



Replizierung

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

- 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 all dieser Verwendungen ist die ONTAP Snapshot Technologie.

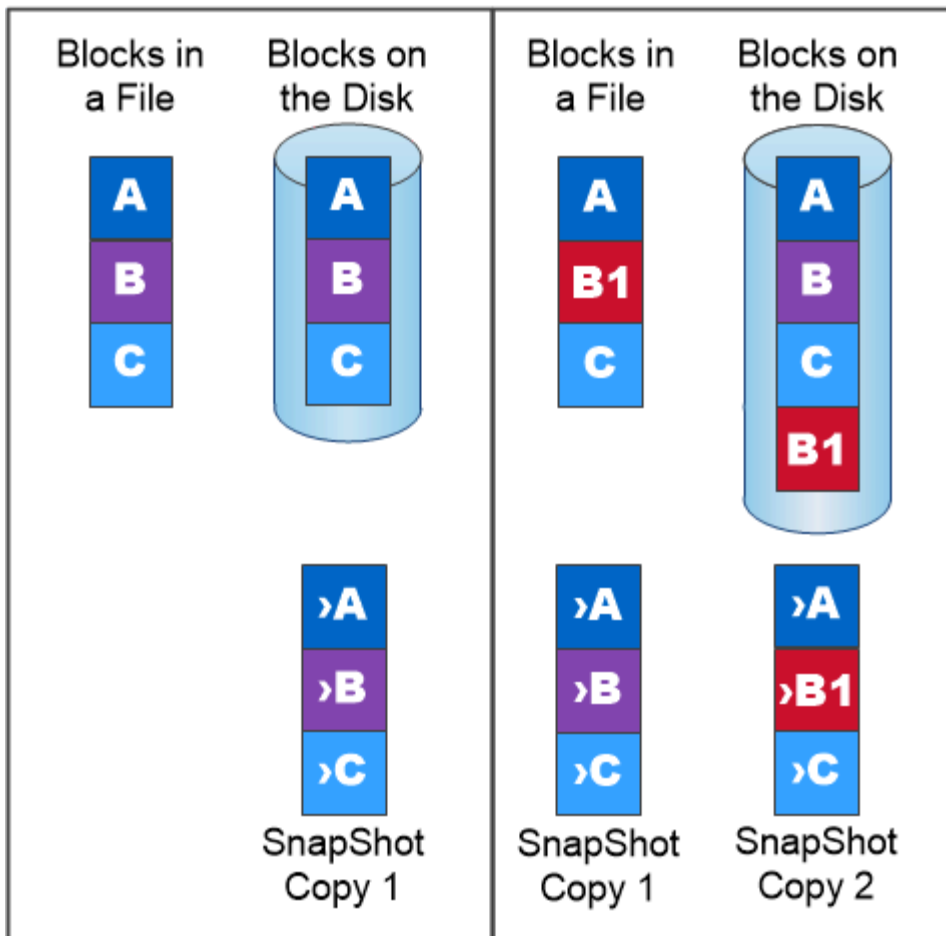
Eine *Snapshot Kopie* ist ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes. Das Image verbraucht nur wenig Storage und der Performance-Overhead ist minimal, da seit der letzten Snapshot Kopie nur Änderungen an Dateien aufgezeichnet werden.

Snapshot Kopien sind der Kerntechnologie der Storage-Virtualisierung von ONTAP verdanken, seinem *Write Anywhere File Layout (WAFL)*. wie eine Datenbank verwendet WAFL Metadaten, um 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.

Der Grund dafür ist, dass ONTAP bei der Erstellung einer Snapshot Kopie Metadaten referenziert, statt Datenblöcke zu kopieren. Somit sind die Snapshot Kopien so effizient. Damit entfallen die „seek time“, die andere Systeme beim Suchen der zu kopierenden Blöcke verursachen, sowie die Kosten für die Erstellung der Kopie selbst.

Sie können eine Snapshot Kopie verwenden, um einzelne Dateien oder LUNs wiederherzustellen oder den gesamten Inhalt eines Volume wiederherzustellen. ONTAP vergleicht Zeigerinformationen in der Snapshot-Kopie mit Daten auf der Festplatte, um das fehlende oder beschädigte Objekt ohne Ausfallzeiten und hohe Performance-Kosten zu rekonstruieren.

