Schutzbeziehungen erstellen und Fehler beheben

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/data-protection/concept_types_of_snapmirror_protection.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Schutzbeziehungen erstellen und Fehler beheben . . . 1
Arten des SnapMirror Schutzes in Active IQ Unified Manager . . . 1
Traditionelle SnapMirror asynchrone Schutzbeziehungen . . . 1
SnapMirror Asynchroner Schutz mit versionsflexibler Replikation . . . 1
SnapMirror Asynchroner Schutz mit versionsflexibler Replikation und Backup-Option . . . 1
SnapMirror Einheitliche Replikation (Spiegelung und Vault) . . . 2
SnapMirror synchroner Schutz mit strenger Synchronisierung . . . 2
SnapMirror synchroner Schutz mit regelmäßiger Synchronisierung . . . 2
SnapMirror Active Sync . . . 2
Einrichten von Schutzbeziehungen in Unified Manager . . . 3
Einrichtung von Schutzbeziehungen in Active IQ Unified Manager . . . 3
Konfiguration einer Verbindung zwischen Workflow Automation und Active IQ Unified Manager . . . 3
Überprüfung des Caching der Active IQ Unified Manager Datenquelle in Workflow Automation . . . 4
Wie sich die Neuinstallation oder das Upgrade von OnCommand Workflow Automation auf Active IQ Unified Manager auswirken . . . 5
Entfernen der OnCommand Workflow Automation Einrichtung aus Active IQ Unified Manager . . . 5
Durchführen eines Failovers und Failbacks für eine Schutzbeziehung . . . 5
Durchführen eines Failovers und Failbacks einer Schutzbeziehung in Active IQ Unified Manager . . . 5
Eine SnapMirror Schutzbeziehung auf der Seite „Volume/Integrität“ von Active IQ Unified Manager trennen . . . 7
Umgekehrte Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager . . . 7
Eine Schutzbeziehung wird auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager entfernt . . . 8
Neusynchronisierung von Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager . . . 9
Fehler in einem Schutzauftrag beheben . . . 10
Beheben eines Fehlers bei einem Schutzauftrag in Active IQ Unified Manager . . . 10
Das Problem und die Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag in Active IQ Unified Manager werden identifiziert und durchgeführt . . . 10
Behebung von Verzögerungsproblemen in Active IQ Unified Manager . . . 13

Schutzbeziehungen erstellen und Fehler beheben

Arten des SnapMirror Schutzes in Active IQ Unified Manager

Je nach Deployment Ihrer Storage-Topologie ermöglicht Ihnen Unified Manager die Konfiguration mehrerer Arten von SnapMirror Schutzbeziehungen. Alle Varianten der SnapMirror Datensicherung bieten Failover- und Disaster-Recovery-Schutz, unterscheiden sich jedoch hinsichtlich Performance, Versionsflexibilität und des Schutzes durch mehrere Sicherungskopien.

Traditionelle SnapMirror asynchrone Schutzbeziehungen

Der traditionelle SnapMirror asynchrone Schutz bietet Spiegelungsschutz durch Blockreplikation zwischen Quell- und Ziel-Volumes.

In traditionellen SnapMirror Beziehungen werden Spiegelungsoperationen schneller ausgeführt als in alternativen SnapMirror Beziehungen, da die Spiegelungsoperation auf Blockreplikation basiert. Traditioneller SnapMirror Schutz erfordert jedoch, dass das Zielvolume mit derselben oder einer neueren Minor-Version der ONTAP Software wie das Quellvolume innerhalb derselben Hauptversion ausgeführt wird, z. B. Version 8.x zu 8.x oder 9.x zu 9.x. Die Replikation von einer 9.1 Quelle zu einem 9.0 Ziel wird nicht unterstützt, da auf dem Ziel eine ältere Hauptversion ausgeführt wird.

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation bietet logischen Replikationsspiegelschutz zwischen Quell- und Ziel-Volumes, selbst wenn diese Volumes unter verschiedenen Versionen der Software ONTAP 8.3 oder höher ausgeführt werden (z. B. Version 8.3 bis 8.3.1, oder 8.3 bis 9.1, oder 9.2.2 bis 9.2).

In SnapMirror Beziehungen mit versionsflexibler Replikation werden Spiegelungsvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

Aufgrund der langsameren Ausführung ist SnapMirror mit versionsflexiblem Replikationsschutz in den folgenden Fällen nicht für die Implementierung geeignet:

- Das Quellobjekt enthält mehr als 10 Millionen zu schützende Dateien.
- Das Wiederherstellungspunktziel für die geschützten Daten beträgt zwei Stunden oder weniger. (Das heißt, das Ziel muss stets gespiegelte, wiederherstellbare Daten enthalten, die höchstens zwei Stunden älter sind als die Daten an der Quelle.)

Unter beiden genannten Umständen ist die schnellere, auf Blockreplikation basierende Ausführung des standardmäßigen SnapMirror Schutzes erforderlich.

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation und Backup-Option

SnapMirror Asynchroner Schutz mit versionsflexibler Replikations- und Backup-Option bietet Spiegelschutz zwischen Quell- und Ziel-Volumes sowie die Möglichkeit, mehrere Kopien der gespiegelten Daten am Ziel zu

speichern.

