



# Replizierung

## ONTAP 9

NetApp  
January 08, 2026

# Inhalt

- Replizierung ..... 1
  - Snapshots ..... 1
  - SnapMirror Disaster Recovery und Datentransfer ..... 2
  - SnapMirror Cloud Backups auf Objekt-Storage ..... 4
  - SnapVault-Archivierung ..... 5
  - Cloud-Backup und Unterstützung für herkömmliche Backups ..... 6
  - Kontinuierliche Verfügbarkeit mit MetroCluster ..... 7

# Replizierung

## Snapshots

Herkömmliche ONTAP Replizierungstechnologien dienten der Notwendigkeit für Disaster Recovery (DR) und Datenarchivierung. Mit der Einführung von Cloud-Services wurde die ONTAP Replizierung auf den Datentransfer zwischen Endpunkten in der NetApp Data-Fabric-Infrastruktur angepasst. Die Grundlage für diesen Einsatz bildet die ONTAP Snapshot Technologie.

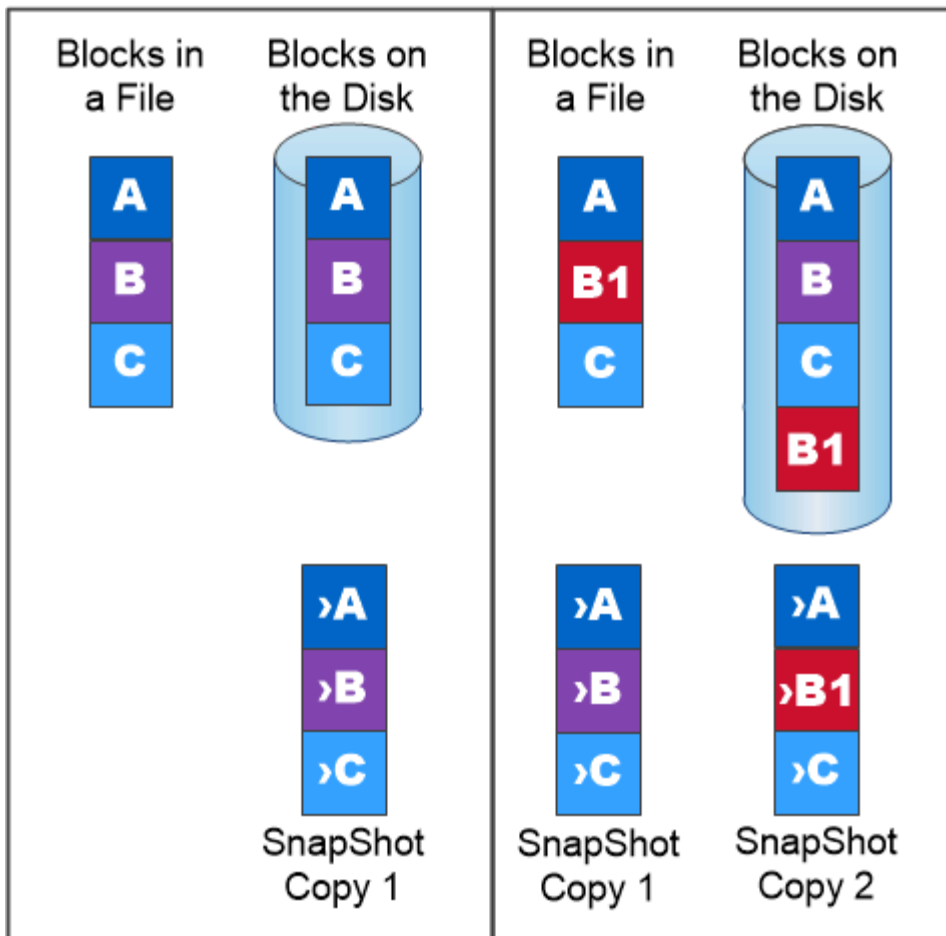
Ein *Snapshot* (früher *Snapshot Copy*) ist ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes. Nach der Erstellung eines Snapshots verweisen das aktive Dateisystem und der Snapshot auf dieselben Festplattenblöcke. Daher wird für den Snapshot kein zusätzlicher Speicherplatz benötigt. Mit der Zeit benötigt das Image nur minimalen Speicherplatz und verursacht vernachlässigbaren Performance-Overhead, da seit Erstellung des letzten Snapshots nur Dateiänderungen aufgezeichnet werden.