Eine *Snapshot Richtlinie* definiert, wie das System Snapshot Kopien von Volumes erstellt. Die Richtlinie gibt an, wann die Snapshot Kopien erstellt werden sollen, wie viele Kopien sie aufbewahrt werden sollen, wie benennen sie und wie man sie für die Replizierung benennt. Ein System könnte beispielsweise jeden Tag um 12:10 Uhr eine Snapshot-Kopie erstellen, die beiden neuesten Kopien aufbewahren, sie mit „daily“ benennen (angefügt mit einem Zeitstempel) und sie als „daily“ für die Replikation bezeichnen.



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.

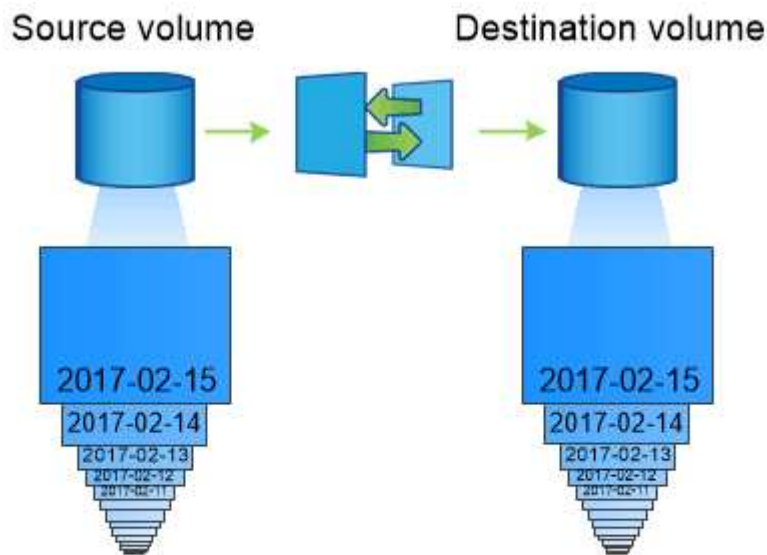
Ab ONTAP 9.10.1 können Sie Datensicherungsbeziehungen zwischen S3 Buckets mithilfe von S3 SnapMirror erstellen. Ziel-Buckets können sich auf lokalen oder Remote-ONTAP Systemen oder auf Systemen anderer Anbieter wie StorageGRID und AWS befinden.

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

- Erstellen einer Snapshot Kopie des Quell-Volumen
- Übertragen Sie die Snapshot Kopie und alle Datenblöcke, auf die sie auf das Ziel-Volumen verweist.
- Übertragen Sie die verbleibenden, weniger aktuellen Snapshot Kopien auf dem Quell-Volumen auf das Ziel-Volumen, falls die „aktive“-Spiegelung beschädigt ist.

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

Da SnapMirror nur Snapshot Kopien 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.



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

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 Technologie für Backup und Recovery, die für ONTAP Benutzer entwickelt wurde, die ihre Datensicherungs-Workflows in die Cloud verschieben möchten. Unternehmen, die sich von älteren auf Tape-Backup-Architekturen verabschieden, können Objekt-Storage als alternatives Repository für die langfristige Datenaufbewahrung und Archivierung verwenden. SnapMirror Cloud bietet die Replizierung von ONTAP-zu-Objekt-Storage im Rahmen einer inkrementellen Backup-Strategie.

