Upgrade und Revert von ONTAP

ONTAP 9

NetApp
November 17, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/upgrade/index.html on November 17, 2026. Always check docs.netapp.com for the latest.

Inhalt

ONTAP Software und Firmware aktualisieren und zurücksetzen . . . 1
ONTAP aktualisieren . . . 1
Informationen zu ONTAP Upgrades . . . 1
Zeitpunkt für ein Upgrade von ONTAP . . . 2
Automatisierte ONTAP-Vorabprüfungen vor einem geplanten Upgrade ausführen . . . 4
ONTAP Richtlinien zur Dauer des ONTAP Upgrades . . . 13
Bereiten Sie ein ONTAP-Upgrade mit dem Upgrade Advisor oder dem Upgrade Health Checker vor . . . 14
Manuelle Vorbereitung auf das Upgrade . . . 15
Das ONTAP Software-Image sollte vor einem Upgrade heruntergeladen werden. . . . 109
ONTAP Upgrade-Methoden . . . 110
Überprüfungen nach dem Upgrade . . . 165
Firmware, System- und Sicherheitsupdates . . . 180
Wie ONTAP automatische Updates für die Installation plant . . . 180
Automatische Updates in ONTAP aktivieren . . . 181
Ändern von automatischen Updates in ONTAP . . . 184
Verwaltung empfohlener automatischer Updates in ONTAP . . . 185
ONTAP Firmware manuell aktualisieren . . . 186
System-Firmware vor einem ONTAP Software Upgrade vorbereiten . . . 188
ONTAP zurücksetzen . . . 190
Wann Sie den technischen Support für eine ONTAP Rücksetzung kontaktieren sollten . . . 190
Unterstützte ONTAP Revert-Pfade . . . 190
ONTAP Revert-Probleme und Einschränkungen . . . 191
Überprüfung der Ressourcen vor dem Zurücksetzen eines ONTAP Cluster . . . 192
Überprüfung der Systembereitschaft vor dem Zurücksetzen eines ONTAP Clusters . . . 193
ONTAP versionsspezifische Prüfungen vor dem Zurücksetzen durchführen . . . 198
Das ONTAP Software-Image herunterladen und installieren . . . 216
Ein ONTAP Cluster zurücksetzen . . . 219
Was nach einer ONTAP Rücksetzung zu tun ist . . . 227

ONTAP Software und Firmware aktualisieren und zurücksetzen

ONTAP aktualisieren

Informationen zu ONTAP Upgrades

Beim Upgrade Ihrer ONTAP Software ergeben sich Vorteile durch neue und erweiterte ONTAP Funktionen, die zur Kostensenkung, Beschleunigung kritischer Workloads, Verbesserung der Sicherheit und Erweiterung des für Ihr Unternehmen verfügbaren Datenschutzumfangs beitragen können.

Ein größeres ONTAP-Upgrade besteht darin, von einer niedrigeren zu einer höheren ONTAP-Nummerierten Version zu wechseln. Ein Beispiel wäre ein Upgrade Ihres Clusters von ONTAP 9.14.1 auf ONTAP 9.18.1. Ein kleineres (oder Patch-) Upgrade besteht darin, von einer niedrigeren ONTAP-Version zu einer höheren ONTAP-Version innerhalb derselben nummerierten Version zu wechseln. Ein Beispiel wäre ein Upgrade Ihres Clusters von ONTAP 9.17.1P1 auf 9.17.1P4.

Um zu beginnen, können Sie eine der folgenden Methoden verwenden, um sich auf das Upgrade vorzubereiten.

- Upgrade Advisor

  Wenn Sie einen aktiven SupportEdge-Vertrag für Active IQ Digital Advisor (auch bekannt als Digital Advisor) haben, sollten Sie "Mit dem Upgrade Advisor auf das Upgrade vorbereiten". Upgrade Advisor bietet Intelligenz, die Ihnen hilft, Unsicherheiten und Risiken zu minimieren, indem Ihr Cluster bewertet und ein Upgrade-Plan erstellt wird, der speziell auf Ihre Konfiguration zugeschnitten ist.

  Upgrade Advisor ist für Anwender mit einer kleineren Umgebung geeignet, die eine Cloud-basierte, UI-zentrierte Erfahrung bevorzugen.

  Weitere Informationen zu "Upgrade Advisor".

- Upgrade Health Checker

  Sie können auch "Bereiten Sie sich auf das Upgrade mit dem Upgrade Health Checker vor". Upgrade Health Checker ist ein Upgrade-Beratungsdienst-Tool, das vor Ort umfassende Gesundheitsprüfungen durchführt, um Upgrade-Blocker und Warnungen zu identifizieren. Ein SupportEdge-Vertrag ist nicht erforderlich, um den Upgrade Health Checker zu verwenden.

  Upgrade Health Checker ist geeignet für Benutzer, die eine große oder komplexe Umgebung, eingeschränkten Internetzugang oder ein bestehendes Automatisierungs- und Orchestrierungsframework haben.

  Weitere Informationen zu "Upgrade Health Checker".

- Manuelle Vorbereitung

  Wenn Sie weder Upgrade Advisor noch das Upgrade Health Checker tool verwenden, müssen Sie "Bereiten Sie sich auf das manuelle Upgrade vor". Die manuelle Vorbereitung umfasst mehrere Aufgaben, mit denen bekannte Probleme oder Hindernisse geprüft werden und sichergestellt wird, dass Ihr Cluster die erforderlichen Voraussetzungen für das Upgrade erfüllt.

Weitere Informationen zu "manuelle Upgrade-Vorbereitung".

Nachdem Sie die Aktualisierung vorbereitet haben, wird empfohlen, das Upgrade mit "automatisiertes unterbrechungsfreies Upgrade (ANDU) vom System Manager" durchzuführen. ANDU nutzt die Hochverfügbarkeits-Failover-Technologie (HA) von ONTAP, um sicherzustellen, dass die Cluster während des Upgrades weiterhin Daten ohne Unterbrechung bereitstellen.

Ab ONTAP 9.12.1 ist der System Manager vollständig in die NetApp Console integriert. Wenn die Console auf Ihrem System konfiguriert ist, ist ein Upgrade über die Seite Systeme möglich.

Wenn Sie Unterstützung bei der Aktualisierung Ihrer ONTAP Software wünschen, bietet NetApp Professional Services einen "Managed Upgrade Service". Bei Interesse an diesem Service kann Ihr NetApp Vertriebsmitarbeiter oder "Das Verkaufsanfrageformular von NetApp einreichen" kontaktiert werden. Der Managed Upgrade Service sowie andere Arten von Upgrade-Support stehen Kunden mit "SupportEdge Expert Services" ohne zusätzliche Kosten zur Verfügung.

Verwandte Informationen

- "Unterstützte Upgrade-Pfade"

Zeitpunkt für ein Upgrade von ONTAP

Sie sollten Ihre ONTAP Software regelmäßig aktualisieren. Ein Upgrade von ONTAP ermöglicht die Nutzung neuer und verbesserter Funktionen sowie die Implementierung aktueller Korrekturen für bekannte Probleme.

Wichtige ONTAP Upgrades

Ein größeres ONTAP Upgrade oder eine neue Feature-Version umfasst typischerweise Folgendes:

- Neue ONTAP Funktionen
- Wichtige Infrastrukturänderungen, wie grundlegende Änderungen am NetApp WAFL Betrieb oder am RAID Betrieb
- Unterstützung für neue von NetApp entwickelte Hardwaresysteme
- Unterstützung für Ersatzhardwarekomponenten wie neuere Netzwerkkarten oder Host-Bus-Adapter

Neue ONTAP-Versionen erhalten drei Jahre lang vollen Support. NetApp empfiehlt, die neueste Version nach allgemeiner Verfügbarkeit (GA) ein Jahr lang zu nutzen und anschließend die verbleibende Zeit innerhalb des vollen Supportzeitraums für die Planung des Übergangs zu einer neueren ONTAP Version zu verwenden.

ONTAP Patch-Upgrades

Patch-Upgrades beheben zeitnah kritische Fehler, die nicht bis zum nächsten größeren ONTAP Feature Release warten können. Nicht kritische Patch-Upgrades sollten alle 3-6 Monate eingespielt werden. Kritische Patch-Upgrades sollten so schnell wie möglich installiert werden.

Weitere Informationen zu "Empfohlene Mindest-Patch-Level" für ONTAP Releases.

ONTAP HotFix Upgrades

HotFix Upgrades bieten zeitkritische Fehlerbehebungen für eine breite Kundengruppe. Weitere Informationen zu "ONTAP HotFix Versionen" auf der NetApp Support Site.

ONTAP Veröffentlichungstermine

Ab der ONTAP 9.8-Version liefert NetApp ONTAP-Releases zweimal pro Kalenderjahr aus. Auch wenn sich die Pläne ändern können, ist beabsichtigt, neue ONTAP-Releases im zweiten und vierten Quartal jedes Kalenderjahres bereitzustellen. Diese Informationen können zur Planung des Zeitrahmens für ein Upgrade genutzt werden, um von der neuesten ONTAP-Version zu profitieren.

Version	Veröffentlichungsdatum
9.20.1	November 2026
9.19.1	Juli 2026
9.18.1	November 2025
9.17.1	September 2025
9.16.1	Januar 2025
9.15.1	Juli 2024
9.14.1	Januar 2024
9.13.1	Juni 2023
9.12.1	Februar 2023
9.11.1	Juli 2022
9.10.1	Januar 2022
9.9.1	Juni 2021

ONTAP Unterstützungsstufen

Der Umfang des Supports für eine bestimmte Version von ONTAP variiert je nach Veröffentlichungsdatum der Software.

Supportlevel	Volle Unterstützung			Eingeschränkte Unterstützung		Self-Service-Support		
Jahr	1	2	3	4	5	6	7	8
Zugriff auf die Online-Dokumentation	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Technische Unterstützung	Ja	Ja	Ja	Ja	Ja			
Ursachenanalyse	Ja	Ja	Ja	Ja	Ja			
Software Downloads	Ja	Ja	Ja	Ja	Ja			
Service-Updates (Patch Releases [P-Releases]) und HotFix Releases	Ja	Ja	Ja					
Warnungen zu Sicherheitslücken	Ja	Ja	Ja					

Verwandte Informationen

- Lernen "Was ist neu in den aktuell unterstützten ONTAP Versionen".
- Weitere Informationen zu "empfohlene minimale ONTAP-Releases".
- Weitere Informationen zu "ONTAP Softwareversionsunterstützung".
- Erfahren Sie mehr über das "ONTAP Release-Modell".

Automatisierte ONTAP-Vorabprüfungen vor einem geplanten Upgrade ausführen

Sie müssen sich nicht im Prozess der Aktualisierung Ihrer ONTAP Software befinden, um die automatisierten ONTAP Upgrade-Vorabprüfungen auszuführen. Das unabhängige Ausführen der Vorabprüfungen vom automatisierten ONTAP Upgrade-Prozess ermöglicht es, zu sehen, welche Prüfungen an Ihrem Cluster durchgeführt werden, und liefert eine Liste aller Fehler oder Warnungen, die vor Beginn des eigentlichen Upgrades behoben werden sollten. Beispielsweise kann vorgesehen sein, die ONTAP Software während eines in zwei Wochen geplanten Wartungsfensters zu aktualisieren. Während Sie auf das geplante Datum warten, lassen sich die automatisierten Upgrade-Vorabprüfungen durchführen und notwendige Korrekturmaßnahmen im Voraus vor dem Wartungsfenster ergreifen. Dadurch werden Risiken unerwarteter Konfigurationsfehler nach Beginn des Upgrades verringert.

Wenn Sie bereit sind, mit dem ONTAP Software-Upgrade zu beginnen, ist diese Vorgehensweise nicht erforderlich. Es sollte der "automatisierter Upgrade-Prozess" gefolgt werden, der die Ausführung der automatisierten Upgrade-Vorabprüfungen beinhaltet.

> Für MetroCluster Konfigurationen sollten diese Schritte zuerst auf Cluster A und anschließend die gleichen Schritte auf Cluster B ausgeführt werden.

Bevor Sie beginnen

Sie sollten "das Ziel-ONTAP-Software-Image herunterladen".

Um die automatisierten Vorabprüfungen für ein "direktes Multi-Hop-Upgrade" Upgrade durchzuführen, muss lediglich das Softwarepaket für Ihre Ziel ONTAP-Version heruntergeladen werden. Die Zwischenversion von ONTAP wird erst benötigt, wenn das eigentliche Upgrade beginnt. Wenn beispielsweise automatisierte Vorabprüfungen für ein Upgrade von 9.7 auf 9.11.1 ausgeführt werden, ist das Softwarepaket für ONTAP 9.11.1 herunterzuladen. Das Softwarepaket für ONTAP 9.8.1 muss nicht heruntergeladen werden.

Beispiel 1. Schritte

System Manager

1. Das ONTAP Zielabbild validieren:

   > Wenn Sie eine MetroCluster Konfiguration aktualisieren, sollte Cluster A validiert und anschließend der Validierungsprozess auf Cluster B wiederholt werden.

   a. Je nachdem, welche ONTAP Version verwendet wird, ist einer der folgenden Schritte auszuführen:

Wenn Sie ausführen…	Folgendes ist zu tun…
ONTAP 9.8 oder höher	**Cluster > Übersicht** auswählen.

ONTAP 9.5, 9.6 und 9.7	**Konfiguration** > **Cluster** > **Aktualisieren** auswählen.
ONTAP 9.4 oder früher	**Konfiguration** > **Cluster Update** auswählen.

b. In der rechten Ecke des **Übersicht**-Bereichs auf ⋮ klicken.

c. **ONTAP Update** auswählen.

d. Auf der Registerkarte **Cluster Update** ein neues Image hinzufügen oder ein verfügbares Image auswählen.

Wenn Sie möchten…	Dann…
Ein neues Software-Image aus einem lokalen Ordner hinzufügen. Sie sollten bereits "das Image heruntergeladen" eine Verbindung zum lokalen Client hergestellt haben.	i. Unter **Verfügbare Software-Images** auf **Von lokal hinzufügen** klicken. ii. Navigieren Sie zu dem Speicherort, an dem Sie das Software-Image gespeichert haben, wählen Sie das Image aus und klicken Sie anschließend auf **Open**.
Ein neues Software-Image von einem HTTP- oder FTP-Server hinzufügen	i. **Vom Server hinzufügen** auswählen. ii. Im Dialogfeld **Neues Software-Image hinzufügen** ist die URL des HTTP- oder FTP-Servers einzugeben, auf den das ONTAP Software-Image von der NetApp Support Site heruntergeladen wurde. Für anonymes FTP müssen Sie die URL im Format ftp://anonymous@ftpserver angeben. iii. Klicken Sie auf **Add**.
Wählen Sie ein verfügbares Bild	Eines der aufgelisteten Bilder kann ausgewählt werden.

e. **Validieren** ausführen, um die Validierungsprüfungen vor dem Upgrade zu starten.