Der Storage Administrator kann festlegen, welche Snapshot-Kopien von der Quelle zum Ziel gespiegelt werden, und auch, wie lange diese Kopien am Ziel aufbewahrt werden sollen, selbst wenn sie an der Quelle gelöscht werden.

In SnapMirror Beziehungen mit versionsflexibler Replikation und Backup-Option werden Spiegelungsvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

SnapMirror Einheitliche Replikation (Spiegelung und Vault)

SnapMirror Unified Replication ermöglicht die Konfiguration von Disaster Recovery und Archivierung auf demselben Zielvolume. Wie bei SnapMirror führt die einheitliche Datensicherung beim ersten Aufruf einen Basistransfer durch. Ein Basistransfer gemäß der standardmäßigen Datensicherungsstrategie „MirrorAndVault“ erstellt eine Snapshot Kopie des Quellvolumes und überträgt diese Kopie zusammen mit den Datenblöcken, auf die sie verweist, auf das Zielvolume. Wie bei SnapVault umfasst die einheitliche Datensicherung im Basistransfer keine älteren Snapshot Kopien.

SnapMirror synchroner Schutz mit strenger Synchronisierung

SnapMirror Synchronous protection mit der Synchronisierung “strict” stellt sicher, dass das primäre und das sekundäre Volume stets eine exakte Kopie voneinander sind. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replikationsfehler auftritt, wird die Client-I/O auf dem primären Volume unterbrochen.

SnapMirror synchroner Schutz mit regelmäßiger Synchronisierung

SnapMirror Synchroner Schutz mit „`regular`“-Synchronisierung erfordert nicht, dass das primäre und das sekundäre Volume stets eine exakte Kopie voneinander sind; dadurch wird die Verfügbarkeit des primären Volumes sichergestellt. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replikationsfehler auftritt, geraten das primäre und das sekundäre Volume außer Synchronisation, und die Client-E/A wird weiterhin an das primäre Volume geleitet.

> Die Schaltfläche „Wiederherstellen“ und die Schaltflächen für Beziehungsvorgänge sind bei der Überwachung synchroner Schutzbeziehungen in der Ansicht „Zustand: Alle Volumes“ oder auf der Detailseite „Volume/Health“ nicht verfügbar.

SnapMirror Active Sync

Die SnapMirror active sync Funktion ist mit ONTAP 9.8 und höher verfügbar, und sie kann zum Schutz von Applikationen mit LUNs verwendet werden, sodass ein transparentes Failover von Applikationen möglich ist und die Geschäftskontinuität im Katastrophenfall gewährleistet bleibt.

Es ermöglicht die Identifizierung und Überwachung der synchronen SnapMirror Beziehungen für Konsistenzgruppen (CGs), die auf Clustern und Storage Virtual Machines in Unified Manager verfügbar sind. SnapMirror active sync wird auf AFF Clustern oder All SAN Array (ASA) Clustern unterstützt, wobei die primären und sekundären Cluster entweder AFF oder ASA sein können. SnapMirror active sync schützt Applikationen mit iSCSI oder FCP LUNs.

Wenn Sie die Volumes und LUNs anzeigen, die durch die SnapMirror active sync Beziehung geschützt sind, erhalten Sie eine einheitliche Übersicht über Datensicherungsbeziehungen, Konsistenzgruppen im Volume-Inventar, die Datensicherungstopologie für Konsistenzgruppenbeziehungen sowie historische Daten für Konsistenzgruppenbeziehungen für bis zu ein Jahr. Sie können den Bericht auch herunterladen. Außerdem

können Sie die Zusammenfassung der Konsistenzgruppenbeziehungen anzeigen, nach Unterstützung für Konsistenzgruppenbeziehungen suchen und Informationen zu Volumes abrufen, die durch die Konsistenzgruppe geschützt sind.

Auf der Seite „Beziehungen“ können Sie außerdem die Quell- und Ziel-Storage-Objekte sowie deren Beziehung, die von der Consistency Group geschützt werden, sortieren, filtern und den Schutz erweitern.

Weitere Informationen zu SnapMirror active sync sind unter "ONTAP 9 Dokumentation für Snapmirror active sync (ehemals SM-BC)" verfügbar.

Einrichten von Schutzbeziehungen in Unified Manager

Einrichtung von Schutzbeziehungen in Active IQ Unified Manager

Es gibt mehrere Schritte, die Sie ausführen müssen, um Unified Manager und OnCommand Workflow Automation zum Einrichten von SnapMirror und SnapVault Beziehungen zum Schutz Ihrer Daten zu verwenden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Peer-Beziehungen zwischen zwei Clustern oder zwei Storage Virtual Machines (SVMs) eingerichtet haben.
- OnCommand Workflow Automation muss in Unified Manager integriert sein:
  - "Einrichtung von OnCommand Workflow Automation".
  - "Überprüfung des Unified Manager-Datenquellen-Cachings in Workflow Automation".

Schritte

1. Je nach Typ der Schutzbeziehung, die erstellt werden soll, ist eine der folgenden Optionen auszuwählen:
   - "Erstellung einer SnapMirror Schutzbeziehung".
   - "Erstellen einer SnapVault Schutzbeziehung".
2. Falls eine Richtlinie für die Beziehung erstellt werden soll, hängt das Vorgehen vom Typ der zu erstellenden Beziehung ab:
   - "Eine SnapVault Richtlinie erstellen".
   - "Erstellung einer SnapMirror Richtlinie".
3. "Erstellen eines SnapMirror oder SnapVault Zeitplans".