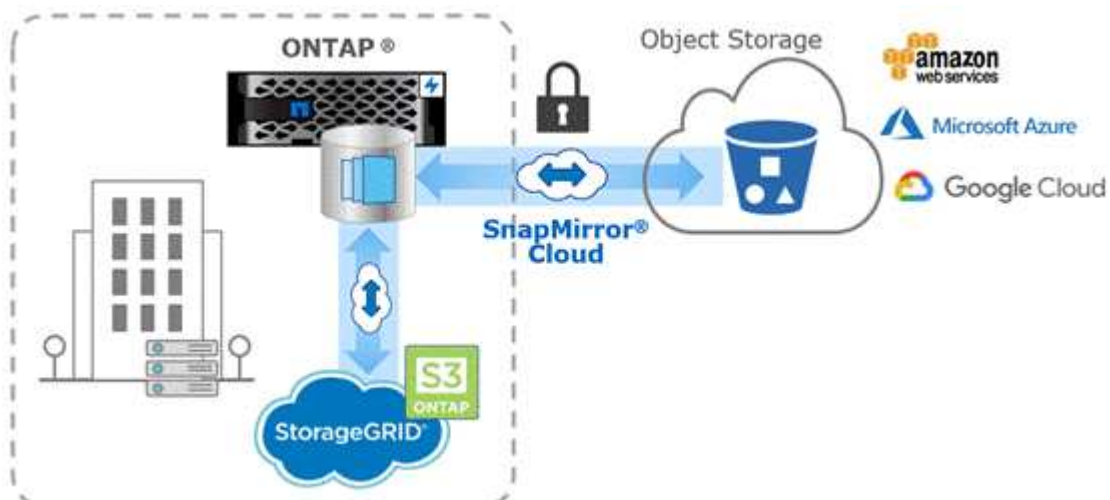
SnapMirror Cloud wurde im ONTAP 9.8 als Erweiterung der SnapMirror Replizierungstechnologien eingeführt. Während SnapMirror häufig für ONTAP-to-ONTAP Backups verwendet wird, nutzt SnapMirror Cloud dieselbe Replizierungs-Engine, um Snapshot Kopien für ONTAP auf S3-konforme Objekt-Storage-Backups zu übertragen.

SnapMirror Cloud ist für Backup-Anwendungsfälle ausgelegt und unterstützt sowohl langfristige Aufbewahrungs- als auch Archiv-Workflows. Wie bei SnapMirror führt auch das erste SnapMirror Cloud Backup einen Basistransfer eines Volumes durch. Bei nachfolgenden Backups generiert SnapMirror Cloud eine Snapshot-Kopie des Quell-Volume und überträgt die Snapshot Kopie nur mit den geänderten Datenblöcken auf ein Objekt-Storage-Ziel.

SnapMirror Cloud-Beziehungen können zwischen ONTAP Systemen konfiguriert und ausgewählte Objekt-Storage-Ziele vor Ort und Public Cloud ausgewählt werden, einschließlich AWS S3, Google Cloud Storage Platform und Microsoft Azure Blob Storage. Zusätzliche Objekt-Storage-Ziele vor Ort sind StorageGRID und ONTAP S3.

SnapMirror Cloud Replizierung ist eine lizenzierte ONTAP Funktion und erfordert eine genehmigte Applikation zur Orchestrierung von Datensicherungs-Workflows. Für das Management von SnapMirror Cloud Backups stehen verschiedene Orchestrierungsoptionen zur Verfügung:

- Mehrere Backup-Partner von Drittanbietern, die Unterstützung für die SnapMirror Cloud-Replizierung anbieten Teilnehmende Anbieter finden Sie auf der "[NetApp Blog](#)".
- BlueXP und Cloud Backup für eine native NetApp 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. SnapVault Lizenzen wurden veraltet und SnapMirror Lizenzen können jetzt verwendet werden, um Vault-, Mirror- und Mirror-and-Vault-Beziehungen zu konfigurieren. SnapMirror Replizierung wird für die Snapshot Kopien von ONTAP-to-ONTAP Replizierung eingesetzt und unterstützt sowohl Backup- als auch Disaster-Recovery-Anwendungsfälle.

SnapVault ist eine Archivierungstechnologie, die für die Disk-to-Disk Snapshot Kopie-Replizierung für Compliance-Standards und andere Governance-bezogene Zwecke entwickelt wurde. Im Gegensatz zu einer SnapMirror Beziehung, in der das Ziel normalerweise nur die derzeit im Quell-Volume befindlichen Snapshot-Kopien enthält, speichert ein SnapVault-Ziel in der Regel zeitpunktgenaue Snapshot-Kopien, die über einen längeren Zeitraum erstellt wurden.

Möglicherweise möchten Sie monatlich Snapshot Kopien Ihrer Daten über einen Zeitraum von 20 Jahren aufbewahren, um beispielsweise gesetzliche Buchhaltungsvorschriften für Ihr Unternehmen einzuhalten. 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 eine Snapshot Kopie des Quell-Volume und überträgt dann die Kopie und die Datenblöcke, auf die er Bezug auf das Ziel-Volume hat. Im Gegensatz zu SnapMirror umfasst SnapVault keine älteren Snapshot Kopien in der Basiskonfiguration.