Ihre Effizienz verdanken Snapshots der zentralen Storage-Virtualisierungstechnologie von ONTAP – dem WAFL (Write Anywhere File Layout).\_ wie eine Datenbank verwendet WAFL Metadaten, um auf die tatsächlichen Datenblöcke auf der Festplatte zu verweisen. Im Gegensatz zu einer Datenbank überschreiben WAFL jedoch keine vorhandenen Blöcke. Aktualisierte Daten werden in einen neuen Block geschrieben und die Metadaten geändert.

Snapshots sind effizient, da ONTAP bei der Erstellung eines Snapshots eher auf Datenblöcke verweist. Dadurch entfällt sowohl die Suchzeit, die bei anderen Systemen bei der Suche nach den zu kopierenden Blöcken anfallen, als auch die Kosten für die Erstellung der Kopie selbst.

Mithilfe eines Snapshots können Sie einzelne Dateien oder LUNs wiederherstellen oder den gesamten Inhalt eines Volumes wiederherstellen. ONTAP vergleicht die Zeigerinformationen im Snapshot mit den Daten auf der Festplatte, um das fehlende oder beschädigte Objekt ohne Ausfallzeit oder erhebliche Performance-Kosten zu rekonstruieren.

Eine *Snapshot-Richtlinie* definiert, wie das System Snapshots von Volumes erstellt. Die Richtlinie gibt an, wann die Snapshots erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen, wie sie benannt werden und wie sie für die Replikation beschriftet werden sollen. Ein System kann beispielsweise jeden Tag um 12:10 Uhr einen Snapshot erstellen, die beiden neuesten Kopien beibehalten, sie mit "daily" (angehängt mit einem Zeitstempel) benennen und sie für die Replikation mit "daily" beschriften.



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

## SnapMirror Disaster Recovery und Datentransfer

*SnapMirror* ist eine Disaster Recovery-Technologie für den Failover von primärem Storage zu sekundärem Storage an einem geografisch verteilten Standort. Wie der Name schon andeutet, erstellt SnapMirror ein Replikat, oder *Mirror* Ihrer Arbeitsdaten im Sekundärspeicher, von dem Sie im K-Fall am primären Standort weiter Daten bereitstellen können.

Daten werden auf Volume-Ebene gespiegelt. Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als „*Data Protection Relationship*“ bezeichnet. Die Cluster, in denen sich die Volumes befinden, und die SVMs, die Daten aus den Volumes bereitstellen, müssen *peering durchgeführt werden*. Eine Peer-Beziehung ermöglicht den Austausch von Clustern und SVMs Sicher aus Daten.



Sie können auch eine Datensicherungsbeziehung zwischen SVMs erstellen. In dieser Art der Beziehung wird die gesamte Konfiguration der SVM, von NFS-Exporten und SMB-Freigaben bis hin zur rollenbasierten Zugriffssteuerung, sowie die Daten in den Volumes repliziert, die die SVM besitzt.