Konfiguration einer Verbindung zwischen Workflow Automation und Active IQ Unified Manager

Sie können eine sichere Verbindung zwischen OnCommand Workflow Automation (WFA) und Unified Manager konfigurieren. Die Verbindung zu Workflow Automation ermöglicht Ihnen die Nutzung von Schutzfunktionen wie SnapMirror- und SnapVault Konfigurationsworkflows sowie von Befehlen zum Verwalten von SnapMirror Beziehungen.

Bevor Sie beginnen

- Die installierte Version von Workflow Automation muss 5.1.1P6 oder höher sein.

> Das „WFA-Paket zur Verwaltung von Clustered Data ONTAP“ ist in WFA 5.1.1P6 enthalten, sodass es nicht mehr erforderlich ist, dieses Paket aus dem NetAppStorage Automation Store herunterzuladen und separat auf Ihrem WFA-Server zu installieren, wie es in der Vergangenheit notwendig war. "WFA-Download"

- Sie benötigen den Namen des Datenbankbenutzers, den Sie in Unified Manager erstellt haben, um WFA und Unified Manager Verbindungen zu unterstützen.

  Diesem Datenbankbenutzer muss die Benutzerrolle „Integration Schema“ zugewiesen worden sein.

- Ihnen muss in Workflow Automation entweder die Administratorrolle oder die Architektenrolle zugewiesen sein.
- Für die Workflow Automation Einrichtung benötigen Sie die Hostadresse, die Portnummer 443, den Benutzernamen und das Passwort.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **Workflow Automation**.
2. Im Bereich **Datenbankbenutzer** der **Workflow Automation Seite** erfolgt die Auswahl des Namens sowie die Eingabe des Passworts für den Datenbankbenutzer, den Sie zur Unterstützung von Verbindungen zwischen Unified Manager und Workflow Automation erstellt haben.
3. Im Bereich **Workflow Automation Credentials** der Seite sind der Hostname oder die IP-Adresse (IPv4 oder IPv6) sowie der Benutzername und das Passwort für die Workflow Automation Einrichtung einzugeben.

   Sie müssen den Unified Manager Server-Port (Port 443) verwenden.

4. Auf **Speichern** klicken.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, erfolgt die Autorisierung des Sicherheitszertifikats durch Klicken auf **Ja**.

   Die Seite „Workflow Automation“ wird angezeigt.

6. Nach einem Klick auf **Yes** wird die Web UI neu geladen, und die Workflow Automation Funktionen werden hinzugefügt.

Verwandte Informationen

"NetApp Dokumentation: OnCommand Workflow Automation (aktuelle Versionen)"

Überprüfung des Caching der Active IQ Unified Manager Datenquelle in Workflow Automation

Sie können feststellen, ob das Caching der Datenquellen in Unified Manager ordnungsgemäß funktioniert, indem Sie prüfen, ob die Datenquellenerfassung in Workflow Automation erfolgreich ist. Dies empfiehlt sich beispielsweise bei der Integration von Workflow Automation mit Unified Manager, um sicherzustellen, dass die Funktionen von Workflow Automation nach der Integration verfügbar sind.

Bevor Sie beginnen

Um diese Aufgabe ausführen zu können, muss Ihnen in Workflow Automation entweder die Administratorrolle oder die Architektenrolle zugewiesen sein.

Schritte

1. In der Workflow Automation UI erfolgt die Auswahl von **Execution** > **Data Sources**.
2. Per Rechtsklick auf den Namen der Unified Manager Datenquelle und anschließendes Auswählen von **Acquire Now**.
3. Zu überprüfen ist, ob die Datenerfassung fehlerfrei verläuft.

   Für eine erfolgreiche Integration von Workflow Automation mit Unified Manager müssen Erfassungsfehler behoben werden.

Wie sich die Neuinstallation oder das Upgrade von OnCommand Workflow Automation auf Active IQ Unified Manager auswirken

Vor der Neuinstallation oder dem Upgrade von OnCommand Workflow Automation müssen Sie zunächst die Verbindung zwischen OnCommand Workflow Automation und Unified Manager entfernen und sicherstellen, dass alle derzeit ausgeführten oder geplanten Aufträge von OnCommand Workflow Automation gestoppt sind.

Sie müssen Unified Manager außerdem manuell aus OnCommand Workflow Automation löschen.

Nach der Neuinstallation oder dem Upgrade von OnCommand Workflow Automation müssen Sie die Verbindung mit Unified Manager erneut einrichten.

Entfernen der OnCommand Workflow Automation Einrichtung aus Active IQ Unified Manager

Die Einrichtung von OnCommand Workflow Automation kann aus Unified Manager entfernt werden, wenn Workflow Automation nicht mehr verwendet werden soll.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **General** > **Workflow Automation** im linken Setup-Menü.
2. Auf der Seite **Workflow Automation** erfolgt die Auswahl von **Remove Setup**.