Updates werden asynchron und folgen dem von Ihnen konfigurierten Zeitplan. Die in der Richtlinie definierten Regeln für die Beziehung ermitteln, welche neuen Snapshot Kopien in Updates enthalten sein sollen, und wie viele Kopien sie aufbewahren sollen. Die in der Richtlinie definierten Labels ("monthly," zum Beispiel) müssen mit einer oder mehreren in der Snapshot-Richtlinie auf der Quelle definierten Labels 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.

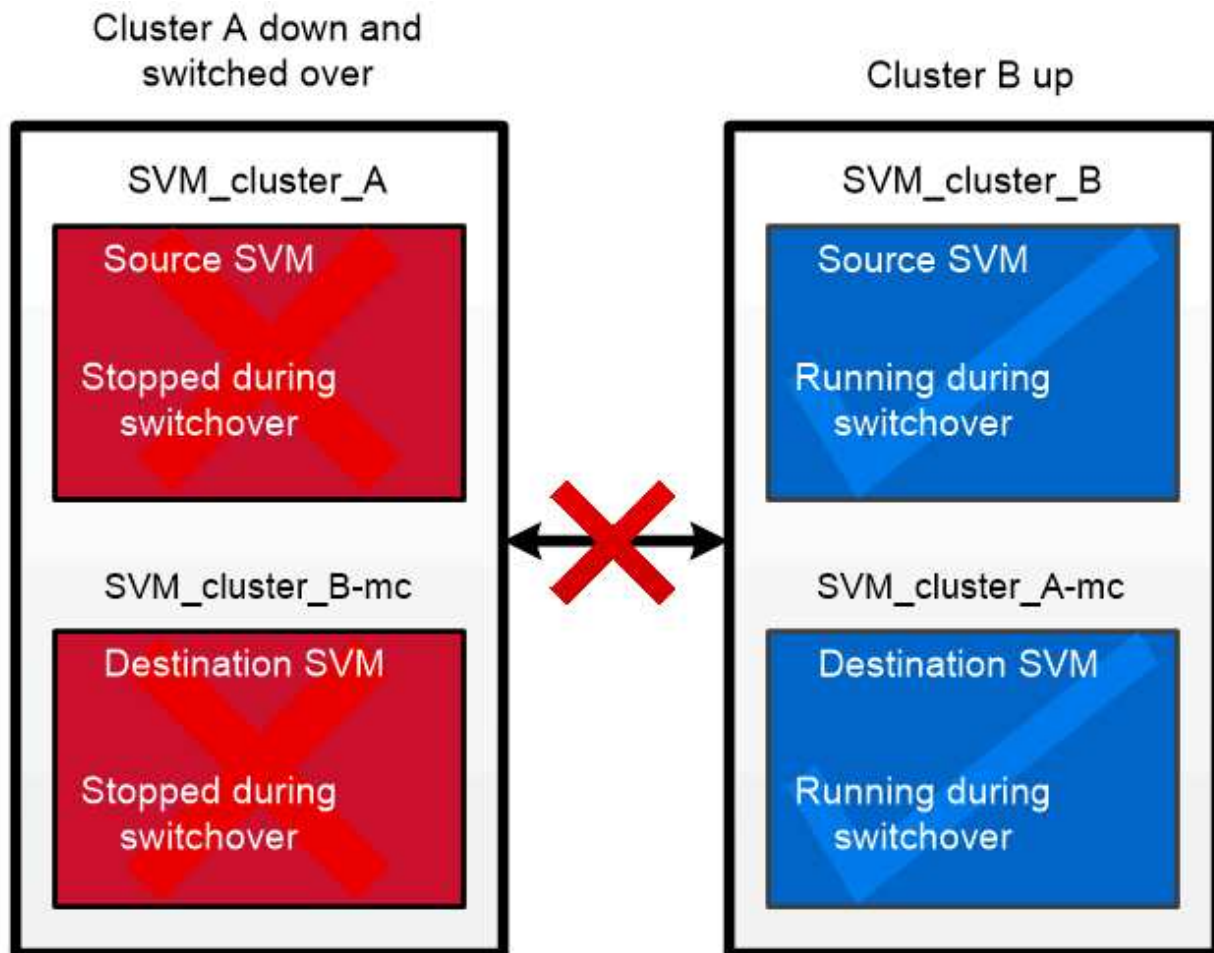
Kontinuierliche Verfügbarkeit mit MetroCluster

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* Konfigurationen unterstützen Cluster im Großraumgebiet.
- *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.



SyncMirror ist auch für FlexArray-Virtualisierungsimplementierungen verfügbar.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.