Werden während der Validierung Fehler oder Warnungen gefunden, werden diese zusammen mit einer Liste von Korrekturmaßnahmen angezeigt. Alle Fehler müssen behoben werden, bevor mit dem Upgrade fortgefahren werden kann. Es gilt als Best Practice, auch Warnungen zu beheben.

Ab ONTAP 9.19.1 werden Fehler und Warnungen separat angezeigt, damit Sie Probleme, die vor dem Upgrade behoben werden müssen, leichter erkennen können.

CLI

1. Das Ziel-ONTAP Software-Image wird in das Cluster-Paket-Repository geladen:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.15.1/image.tgz
```

```
Package download completed.
Package processing completed.
```

2. Es sollte sichergestellt sein, dass das Softwarepaket im Cluster-Paket-Repository verfügbar ist:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.15.1              MM/DD/YYYY 10:32:15
```

3. Die automatisierten Vorabprüfungen für das Upgrade werden ausgeführt:

```
cluster image validate -version <package_version_number> -show
-validation-details true
```

```
cluster1::> cluster image validate -version 9.15.1 -show-validation
-details true

It can take several minutes to complete validation...
Validation checks started successfully.  Run the "cluster image
show-update-progress" command to check validation status.
```

4. Validierungsstatus prüfen:

```
cluster image show-update-progress
```

> Wenn der **Status** „in Bearbeitung“ ist, abwarten und den Befehl erneut ausführen, bis er abgeschlossen ist.

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                    Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                 00:10:00
00:01:03
```

```
Details:

Pre-update Check     Status            Error-Action
-------------------- ----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
...
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

Es wird eine Liste aller automatisierten Vorabprüfungen für das Upgrade angezeigt, zusammen mit allen Fehlern und Warnungen, die vor Beginn des Upgrade-Prozesses behoben werden sollten.

Ab ONTAP 9.19.1 werden Fehler und Warnungen separat angezeigt, damit Sie Probleme, die vor dem Upgrade behoben werden müssen, leichter erkennen können.

Beispielausgabe

▼ Vollständige Beispielausgabe der Upgrade-Vorabprüfungen

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that must
```

```
be performed after these automated validation checks have completed
successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to be
performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Use the Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system supportability
configuration information.

Validation checks started successfully.  Run the "cluster image show-
update-progress" command to check validation status.


fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    in-progress            00:10:00        00:00:42

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------

fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    completed              00:10:00        00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
```

```
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
Configuration Status
Boot Menu Status     Warning           Warning: bootarg.init.bootmenu is
                                       enabled on nodes: fas2820-wic-1a,
                                       fas2820-wic-1b. The boot process
of
                                       the nodes will be delayed.
                                       Action: Set the
bootarg.init.bootmenu
                                       bootarg to false before
proceeding
                                       with the upgrade.
Broadcast Domain     OK                N/A
availability and
uniqueness for HA
pair status
CIFS compatibility   OK                N/A
status check
CLAM quorum online   OK                N/A
status check
CPU Utilization      OK                N/A
Status
Capacity licenses    OK                N/A
install status check
Check For SP/BMC     OK                N/A
Connectivity To
Nodes
Check LDAP fastbind  OK                N/A
users using
unsecure connection.
Check for unsecure   OK                N/A
kex algorithm
configurations.
Check for unsecure   OK                N/A
mac configurations.
Cloud keymanager     OK                N/A
```

```
connectivity check
Cluster health and   OK                N/A
eligibility status
Cluster quorum       OK                N/A
status check
Cluster/management   OK                N/A
switch check
Compatible New       OK                N/A
Image Check
Current system       OK                N/A
version check if it
is susceptible to
possible outage
during NDU
Data ONTAP Version   OK                N/A
and Previous
Upgrade Status
Data aggregates HA   OK                N/A
policy check
Disk status check    OK                N/A
for failed, broken
or non-compatibility
Duplicate Initiator  OK                N/A
Check
Encryption key       OK                N/A
migration status
check
External             OK                N/A
key-manager with
legacy KMIP client
check
External keymanager  OK                N/A
key server status
check
Fabricpool Object    OK                N/A
Store Availability
High Availability    OK                N/A
configuration
status check
Infinite Volume      OK                N/A
availibility check
LIF failover         OK                N/A
capability status
check
LIF health check     OK                N/A
LIF load balancing   OK                N/A
```

```
status check
LIFs is on home      OK                N/A
node status
Logically over       OK                N/A
allocated DP
volumes check
MetroCluster         OK                N/A
configuration
status check for
compatibility
Minimum number of    OK                N/A
aggregate disks
check
NAE Aggregate and    OK                N/A
NVE Volume
Encryption Check
NDMP sessions check  OK                N/A
NFS mounts status    Warning           Warning: This cluster is serving
NFS
check                                  clients. If NFS soft mounts are
used,
                                       there is a possibility of
frequent
                                       NFS timeouts and race conditions
that
                                       can lead to data corruption
during
                                       the upgrade.
                                       Action: Use NFS hard mounts, if
                                       possible. To list Vservers
running
                                       NFS, run the following command:
                                       vserver nfs show
Name Service         OK                N/A
Configuration DNS
Check
Name Service         OK                N/A
Configuration LDAP
Check
Node to SP/BMC       OK                N/A
connectivity check
OKM/KMIP enabled     OK                N/A
systems - Missing
keys check
ONTAP API to REST    Warning           Warning: NetApp ONTAP API has
been
```

```
transition warning                      used on this cluster for ONTAP
data
                                        storage management within the
last 30
                                        days. NetApp ONTAP API is
approaching
                                        end of availability.
                                        Action: Transition your
automation
                                        tools from ONTAP API to ONTAP
REST
                                        API. For more details, refer to
                                        CPC-00410 - End of availability:
                                        ONTAPI

https://mysupport.netapp.com/info/
                                        communications/ECMLP2880232.html
ONTAP Image          OK                 N/A
Capability Status
OpenSSL 3.0.x        OK                 N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                 N/A
validation check
Platform Health      OK                 N/A
Monitor check
Pre-Update           OK                 N/A
Configuration
Verification
RDB Replica Health   OK                 N/A
Check
Replicated database  OK                 N/A
schema consistency
check
Running Jobs Status  OK                 N/A
SAN LIF association  OK                 N/A
status check
SAN compatibility    OK                 N/A
for manual
configurability
check
SAN kernel agent     OK                 N/A
status check
Secure Purge         OK                 N/A
operation Check
Shelves and Sensors  OK                 N/A
```

```
check
SnapLock Version     OK                N/A
Check
SnapMirror           OK                N/A
Synchronous
relationship status
check
SnapMirror           OK                N/A
compatibility
status check
Supported platform   OK                N/A
check
Target ONTAP         OK                N/A
release support for
FiberBridge 6500N
check
Upgrade Version      OK                N/A
Compatibility Status
Verify all bgp       OK                N/A
peer-groups are in
the up state
Verify if a cluster  OK                N/A
management LIF
exists
Verify that e0M is   OK                N/A
home to no LIFs
with high speed
services.
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

ONTAP Richtlinien zur Dauer des ONTAP Upgrades

Es ist mit mindestens 30 Minuten für die Vorbereitungsschritte eines ONTAP Upgrades, 60 Minuten für das Upgrade jedes HA Paars und mindestens 30 Minuten für die Nachbereitungsschritte zu rechnen.

Wenn Sie NetApp Encryption mit einem externen Schlüsselverwaltungsserver und dem Key Management Interoperability Protocol (KMIP) verwenden, sollten Sie für jedes HA-Paar mit einer Upgrade-Dauer von über einer Stunde rechnen. Diese zusätzliche Zeit gilt nicht für ein automatisiertes, unterbrechungsfreies Upgrade ab ONTAP 9.20.1, wenn der Cluster einen externen KMIP-Schlüsselmanager verwendet, sich nicht in einer MetroCluster Konfiguration befindet und der HA-Partner die Schlüssel bereitstellen kann. Ab ONTAP 9.20.1 stellen diese Cluster die Schlüssel vom HA-Partner wieder her. Weitere Informationen finden Sie unter Clusterinterner Schlüsselaustausch. Beim Upgrade auf ONTAP 9.20.1 werden die Schlüssel weiterhin vom Schlüsselserver wiederhergestellt, daher ist für dieses Upgrade mit einer Dauer von über einer Stunde pro HA-Paar zu rechnen.

Diese Richtlinien zur Upgrade-Dauer basieren auf typischen Konfigurationen und Arbeitslasten. Diese Richtlinien ermöglichen eine Schätzung der Zeit, die für ein unterbrechungsfreies Upgrade in Ihrer Umgebung erforderlich ist. Die tatsächliche Dauer des Upgrade-Prozesses hängt von Ihrer individuellen Umgebung und der Anzahl der Nodes ab.

Bereiten Sie ein ONTAP-Upgrade mit dem Upgrade Advisor oder dem Upgrade Health Checker vor

Sie können den Upgrade Advisor in Active IQ Digital Advisor oder den Upgrade Health Checker verwenden, um automatisch einen Upgrade-Bericht zu erstellen, der speziell auf Ihre Umgebung und Clusterkonfiguration zugeschnitten ist. Beide Tools liefern Informationen, die Ihnen bei der Planung Ihres Upgrades helfen, Blocker und Warnungen identifizieren und Unsicherheiten sowie Risiken minimieren.

Vorbereitung auf das Upgrade mit Upgrade Advisor

Upgrade Advisor identifiziert Probleme in Ihrer Umgebung, die durch ein Upgrade auf eine neuere Version von ONTAP behoben werden können, und stellt einen Bericht über Probleme bereit, die in der ONTAP Version, auf die Sie aktualisieren, beachtet werden sollten. Upgrade Advisor bietet außerdem einen empfohlenen Upgrade-Pfad und erstellt einen Upgrade-Plan, der speziell auf die Konfiguration Ihres Clusters zugeschnitten ist.

Upgrade Advisor eignet sich besonders für Benutzer mit einer kleineren Umgebung, die eine Cloud-basierte, UI-zentrierte Benutzererfahrung bevorzugen.

Bevor Sie beginnen

- Ein aktiver "Support Services mit KI-gestütztem SupportEdge" Vertrag für "Digital Advisor" ist erforderlich, um Upgrade Advisor zu nutzen.
- AutoSupport must be enabled, damit Upgrade Advisor automatisch auf die AutoSupport-Protokolle zugreifen kann, die zur Erstellung eines Upgrade-Plans erforderlich sind. Wenn Sie AutoSupport nicht aktiviert haben, können Sie "AutoSupport Dateien manuell hochladen".

Schritte

1. "Active IQ Digital Advisor starten"
2. Im Digital Advisor "alle mit Ihrem Cluster verbundenen Risiken anzeigen und manuell Korrekturmaßnahmen ergreifen".

   Risiken, die in den Kategorien **SW Config Change**, **HW Config Change** und **HW Replacement** enthalten sind, müssen vor der Durchführung eines ONTAP Upgrades behoben werden.

3. Der empfohlene Upgrade-Pfad und "Ihren Upgrade-Plan generieren" werden angezeigt.

Was kommt als Nächstes?

- Prüfen Sie die "ONTAP Versionshinweise" auf Informationen zu den Änderungen in der ONTAP-Version, die Upgrade Advisor als Ihr Upgrade-Ziel empfiehlt. Führen Sie anschließend das Upgrade Ihres Clusters gemäß dem von Upgrade Advisor erstellten Plan durch.
- "SP oder BMC neu starten" vor Beginn des Upgrades.

Bereiten Sie sich auf das Upgrade mit dem Upgrade Health Checker vor

Upgrade Health Checker ist ein On-Premise-Tool, das sich für Anwender mit großen oder komplexen Umgebungen, eingeschränktem Internetzugang oder bestehenden Automatisierungs- und Orchestrierungsframeworks eignet. Ein SupportEdge-Vertrag ist nicht erforderlich, um den Upgrade Health Checker zu verwenden.

Bevor Sie beginnen

Sie müssen "Upgrade Health Checker herunterladen und einrichten" ausführen, bevor Sie es zur Erstellung eines Upgrade-Plans verwenden können.

Schritte

1. "Erstellen Sie einen Upgrade-Plan mit dem Upgrade Health Checker".

Was kommt als Nächstes?

- Überprüfen Sie die "ONTAP Versionshinweise" für Informationen über Änderungen, die in der ONTAP-Version eingeführt wurden, die Upgrade Health Checker als Ihr Upgrade-Ziel empfiehlt. Führen Sie danach das Upgrade Ihres Clusters gemäß dem von Upgrade Health Checker generierten Plan durch.
- "SP oder BMC neu starten" vor Beginn des Upgrades.

Manuelle Vorbereitung auf das Upgrade

Workflow zur manuellen Upgrade-Vorbereitung für ONTAP

Wenn Sie sich entscheiden, Ihre Aktualisierung manuell vorzubereiten, müssen Sie mehrere Aufgaben erledigen, um bekannte Probleme oder Blockierungen zu erkennen und sicherzustellen, dass Ihr Cluster die notwendigen Anforderungen für die Aktualisierung erfüllt. Wenn beispielsweise der SSL-FIPs-Modus auf Ihrem Cluster aktiviert ist und die Administratorkonten SSH-öffentliche Schlüssel zur Authentifizierung verwenden, müssen Sie überprüfen, ob der Host-Key-Algorithmus in Ihrer Ziel-ONTAP-Version unterstützt wird.

> Eine manuelle Vorbereitung ist nicht erforderlich, wenn Sie den Upgrade Advisor im Active IQ Digital Advisor oder den Upgrade Health Checker verwenden. Beide Tools liefern Informationen, die Ihnen bei der Planung Ihres Upgrades helfen, Blocker und Warnungen identifizieren und Unsicherheiten sowie Risiken minimieren. Weitere Informationen zu "Vorbereitung auf ein Upgrade mit Upgrade Advisor oder Upgrade Health Checker".

Schritte

1. "Wählen Sie Ihre gewünschte ONTAP Version aus.".
2. Lesen Sie die Abschnitte „Upgrade-Vorsichtsmaßnahmen“ und „Bekannte Probleme und Einschränkungen“ in der "ONTAP 9 Versionshinweise" für Ihre Zielversion.

Warnhinweise zum Upgrade beschreiben potenzielle Probleme, die Sie vor dem Upgrade beachten sollten. *Bekannte Probleme und Einschränkungen* beschreiben potenziell unerwartetes Systemverhalten, das nach dem Upgrade auftreten kann.

Eine Anmeldung mit Ihrem NetApp Account oder die Erstellung eines Accounts ist erforderlich, um auf die Release Notes zuzugreifen.

3. "Bestätigung der ONTAP Unterstützung für Ihre Hardwarekonfiguration".

   Ihre Hardwareplattform, Cluster-Management-Switches und MetroCluster IP-Switches müssen die Zielversion unterstützen. Wenn Ihr Cluster für SAN konfiguriert ist, muss die SAN-Konfiguration vollständig unterstützt werden.