Durchführen eines Failovers und Failbacks für eine Schutzbeziehung

Durchführen eines Failovers und Failbacks einer Schutzbeziehung in Active IQ Unified Manager

Wenn ein Quellvolume in Ihrer Schutzbeziehung aufgrund eines Hardwareausfalls oder einer Katastrophe deaktiviert wird, können Sie die Schutzbeziehungsfunktionen in Unified

Manager verwenden, um das Schutzziel für lesen/schreiben zugänglich zu machen und ein Failover auf dieses Volume durchzuführen, bis die Quelle wieder online ist; anschließend können Sie ein Failback zur ursprünglichen Quelle durchführen, sobald diese wieder für die Datenbereitstellung verfügbar ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen OnCommand Workflow Automation eingerichtet haben, um diesen Vorgang durchzuführen.

Schritte

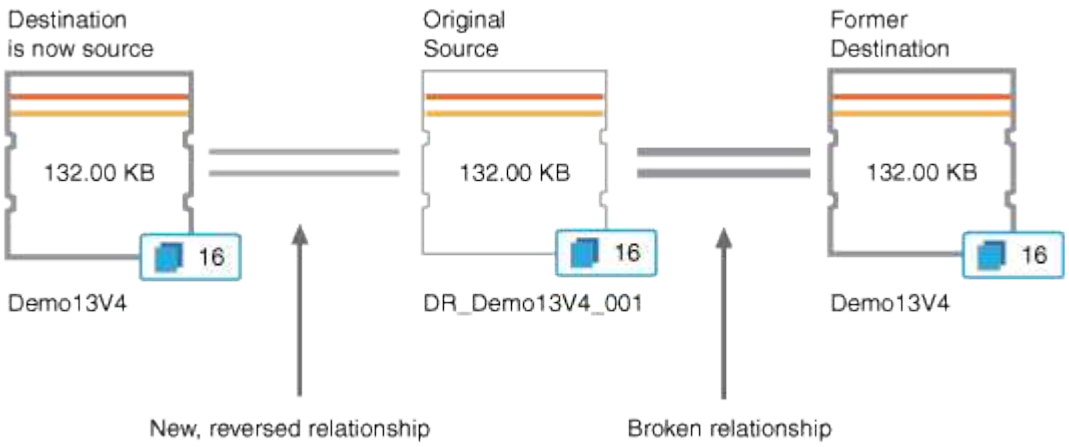
1. "Aufheben der SnapMirror Beziehung".

   Sie müssen die Beziehung aufheben, bevor Sie das Ziel von einem Datensicherungs-Volume in ein Volume mit lesen/schreiben konvertieren können und bevor Sie die Beziehung umkehren können.

2. "Umkehrung der Schutzbeziehung".

   Wenn das ursprüngliche Quellvolume wieder verfügbar ist, können Sie die ursprüngliche Schutzbeziehung wiederherstellen, indem Sie das Quellvolume wiederherstellen. Bevor Sie das Quellvolume wiederherstellen können, müssen Sie es mit den Daten synchronisieren, die auf das frühere Ziel geschrieben wurden. Mithilfe der umgekehrten Resynchronisierung erstellen Sie eine neue Schutzbeziehung, indem Sie die Rollen der ursprünglichen Beziehung umkehren und das Quellvolume mit dem früheren Ziel synchronisieren. Für die neue Beziehung wird eine neue Snapshot Basiskopie erstellt.

   Die umgekehrte Beziehung ähnelt einer Kaskadenbeziehung:



3. "Aufheben der umgekehrten SnapMirror Beziehung".

   Wenn das ursprüngliche Quellvolume erneut synchronisiert ist und wieder Daten bereitstellen kann, kann die umgekehrte Beziehung mit der Break-Operation aufgehoben werden.

4. "Beziehung entfernen".

   Wenn die umgekehrte Beziehung nicht mehr benötigt wird, sollte diese Beziehung entfernt werden, bevor die ursprüngliche Beziehung erneut eingerichtet wird.

5. "Neusynchronisieren der Beziehung".

   Die Resynchronisierungsoperation synchronisiert Daten von der Quelle zum Ziel und stellt die

ursprüngliche Beziehung wieder her.

Eine SnapMirror Schutzbeziehung auf der Seite „Volume/Integrität“ von Active IQ Unified Manager trennen

Auf der Seite „Volume/Health-Details“ können Sie eine Schutzbeziehung aufheben und Datentransfers zwischen einem Quell- und einem Zielvolume in einer SnapMirror Beziehung beenden. Eine Beziehung kann aufgehoben werden, wenn Sie Daten migrieren möchten, für Disaster Recovery oder für Applikationstests. Das Zielvolume wird in ein Volume mit lesen/schreiben geändert. Eine SnapVault Beziehung kann nicht aufgehoben werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Integrität** erfolgt die Auswahl der SnapMirror Beziehung, die in der Topologie getrennt werden soll.
2. Rechtsklick auf das Ziel und Auswahl von **Break** im Menü.

   Das Dialogfeld „Beziehung aufheben“ wird angezeigt.
3. Über **Weiter** lässt sich die Beziehung beenden.
4. In der Topologie lässt sich überprüfen, ob die Beziehung unterbrochen ist.