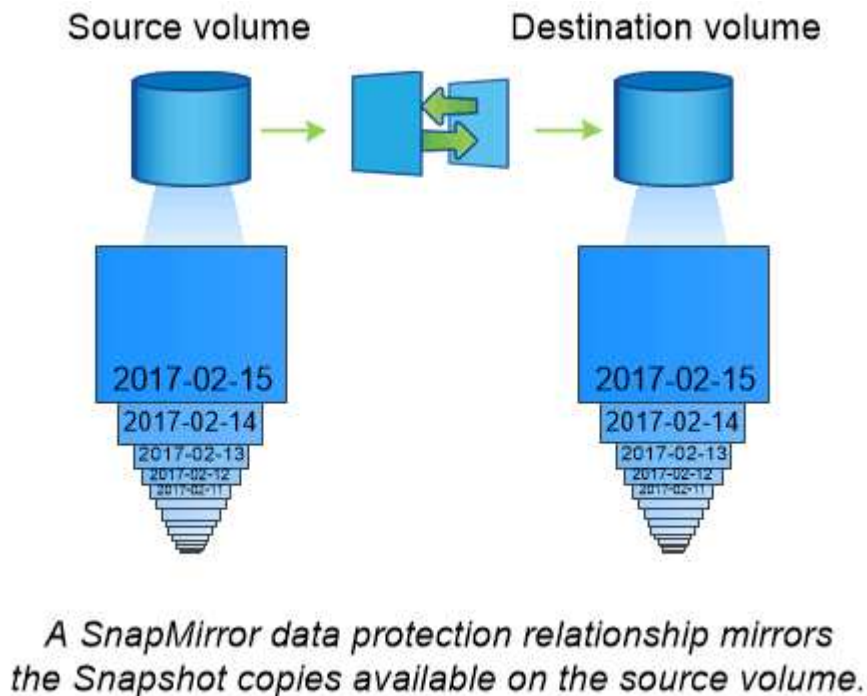
Ab ONTAP 9.10.1 können Datensicherungsbeziehungen zwischen S3-Buckets mithilfe von SnapMirror S3 erstellt werden. Ziel-Buckets können sich auf lokalen oder Remote-ONTAP Systemen oder auf Systemen anderer Anbieter wie StorageGRID und AWS befinden.

Beim ersten Aufruf von SnapMirror führt es einen *Baseline-Transfer* vom Quell-Volume zum Ziel-Volume durch. Der Basistransfer umfasst die folgenden Schritte:

- Erstellen Sie einen Snapshot des Quell-Volumes.
- Übertragen Sie den Snapshot und alle Datenblöcke, die er auf das Ziel-Volume verweist.
- Übertragen Sie die verbleibenden, weniger aktuellen Snapshots auf dem Quellvolume auf das Zielvolume für den Fall, dass der „Active“-Spiegel beschädigt ist.

Nach Abschluss eines Basistransfers überträgt SnapMirror nur neue Snapshots auf den Spiegel. Updates werden asynchron und folgen dem von Ihnen konfigurierten Zeitplan. Die Aufbewahrung spiegelt die Snapshot-Richtlinie auf der Quelle. Sie können das Ziel-Volume bei minimalen Unterbrechungen im Falle eines Ausfalls am primären Standort aktivieren und das Quell-Volume wieder aktivieren, wenn der Service wiederhergestellt ist.

Da SnapMirror nur Snapshots überträgt, nachdem die Basis erstellt wurde, erfolgt die Replizierung schnell und unterbrechungsfrei. Wie der Anwendungsfall für Failover impliziert, sollten die Controller auf dem sekundären System äquivalent oder fast vergleichbar mit den Controllern auf dem Primärsystem sein, um Daten effizient aus dem gespiegelten Storage bereitzustellen.



#### **Verwenden von SnapMirror für Datentransfer**

Daten können auch mit SnapMirror zwischen Endpunkten in der NetApp Data-Fabric-Infrastruktur repliziert werden. Bei der Erstellung der SnapMirror-Richtlinie kann zwischen einer einmaligen Replizierung oder wiederkehrenden Replizierung gewählt werden.

# SnapMirror Cloud Backups auf Objekt-Storage

*SnapMirror Cloud* ist eine Backup- und Recovery-Technologie für ONTAP-Benutzer, die ihre Datensicherungs-Workflows in die Cloud migrieren möchten. Unternehmen, die sich von älteren auf Tape-Backup-Architekturen verabschieden, können Objekt-Storage als alternatives Repository für die langfristige Datenaufbewahrung und Archivierung verwenden. Die SnapMirror Cloud bietet ONTAP-to-Object-Storage-Replizierung als Teil einer fortlaufend inkrementellen Backup-Strategie.