4. "Mit Active IQ Config Advisor lässt sich überprüfen, ob keine häufigen Konfigurationsfehler vorliegen."
5. Die unterstützte ONTAP "Upgrade-Pfade" sollte geprüft werden, um festzustellen, ob ein direktes Upgrade möglich ist oder ob das Upgrade in mehreren Schritten durchgeführt werden muss.
6. "LIF-Failover-Konfiguration überprüfen".

   Bevor ein Upgrade durchgeführt wird, ist zu überprüfen, ob die Failover-Richtlinien und Failover-Gruppen des Clusters korrekt konfiguriert sind.

7. "Die SVM Routing-Konfiguration überprüfen".
8. "Besondere Anforderungen überprüfen" für Ihren Cluster.

   Wenn in Ihrem Cluster bestimmte Konfigurationen vorhanden sind, sind vor Beginn eines ONTAP Software Upgrades spezifische Maßnahmen erforderlich.

9. "SP oder BMC neu starten".

Eine von NetApp empfohlene ONTAP Zielversion für ein Upgrade auswählen

Wenn mit dem Upgrade Advisor ein Upgrade-Plan für Ihren Cluster erstellt wird, enthält dieser eine empfohlene Ziel-ONTAP-Version für das Upgrade. Die Empfehlung des Upgrade Advisor basiert auf Ihrer aktuellen Konfiguration und Ihrer aktuellen ONTAP Version.

Wenn Sie Upgrade Advisor nicht zur Planung Ihres Upgrades verwenden, sollte die Ziel-ONTAP-Version für das Upgrade anhand von NetApp Empfehlungen oder Ihrer Notwendigkeit, die Mindestversion zu erreichen, um Ihre Leistungsanforderungen zu erfüllen, ausgewählt werden.

- Upgrade auf die neueste verfügbare Version (empfohlen)

  NetApp empfiehlt, die ONTAP Software auf die neueste Patch-Version der neuesten nummerierten ONTAP Version zu aktualisieren. Falls dies nicht möglich ist, weil die neueste nummerierte Version von den Speichersystemen in Ihrem Cluster nicht unterstützt wird, sollte auf die neueste nummerierte unterstützte Version aktualisiert werden.

- Empfohlene Mindestversion

  Wenn das Upgrade auf die für Ihren Cluster empfohlene Mindestversion beschränkt werden soll, siehe "Empfohlene minimale ONTAP Versionen" zur Ermittlung der ONTAP Version, auf die ein Upgrade erfolgen sollte.

Hardwarekonfigurationsanforderungen für ein ONTAP Upgrade

Bevor Sie ONTAP aktualisieren, sollte bestätigt werden, dass Ihre Hardwarekonfiguration die Zielversion von ONTAP unterstützt.

Alle Konfigurationen

Mit "NetApp Hardware Universe" lässt sich bestätigen, dass Ihre Hardwareplattform sowie Ihre Cluster- und Management-Switches in der Zielversion von ONTAP unterstützt werden.

Die Version von ONTAP, auf die Sie ein Upgrade durchführen können, ist möglicherweise durch Ihre Hardwarekonfiguration eingeschränkt. Wenn Ihre Hardware die ONTAP-Softwareversion, auf die Sie ein Upgrade durchführen möchten, nicht unterstützt, müssen zunächst neue Knoten zu Ihrem Cluster hinzugefügt, Ihre Daten migriert, die älteren Knoten entfernt und anschließend Ihre ONTAP-Software aktualisiert werden. Das Verfahren ist zu befolgen, um "Neue Knoten zu einem ONTAP Cluster hinzufügen".

Zu den Cluster- und Management-Switches gehören die Cluster-Netzwerk-Switches (NX-OS), die Management-Netzwerk-Switches (IOS) und die Referenz-Konfigurationsdatei (RCF). Wenn Ihre Cluster- und Management-Switches unterstützt werden, aber nicht die für die Zielversion von ONTAP erforderlichen Mindestsoftwareversionen ausführen, sollten die Switches auf unterstützte Softwareversionen aktualisiert werden.

- "NetApp Downloads: Broadcom Cluster-Switches"
- "NetApp Downloads: Cisco Ethernet-Switches"
- "NetApp Downloads: NetApp Cluster-Switches"

Falls Sie Ihre Switches aktualisieren müssen, NetApp empfiehlt, zunächst das ONTAP-Software-Upgrade durchzuführen und anschließend das Software-Upgrade für Ihre Switches vorzunehmen.

MetroCluster Konfigurationen

Bevor ONTAP aktualisiert wird, kann bei einer MetroCluster Konfiguration das "NetApp Interoperabilitätsmatrix-Tool" verwendet werden, um zu bestätigen, dass die MetroCluster IP Switches in der Zielversion von ONTAP unterstützt werden.

SAN Konfigurationen

Bevor ONTAP aktualisiert wird, kann mit dem "NetApp Interoperabilitätsmatrix-Tool" überprüft werden, ob die SAN-Konfiguration bei einem für SAN konfigurierten Cluster vollständig unterstützt wird.

Alle SAN-Komponenten, einschließlich der Ziel ONTAP Softwareversion, des Host-Betriebssystems und der Patches, der erforderlichen Host Utilities Software, der Multipathing-Software sowie der Adaptertreiber und Firmware, sollten unterstützt werden.

Konfigurationsfehler vor dem Upgrade von ONTAP mit Config Advisor erkennen

Bevor Sie ONTAP aktualisieren, kann mit dem Active IQ Config Advisor Tool auf häufige Konfigurationsfehler geprüft werden.

Active IQ Config Advisor ist ein Konfigurationsvalidierungstool für NetApp Systeme. Es kann sowohl an sicheren als auch an ungesicherten Standorten zur Datenerfassung und Systemanalyse eingesetzt werden.

Der Support für Active IQ Config Advisor ist eingeschränkt und nur online verfügbar.

Schritte

1. Melden Sie sich bei der "NetApp Support Site" Website an und wählen Sie anschließend **TOOLS** > **Tools**.
2. Unter **Active IQ Config Advisor** auf "App herunterladen" klicken.
3. Active IQ Config Advisor kann heruntergeladen, installiert und ausgeführt werden.
4. Nach dem Ausführen von Active IQ Config Advisor die Ausgabe des Tools prüfen und die bereitgestellten Empfehlungen berücksichtigen, um etwaige vom Tool festgestellte Probleme zu adressieren.

Unterstützte ONTAP Upgradepfade

Die Version von ONTAP, auf die Sie ein Upgrade durchführen können, hängt von Ihrer Hardwareplattform und der aktuell auf den Knoten Ihres Clusters ausgeführten ONTAP-Version ab.

Zur Überprüfung, ob Ihre Hardwareplattform für die Ziel-Upgrade-Version unterstützt wird, siehe "NetApp Hardware Universe". Die "NetApp Interoperabilitätsmatrix-Tool" kann verwendet werden, um "Unterstützung für Ihre Konfiguration bestätigen".

Zur Ermittlung Ihrer aktuellen ONTAP Version:

- Im System Manager auf **Cluster > Übersicht** klicken.
- Über die Befehlszeilenschnittstelle (CLI) kann der `cluster image show` Befehl verwendet werden. + Auch der `system node image show` Befehl auf dem erweiterten Berechtigungsniveau zeigt Details an.

Arten von Upgrade-Pfaden

Automatisierte unterbrechungsfreie Upgrades (ANDU) werden nach Möglichkeit empfohlen. Abhängig von Ihren aktuellen und Zielversionen erfolgt der Upgrade-Pfad **direkt**, **direkt über mehrere Zwischenstationen** oder **mehrstufig**.

- **Direkt**

  Sie können jederzeit direkt auf die nächstgelegene ONTAP-Versionsfamilie mit einem einzigen Software-Image aktualisieren. Für viele Versionen kann auch ein Software-Image installiert werden, das eine direkte Aktualisierung auf Versionen ermöglicht, die bis zu vier Versionen nach der aktuell ausgeführten Version liegen.

  Beispielsweise können Sie den direkten Upgrade-Pfad von 9.17.1 auf 9.18.1 oder von 9.15.1 auf 9.19.1 nutzen.

  Alle *direkten* Upgrade-Pfade werden für "Cluster mit gemischten Versionen" unterstützt.

- **Direkter Multi-Hop**

  Für einige automatisierte unterbrechungsfreie Upgrades (ANDU) auf nicht benachbarte Versionen ist es erforderlich, das Software-Image einer Zwischenversion sowie das der Zielversion zu installieren. Der automatisierte Upgrade-Prozess verwendet das Zwischen-Image im Hintergrund, um das Update auf die Zielversion abzuschließen.

  Wenn der Cluster beispielsweise unter Version 9.3 läuft und Sie auf 9.7 aktualisieren möchten, werden die ONTAP Installationspakete für 9.5 und 9.7 geladen, anschließend wird ANDU auf 9.7 initiiert. ONTAP

aktualisiert den Cluster automatisch zuerst auf 9.5 und dann auf 9.7. Während des Vorgangs sind mehrere Übernahme- und Rückgabevorgänge sowie damit verbundene Neustarts zu erwarten.

- **Mehrstufig**

  Wenn für Ihre nicht benachbarte Zielversion kein direkter oder direkter Multi-Hop-Pfad verfügbar ist, ist zunächst ein Upgrade auf eine unterstützte Zwischenversion erforderlich, gefolgt von einem Upgrade auf die Zielversion.

  Wenn Sie beispielsweise derzeit Version 9.14.1 verwenden und auf 9.19.1 aktualisieren möchten, müssen Sie ein mehrstufiges Upgrade durchführen: zuerst von 9.14.1 auf 9.18.1 und dann von 9.18.1 auf 9.19.1. Upgrades von früheren Versionen können drei oder mehr Stufen mit mehreren Zwischenaktualisierungen erfordern.

  ⓘ Vor Beginn von mehrstufigen Upgrades sollte sichergestellt sein, dass Ihre Zielversion auf Ihrer Hardwareplattform unterstützt wird.

Vor einem größeren Upgrade empfiehlt es sich, zunächst die neueste Patch-Version der auf Ihrem Cluster laufenden ONTAP-Version zu installieren. Dadurch wird sichergestellt, dass alle Probleme in Ihrer aktuellen ONTAP-Version vor dem Upgrade behoben sind.

Wenn auf Ihrem System beispielsweise ONTAP 9.14.1P9 läuft und Sie ein Upgrade auf 9.19.1 planen, sollten Sie zuerst auf die neueste Patch-Version von 9.14.1 aktualisieren und dann dem Upgrade-Pfad von 9.14.1 auf 9.19.1 folgen.

Weitere Informationen "Empfohlene Mindestversionen von ONTAP auf der NetApp Support Site".

Unterstützte Upgrade-Pfade

Die folgenden Upgrade-Pfade werden für automatisierte und manuelle Upgrades Ihrer ONTAP Software unterstützt. Diese Upgrade-Pfade gelten für On-Premises ONTAP und ONTAP Select. Es gibt verschiedene "Unterstützte Upgrade-Pfade für Cloud Volumes ONTAP".

ⓘ **Für ONTAP Cluster mit gemischten Versionen**: Alle *direkten* und *direkten Multi-Hop*-Upgrade -Pfade beinhalten ONTAP Versionen, die mit Clustern mit gemischten Versionen kompatibel sind. ONTAP Versionen, die in *mehrstufigen* Upgrades enthalten sind, sind nicht mit Clustern mit gemischten Versionen kompatibel. Zum Beispiel ist ein Upgrade von 9.8 auf 9.12.1 ein *direktes* Upgrade. Ein Cluster mit Knoten, auf denen 9.8 und 9.12.1 ausgeführt werden, ist ein unterstützter Cluster mit gemischten Versionen. Ein Upgrade von 9.8 auf 9.13.1 ist ein *mehrstufiges* Upgrade. Ein Cluster mit Knoten, auf denen 9.8 und 9.13.1 ausgeführt werden, ist kein unterstützter Cluster mit gemischten Versionen.

Ab ONTAP 9.8 und höher

Automatisierte und manuelle Upgrades von ONTAP 9.8 und später folgen den gleichen Upgrade-Pfaden.

▼ **Ab ONTAP 9.15.1 und höher**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.15.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.19.1	9.20.1	direkt
9.18.1	9.20.1	direkt
	9.19.1	direkt
9.17.1	9.20.1	direkt
	9.19.1	direkt
	9.18.1	direkt
9.16.1	9.20.1	direkt
	9.19.1	direkt
	9.18.1	direkt
	9.17.1	direkt
9.15.1	9.20.1	mehrstufig • 9.15.1 → 9.19.1 • 9.19.1 → 9.20.1
	9.19.1	direkt
	9.18.1	direkt
	9.17.1	direkt
	9.16.1	direkt

▼ **Ab ONTAP 9.14.1**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.14.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.14.1	9.20.1	mehrstufig • 9.14.1 → 9.18.1 • 9.18.1 → 9.20.1
	9.19.1	mehrstufig • 9.14.1 → 9.18.1 • 9.18.1 → 9.19.1
	9.18.1	direkt
	9.17.1	direkt
	9.16.1	direkt
	9.15.1	direkt

▼ **Ab ONTAP 9.13.1**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.13.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.13.1	9.20.1	mehrstufig • 9.13.1 → 9.17.1 • 9.17.1 → 9.20.1
	9.19.1	mehrstufig • 9.13.1 → 9.17.1 • 9.17.1 → 9.19.1
	9.18.1	mehrstufig • 9.13.1 → 9.17.1 • 9.17.1 → 9.18.1
	9.17.1	direkt
	9.16.1	direkt
	9.15.1	direkt
	9.14.1	direkt

▼ **Ab ONTAP 9.12.1**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.12.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.12.1	9.20.1	mehrstufig • 9.12.1 → 9.16.1 • 9.16.1 → 9.20.1
	9.19.1	mehrstufig • 9.12.1 → 9.16.1 • 9.16.1 → 9.19.1
	9.18.1	mehrstufig • 9.12.1 → 9.16.1 • 9.16.1 → 9.18.1
	9.17.1	mehrstufig • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	direkt
	9.15.1	direkt
	9.14.1	direkt
	9.13.1	direkt

▼ **Ab ONTAP 9.11.1**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.11.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.11.1	9.20.1	mehrstufig • 9.11.1 → 9.15.1 • 9.15.1 → 9.19.1 • 9.19.1 → 9.20.1
	9.19.1	mehrstufig • 9.11.1 → 9.15.1 • 9.15.1 → 9.19.1
	9.18.1	mehrstufig • 9.11.1 → 9.15.1 • 9.15.1 → 9.18.1
	9.17.1	mehrstufig • 9.11.1 → 9.15.1 • 9.15.1 → 9.17.1
	9.16.1	mehrstufig • 9.11.1 → 9.15.1 • 9.15.1 → 9.16.1
	9.15.1	direkt
	9.14.1	direkt
	9.13.1	direkt
	9.12.1	direkt

▼ **Ab ONTAP 9.10.1**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.10.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.10.1	9.20.1	mehrstufig • 9.10.1 → 9.14.1 • 9.14.1 → 9.18.1 • 9.18.1 → 9.20.1
	9.19.1	mehrstufig • 9.10.1 → 9.14.1 • 9.14.1 → 9.18.1 • 9.18.1 → 9.19.1
	9.18.1	mehrstufig • 9.10.1 → 9.14.1 • 9.14.1 → 9.18.1
	9.17.1	mehrstufig • 9.10.1 → 9.14.1 • 9.14.1 → 9.17.1
	9.16.1	mehrstufig • 9.10.1 → 9.14.1 • 9.14.1 → 9.16.1
	9.15.1	mehrstufig • 9.10.1 → 9.14.1 • 9.14.1 → 9.15.1
	9.14.1	direkt
	9.13.1	direkt
	9.12.1	direkt
	9.11.1	direkt

▼ **Ab ONTAP 9.9.1**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.9.1 für automatisierte und manuelle Upgrades unterstützt.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9.9.1	9.20.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.17.1 • 9.17.1→9.20.1
	9.19.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.17.1 • 9.17.1→9.19.1
	9.18.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.17.1 • 9.17.1→9.18.1
	9.17.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.17.1
	9.16.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.16.1
	9.15.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.15.1
	9.14.1	mehrstufig • 9.9.1→9.13.1 • 9.13.1→9.14.1
	9.13.1	direkt
	9.12.1	direkt
	9.11.1	direkt
	9.10.1	direkt

▼ **Ab ONTAP 9.8**

Die folgenden Upgrade-Pfade werden ab ONTAP 9.8 für automatisierte und manuelle Upgrades unterstützt.