Umgekehrte Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Wenn ein Katastrophenfall das Quellvolume in Ihrer Schutzbeziehung außer Betrieb setzt, kann das Zielvolume zur Bereitstellung von Daten verwendet werden, indem es während der Reparatur oder des Austauschs des Quellvolumes in lesen/schreiben konvertiert wird. Sobald das Quellvolume wieder für den Datenempfang verfügbar ist, kann mit dem Vorgang der umgekehrten Resynchronisierung die Beziehung in umgekehrter Richtung hergestellt werden, wobei die Daten auf dem Quellvolume mit den Daten auf dem lesen/schreiben Zielvolume synchronisiert werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss getrennt werden.
- Sowohl Quelle als auch Ziel müssen online sein.
- Die Quelle darf nicht das Ziel eines anderen Datensicherungs-Volumes sein.

- Wenn Sie diese Aufgabe ausführen, werden auf der Quelle Daten gelöscht, die neuer sind als die Daten in der gemeinsamen Snapshot Kopie.
- Die in der umgekehrten Resynchronisierungsbeziehung erstellten Richtlinien und Zeitpläne entsprechen denen der ursprünglichen Schutzbeziehung.

  Falls keine Richtlinien und Zeitpläne existieren, werden sie erstellt.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Health** kann in der Topologie die SnapMirror Beziehung, für die Quelle und Ziel umgekehrt werden sollen, per Rechtsklick ausgewählt werden.
2. Sie wählen im Menü **Reverse Resync** aus.

   Das Dialogfeld „Umgekehrte Resynchronisierung“ wird angezeigt.
3. Stellen Sie sicher, dass die im Dialogfeld **Reverse Resync** angezeigte Beziehung diejenige ist, für die Sie die umgekehrte Resynchronisierung durchführen möchten, und klicken Sie anschließend auf **Submit**.

   Das Dialogfeld „Resynchronisierung rückgängig machen“ wird geschlossen, und oben auf der Seite „Volume / Zustandsdetails“ wird ein Job-Link angezeigt.
4. **Optional:** Auf der Detailseite **Volume / Health** lässt sich über **View Jobs** der Status jedes umgekehrten Resynchronisierungsjobs verfolgen.

   Eine gefilterte Liste der Jobs wird angezeigt.
5. **Optional:** Über den **Back**-Pfeil in Ihrem Browser gelangen Sie zurück zur Detailseite **Volume / Health**.

   Der umgekehrte Resynchronisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Eine Schutzbeziehung wird auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager entfernt

Sie können eine Schutzbeziehung entfernen, um eine bestehende Beziehung zwischen der ausgewählten Quelle und dem Ziel dauerhaft zu löschen, beispielsweise wenn Sie eine Beziehung mit einem anderen Ziel erstellen möchten. Dieser Vorgang löscht alle Metadaten und kann nicht rückgängig gemacht werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Protection** der Detailseite **Volume / Health** wird in der Topologie die SnapMirror Beziehung ausgewählt, die entfernt werden soll.
2. Sie entfernen das Ziel, indem Sie mit der rechten Maustaste auf den Namen des Ziels klicken und im Menü **Entfernen** auswählen.

   Das Dialogfeld „Beziehung entfernen“ wird angezeigt.
3. Mit **Weiter** lässt sich die Beziehung entfernen.

Die Beziehung wird von der Seite „Volume / Health details“ entfernt.

Neusynchronisierung von Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Sie können Daten in einer unterbrochenen SnapMirror oder SnapVault Beziehung neu synchronisieren, nachdem das Ziel auf lesen/schreiben gesetzt wurde, sodass die Daten auf der Quelle mit den Daten auf dem Ziel übereinstimmen. Eine erneute Synchronisierung kann auch erforderlich sein, wenn eine erforderliche gemeinsame Snapshot Kopie auf dem Quell-Volume gelöscht wurde und dadurch SnapMirror oder SnapVault Aktualisierungen fehlschlagen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Protection** der Detailseite **Volume / Health** wird in der Topologie die Schutzbeziehung, die neu synchronisiert werden soll, mit der rechten Maustaste angeklickt.
2. Die Auswahl im Menü erfolgt über **Resynchronize**.

   Alternativ lässt sich im Menü **Aktionen** die Option **Beziehung** > **Neu synchronisieren** auswählen, um die Beziehung, deren Details aktuell angezeigt werden, erneut zu synchronisieren.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.
3. Auf der Registerkarte **Resynchronisierungsoptionen** lassen sich eine Übertragungspriorität und die maximale Transferrate auswählen.
4. Nach einem Klick auf **Source Snapshot Copies** ist in der Spalte **Snapshot Copy** auf **Default** zu klicken.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.
5. Zum Angeben einer vorhandenen Snapshot-Kopie anstelle der Standard-Snapshot-Kopie ist **Vorhandene Snapshot Copy** anzuklicken und eine Snapshot-Kopie aus der Liste auszuwählen.
6. Anschließend **Absenden** auswählen.

   Sie kehren zum Dialogfeld „Resynchronisieren“ zurück.
7. Bei Auswahl von mehr als einer Quelle für die Resynchronisierung wird für die nächste Quelle, für die eine vorhandene Snapshot-Kopie angegeben werden soll, **Default** ausgewählt.
8. Mit **Submit** wird der Resynchronisierungsvorgang gestartet.

   Der Resynchronisierungsauftrag wird gestartet, Sie kehren zur Seite „Volume / Health details“ zurück, und oben auf der Seite wird ein Link zu Jobs angezeigt.
9. **Optional:** Auf der Seite **Volume / Health details** lässt sich über **View Jobs** der Status jedes Resynchronisierungsauftrags nachverfolgen.

