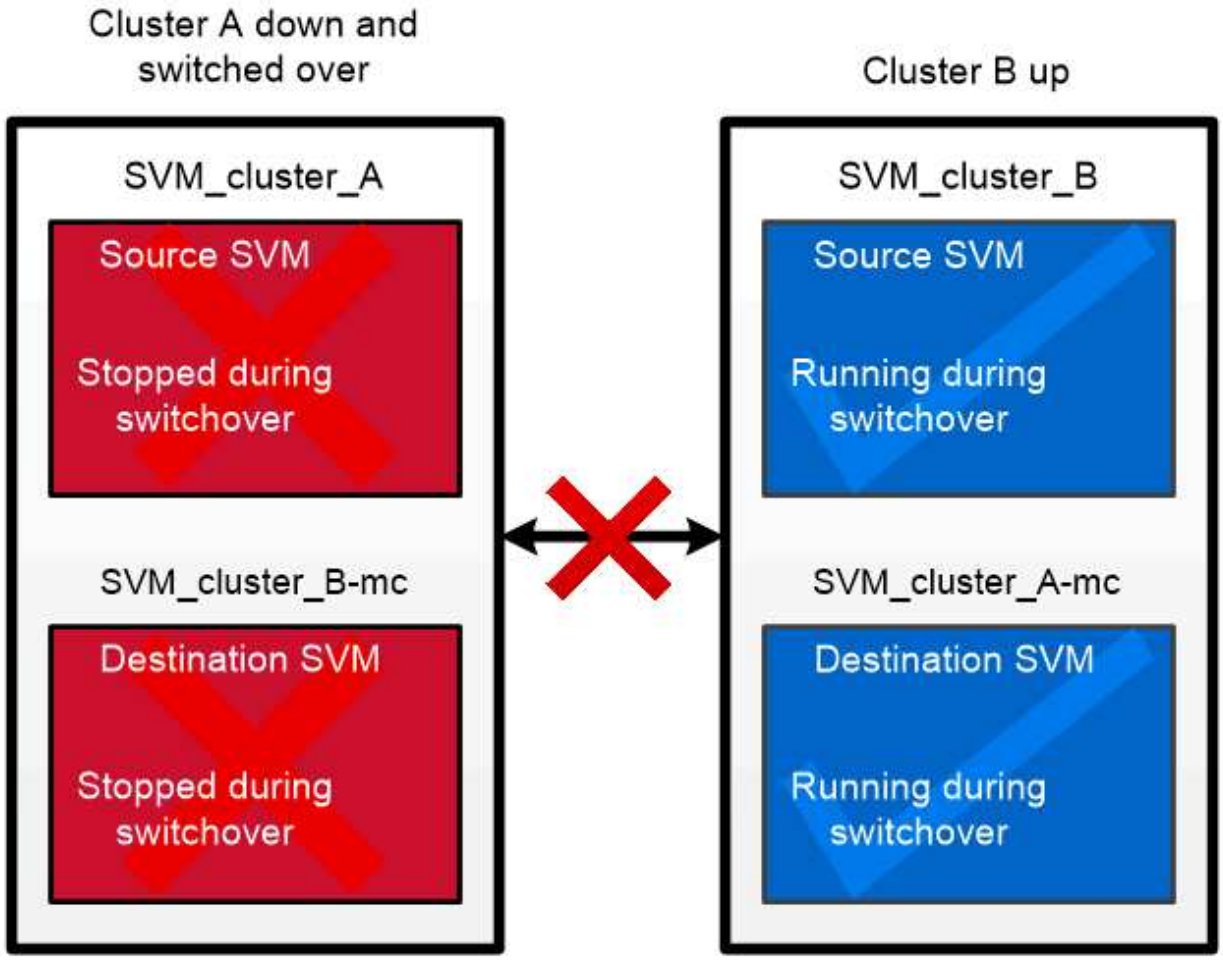
ONTAP MetroCluster kontinuierliche Verfügbarkeit

MetroCluster Konfigurationen schützen Daten durch die Implementierung zweier physisch getrennter, gespiegelter Cluster. Jeder Cluster repliziert synchron die Daten und die SVM-Konfiguration des anderen. Im Katastrophenfall an einem Standort kann ein Administrator die gespiegelte SVM aktivieren und Daten vom verbleibenden Standort bereitstellen.

- *Fabric-attached MetroCluster* und *MetroCluster IP* Konfigurationen unterstützen stadtweite Cluster.
- *Stretch MetroCluster* Konfigurationen unterstützen campusweite Cluster.

Die Cluster müssen in jedem Fall miteinander verbunden sein.

MetroCluster verwendet eine ONTAP-Funktion namens *SyncMirror*, um Aggregatdaten für jeden Cluster synchron in Kopien, oder *Plexen*, im Speicher des anderen Clusters zu spiegeln. Wenn ein Switchover erfolgt, wird der Remote-Plex auf dem verbleibenden Cluster online geschaltet und die sekundäre SVM beginnt mit der Datenbereitstellung.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

Verwendung von SyncMirror in Nicht-MetroCluster-Implementierungen SyncMirror kann optional in einer Nicht-MetroCluster-Implementierung eingesetzt werden, um vor Datenverlust zu schützen, falls mehr Festplatten ausfallen, als der RAID-Typ abdeckt, oder wenn die Verbindung zu den Festplatten der RAID-Gruppe verloren geht. Die Funktion ist nur für HA-Paare verfügbar.

Die aggregierten Daten werden in Plexen gespiegelt, die auf verschiedenen Festplattengehäusen gespeichert sind. Wenn eines der Gehäuse nicht verfügbar ist, stellt der nicht betroffene Plex weiterhin Daten bereit, während die Ursache des Ausfalls behoben wird.

Es ist zu beachten, dass ein mit SyncMirror gespiegeltes Aggregat doppelt so viel Speicherplatz benötigt wie ein nicht gespiegeltes Aggregat. Jeder Plex benötigt genauso viele Festplatten wie der Plex, den er spiegelt. Zum Spiegeln eines 1.440 GB Aggregats wären beispielsweise 2.880 GB Speicherplatz erforderlich, also 1.440 GB für jeden Plex.

Mit SyncMirror wird empfohlen, mindestens 20 % freien Speicherplatz für gespiegelte Aggregate vorzuhalten, um eine optimale Speicherleistung und Verfügbarkeit zu gewährleisten. Obwohl für nicht gespiegelte Aggregate 10 % empfohlen werden, kann das Dateisystem die zusätzlichen 10 % des Speicherplatzes nutzen, um inkrementelle Änderungen aufzufangen. Inkrementelle Änderungen erhöhen die Speicherauslastung gespiegelter Aggregate aufgrund der Copy-on-Write-Snapshot-basierten Architektur von ONTAP. Die Nichteinhaltung dieser Best Practices kann die Resynchronisierungsleistung von SyncMirror negativ beeinflussen, was sich indirekt auf operative Workflows wie NDU für nicht gemeinsam genutzte Cloud-Bereitstellungen und Switchback für MetroCluster Bereitstellungen auswirkt.

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 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.