Wenn Sie eines der folgenden Plattformmodelle in einer MetroCluster IP-Konfiguration von ONTAP 9.8 auf 9.10.1 oder höher aktualisieren, ist zunächst ein Upgrade auf ONTAP 9.9.1 erforderlich:

- FAS2750
- FAS500f
- AFF A220
- AFF A250

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9,8	9.20.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.20.1
	9.19.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.19.1
	9.18.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.18.1
	9.17.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.16.1
	9.15.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.15.1
	9.14.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
	9.13.1	mehrstufig • 9.8 → 9.12.1 • 9.12.1 → 9.13.1
	9.12.1	direkt
	9.11.1	direkt
	9.10.1	direkt
	9.9.1	direkt

Von ONTAP 9.7 und 9.6

Für ONTAP 9.7 und 9.6 können die automatisierten und manuellen Upgrade-Pfade je nach der Ziel-ONTAP-Version variieren.

▼ **Ab ONTAP 9.7**

Der manuelle Upgrade-Pfad von ONTAP 9.7 auf 9.10.1 und 9.11.1 unterscheidet sich vom automatisierten Upgrade-Pfad. Diese Unterschiede sind in der folgenden Tabelle aufgeführt. Für Upgrades von ONTAP 9.7 auf alle anderen ONTAP Versionen folgen automatisierte und manuelle Upgrades demselben Upgrade-Pfad.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9,7		

		mehrstufig • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
Wenn Ihre aktuelle ONTAP Release…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter oder manueller Upgrade-Pfad ist…**
	9.13.1	mehrstufig • 9.7 → 9.9.1 • 9.9.1 → 9.13.1
	9.12.1	mehrstufig • 9.7 → 9.8 • 9.8 → 9.12.1
	9.11.1	• Automatisierter Upgrade-Pfad direkter Multi-Hop (erfordert Images für 9.8 und 9.11.1) • Manueller Upgrade-Pfad mehrstufig ◦ 9.7 → 9.8 ◦ 9.8 → 9.11.1
	9.10.1	Direkter Multi-Hop (erfordert Images für 9.8 und 9.10.1P1 oder spätere P Release)
	9.9.1	direkt
	9,8	direkt

▼ **Ab ONTAP 9.6**

Der manuelle Upgrade-Pfad von ONTAP 9.6 auf 9.10.1 unterscheidet sich vom automatisierten Upgrade-Pfad. Die Abweichung ist in der untenstehenden Tabelle aufgeführt. Für Upgrades von ONTAP 9.6 auf alle anderen ONTAP Versionen folgen automatisierte und manuelle Upgrades demselben Upgrade-Pfad.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter oder manueller Upgrade-Pfad ist…
9,6		

		mehrstufig • 9.6 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
Wenn Ihre aktuelle ONTAP Release…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter oder manueller Upgrade-Pfad ist…**
	9.13.1	mehrstufig • 9.6 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.13.1
	9.12.1	mehrstufig • 9.6 → 9.8 • 9.8 → 9.12.1
	9.11.1	mehrstufig • 9.6 → 9.8 • 9.8 → 9.11.1
	9.10.1	• Automatisierter Upgrade-Pfad: Direkter Multi-Hop (erfordert Images für 9.8 und 9.10.1P1 oder spätere P Release) • Manueller Upgrade-Pfad: mehrstufig ◦ 9.6 → 9.8 ◦ 9.8 → 9.10.1
	9.9.1	mehrstufig • 9.6 → 9.8 • 9.8 → 9.9.1
	9,8	direkt
	9,7	direkt

Ab ONTAP 9.5

Die Upgrade-Pfade von ONTAP 9.5 unterscheiden sich je nachdem, ob Sie ein automatisiertes oder ein manuelles Upgrade durchführen.

▼ Automatisierte Upgrade-Pfade

Verwenden Sie die folgenden Upgrade-Pfade für automatisierte Upgrades von ONTAP 9.5.

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
9,5		

		• 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.13.1 • 9.13.1 → 9.15.1
Wenn Ihre aktuelle ONTAP Release…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter Upgrade-Pfad ist…**
	9.14.1	mehrstufig • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.13.1 • 9.13.1 → 9.14.1
	9.13.1	mehrstufig • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.13.1
	9.12.1	mehrstufig • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.12.1
	9.11.1	mehrstufig • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.11.1
	9.10.1	mehrstufig • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.10.1
	9.9.1	Direkter Multi-Hop (erfordert Images für 9.7 und 9.9.1)
	9,8	mehrstufig • 9.5 → 9.7 • 9.7 → 9.8
	9,7	direkt
	9,6	direkt

▼ **Manuelle Upgrade-Pfade**

Verwenden Sie die folgenden Upgrade-Pfade für manuelle Upgrades von ONTAP 9.5

Wenn Ihre aktuelle ONTAP Release…	Und Ihre angestrebte ONTAP release ist…	Ihr manueller Upgrade-Pfad ist…
9,5		

		• 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.13.1 • 9.13.1 → 9.15.1
Wenn Ihre aktuelle ONTAP Release…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr manueller Upgrade-Pfad ist…**
	9.14.1	mehrstufig • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.13.1 • 9.13.1 → 9.14.1
	9.13.1	mehrstufig • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.13.1
	9.12.1	mehrstufig • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
	9.11.1	mehrstufig • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	mehrstufig • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
	9.9.1	mehrstufig • 9.5 → 9.7 • 9.7 → 9.9.1
	9,8	mehrstufig • 9.5 → 9.7 • 9.7 → 9.8
	9,7	direkt
	9,6	direkt

Von ONTAP 9.4-9.0

Die Upgrade-Pfade von ONTAP 9.4, 9.3, 9.2, 9.1 und 9.0 unterscheiden sich je nachdem, ob Sie ein automatisiertes oder ein manuelles Upgrade durchführen.

▼ **Automatisierte Upgrade-Pfade**

Nutzen Sie die folgenden Upgrade-Pfade für automatisierte Upgrades von ONTAP 9.4, 9.3, 9.2, 9.1 und 9.0.

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
9,4		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

		• 9.4 → 9.5 • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1) • 9.9.1 → 9.10.1
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter Upgrade-Pfad ist…**
	9.9.1	mehrstufig • 9.4 → 9.5 • 9.5 → 9.9.1 (direkter Multi-Hop, erfordert Images für 9.7 und 9.9.1)
	9,8	mehrstufig • 9.4 → 9.5 • 9.5 → 9.8 (direkter Multi-Hop, erfordert Images für 9.7 und 9.8)
	9,7	mehrstufig • 9.4 → 9.5 • 9.5 → 9.7
	9,6	mehrstufig • 9.4 → 9.5 • 9.5 → 9.6
	9,5	direkt

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
9,3		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

		• 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7)
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter Upgrade-Pfad ist…**
		• 9.7 → 9.10.1 (direkter Multi-Hop, erfordert Images für 9.8 und 9.10.1)
	9.9.1	mehrstufig • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.9.1
	9,8	mehrstufig • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.8
	9,7	Direkter Multi-Hop (erfordert Images für 9.5 und 9.7)
	9,6	mehrstufig • 9.3 → 9.5 • 9.5 → 9.6
	9,5	direkt
	9,4	nicht verfügbar

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
9,2		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

		• 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter Upgrade-Pfad ist…**
	9.11.1	mehrstufig • 9.2 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	mehrstufig • 9.2 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.10.1 (direkter Multi-Hop, erfordert Images für 9.8 und 9.10.1)
	9.9.1	mehrstufig • 9.2 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.9.1
	9,8	mehrstufig • 9.2 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.8
	9,7	mehrstufig • 9.2 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7)
	9,6	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9,5	mehrstufig • 9.3 → 9.5 • 9.5 → 9.6
	9,4	nicht verfügbar
	9,3	direkt

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
9,1		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
		• 9.1 → 9.3 • 9.3 → 9.5
	9,4	nicht verfügbar
	9,5	direkt
	9,2	nicht verfügbar

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…
9,0		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr automatisierter Upgrade-Pfad ist…

		• 9.1 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7) • 9.7 → 9.8
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr automatisierter Upgrade-Pfad ist…**
	9,7	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.7 (direkter Multi-Hop, erfordert Images für 9.5 und 9.7)
	9,6	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9,5	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9,4	nicht verfügbar
	9,3	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3
	9,2	nicht verfügbar
	9,1	direkt

▼ **Manuelle Upgrade-Pfade**

Verwenden Sie die folgenden Upgrade-Pfade für manuelle Upgrades von ONTAP 9.4, 9.3, 9.2, 9.1 und 9.0.

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…
9,4		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

		• 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr ANDU Upgrade-Pfad ist…** • 9.9.1 → 9.10.1
	9.9.1	mehrstufig • 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9,8	mehrstufig • 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9,7	mehrstufig • 9.4 → 9.5 • 9.5 → 9.7
	9,6	mehrstufig • 9.4 → 9.5 • 9.5 → 9.6
	9,5	direkt

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…
9,3		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

		• 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr ANDU Upgrade-Pfad ist…**
	9.9.1	mehrstufig • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9,8	mehrstufig • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9,7	mehrstufig • 9.3 → 9.5 • 9.5 → 9.7
	9,6	mehrstufig • 9.3 → 9.5 • 9.5 → 9.6
	9,5	direkt
	9,4	nicht verfügbar

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…
9,2		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

		• 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr ANDU Upgrade-Pfad ist…**
	9.10.1	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
	9.9.1	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9,8	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9,7	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9,6	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9,5	mehrstufig • 9.2 → 9.3 • 9.3 → 9.5
	9,4	nicht verfügbar
	9,3	direkt

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…
9,1		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

	9,5	mehrstufig • 9.1 → 9.3 • 9.3 → 9.5
Wenn Ihre aktuelle ONTAP Release ist…	**Und Ihre angestrebte ONTAP release ist…**	**Ihr ANDU Upgrade-Pfad ist…**
	9,4	nicht verfügbar
	9,3	direkt
	9,2	nicht verfügbar

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…
9,0		

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Ihr ANDU Upgrade-Pfad ist…
		• 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9,8	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9,7	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9,6	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9,5	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9,4	nicht verfügbar
	9,3	mehrstufig • 9.0 → 9.1 • 9.1 → 9.3
	9,2	nicht verfügbar
	9,1	direkt

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "cluster image show"
- "system node image show"

Die LIF-Failover-Konfiguration des ONTAP-Clusters sollte vor einem Upgrade überprüft werden.

Bevor ONTAP aktualisiert wird, muss überprüft werden, ob die Failover-Richtlinien und

Failover-Gruppen des Clusters korrekt konfiguriert sind.

Während des Upgrade-Prozesses werden LIFs entsprechend der Upgrade-Methode migriert. Abhängig von der Upgrade-Methode wird die LIF-Failover-Richtlinie möglicherweise verwendet oder auch nicht.

Bei Clustern mit 8 oder mehr Knoten erfolgt das automatische Upgrade mit der Batch-Methode. Die Batch-Upgrade-Methode beinhaltet die Aufteilung des Clusters in mehrere Upgrade-Batches, die Aktualisierung der Knoten des ersten Batches, die Aktualisierung ihrer Hochverfügbarkeitspartner (HA-Partner) und anschließend die Wiederholung dieses Prozesses für die verbleibenden Batches. In ONTAP 9.7 und früher, wenn die Batch-Methode verwendet wird, werden LIFs auf den HA-Partner des Knotens migriert, der aktualisiert wird. In ONTAP 9.8 und später, wenn die Batch-Methode verwendet wird, werden LIFs auf die andere Batch-Gruppe migriert.

Bei Clustern mit weniger als 8 Knoten wird das automatische Upgrade mit der Rolling-Methode durchgeführt. Die Rolling-Upgrade-Methode umfasst das Initiieren eines Failover-Vorgangs auf jedem Knoten eines HA-Paares, das Aktualisieren des übergebenen Knotens, das Initiieren der Rückgabe und das anschließende Wiederholen dieses Prozesses für jedes HA-Paar im Cluster. Wenn die Rolling-Methode verwendet wird, werden LIFs entsprechend der LIF-Failover-Richtlinie auf den Failover-Zielknoten migriert.