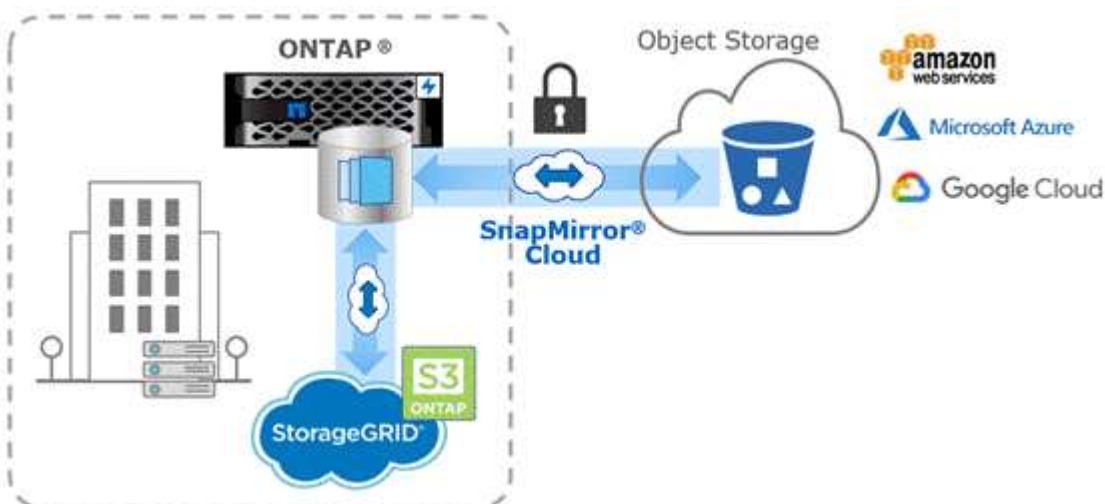
Bei SnapMirror Cloud Replication handelt es sich um eine lizenzierte ONTAP Funktion. SnapMirror Cloud wurde in ONTAP 9.8 als Erweiterung der Familie der SnapMirror Replizierungstechnologien eingeführt. SnapMirror wird häufig für ONTAP-to-ONTAP-Backups verwendet, aber SnapMirror Cloud verwendet dieselbe Replizierungs-Engine für die Übertragung von Snapshots für ONTAP auf S3-konforme Objekt-Storage-Backups.

SnapMirror Cloud ist für Backup-Anwendungsfälle ausgelegt und unterstützt sowohl die langfristige Aufbewahrung als auch Archivierungs-Workflows. Wie bei SnapMirror wird beim ersten SnapMirror Cloud Backup der Basistransfer eines Volumes durchgeführt. Für nachfolgende Backups generiert die SnapMirror Cloud einen Snapshot des Quell-Volumes und überträgt den Snapshot nur mit den geänderten Datenblöcken auf ein Objekt-Storage-Ziel.

SnapMirror Cloud-Beziehungen können zwischen ONTAP Systemen konfiguriert und Objekt-Storage-Ziele für On-Premises- und Public-Cloud-Umgebungen ausgewählt werden, einschließlich Amazon S3, Google Cloud Storage und Microsoft Azure Blob Storage. Weitere lokale Objekt-Storage-Ziele sind StorageGRID und ONTAP S3.

Neben ONTAP System Manager für das Management von SnapMirror Cloud-Konfigurationen stehen für das Management von SnapMirror Cloud-Backups verschiedene Orchestrierungsoptionen zur Verfügung:

- Mehrere Backup-Partner von Drittanbietern, die Support für die SnapMirror Cloud-Replizierung anbieten  
Teilnehmende Anbieter finden Sie auf der ["NetApp Blog"](#).
- NetApp Backup und Recovery für eine NetApp-native Lösung für ONTAP Umgebungen
- APIs zum entwickeln individueller Software für Datensicherungs-Workflows oder zur Nutzung von Automatisierungs-Tools



# SnapVault-Archivierung

Die SnapMirror Lizenz wird verwendet, um sowohl SnapVault Beziehungen für Backups als auch SnapMirror Beziehungen für Disaster Recovery zu unterstützen. Ab ONTAP 9.3 sind die SnapVault Lizenzen veraltet und mit SnapMirror Lizenzen können Vault-, Mirror- und Mirror-and-Vault-Beziehungen konfiguriert werden. SnapMirror Replizierung wird für die ONTAP-zu-ONTAP-Replizierung von Snapshots verwendet, um Backup- und Disaster-Recovery-Anwendungsfälle zu unterstützen.