   Eine gefilterte Liste der Jobs wird angezeigt.

10. **Optional:** Über den **Back**-Pfeil in Ihrem Browser gelangen Sie zurück zur Detailseite **Volume / Health**.

    Der Resynchronisierungsvorgang ist beendet, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Fehler in einem Schutzauftrag beheben

Beheben eines Fehlers bei einem Schutzauftrag in Active IQ Unified Manager

Dieser Workflow zeigt beispielhaft, wie sich ein Fehler bei einem Schutzauftrag im Unified Manager Dashboard identifizieren und beheben lässt.

Bevor Sie beginnen

Da einige Aufgaben in diesem Arbeitsablauf die Anmeldung mit der Administratorrolle erfordern, müssen Sie mit den Rollen vertraut sein, die zur Nutzung der verschiedenen Funktionen erforderlich sind.

In diesem Szenario greifen Sie auf die Dashboard Seite zu, um festzustellen, ob es Probleme mit Ihren Schutzaufträgen gibt. Im Bereich Protection Incident stellen Sie fest, dass ein Job Terminated Incident vorliegt, der auf einem Volume einen Fehler Protection Job Failed anzeigt. Sie untersuchen diesen Fehler, um die mögliche Ursache und eine potenzielle Lösung zu ermitteln.

Schritte

1. Im Bereich „Ungelöste Vorfälle und Risiken“ des Dashboards im Fenster „Schutzvorfälle“ klicken Sie auf das Ereignis „**Protection job failed**“.

   Der verlinkte Text für das Ereignis ist in der Form `object_name:/object_name - Error Name` geschrieben, z. B. `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Die Seite mit den Ereignisdetails für den fehlgeschlagenen Schutzvorgang wird angezeigt.

2. Anhand der Fehlermeldung im Feld „Cause“ des Bereichs **Summary** lassen sich das Problem bestimmen und mögliche Korrekturmaßnahmen bewerten.

   Weitere Informationen finden Sie unter "Identifizierung des Problems und Durchführung von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzjob".

Das Problem und die Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag in Active IQ Unified Manager werden identifiziert und durchgeführt

Sie prüfen die Fehlermeldung im Feld „Ursache“ auf der Seite mit den Ereignisdetails und stellen fest, dass der Auftrag aufgrund eines Fehlers bei der Snapshot Kopie fehlgeschlagen ist. Anschließend rufen Sie die Seite mit den Volume-/Integritätsdetails auf, um weitere Informationen zu erhalten.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Die im Feld „Ursache“ auf der Seite „Ereignisdetails“ angegebene Fehlermeldung enthält folgenden Text über den fehlgeschlagenen Job:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Diese Nachricht enthält folgende Informationen:

- Ein Sicherungs- oder Spiegelungsauftrag wurde nicht erfolgreich abgeschlossen.

  Die Aufgabe umfasste eine Schutzbeziehung zwischen dem Quellvolume `cluster2_src_vol2` auf dem virtuellen Server `cluster2_src_svm` und dem Zielvolume `managed_svc2_vol3` auf dem virtuellen Server mit dem Namen `cluster3_dst_svm`.

- Ein Auftrag für eine Snapshot Kopie ist fehlgeschlagen für `0426cluster2_src_vol2snap` auf dem Quell-Volume `cluster2_src_svm:/cluster2_src_vol2`.

In diesem Szenario können Sie die Ursache und mögliche Korrekturmaßnahmen für den Jobfehler ermitteln. Für die Behebung des Fehlers müssen Sie jedoch entweder auf die System Manager Web-UI zugreifen oder ONTAP CLI-Befehle verwenden.

Schritte

1. Sie überprüfen die Fehlermeldung und stellen fest, dass ein Snapshot Kopierauftrag auf dem Quellvolume fehlgeschlagen ist, was darauf hindeutet, dass wahrscheinlich ein Problem mit Ihrem Quellvolume besteht.

   Optional wäre es möglich, am Ende der Fehlermeldung auf den Link **Job Details** zu klicken; in diesem Szenario wird jedoch darauf verzichtet.