Schritte

1. Die Failover-Richtlinie für jede Daten-LIF wird angezeigt:

Wenn Ihre ONTAP Version …	Verwenden Sie diesen Befehl
9.6 oder höher	`network interface show -service-policy *data* -failover`
9.5 oder früher	`network interface show -role data -failover`

Dieses Beispiel zeigt die Standard-Failover-Konfiguration für ein Zwei-Node-Cluster mit zwei Daten-LIFs:

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
```

```
                                                node1:e0f, node0:e0b,
                                                node0:e0c, node0:e0d,
                                                node0:e0e, node0:e0f
```

Das Feld **Failover Targets** zeigt eine priorisierte Liste der Failover-Ziele für jede LIF. Wenn beispielsweise 'lif0' von seinem Home-Port (e0b auf node0) ausfällt, wird zunächst versucht, auf Port e0c auf node0 umzuschalten. Wenn lif0 nicht auf e0c umschalten kann, wird anschließend versucht, auf Port e0d auf node0 umzuschalten, und so weiter.

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Wenn die Failover-Richtlinie für LIFs außer SAN LIFs auf **deaktiviert** gesetzt ist, kann das Failover mit dem `network interface modify` Befehl aktiviert werden.

   Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Für jede LIF ist zu prüfen, ob das Feld **Failover Targets** Datenports von einem anderen Node enthält, die während des Upgrades des Home-Nodes der LIF aktiv bleiben.

   Mit dem `network interface failover-groups modify` Befehl lässt sich ein Failover-Ziel zur Failover-Gruppe hinzufügen.

   Beispiel

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

Verwandte Informationen

- "Netzwerk- und LIF-Management"
- "Netzwerkschnittstelle"
- "Netzwerkschnittstelle Failover-Gruppen ändern"

Anforderungen an die SVM Routing-Konfiguration vor einem ONTAP Upgrade

Um Unterbrechungen zu vermeiden, sollte vor dem Upgrade der ONTAP Software sichergestellt werden, dass die Standardroute der SVM jede Netzwerkadresse erreichen kann, die nicht durch eine spezifischere Route erreichbar ist. Es gilt als Best Practice, eine Standardroute für eine SVM zu konfigurieren. Weitere Informationen finden sich unter "SU134: Der Netzwerkzugriff kann durch eine fehlerhafte Routing-Konfiguration in ONTAP beeinträchtigt werden".

Die Routingtabelle einer SVM legt den Netzwerkpfad fest, den die SVM zur Kommunikation mit einem Ziel verwendet. Es ist wichtig zu verstehen, wie Routingtabellen funktionieren, damit Netzwerkprobleme bereits im Vorfeld vermieden werden können.

Die Routing-Regeln lauten wie folgt:

- ONTAP leitet den Datenverkehr über die spezifischste verfügbare Route.
- ONTAP leitet den Datenverkehr als letzte Möglichkeit über eine Standard-Gateway-Route (mit 0 Bits

Netzmaske), wenn spezifischere Routen nicht verfügbar sind.

Bei Routen mit gleichem Ziel, gleicher Netzmaske und gleicher Metrik kann nicht garantiert werden, dass das System nach einem Neustart oder einem Upgrade dieselbe Route verwendet. Dies kann insbesondere dann problematisch sein, wenn mehrere Standardrouten konfiguriert wurden.

Besondere Überlegungen

Spezielle Konfigurationsprüfungen vor einem ONTAP Upgrade

Bei bestimmten Clusterkonfigurationen sind vor einem ONTAP Software-Upgrade spezifische Maßnahmen erforderlich. Wenn beispielsweise eine SAN-Konfiguration vorhanden ist, sollte vor dem Upgrade überprüft werden, dass jeder Host mit der korrekten Anzahl direkter und indirekter Pfade konfiguriert ist.

Anhand der folgenden Tabelle lässt sich feststellen, welche zusätzlichen Schritte gegebenenfalls erforderlich sind.

Bevor Sie ONTAP aktualisieren, sollten Sie sich folgende Fragen stellen…	**Wenn Ihre Antwort ja lautet, ist Folgendes zu tun…**
Befindet sich mein Cluster derzeit in einem gemischten Versionszustand?	Anforderungen für gemischte Versionen prüfen
Habe ich eine MetroCluster Konfiguration?	Spezifische Upgrade-Anforderungen für MetroCluster Konfigurationen prüfen
Liegt eine SAN Konfiguration vor?	Die SAN Host-Konfiguration überprüfen
Sind in meinem Cluster SnapMirror-Beziehungen definiert?	"Kompatibilität der ONTAP Versionen für SnapMirror Beziehungen überprüfen"
Sind DP-Typ-SnapMirror-Beziehungen definiert und erfolgt ein Upgrade auf ONTAP 9.12.1 oder höher?	"Vorhandene DP-Beziehungen in XDP konvertieren"
Wird SnapMirror S3 verwendet und erfolgt ein Upgrade auf ONTAP 9.12.1 oder höher?	"Lizenzierung für SnapMirror S3-Konfigurationen überprüfen"
Sind Langzeit-Snapshots zur Aufbewahrung auf dem mittleren Volume einer Kaskade aktiviert?	"Langzeitaufbewahrungs-Snapshots in mittleren Volumes von Kaskadentopologien deaktivieren"
Wird NetApp Storage Encryption mit externen Schlüsselverwaltungsservern verwendet?	Alle bestehenden Verbindungen zum Schlüsselverwaltungsserver löschen
Sind Netzgruppen in die SVMs geladen?	Es sollte sichergestellt sein, dass die netgroup-Datei auf jedem Knoten vorhanden ist.
Habe ich eine SVM erstellt und führe ich ein Upgrade von ONTAP 9.12.1 oder einer früheren Version auf eine neuere Version durch?	Einen expliziten Wert für die Option v4.2-xattrs zuweisen
Habe ich LDAP-Clients, die SSLv3 verwenden?	LDAP-Clients für die Verwendung von TLS konfigurieren
Werden sitzungsorientierte Protokolle verwendet?	Überprüfung der negativen Auswirkungen von sitzungsorientierten Protokollen

Bevor Sie ONTAP aktualisieren, sollten Sie sich folgende Fragen stellen…	Wenn Ihre Antwort ja lautet, ist Folgendes zu tun…
Ist der SSL-FIPS-Modus auf einem Cluster aktiviert, auf dem sich Administratorkonten mit einem öffentlichen SSH-Schlüssel authentifizieren?	Unterstützung des SSH-Hostschlüsselalgorithmus überprüfen
Liegt bei meinem Autonomous Ransomware Protection eine aktive Warnung vor?	Auf Warnungen des autonomen Ransomware-Schutzes bezüglich ungewöhnlicher Aktivität reagieren

ONTAP Versionskompatibilität für Cluster mit gemischten Versionen

In einem ONTAP Cluster mit gemischten Versionen laufen auf den Knoten für kurze Zeit zwei verschiedene Hauptversionen von ONTAP. Ein Cluster mit Knoten, auf denen ONTAP 9.8 und 9.12.1 oder ONTAP 9.9.1 und 9.13.1 ausgeführt wird, ist beispielsweise ein Cluster mit gemischten Versionen. Cluster mit Knoten, auf denen innerhalb derselben Version unterschiedliche Patch-Level wie ONTAP 9.9.1P1 und 9.9.1P5 ausgeführt werden, sind keine Cluster mit gemischten Versionen.

Cluster mit gemischten Versionen werden für Cloud Volumes ONTAP nicht unterstützt.

NetApp unterstützt ONTAP Cluster mit gemischten Versionen für begrenzte Zeiträume und in bestimmten Szenarien.

Im Folgenden sind die häufigsten Szenarien, in denen sich ein ONTAP Cluster in einem gemischten Versionszustand befindet:

- ONTAP Software-Upgrades in großen Clustern

  Die Aktualisierung aller Knoten in einem großen Cluster kann mehrere Tage oder Wochen dauern. Der Cluster befindet sich in einem Zustand mit gemischten Versionen, bis alle Knoten aktualisiert sind.

- ONTAP Software-Upgrades sind erforderlich, wenn geplant ist, einem Cluster neue Knoten hinzuzufügen.

  Sie können Ihrem Cluster neue Knoten hinzufügen, um dessen Kapazität zu erweitern, oder Sie können neue Knoten im Zuge eines vollständigen Austauschs Ihrer Controller hinzufügen. In beiden Fällen kann es erforderlich sein, einen gemischten Versionszustand zu aktivieren, um die Migration Ihrer Daten von den bestehenden Controllern auf die neuen Knoten in Ihrem neuen System zu ermöglichen.

Für einen optimalen Clusterbetrieb sollte die Zeitspanne, in der sich der Cluster in einem gemischten Versionszustand befindet, so kurz wie möglich sein. Die maximale Zeitspanne, in der ein Cluster in einem gemischten Versionszustand unterstützt werden kann, hängt von der niedrigsten ONTAP Version im Cluster ab.

Wenn die niedrigste Version von ONTAP im Cluster mit gemischten Versionen ausgeführt wird, …	Anschließend ist es möglich, sich maximal für… im gemischten Versionszustand zu befinden.
ONTAP 9.8 oder höher	90 Tage
ONTAP 9.7 oder früher	7 Tage

Solange sich der Cluster in einem gemischten Versionszustand befindet, sollten keine Befehle eingegeben

werden, die den Clusterbetrieb oder die Konfiguration verändern, außer jenen, die für das Upgrade oder die Datenmigration erforderlich sind. Beispielsweise sollten Aktivitäten wie (aber nicht beschränkt auf) LIF-Migration, geplante Storage-Failover-Operationen oder das Erstellen oder Löschen großer Mengen von Objekten erst nach Abschluss des Upgrades und der Datenmigration durchgeführt werden.

Unterstützung für Cluster mit gemischten Versionen bei ONTAP Software-Upgrades

Sie können einen gemischten Versionszustand mit jeder ONTAP Version erreichen, die für ein direktes Upgrade von Ihrer niedrigsten aktuellen Version unterstützt wird. Wenn Sie beispielsweise ONTAP 9.11.1 verwenden, können Sie einen gemischten Versionszustand mit Knoten erreichen, auf denen ONTAP 9.15.1 ausgeführt wird. Ein gemischter Versionszustand ist nicht möglich, wenn Knoten auf ONTAP 9.11.1 und ONTAP 9.16.1 ausgeführt werden. ONTAP 9.16.1 wird für ein direktes Upgrade von ONTAP 9.11.1 nicht unterstützt.

ONTAP Patch-(P)-Versionen haben keinen Einfluss auf die Kompatibilität bei Clustern mit gemischten Versionen. Beispielsweise gilt bei Verwendung von ONTAP 9.11.1P6 als aktuelle ONTAP Version für die Kompatibilität in Clustern mit gemischten Versionen ONTAP 9.11.1. Oder bei Verwendung von ONTAP 9.12.1 und einem Upgrade auf ONTAP 9.15.1P2 ist die Ziel-ONTAP Version für die Kompatibilität in Clustern mit gemischten Versionen ONTAP 9.15.1.

Um auf eine ONTAP Version zu aktualisieren, die für ein direktes Upgrade von Ihrer aktuellen Version nicht unterstützt wird, ist ein mehrstufiges Upgrade erforderlich. Bei einem mehrstufigen Upgrade wechseln Sie zunächst in einen gemischten Versionszustand mit der höchsten Version, die für ein direktes Upgrade von Ihrer aktuellen Version unterstützt wird. Dieses Upgrade wird abgeschlossen, danach erfolgt ein separates Upgrade auf Ihre Zielversion. Beispielsweise gilt: Wenn Ihre niedrigste aktuelle Version ONTAP 9.10.1 ist und ein Upgrade auf ONTAP 9.16.1 gewünscht ist, wechseln Sie zunächst in einen gemischten Versionszustand, um alle Ihre Knoten auf ONTAP 9.14.1 zu aktualisieren, danach erfolgt ein separates Upgrade von ONTAP 9.14.1 auf ONTAP 9.16.1. Weitere Informationen zu "mehrstufige Upgrades" und "Unterstützte Upgrade-Pfade".

Ein Cluster mit gemischten Versionen kann nur zwei Hauptversionen von ONTAP enthalten. Beispielsweise kann ein gemischter Versions-Cluster Knoten mit ONTAP 9.13.1 und 9.15.1 oder Knoten mit ONTAP 9.13.1 und 9.16.1 enthalten. Ein gemischter Versions-Cluster mit Knoten, auf denen ONTAP 9.13.1, 9.15.1 und 9.16.1 ausgeführt werden, ist nicht zulässig.

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Gemischter Versionsstatus für das Upgrade ist…
9.17.1	9.18.1	Unterstützt
9.16.1	9.18.1	Unterstützt
	9.17.1	Unterstützt
9.15.1	9.18.1	Unterstützt
	9.17.1	Unterstützt
	9.16.1	Unterstützt
9.14.1	9.18.1	Unterstützt
	9.17.1	Unterstützt
	9.16.1	Unterstützt
	9.15.1	Unterstützt

Wenn Ihre aktuelle ONTAP Release ist…	Und Ihre angestrebte ONTAP release ist…	Gemischter Versionsstatus für das Upgrade ist…
9.13.1	9.18.1	Nicht unterstützt
	9.17.1	Unterstützt
	9.16.1	Unterstützt
	9.15.1	Unterstützt
	9.14.1	Unterstützt
9.12.1	9.17.1 oder höher	Nicht unterstützt
	9.16.1	Unterstützt
	9.15.1	Unterstützt
	9.14.1	Unterstützt
	9.13.1	Unterstützt
9.11.1	9.16.1 oder höher	Nicht unterstützt
	9.15.1	Unterstützt
	9.14.1	Unterstützt
	9.13.1	Unterstützt
	9.12.1	Unterstützt
9.10.1	9.15.1 oder höher	Nicht unterstützt
	9.14.1	Unterstützt
	9.13.1	Unterstützt
	9.12.1	Unterstützt
	9.11.1	Unterstützt
9.9.1	9.14.1 oder höher	Nicht unterstützt
	9.13.1	Unterstützt
	9.12.1	Unterstützt
	9.11.1	Unterstützt
	9.10.1	Unterstützt
9,8	9.13.1 oder später	Nicht unterstützt
	9.12.1	Unterstützt
	9.11.1	Unterstützt
	9.10.1	Unterstützt
	9.9.1	Unterstützt

Hinzufügen neuer Knoten zu einem ONTAP Cluster

Wenn Sie planen, Ihrem Cluster neue Knoten hinzuzufügen und diese Knoten eine Mindestversion von ONTAP

benötigen, die neuer ist als die derzeit im Cluster ausgeführte Version, müssen auf den vorhandenen Knoten in Ihrem Cluster alle unterstützten Software-Upgrades durchgeführt werden, bevor die neuen Knoten hinzugefügt werden. Idealerweise werden alle vorhandenen Knoten auf die von den hinzuzufügenden Knoten benötigte Mindestversion von ONTAP aktualisiert. Sollte dies jedoch nicht möglich sein, weil einige Ihrer vorhandenen Knoten die neuere Version von ONTAP nicht unterstützen, ist im Rahmen des Upgrade-Prozesses für einen begrenzten Zeitraum ein gemischter Versionszustand erforderlich.

Schritte

1. "Upgrade"Die Knoten, die die von Ihren neuen Controllern benötigte minimale ONTAP-Version nicht unterstützen, werden auf die höchste ONTAP-Version aktualisiert, die sie unterstützen.

   Wenn Sie beispielsweise ein FAS8080 mit ONTAP 9.5 betreiben und eine neue C-Series Plattform mit ONTAP 9.12.1 hinzufügen, sollte Ihr FAS8080 auf ONTAP 9.8 aktualisiert werden (das ist die höchste ONTAP Version, die unterstützt wird).

2. "Die neuen Knoten zum Cluster hinzufügen".
3. "Daten migrieren"von den aus dem Cluster entfernten Knoten zu den neu hinzugefügten Knoten.
4. "Die nicht unterstützten Knoten aus dem Cluster entfernen".
5. "Upgrade"den Cluster auf die gleiche ONTAP Version und den gleichen Patch-Level, der auf den neuen Knoten läuft, oder auf "neueste empfohlene Patch-Version"die ONTAP Version, die auf den neuen Knoten läuft.
6. Es sollte sichergestellt sein, dass auf allen Knoten die gleiche ONTAP Version ausgeführt wird.

   a. Die auf dem Cluster ausgeführte ONTAP-Version anzeigen:

   ```
   version
   ```

   b. Die auf jedem Knoten des Clusters ausgeführte ONTAP Version anzeigen:

   ```
   version *
   ```

   Wenn es einen Unterschied zwischen der in der Ausgabe für die `version *` (Cluster) und `version` (einzelne Nodes) gemeldeten ONTAP-Version gibt, sollten alle Nodes auf dieselbe ONTAP- und Patch-Version aktualisiert werden, indem ein "Cluster-Image-Update" ausgeführt wird.

Einzelheiten zur Datenmigration sind hier zu finden:

- "Ein Aggregat erstellen und Volumes auf die neuen Knoten verschieben"
- "Einrichten neuer iSCSI-Verbindungen für SAN Volume-Verschiebungen"
- "Verschieben von Volumes mit Verschlüsselung"

ONTAP Upgrade-Anforderungen für MetroCluster Konfigurationen

Bevor Sie Ihre ONTAP Software in einer MetroCluster Konfiguration aktualisieren, müssen Ihre Cluster bestimmte Anforderungen erfüllen.

- Beide Cluster müssen mit derselben Version von ONTAP ausgeführt werden.

  Die ONTAP Version lässt sich mit dem Befehl version überprüfen.

- Bei einem größeren ONTAP Upgrade muss sich die MetroCluster Konfiguration im Normalmodus befinden.