*SnapVault* ist eine Archivierungstechnologie, die für die Disk-to-Disk Snapshot-Replikation zur Einhaltung von Standards und anderen Governance-bezogenen Zwecken entwickelt wurde. Im Gegensatz zu einer SnapMirror Beziehung, bei der das Ziel normalerweise nur die im Quell-Volume vorhandenen Snapshots enthält, behält ein SnapVault Ziel in der Regel zeitpunktgenaue Snapshots, die über einen viel längeren Zeitraum erstellt wurden.

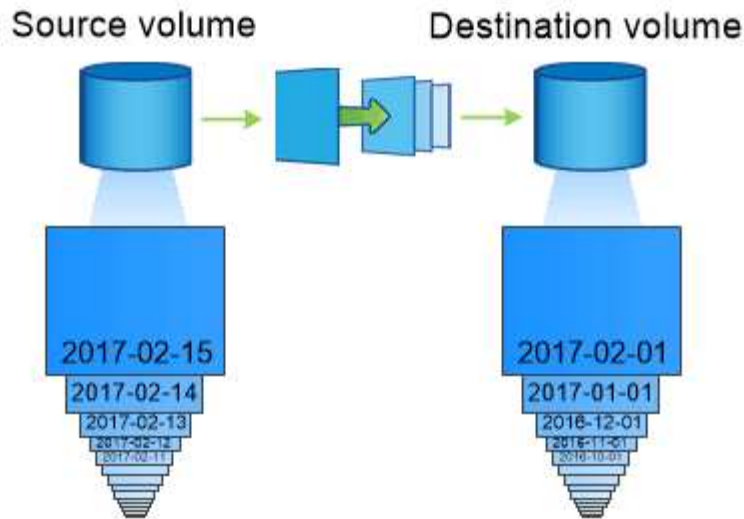
Möglicherweise möchten Sie monatliche Snapshots Ihrer Daten über einen Zeitraum von 20 Jahren speichern, um beispielsweise gesetzliche Buchhaltungsvorschriften in Ihrem Unternehmen zu erfüllen. Da keine Daten aus dem Vault-Speicher bereitgestellt werden müssen, können Sie langsamere und kostengünstigere Festplatten auf dem Zielsystem verwenden.

Wie SnapMirror führt SnapVault auch bei seinem ersten Aufruf einen Basistransfer durch. Es erstellt einen Snapshot des Quell-Volume, überträgt dann die Kopie und die Datenblöcke, die es auf das Ziel-Volume verweist. Im Gegensatz zu SnapMirror enthält SnapVault keine älteren Snapshots in der Basislinie.

Updates werden asynchron und folgen dem von Ihnen konfigurierten Zeitplan. Die Regeln, die Sie in der Richtlinie für die Beziehung definieren, identifizieren, welche neuen Snapshots in Updates aufgenommen werden sollen und wie viele Kopien aufbewahrt werden sollen. Die in der Richtlinie definierten Bezeichnungen („monatlich,“ zum Beispiel) müssen mit einer oder mehreren in der Snapshot-Richtlinie auf der Quelle definierten Bezeichnungen übereinstimmen. Andernfalls schlägt die Replizierung fehl.



SnapMirror und SnapVault nutzen dieselbe Befehlsinfrastruktur. Sie geben an, welche Methode Sie beim Erstellen einer Richtlinie verwenden möchten. Beide Methoden erfordern Peering Cluster und Peering 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.*

## Cloud-Backup und Unterstützung für herkömmliche Backups

Neben SnapMirror und SnapVault Datensicherungsbeziehungen, die Disk-to-Disk nur für ONTAP 9.7 und frühere Versionen waren, gibt es nun mehrere Backup-Lösungen, die eine kostengünstigere Alternative für die langfristige Datenaufbewahrung bieten.