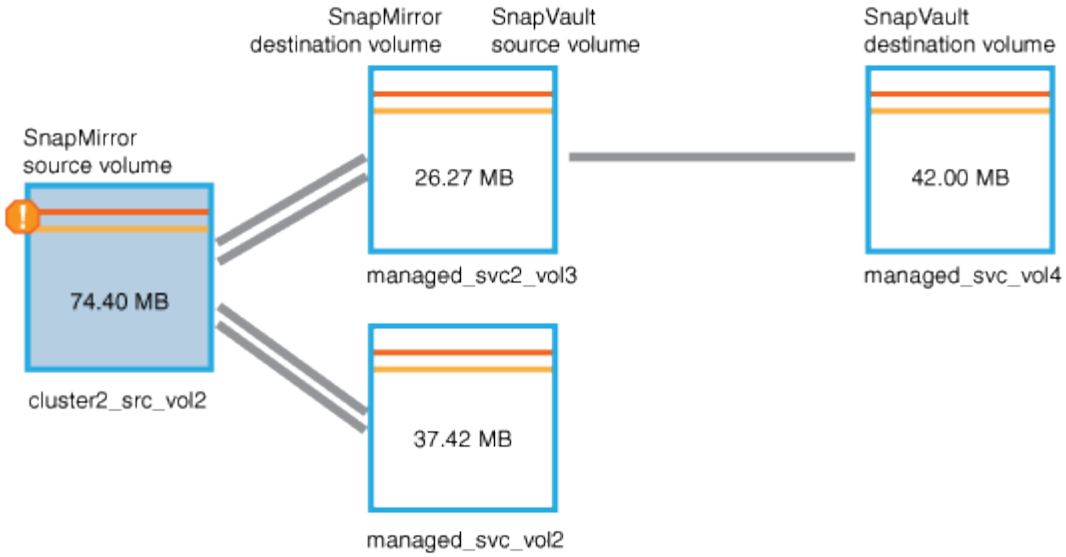
2. Sie beschließen, zu versuchen, das Ereignis zu beheben, und gehen daher wie folgt vor:
   a. Über die Schaltfläche **Zuweisen an** lässt sich im Menü **Ich** auswählen.
   b. Über die Schaltfläche **Acknowledge** lässt sich der weitere Erhalt wiederholter Warnungsbenachrichtigungen verhindern, sofern für das Ereignis Warnmeldungen eingerichtet wurden.
   c. Optional können Sie auch Notizen zum Ereignis hinzufügen.
3. Im Bereich **Zusammenfassung** können Sie das Feld **Quelle** auswählen, um Details zum Quellvolume anzuzeigen.

   Das Feld **Source** enthält den Namen des Quellobjekts: in diesem Fall das Volume, auf dem der Snapshot-Kopierauftrag geplant war.

   Die Seite „Volume / Statusdetails“ für `cluster2_src_vol2` wird angezeigt und zeigt den Inhalt der Registerkarte „Schutz“.

4. Beim Betrachten des Schutztopologiediagramms ist ein Fehlersymbol beim ersten Volume in der Topologie zu sehen, das das Quellvolume für die SnapMirror Beziehung darstellt.

   Außerdem sehen Sie die horizontalen Balken im Quell-Volume-Symbol, die die für dieses Volume festgelegten Warn- und Fehlerschwellenwerte anzeigen.



5. Wenn Sie den Mauszeiger über das Fehlersymbol bewegen, wird das Popup-Dialogfeld mit den Schwellenwerteinstellungen angezeigt, und Sie sehen, dass das Volume den Fehlerschwellenwert überschritten hat, was auf ein Kapazitätsproblem hinweist.
6. Die Auswahl erfolgt über die Registerkarte **Kapazität**.

   Kapazitätsinformationen zu Volume `cluster2_src_vol2`Anzeigen.

7. Im Bereich **Capacity** ist im Balkendiagramm ein Fehlersymbol zu sehen, das erneut darauf hinweist, dass die Volume-Kapazität den für das Volume festgelegten Schwellenwert überschritten hat.
8. Unterhalb des Kapazitätsdiagramms ist zu sehen, dass die automatische Volume Erweiterung deaktiviert und eine Volume Speicherplatzzusage festgelegt wurde.

   Es wäre möglich, die automatische Erweiterung zu aktivieren, für dieses Szenario fällt die Entscheidung jedoch darauf, vor einer Entscheidung zur Behebung des Kapazitätsproblems weitere Untersuchungen durchzuführen.

9. Beim Herunterscrollen zur Liste **Events** ist zu sehen, dass die Ereignisse Protection Job Failed, Volume Days Until Full und Volume Space Full generiert wurden.
10. In der **Ereignisliste** klicken Sie auf das Ereignis **Volume Space Full**, um weitere Informationen zu erhalten, da Sie entschieden haben, dass dieses Ereignis für Ihr Kapazitätsproblem am relevantesten erscheint.

    Auf der Seite „Ereignisdetails“ wird das Ereignis „Volume-Speicherplatz voll“ für das Quell-Volume angezeigt.

11. Im Bereich **Summary** befindet sich für das Ereignis das Feld „Cause“: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Unterhalb des Zusammenfassungsbereichs sehen Sie die vorgeschlagenen Korrekturmaßnahmen.

    Die vorgeschlagenen Korrekturmaßnahmen werden nur für bestimmte Ereignisse angezeigt, daher ist dieser Bereich nicht bei allen Ereignistypen sichtbar.

    Sie klicken sich durch die Liste der vorgeschlagenen Aktionen, die Sie zur Behebung des Events „Volume Space Full“ ausführen können:

- Die automatische Vergrößerung für dieses Volume aktivieren.
- Größe des Volumens ändern.
- Aktivierung und Ausführung der Deduplizierung auf diesem Volume.
- Für dieses Volume lässt sich die Komprimierung aktivieren und ausführen.

13. Sie beschließen, das automatische Wachstum des Volumes zu aktivieren; dazu müssen Sie jedoch den verfügbaren freien Speicherplatz auf dem übergeordneten Aggregat und die aktuelle Wachstumsrate des Volumes ermitteln:
    a. Das übergeordnete Aggregat, `cluster2_src_aggr1`, befindet sich im Bereich **Verwandte Geräte**.

    Sie können auf den Namen des Aggregats klicken, um weitere Details zum Aggregat zu erhalten.