- Bei einem Patch-ONTAP-Upgrade kann sich die MetroCluster Konfiguration entweder im Normalmodus oder im Switchover-Modus befinden.
- Bei allen Konfigurationen außer Zwei-Knoten-Clustern ist ein unterbrechungsfreies Upgrade beider Cluster gleichzeitig möglich.

  Für ein unterbrechungsfreies Upgrade in Zwei-Knoten-Clustern müssen die Cluster jeweils Knoten für Knoten aktualisiert werden.

- Die Aggregate in beiden Clustern dürfen sich nicht im RAID-Resynchronisierungsstatus befinden.

  Während der MetroCluster-Heilung werden die gespiegelten Aggregate resynchronisiert. Ob sich die MetroCluster Konfiguration in diesem Zustand befindet, lässt sich mit dem `storage aggregate plex show -in-progress true` Befehl überprüfen. Werden Aggregate synchronisiert, sollte ein Upgrade erst nach Abschluss der Resynchronisierung erfolgen.

  Weitere Informationen zu `storage aggregate plex show` finden sich in der "ONTAP-Befehlsreferenz".

- Die ausgehandelten Umschaltungsvorgänge schlagen während des laufenden Upgrades fehl.

  Um Probleme bei Upgrade- oder Rücksetzvorgängen zu vermeiden, darf während eines Upgrade- oder Rücksetzvorgangs kein ungeplanter Switchover durchgeführt werden, es sei denn, auf allen Knoten beider Cluster läuft die gleiche Version von ONTAP.

Konfigurationsanforderungen für den normalen Betrieb von MetroCluster

- Die Quell-SVM-LIFs müssen aktiv sein und sich auf ihren Home-Nodes befinden.

  Die Daten-LIFs für die Ziel-SVMs müssen weder aktiv sein noch sich auf ihren Heimatknoten befinden.

- Alle Aggregate am lokalen Standort müssen online sein.
- Alle Root- und Datenvolumes, die den SVMs des lokalen Clusters gehören, müssen online sein.

Konfigurationsanforderungen für MetroCluster Switchover

- Alle LIFs müssen aktiv sein und sich auf ihren Home-Nodes befinden.
- Alle Aggregate müssen online sein, mit Ausnahme der Root Aggregate am DR-Standort.

  Die Root-Aggregate am DR-Standort sind während bestimmter Phasen des Switchover offline.

- Alle Volumes müssen online sein.

Verwandte Informationen

"Überprüfung des Netzwerk- und Speicherstatus für MetroCluster Konfigurationen"

Die SAN-Hostkonfiguration sollte vor einem ONTAP Upgrade überprüft werden.

Das Upgrade von ONTAP in einer SAN-Umgebung ändert, welche Pfade direkt sind. Vor dem Upgrade eines SAN-Clusters sollte überprüft werden, ob jeder Host mit der korrekten Anzahl direkter und indirekter Pfade konfiguriert ist und ob jeder Host mit den richtigen LIFs verbunden ist.

Schritte

1. Auf jedem Host sollte überprüft werden, ob eine ausreichende Anzahl direkter und indirekter Pfade konfiguriert ist und ob jeder Pfad aktiv ist.

   Jeder Host muss einen Pfad zu jedem Node im Cluster haben.

2. Es sollte sichergestellt sein, dass jeder Host mit einem LIF auf jedem Knoten verbunden ist.

   Sie sollten die Liste der Initiatoren nach dem Upgrade zum Vergleich protokollieren. Bei Verwendung von ONTAP 9.11.1 oder höher empfiehlt sich System Manager zur Anzeige des Verbindungsstatus, da dieser eine deutlich übersichtlichere Darstellung als die CLI bietet.

   System Manager

   a. Im System Manager auf **Hosts > SAN Initiatorgruppen** klicken.

      Auf der Seite wird eine Liste der Initiatorgruppen (Initiatorgruppen) angezeigt. Wenn die Liste lang ist, können zusätzliche Seiten der Liste angezeigt werden, indem auf die Seitenzahlen in der unteren rechten Ecke der Seite geklickt wird.

      Die Spalten zeigen verschiedene Informationen zu den Initiatorgruppen an. Ab Version 9.11.1 wird auch der Verbindungsstatus der Initiatorgruppe angezeigt. Durch das Überfahren der Statusmeldungen mit dem Mauszeiger werden Details angezeigt.

   CLI

   ◦ Liste der iSCSI-Initiatoren:

   ```
   iscsi initiator show -fields igroup,initiator-name,tpgroup
   ```

   ◦ Liste der FC-Initiatoren:

   ```
   fcp initiator show -fields igroup,wwpn,lif
   ```

Kompatible ONTAP Versionen für SnapMirror Beziehungen

Die Quell- und Zielvolumes müssen kompatible ONTAP Versionen ausführen, bevor eine SnapMirror Datenschutzbeziehung erstellt wird. Vor einem ONTAP Upgrade sollte überprüft werden, ob die aktuelle ONTAP Version mit der Ziel-ONTAP Version für SnapMirror Beziehungen kompatibel ist.

Vereinheitlichte Replikationsbeziehungen

Für SnapMirror Beziehungen vom Typ “XDP”, bei Verwendung von lokalen oder Cloud Volumes ONTAP Versionen:

Ab ONTAP 9.9.0:

- ONTAP 9.x.0 Releases sind ausschließlich für die Cloud verfügbar und unterstützen Cloud Volumes ONTAP Systeme. Das Sternchen (*) nach der Versionsnummer kennzeichnet eine reine Cloud-Version.

ONTAP 9.16.0 bildet eine Ausnahme von der Cloud-only-Regel, da es Unterstützung für "ASA r2-Systeme" bietet. Das Pluszeichen (+) nach der Release-Version zeigt sowohl eine ASA r2- als auch eine Cloud-unterstützte Version an. ASA r2-Systeme unterstützen SnapMirror-Beziehungen nur zu anderen ASA r2-Systemen.

- ONTAP 9.x.1 Releases sind allgemeine Releases und unterstützen sowohl On-Premises als auch Cloud Volumes ONTAP Systeme.

Wenn "fortschrittlicher Kapazitätsausgleich" auf Volumes in Clustern aktiviert ist, auf denen ONTAP 9.16.1 oder höher ausgeführt wird, werden SnapMirror-Übertragungen zu Clustern, auf denen ONTAP Versionen vor ONTAP 9.16.1 ausgeführt werden, nicht unterstützt.

Interoperabilität ist bidirektional.

Interoperabilität für ONTAP Version 9.5 und höher

ONTAP Version …	**Ist mit diesen früheren ONTAP Versionen kompatibel…**																						
	9.19.1	9.18.1	9.17.1	9.16.1	9.16.0+	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9,8	9,7	9,6	9,5
9.19.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.18.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.17.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.0+	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.15.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein
9.15.0*	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein
9.14.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein

ONTAP Version…	Ist mit diesen früheren ONTAP Versionen kompatibel…																							
9.14.0*	Nein	Nein	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein
9.13.1	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.13.0*	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein
9.12.1	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.12.0*	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	Nein	Nein
9.11.1	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein
9.11.0*	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein
9.10.1	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.10.0*	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**
9.9.1	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.9.0*	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,8	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,7	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,6	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**

SnapMirror synchron Beziehungen

SnapMirror synchron wird für ONTAP Cloud Instanzen nicht unterstützt.

ONTAP Version…	Ist mit diesen früheren ONTAP Versionen kompatibel…														
	9.19.1	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.19.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.18.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.17.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein
9.15.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein
9.14.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.13.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.12.1	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.11.1	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.10.1	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.9.1	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9,8	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein
9,7	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,6	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**
9,5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**

SnapMirror SVM-Beziehungen zur Katastrophenwiederherstellung

- Diese Matrix gilt für die SVM Datenmobilität Migrationsfunktion ab ONTAP 9.10.1.
- Sie können SVM DR verwenden, um eine SVM zu migrieren, die die für "SVM Migration (SVM Datenmobilität)" angegebenen Einschränkungen nicht erfüllt.
- In beiden Fällen dürfen maximal 2 **neuere** Hauptversionen von ONTAP zwischen Quell- und Ziel-Cluster liegen, wobei die Zielversion die gleiche oder eine neuere ONTAP Version als

die Quellversion sein muss.

Für SVM-Notfallwiederherstellungsdaten und SVM-Schutz:

Die SVM-Notfallwiederherstellung wird nur zwischen Clustern unterstützt, auf denen dieselbe Version von ONTAP ausgeführt wird. **Versionsunabhängigkeit wird für die SVM-Replikation nicht unterstützt**.

Für die SVM-Notfallwiederherstellung bei der SVM-Migration:

- Die Replikation wird in eine Richtung unterstützt, von einer früheren Version von ONTAP auf dem Quell-Cluster zur gleichen oder einer späteren Version von ONTAP auf dem Ziel-Cluster.
- Die ONTAP Version auf dem Ziel-Cluster darf höchstens zwei Hauptversionen der lokalen Version oder zwei Hauptversionen der Cloud-Version neuer sein (beginnend mit ONTAP 9.9.0), wie in der folgenden Tabelle gezeigt.
  - Die Replikation wird für Anwendungsfälle des langfristigen Datenschutzes nicht unterstützt.

Das Sternchen (*) nach der Versionsnummer kennzeichnet eine reine Cloud-Version.

Zur Ermittlung der Unterstützung befindet sich die Quellversion in der linken Tabellenspalte, die Zielversion in der obersten Zeile (DR/Migration für gleichartige Versionen und nur Migration für neuere Versionen).

Wenn Sie ONTAP 9.10.1 oder höher verwenden, kann die "SVM Datenmobilität" Funktion anstelle von SVM DR verwendet werden, um SVMs von einem Cluster auf einen anderen zu migrieren.

Quelle	**Ziel**																				
	9,5	9,6	9,7	9,8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1	9.19.1
9,5	DR/Migration nur	nur Migration	nur Migration																				
9,6		DR/Migration nur	nur Migration	nur Migration																			
9,7			DR/Migration nur	nur Migration	nur Migration																		

Quelle	Ziel																						
9,8				DR/Migration nur	Migration	Migration		Migration															
9.9.0*					DR/Migration	Migration	Migration	Migration	Migration	Migration													
9.9.1						DR/Migration	Migration	Migration	Migration	Migration													
9.10.0*							DR/Migration	Migration	Migration	Migration	Migration												
9.10.1								DR/Migration	Migration	Migration	Migration	Migration											
9.11.0*									DR/Migration	Migration	Migration	Migration	Migration										
9.11.1										DR/Migration	Migration	Migration	Migration	Migration									
9.12.0*											DR/Migration	Migration	Migration	Migration	Migration	Migration							

Quelle	Ziel																					
9.12.1												DR/Migration	Migration	Migration	Migration	Migration							
9.13.0*													DR/Migration	Migration	Migration	Migration	Migration	Migration					
9.13.1														DR/Migration	Migration	Migration	Migration	Migration					
9.14.0*															DR/Migration	Migration	Migration	Migration	Migration	Migration			
9.14.1																DR/Migration	Migration	Migration	Migration	Migration			
9.15.0*																	DR/Migration	Migration	Migration	Migration	Migration		
9.15.1																		DR/Migration	Migration	Migration	Migration		
9.16.0																			DR/Migration	Migration	Migration	Migration	
9.16.1																				DR/Migration	Migration	Migration	

Quelle	Ziel																				
9.17.1																				DR/Migration	Migration	Migration
9.18.1																					DR/Migration	Migration
9.19.1																						DR/Migration

SnapMirror Disaster-Recovery-Beziehungen

Für SnapMirror Beziehungen vom Typ “DP” und Richtlinientyp “async-mirror”:

DP-Typ-Spiegel können ab ONTAP 9.11.1 nicht mehr initialisiert werden und sind in ONTAP 9.12.1 vollständig veraltet. Weitere Informationen finden sich unter "Abschaffung von Datenschutz-SnapMirror-Beziehungen".

In der folgenden Tabelle gibt die Spalte links die ONTAP Version auf dem Quellvolume an, und die oberste Zeile gibt die ONTAP Versionen an, die auf dem Zielvolume vorhanden sein können.

Quelle	Ziel								
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3
9.11.1	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.10.1	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.9.1	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
9,8	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
9,7	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
9,6	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein
9,5	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein
9,4	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein
9,3	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja

Interoperabilität ist nicht bidirektional.

Konvertieren einer bestehenden ONTAP SnapMirror DP-Beziehung in XDP

Wenn Sie auf ONTAP 9.12.1 oder höher aktualisieren, müssen DP-Typ-Beziehungen vor dem Upgrade in XDP konvertiert werden. ONTAP 9.12.1 und höher unterstützt keine DP-Typ-Beziehungen. Eine bestehende DP-Typ-Beziehung kann einfach in XDP konvertiert werden, um die versionsflexible SnapMirror Funktionalität zu nutzen.

Vor dem Upgrade auf ONTAP 9.12.1 müssen bestehende DP-Beziehungen in XDP konvertiert werden, bevor ein Upgrade auf ONTAP 9.12.1 und spätere Versionen möglich ist.

Über diese Aufgabe

- SnapMirror konvertiert bestehende DP-Beziehungen nicht automatisch in XDP-Beziehungen. Für die Konvertierung der Beziehung ist es erforderlich, die bestehende Beziehung zu unterbrechen und zu löschen, eine neue XDP-Beziehung zu erstellen und die Beziehung erneut zu synchronisieren.
- Bei der Planung Ihrer Umstellung sollten Sie beachten, dass die Vorbereitung im Hintergrund und die Datenspeicherungsphase einer XDP SnapMirror Beziehung viel Zeit in Anspruch nehmen können. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „preparing“ über einen längeren Zeitraum meldet.

> Nach der Konvertierung eines SnapMirror Beziehungstyps von DP zu XDP werden speicherbezogene Einstellungen, wie automatische Größenanpassung und Speicherplatzzusage, nicht mehr an das Ziel repliziert.

Schritte

1. Im Ziel-Cluster ist sicherzustellen, dass die SnapMirror Beziehung vom Typ DP ist, der Spiegelungsstatus SnapMirrored ist, der Beziehungsstatus auf Idle steht und die Beziehung fehlerfrei ist:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   Das folgende Beispiel zeigt die Ausgabe des `snapmirror show` Befehls:

   ```
   cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