Zahlreiche Datensicherungsapplikationen von Drittanbietern bieten herkömmliche Backups von von von von ONTAP gemanagten Daten. Veeam, Veritas und CommVault bieten u. a. integriertes Backup für ONTAP Systeme.

Ab ONTAP 9.8 ermöglicht die SnapMirror Cloud die asynchrone Replizierung von Snapshots von ONTAP Instanzen auf Objekt-Storage-Endpunkte. Für SnapMirror Cloud Replication ist eine lizenzierte Applikation zur Orchestrierung und zum Management von Datensicherungs-Workflows erforderlich. SnapMirror Cloud-Beziehungen werden von ONTAP Systemen für die Auswahl von Objekt-Storage-Zielen in On-Premises- und Public-Cloud-Umgebungen unterstützt – einschließlich AWS S3, Google Cloud Storage-Plattform oder Microsoft Azure Blob Storage – wodurch sich die Effizienz mit Backup-Software der Anbieter erhöht. Kontaktieren Sie Ihren NetApp Ansprechpartner, um eine Liste der unterstützten zertifizierten Applikationen und Objekt-Storage-Anbieter zu erhalten.

Wenn Sie an Cloud-nativem Datenschutz interessiert sind, können Sie mit der NetApp Konsole SnapMirror oder SnapVault Beziehungen zwischen lokalen Volumes und Cloud Volumes ONTAP Instanzen in der öffentlichen Cloud konfigurieren.

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

["Cloud Volumes ONTAP-Dokumentation"](#)

["Dokumentation zur NetApp -Konsole"](#)



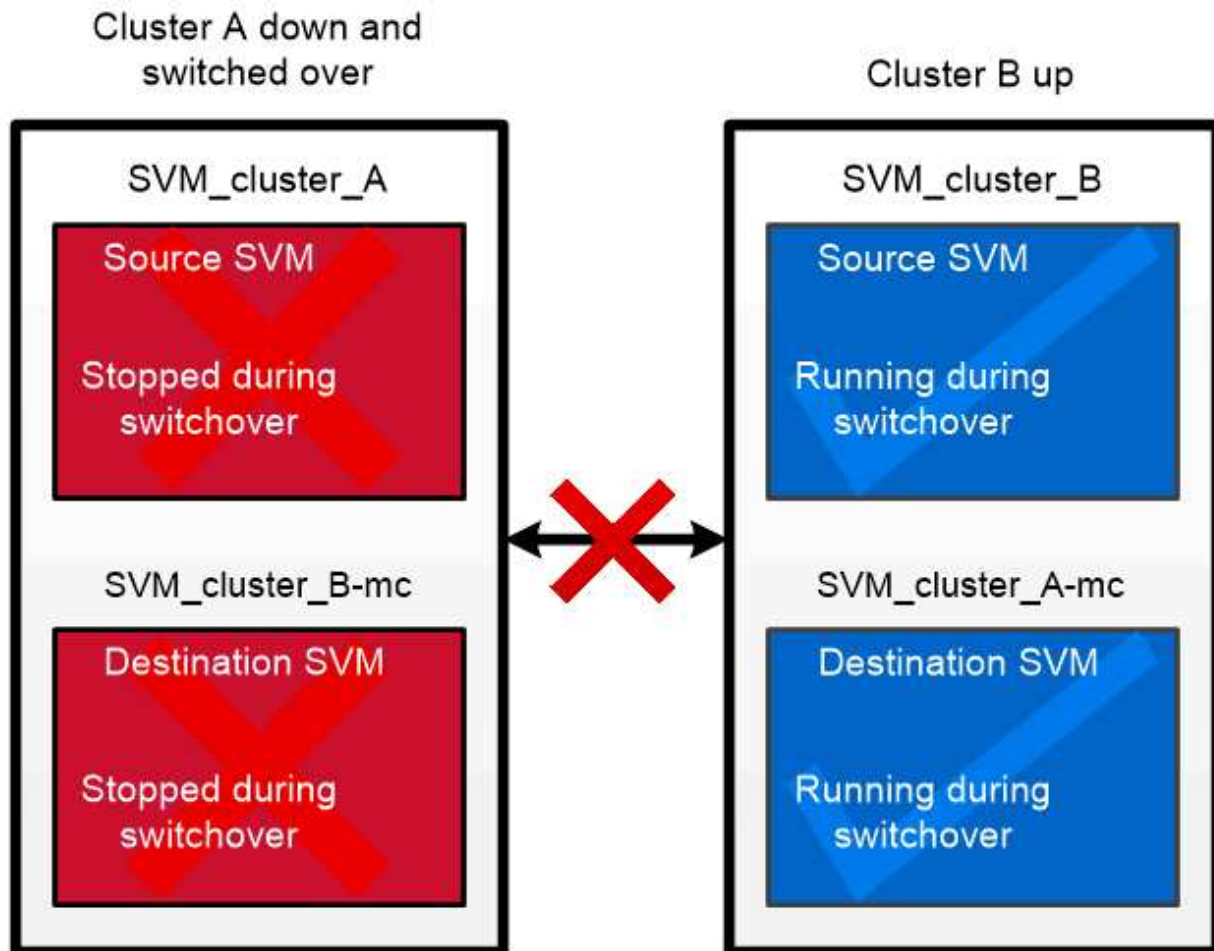
## Kontinuierliche Verfügbarkeit mit MetroCluster