    Sie stellen fest, dass das Aggregat über ausreichend Speicherplatz verfügt, um die automatische Vergrößerung des Volumes zu ermöglichen.

    b. Oben auf der Seite ist das Symbol zu sehen, das einen kritischen Incident anzeigt, sowie der Text unterhalb des Symbols.

    Sie stellen fest, dass „Tage bis zur vollständigen Belegung: Weniger als ein Tag | Tägliche Wachstumsrate: 5,4 %“ angezeigt wird.

14. Die `volume autogrow`Option kann im System Manager oder über die ONTAP CLI aktiviert werden.

    Die Namen des Volumes und des Aggregats sollten notiert werden, damit sie beim Aktivieren von autogrow verfügbar sind.

15. Nach Behebung des Kapazitätsproblems ist die Unified Manager **Ereignis**-Detailseite wieder aufzurufen und das Ereignis als gelöst zu markieren.

Behebung von Verzögerungsproblemen in Active IQ Unified Manager

Dieser Workflow zeigt beispielhaft, wie Sie ein Verzögerungsproblem beheben können. In diesem Szenario sind Sie Administrator oder Operator und greifen auf die Unified ManagerDashboard Seite zu, um zu prüfen, ob Probleme mit Ihren Schutzbeziehungen bestehen und gegebenenfalls Lösungen zu finden.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Auf der Dashboard-Seite sehen Sie im Bereich „Ungelöste Incidents und Risiken“ im Bereich „Schutz“ unter „Schutzrisiken“ einen SnapMirror Lag-Fehler.

Schritte

1. Im Bereich **Schutz** auf der Seite **Dashboard** den Verzögerungsfehler der SnapMirror Beziehung suchen und anklicken.

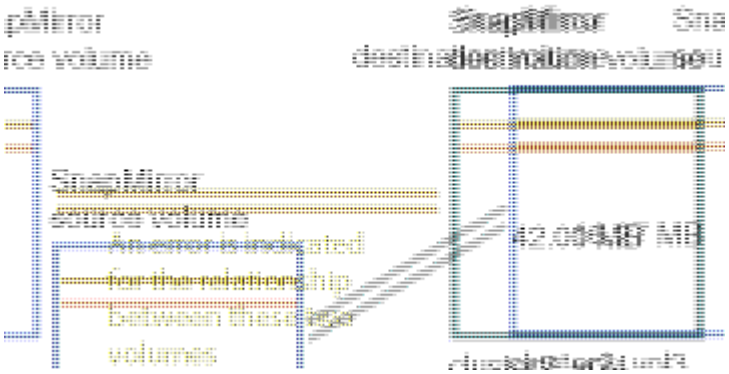
    Die Seite mit den Ereignisdetails für das Lag-Fehlerereignis erscheint.

2. Auf der Detailseite **Event** können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Anhand der Fehlermeldung im Feld „Ursache“ des Zusammenfassungsbereichs lässt sich feststellen, ob eine Korrekturmaßnahme vorgeschlagen wird.
   - Im Feld „Quelle“ des Bereichs „Zusammenfassung“ kann der Objektname, in diesem Fall ein Volume, ausgewählt werden, um Details zu diesem Volume zu erhalten.
   - Möglicherweise wurden diesem Ereignis Notizen hinzugefügt.
   - Dem Ereignis eine Notiz hinzufügen.
   - Zuweisung des Ereignisses an einen bestimmten Benutzer.
   - Das Ereignis bestätigen oder beheben.
3. In diesem Szenario klicken Sie im Feld „Quelle“ des Bereichs **Summary** auf den Objektnamen (in diesem Fall ein Volume), um Details zum Volume zu erhalten.

   Die Registerkarte „Schutz“ der Seite „Volume/Health-Details“ wird angezeigt.

4. Auf der Registerkarte **Schutz** sehen Sie das Topologiediagramm.

   Sie stellen fest, dass das Volume mit dem Lag-Fehler das letzte Volume in einer dreistufigen SnapMirror Kaskade ist. Das von Ihnen ausgewählte Volume ist dunkelgrau umrandet, und eine doppelte orange Linie vom Quell-Volume zeigt einen Fehler in der SnapMirror Beziehung an.



5. Jedes der Volumes in der SnapMirror Kaskade auswählen.

   Wenn Sie jedes Volume auswählen, ändern sich die Schutzinformationen in den Bereichen Zusammenfassung, Topologie, Verlauf, Ereignisse, Zugehörige Geräte und Zugehörige Warnungen und zeigen Details an, die für das ausgewählte Volume relevant sind.

6. Im Bereich **Zusammenfassung** liegt der Cursor für jedes Volume über dem Informationssymbol im Feld **Aktualisierungsplan**.

   In diesem Szenario stellen Sie fest, dass die SnapMirror Richtlinie DPDefault lautet und der SnapMirror Zeitplan stündlich fünf Minuten nach der vollen Stunde aktualisiert wird. Sie stellen fest, dass alle Volumes in der Beziehung versuchen, gleichzeitig einen SnapMirror Transfer abzuschließen.

7. Zur Behebung des Verzögerungsproblems werden die Zeitpläne für zwei der kaskadierten Volumes so geändert, dass jedes Ziel eine SnapMirror Übertragung startet, nachdem seine Quelle eine Übertragung abgeschlossen hat.

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.