   Source Path: svm1:volA
   Destination Path: svm_backup:volA_dst
   Relationship Type: DP
   SnapMirror Schedule: -
   Tries Limit: -
   Throttle (KB/sec): unlimited
   Mirror State: Snapmirrored
   Relationship Status: Idle
   Transfer Snapshot: -
   Snapshot Progress: -
   Total Progress: -
   Snapshot Checkpoint: -
   Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
   123478563412_2147484682.2014-06-27_100026
   ```

```
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

Es kann hilfreich sein, eine Kopie der `snapmirror show` Befehlsausgabe aufzubewahren, um die bestehenden Beziehungseinstellungen nachzuverfolgen. Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

2. Anhand der Quell- und Ziel-Volumes ist sicherzustellen, dass beide Volumes über einen gemeinsamen Snapshot verfügen:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Das folgende Beispiel zeigt die `volume snapshot show` Ausgabe für die Quell- und Ziel-Volumes:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
```

```
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Um sicherzustellen, dass geplante Aktualisierungen während der Konvertierung nicht ausgeführt werden, die bestehende DP-Typ-Beziehung in einen inaktiven Zustand versetzen:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel versetzt die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup` in den Ruhezustand:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

4. Die bestehende DP-Beziehung auflösen:

```
snapmirror break -destination-path <SVM:volume>
```

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel unterbricht die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

5. Wenn die automatische Löschung von Snapshots auf dem Zielvolume aktiviert ist, sollte sie deaktiviert werden:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

Das folgende Beispiel deaktiviert die automatische Löschung von Snapshots auf dem Zielvolume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Die bestehende DP-Beziehung löschen:

```
snapmirror delete -destination-path <SVM:volume>
```

Weitere Informationen zu `snapmirror-delete` finden sich in der "ONTAP-Befehlsreferenz".

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel löscht die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Die ursprüngliche SVM Disaster Recovery Beziehung auf dem Quell-Cluster freigeben:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

Das folgende Beispiel gibt die SVM Disaster Recovery Beziehung frei:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Weitere Informationen zu `snapmirror release` finden sich in der "ONTAP-Befehlsreferenz".

8. Sie können die Ausgabe, die Sie vom `snapmirror show` Befehl behalten haben, verwenden, um die neue XDP Typ Beziehung zu erstellen:

```
snapmirror create -source-path <SVM:volume> -destination-path
```

```
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

Die neue Beziehung muss dasselbe Quell- und Zielvolume verwenden. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel erstellt eine SnapMirror Disaster-Recovery-Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf `svm_backup` unter Verwendung der Standard `MirrorAllSnapshots`-Richtlinie:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Die Quell- und Ziel-Volumes werden erneut synchronisiert:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Um die Resynchronisierungszeit zu verbessern, können Sie die `-quick-resync` Option verwenden, sollten sich aber darüber im Klaren sein, dass Einsparungen bei der Speichereffizienz verloren gehen können.

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden. Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.

Das folgende Beispiel synchronisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror resync` finden sich in der "ONTAP-Befehlsreferenz".

10. Falls die automatische Löschung von Snapshots deaktiviert wurde, sollte sie wieder aktiviert werden:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Nachdem Sie fertig sind

1. Mit dem `snapmirror show`Befehl lässt sich überprüfen, ob die SnapMirror Beziehung erstellt wurde.

Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

2. Sobald das SnapMirror XDP-Zielvolume mit der Aktualisierung von Snapshots gemäß der SnapMirror Richtlinie beginnt, kann mit der Ausgabe des `snapmirror list-destinations` Befehls aus dem Quell-Cluster die neue SnapMirror XDP-Beziehung angezeigt werden.

Zusätzliche Informationen zu DP-Beziehungen

Ab ONTAP 9.3 ist der XDP Modus standardmäßig aktiviert, und alle Aufrufe des DP Modus in der Befehlszeile oder in neuen oder bestehenden Skripten werden automatisch in den XDP Modus konvertiert.

Bestehende Beziehungen bleiben unberührt. Wenn eine Beziehung bereits vom Typ DP ist, bleibt sie vom Typ DP. Ab ONTAP 9.5 ist MirrorAndVault die Standardrichtlinie, wenn kein Datenschutzmodus angegeben ist oder wenn der XDP-Modus als Beziehungstyp festgelegt wurde. Die folgende Tabelle zeigt das erwartete Verhalten.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) ist…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nichts	XDP	MirrorAndVault (einheitliche Replikation)
XDP	XDP	MirrorAndVault (einheitliche Replikation)

Wie die Tabelle zeigt, gewährleisten die unter verschiedenen Umständen XDP zugewiesenen Standardrichtlinien, dass die Konvertierung die funktionale Äquivalenz der vorherigen Typen beibehält. Es können selbstverständlich auch andere Richtlinien verwendet werden, einschließlich Richtlinien für die einheitliche Replikation.

Wenn Sie angeben…	Und die Richtlinie lautet…	Das Ergebnis ist…
DP	MirrorAllSnapshots	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault
Einheitliche Replikation	XDP	MirrorAllSnapshots
SnapMirror DR	XDPDefault	SnapVault

Die einzigen Ausnahmen von der Umwandlung sind wie folgt:

- SVM-Datensicherungsbeziehungen sind in ONTAP 9.3 und früher weiterhin standardmäßig im DP-Modus.

  Ab ONTAP 9.4 sind SVM-Datensicherungsbeziehungen standardmäßig im XDP-Modus.

- Die Load-Sharing-Datenschutzbeziehungen des Root-Volumes verbleiben weiterhin standardmäßig im DP-Modus.
- SnapLock Datenschutzbeziehungen verbleiben in ONTAP 9.4 und früher weiterhin standardmäßig im DP-Modus.

  Ab ONTAP 9.5 werden SnapLock Datenschutzbeziehungen standardmäßig im XDP-Modus hergestellt.

- Explizite Aufrufe von DP verwenden weiterhin standardmäßig den DP-Modus, wenn die folgende clusterweite Option festgelegt ist:

```
options replication.create_data_protection_rels.enable on
```

Diese Option wird ignoriert, wenn DP nicht explizit aufgerufen wird.

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"
- "snapmirror quiesce"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

Langzeit-Snapshots sollten vor dem ONTAP Upgrade deaktiviert werden.

In einer Beziehung von kaskadierten Volumes werden Langzeitaufbewahrungs-Snapshots nur auf dem finalen SnapMirror Ziel-Volume der Kaskade in allen Versionen von ONTAP 9 unterstützt. Die Aktivierung von Langzeitaufbewahrungs-Snapshots auf einem beliebigen Zwischen-Volume in der Kaskade führt zu fehlenden Backups und Snapshots.

Weitere Informationen zu "Langzeitaufbewahrungs-Snapshots".

Wenn eine nicht unterstützte Konfiguration vorliegt, bei der Langzeitaufbewahrungs-Snapshots auf einem beliebigen Zwischen-Volume einer Kaskade aktiviert wurden, sollte der technische Support kontaktiert und auf die "NetApp Knowledge Base: Das Kaskadieren eines Volumes mit aktivierten Langzeitaufbewahrungs-Snapshots (LTR) wird nicht unterstützt." verwiesen werden.

Die folgenden ONTAP Versionen erlauben es nicht, Langzeit-Snapshots auf einem beliebigen Volume in einer Kaskade zu aktivieren, außer auf dem endgültigen SnapMirror Zielvolume.

- 9.15.1 und später
- 9.14.1P2 und P4 bis P14
- 9.13.1P9 bis P17
- 9.12.1 P12 bis P19
- 9.11.1P15 bis P20
- 9.10.1P18 bis P20
- 9.9.1P20

Bevor von einer ONTAP Version, die das Aktivieren von Langzeitaufbewahrungs-Snapshots auf mittleren Volumes einer Kaskade ermöglicht, auf eine ONTAP Version aktualisiert wird, die dies blockiert, ist es erforderlich, die Langzeitaufbewahrungs-Snapshots zu deaktivieren, um verpasste Backups und Snapshots zu vermeiden.

In den folgenden Szenarien ist eine Aktion erforderlich:

- Langzeit-Snapshots werden auf dem „B“-Volume in einer „A > B > C“ SnapMirror Kaskade oder auf einem anderen mittleren SnapMirror Zielvolume in Ihrer größeren Kaskade konfiguriert.

- Langzeitaufbewahrungs-Snapshots werden durch einen Zeitplan definiert, der auf eine SnapMirror Richtlinienregel angewendet wird. Diese Regel repliziert keine Snapshots vom Quellvolume, sondern erstellt sie direkt auf dem Zielvolume.

> Weitere Informationen zu Zeitplänen und SnapMirror-Richtlinien finden sich im "NetApp Knowledge Base: Wie funktioniert der Parameter "schedule" in einer ONTAP 9 SnapMirror-Richtlinienregel?".

Schritte

1. Die Regel zur langfristigen Aufbewahrung aus der SnapMirror Richtlinie für das mittlere Volume der Kaskade entfernen:

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
-snapmirror-label <>
```

Weitere Informationen zu `snapmirror policy remove-rule` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Regel für das SnapMirror Label ohne den langfristigen Aufbewahrungsplan erneut hinzufügen:

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>
-snapmirror-label <> -keep <>
```

> Das Entfernen von Snapshots zur Langzeitaufbewahrung aus den SnapMirror-Richtlinienregeln bedeutet, dass SnapMirror die Snapshots mit dem angegebenen Label vom Quell-Volume abruft. Es kann außerdem erforderlich sein, einen Zeitplan in der Snapshot-Richtlinie des Quell-Volumes hinzuzufügen oder zu ändern, um korrekt gekennzeichnete Snapshots zu erstellen.

Weitere Informationen zu `snapmirror policy add-rule` finden sich in der "ONTAP-Befehlsreferenz".

3. Gegebenenfalls kann ein Zeitplan in der Snapshot-Richtlinie des Quellvolumes geändert oder erstellt werden, damit Snapshots mit einer SnapMirror Bezeichnung erstellt werden können:

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

> Langzeitaufbewahrungs-Snapshots können weiterhin auf dem endgültigen SnapMirror Zielvolume innerhalb einer SnapMirror Kaskadenkonfiguration aktiviert werden.

ONTAP Lizenzanforderungen für SnapMirror S3 Konfigurationen

Bevor Sie ONTAP aktualisieren, falls Sie SnapMirror S3 verwenden und auf ONTAP 9.12.1 oder höher aktualisieren, sollte überprüft werden, ob die entsprechenden SnapMirror Lizenzen vorhanden sind.

Nach einem Upgrade von ONTAP können Lizenzänderungen, die zwischen ONTAP 9.11.1 und früher und ONTAP 9.12.1 und später vorgenommen wurden, dazu führen, dass SnapMirror S3-Beziehungen fehlschlagen.

ONTAP 9.11.1 und früher

- Bei der Replikation in einen von NetApp gehosteten Ziel-Bucket (ONTAP S3 oder StorageGRID) prüft SnapMirror S3, ob die SnapMirror synchron Lizenz vorhanden ist, die vor der Einführung der "ONTAP One" Software Suite im Data Protection Bundle enthalten war.
- Bei der Replikation in einen Nicht-NetApp-Ziel-Bucket prüft SnapMirror S3, ob die SnapMirror Cloud-Lizenz im Hybrid Cloud Bundle enthalten ist, das vor der Einführung der "ONTAP One" Software Suite verfügbar war.

ONTAP 9.12.1 und höher

- Bei der Replikation in einen von NetApp gehosteten Ziel-Bucket (ONTAP S3 oder StorageGRID) prüft SnapMirror S3, ob die SnapMirror S3-Lizenz vorhanden ist, die im Data Protection Bundle enthalten war, das vor der Einführung der "ONTAP One" Software Suite verfügbar war.
- Bei der Replikation in einen Nicht-NetApp-Ziel-Bucket prüft SnapMirror S3, ob die SnapMirror S3 External-Lizenz vorhanden ist, die im Hybrid Cloud Bundle enthalten ist, welches vor der Einführung der "ONTAP One" Software Suite und der "ONTAP One Kompatibilitätspaket" verfügbar war.

Bestehende SnapMirror S3-Beziehungen

Bestehende SnapMirror S3-Beziehungen sollten auch nach einem Upgrade von ONTAP 9.11.1 oder früher auf ONTAP 9.12.1 oder später weiterhin funktionieren, selbst wenn der Cluster nicht über die neue Lizenzierung verfügt.

Die Erstellung neuer SnapMirror S3-Beziehungen schlägt fehl, wenn auf dem Cluster nicht die erforderliche Lizenz installiert ist.

Externe Schlüsselverwaltungsserver-Verbindungen vor dem Upgrade von ONTAP löschen

Bevor ONTAP aktualisiert wird, falls ONTAP 9.2 oder eine frühere Version mit NetApp Storage Encryption (NSE) verwendet wird und ein Upgrade auf ONTAP 9.3 oder höher erfolgt, muss die Befehlszeilenschnittstelle (CLI) verwendet werden, um alle vorhandenen externen Key Management (KMIP) Serververbindungen zu löschen.

Schritte

1. Es sollte sichergestellt werden, dass die NSE-Laufwerke entsperrt, geöffnet und auf die Standard-Hersteller-Sicherheits-ID 0x0 gesetzt sind:

```
storage encryption disk show -disk *
```

Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

2. In den erweiterten Berechtigungsmodus wechseln:

```
set -privilege advanced
```

Weitere Informationen zu `set` finden sich in der "ONTAP-Befehlsreferenz".

3. Die standardmäßige Hersteller-Sicherheits-ID 0x0 dient dazu, den FIPS-Schlüssel den selbstverschlüsselnden Festplatten (SEDs) zuzuweisen:

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

Weitere Informationen zu `storage encryption disk modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Es sollte überprüft werden, ob die Zuweisung des FIPS-Schlüssels zu allen Datenträgern abgeschlossen ist:

```
storage encryption disk show-status
```

Weitere Informationen zu `storage encryption disk show-status` finden sich in der "ONTAP-Befehlsreferenz".

5. Es sollte sichergestellt sein, dass der **Modus** für alle Datenträger auf Daten eingestellt ist.