MetroCluster Konfigurationen sichern Daten, indem sie zwei physisch getrennte, gespiegelte Cluster implementieren. Jedes Cluster repliziert die Daten synchron zur SVM-Konfiguration des anderen. Bei einem Ausfall an einem Standort kann ein Administrator die gespiegelte SVM aktivieren und vom verbleibenden Standort aus Daten bereitstellen.

- Fabric-Attached MetroCluster\_- und MetroCluster IP\_-Konfigurationen unterstützen Cluster auf Großraumbene.
- *Stretch MetroCluster* Konfigurationen unterstützen Cluster auf dem gesamten Campus.

In beiden Fällen müssen Cluster Peering durchgeführt werden.

MetroCluster verwendet eine ONTAP Funktion namens *SyncMirror*, um Aggregatdaten für jeden Cluster in Kopien bzw. *plexes*, im Storage des anderen Clusters synchron zu spiegeln. Tritt eine Umschaltung auf, wird der Remote-Plex auf dem verbleibenden Cluster online geschaltet, und die sekundäre SVM stellt Daten bereit.



*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** optional können Sie SyncMirror in einer nicht-MetroCluster-Implementierung zum Schutz vor Datenverlust einsetzen, wenn mehr Festplatten ausfallen als der RAID-Typ schützt oder wenn die Verbindung zu den Festplatten der RAID-Gruppe unterbrochen wird. Die Funktion ist nur für HA-Paare verfügbar.

Zusammengefasste Daten werden in Plexen gespiegelt, die auf unterschiedlichen Festplatten-Shelfs gespeichert sind. Wenn eines der Shelfs nicht mehr verfügbar ist, wird der nicht betroffene Plex weiterhin Daten bereitstellen, während Sie die Ursache des Fehlers korrigieren.

Beachten Sie, dass ein mit SyncMirror gespiegeltes Aggregat doppelt so viel Storage erfordert wie ein nicht gespiegeltes Aggregat. Jeder Plex benötigt so viele Festplatten wie der Plex er spiegelt. Sie würden 2,880 GB Festplattenspeicher benötigen, zum Beispiel, um ein 1,440 GB Aggregat zu spiegeln, 1,440 GB für jeden Plex.

Mit SyncMirror wird empfohlen, mindestens 20 % freien Speicherplatz für gespiegelte Aggregate freizuhalten, um so eine optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Copy-on-Write-Architektur von ONTAP. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance der SyncMirror-Resynchronisierung auswirken, die sich indirekt auf betriebliche Workflows wie NDU bei nicht-Shared Cloud-Implementierungen und auf den Wechsel zu MetroCluster-Implementierungen 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 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.