```
storage encryption disk show
```

Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

6. Anzeigen der konfigurierten KMIP Server:

```
security key-manager keystore show
```

Weitere Informationen zu `security key-manager keystore show` finden sich in der "ONTAP-Befehlsreferenz".

7. Die konfigurierten KMIP-Server löschen:

```
security key-manager delete -address <kmip_ip_address>
```

Weitere Informationen zu `security key-manager delete` finden sich in der "ONTAP-

Befehlsreferenz".

8. Die Konfiguration des externen Schlüsselmanagers löschen:

```
security key-manager external disable
```

Weitere Informationen zu `security key-manager external disable` finden sich in der "ONTAP-Befehlsreferenz".

Durch diesen Schritt werden die NSE-Zertifikate nicht entfernt.

Was kommt als Nächstes

Nach Abschluss des Upgrades ist es erforderlich, Die KMIP Serververbindungen neu konfigurieren.

Vor einem ONTAP Upgrade ist sicherzustellen, dass die Netgroup-Datei auf allen Knoten vorhanden ist.

Bevor Sie ONTAP aktualisieren, muss, falls Netzgruppen in Storage Virtual Machines (SVMs) geladen wurden, überprüft werden, ob die Netzgruppendatei auf jedem Node vorhanden ist. Eine fehlende Netzgruppendatei auf einem Node kann dazu führen, dass das Upgrade fehlschlägt.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Der Netgroup-Status für jede SVM wird angezeigt:

```
vserver services netgroup status
```

3. Es sollte für jede SVM sichergestellt sein, dass jeder Node denselben Hashwert der Netgroup-Datei anzeigt:

```
vserver services name-service netgroup status
```

In diesem Fall kann der nächste Schritt übersprungen werden und das Upgrade oder die Rücksetzung kann fortgesetzt werden. Andernfalls ist mit dem nächsten Schritt fortzufahren.

4. Auf einem beliebigen Node des Clusters die Netgroup-Datei manuell laden:

```
vserver services netgroup load -vserver vserver_name -source uri
```

Dieser Befehl lädt die Netgroup-Datei auf allen Knoten herunter. Falls auf einem Knoten bereits eine Netgroup-Datei existiert, wird diese überschrieben.

Verwandte Informationen

"Arbeiten mit Netgroups"

Vor dem Upgrade von ONTAP einen Wert für die Option v4.2-xattrs zuweisen

Wenn Sie einen NFSv4.2-Client haben, muss vor dem Upgrade von bestimmten Releases und Patches von ONTAP 9.12.1 und später ein expliziter Wert für die Option NFSv4.2 extended attributes angegeben werden, um NFS-Antwortfehler nach dem Upgrade zu verhindern.

Wenn der `v4.2-xattrs` Option vor dem ONTAP Upgrade auf die betroffenen Versionen niemals explizit ein Wert zugewiesen wird, werden NFSv4.2-Clients nicht darüber informiert, dass sich die Option für die erweiterten Attribute des Servers geändert hat. Dies führt bei bestimmten `xattrs` Aufrufen aufgrund einer Diskrepanz zwischen Client und Server zu NFS-Antwortfehlern.

Bevor Sie beginnen

Sie müssen der Option „NFSv4.2 extended attributes“ einen expliziten Wert zuweisen, wenn Folgendes zutrifft:

- Sie verwenden NFSv4.2 mit einer SVM, die mit ONTAP 9.11.1 oder einer früheren Version erstellt wurde.
- Sie aktualisieren ONTAP von einer der folgenden betroffenen Versionen und Patches:
  - 9.12.1RC1 bis 9.12.1P11
  - 9.13.1RC1 bis 9.13.1P8
  - 9.14.1RC1 bis 9.14.1P1

Über diese Aufgabe

ONTAP 9.12.1 oder höher muss verwendet werden, um den Wert mit dem in diesem Verfahren beschriebenen Befehl festzulegen.

Wenn `v4.2-xattrs` bereits auf `enabled` gesetzt ist, sollte es dennoch explizit auf `enabled` gesetzt werden, um zukünftige Störungen zu vermeiden. Wenn `v4.2-xattrs` auf deaktiviert gesetzt wird, können NFSv4.2 Clients „invalid argument“-Antworten erhalten, bis sie erneut eingebunden werden oder die `v4.2-xattrs` Option auf `enabled` gesetzt wird.

Schritte

- Weisen Sie der Option `v4.2-xattrs` einen expliziten Wert zu:

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

Verwandte Informationen

"Das NFS v4.2-xattrs Feld wird nach Upgrades vertauscht"

LDAP-Clients für die Verwendung von TLS vor einem ONTAP Upgrade konfigurieren

Vor dem Upgrade von ONTAP müssen LDAP-Clients mit SSLv3 für die sichere Kommunikation mit LDAP-Servern zur Nutzung von TLS konfiguriert werden. SSL steht nach dem Upgrade nicht mehr zur Verfügung.

Standardmäßig ist die LDAP-Kommunikation zwischen Client- und Serveranwendungen nicht verschlüsselt.

Die Verwendung von SSL muss deaktiviert und die Nutzung von TLS erzwungen werden.

Schritte

1. Es sollte überprüft werden, ob die LDAP-Server in Ihrer Umgebung TLS unterstützen.

   Falls dies nicht der Fall ist, nicht fortfahren. Ein Upgrade der LDAP-Server auf eine Version, die TLS unterstützt, wird empfohlen.

2. Es wird geprüft, bei welchen ONTAP LDAP-Client Konfigurationen LDAP über SSL/TLS aktiviert ist:

   ```
   vserver services name-service ldap client show
   ```

   Falls keine vorhanden sind, können Sie die restlichen Schritte überspringen. Es empfiehlt sich jedoch aus Sicherheitsgründen, LDAP über TLS zu verwenden.

3. Für jede LDAP-Client Konfiguration SSL deaktivieren, um die Verwendung von TLS zu erzwingen:

   ```
   vserver services name-service ldap client modify -vserver <vserver_name>
   -client-config <ldap_client_config_name> -allow-ssl false
   ```

4. Es wird überprüft, dass die Verwendung von SSL für LDAP-Clients nicht mehr zulässig ist:

   ```
   vserver services name-service ldap client show
   ```

Verwandte Informationen

- "NFS Management"
- "TLS-Hardware-Offload konfigurieren"

Verhalten sitzungsorientierter Protokolle während eines ONTAP Upgrades

Cluster und sitzungsorientierte Protokolle können in bestimmten Bereichen wie dem I/O-Service während Upgrades negative Auswirkungen auf Clients und Anwendungen haben.

Wenn Sie sitzungsorientierte Protokolle verwenden, ist Folgendes zu berücksichtigen:

- SMB

  Wenn kontinuierlich verfügbare (CA) Freigaben mit SMBv3 bereitgestellt werden, kann die automatisierte unterbrechungsfreie Upgrade-Methode (mit System Manager oder der CLI) verwendet werden, ohne dass der Client eine Unterbrechung erfährt.

  Wenn Sie Freigaben mit SMBv1 oder SMBv2 oder Nicht-CA-Freigaben mit SMBv3 bereitstellen, werden Clientsitzungen während der Upgrade-Übernahme und des Neustarts unterbrochen. Benutzern sollte empfohlen werden, ihre Sitzungen vor dem Upgrade zu beenden.

  Hyper-V und SQL Server über SMB unterstützen unterbrechungsfreie Betriebsabläufe (NDOs). Wenn eine Hyper-V- oder SQL Server über SMB-Lösung konfiguriert wurde, bleiben die Anwendungsserver und die darin enthaltenen virtuellen Maschinen oder Datenbanken während des ONTAP Upgrades online und

bieten kontinuierliche Verfügbarkeit.

- NFSv4.x

  NFSv4.x Clients stellen bei Verbindungsabbrüchen, die während des Upgrades auftreten, automatisch die Verbindung mithilfe der normalen NFSv4.x-Wiederherstellungsverfahren wieder her. Anwendungen können während dieses Vorgangs vorübergehend eine Verzögerung bei der Ein-/Ausgabe erleben.

- NDMP

  Der Status geht verloren und der Client-Benutzer muss den Vorgang wiederholen.

- Datensicherung und Wiederherstellung

  Der Status geht verloren und der Client-Benutzer muss den Vorgang wiederholen.

  Während oder unmittelbar vor einem Upgrade sollte keine Datensicherung oder -wiederherstellung initiiert werden. Dies könnte zu Datenverlust führen.

- Anwendungen (zum Beispiel Oracle oder Exchange)

  Die Auswirkungen hängen von den Anwendungen ab. Bei timeout-basierten Anwendungen besteht möglicherweise die Möglichkeit, die Zeitüberschreitungseinstellung auf einen längeren Wert als die ONTAP-Neustartzeit zu setzen, um negative Auswirkungen zu minimieren.

Vor einem ONTAP Upgrade sollte die Unterstützung des SSH-Hostschlüssel-Algorithmus überprüft werden.

Bevor ONTAP aktualisiert wird, muss, falls der SSL-FIPS-Modus auf einem Cluster aktiviert ist, auf dem sich Administratorkonten mit einem öffentlichen SSH-Schlüssel authentifizieren, sichergestellt werden, dass der Host-Algorithmus in der Zielversion von ONTAP unterstützt wird.

Die folgende Tabelle zeigt die für ONTAP SSH-Verbindungen unterstützten Host-Schlüssel-Algorithmen. Diese Schlüsseltypen gelten nicht für die Konfiguration der öffentlichen SSH-Authentifizierung.

ONTAP Release	Im FIPS-Modus unterstützte Schlüsseltypen	Unterstützte Schlüsseltypen im Nicht-FIPS-Modus
9.11.1 und später	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 und früher	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa

Die Unterstützung für den Host-Key-Algorithmus ssh-ed25519 wird ab ONTAP 9.11.1 entfernt.

Weitere Informationen finden sich unter "Netzwerksicherheit mithilfe von FIPS konfigurieren".

Vorhandene SSH-Public-Key-Konten ohne die unterstützten Schlüsselalgorithmen müssen vor dem Upgrade mit einem unterstützten Schlüsseltyp neu konfiguriert werden, andernfalls schlägt die Administratorauthentifizierung fehl.

"Weitere Informationen zur Aktivierung von SSH Public Key Konten."

ARP-Aktivitätswarnungen sollten vor einem ONTAP Upgrade behoben werden

Bevor Sie auf ONTAP 9.16.1 oder höher aktualisieren, sollte auf alle Warnungen zu ungewöhnlichen Aktivitäten reagiert werden, die von Autonomous Ransomware Protection (ARP) gemeldet werden. In ONTAP 9.16.1 wurde ARP auf ein maschinelles Lern-/künstliche Intelligenz (KI)-basiertes Modell umgestellt. Aufgrund dieser Änderung gehen alle ungelösten aktiven Warnungen der bestehenden ARP in ONTAP 9.15.1 oder früher nach dem Upgrade verloren.

Schritte

1. Auf alle von "ARP" gemeldeten Warnungen zu ungewöhnlichen Aktivitäten reagieren und mögliche Probleme beheben.
2. Die Behebung dieser Probleme sollte vor dem Upgrade bestätigt werden, indem **Aktualisieren und verdächtige Dateitypen löschen** ausgewählt wird, um die Entscheidung zu protokollieren und die normale ARP-Überwachung fortzusetzen.

SP oder BMC neu starten, um die Firmware-Aktualisierung während eines ONTAP Upgrades vorzubereiten.

Vor einem ONTAP Upgrade ist keine manuelle Firmware-Aktualisierung erforderlich. Die Firmware für Ihren Cluster ist im ONTAP Upgrade Paket enthalten und wird auf das Boot-Gerät jedes Knotens kopiert. Die neue Firmware wird anschließend im Rahmen des Upgrade-Prozesses installiert.

Die Firmware der folgenden Komponenten wird automatisch aktualisiert, wenn die Version in Ihrem Cluster älter ist als die Firmware, die im ONTAP Upgrade-Paket enthalten ist:

- BIOS/LOADER
- Service Processor (SP) oder Baseboard Management Controller (BMC)
- Storage Shelf
- Festplatte
- Flash Cache

Zur Vorbereitung eines reibungslosen Updates empfiehlt es sich, den SP oder BMC vor Beginn des Upgrades neu zu starten.

Ein Neustart kann mit der ONTAP CLI, dem SP oder dem BMC durchgeführt werden.

CLI

1. SP oder BMC neu starten:

```
system service-processor reboot-sp -node <node_name>
```

SP

1. Starten Sie die SP neu:

```
sp reboot
```

BMC

1. Starten Sie die BMC neu:

```
bmc reboot
```

Nur jeweils einen SP oder BMC neu starten. Warten, bis der neu gestartete SP oder BMC vollständig neu gestartet wurde, bevor der nächste neu gestartet wird.

Das ist auch "Firmware manuell aktualisieren" zwischen ONTAP Upgrades möglich. Wenn Sie Digital Advisor haben, kann "Die Liste der Firmware-Versionen, die derzeit in Ihrem ONTAP Image enthalten sind, wird angezeigt.".

Aktualisierte Firmware-Versionen sind wie folgt verfügbar:

- "Systemfirmware (BIOS, BMC, SP)"
- "Shelf Firmware"
- "Festplatten- und Flash Cache-Firmware"

Das ONTAP Software-Image sollte vor einem Upgrade heruntergeladen werden.

Bevor Sie ONTAP aktualisieren, muss zunächst das Ziel-ONTAP-Software-Image von der NetApp Support-Website heruntergeladen werden. Abhängig von Ihrer ONTAP-Version kann die ONTAP-Software auf einen HTTPS-, HTTP- oder FTP-Server in Ihrem Netzwerk oder in einen lokalen Ordner heruntergeladen werden.

Wenn Sie ausführen…	Das Bild kann an diesem Speicherort heruntergeladen werden…
ONTAP 9.6 und höher	• Ein HTTPS-Server + das CA-Zertifikat des Servers muss auf dem lokalen System installiert sein. • Ein lokaler Ordner • Ein HTTP oder FTP Server
ONTAP 9.4 und höher	• Ein lokaler Ordner • Ein HTTP oder FTP Server
ONTAP 9.0 und höher	Ein HTTP oder FTP Server

Über diese Aufgabe

- Wenn ein automatisiertes unterbrechungsfreies Upgrade (ANDU) mit einem "direkter Multi-Hop Upgrade-Pfad" durchgeführt wird, ist es erforderlich, "herunterladen" das Softwarepaket sowohl für die zwischengeschaltete ONTAP Version als auch für die Ziel-ONTAP Version bereitzustellen, die für das Upgrade benötigt werden. Beispielsweise müssen beim Upgrade von ONTAP 9.8 auf ONTAP 9.13.1 die Softwarepakete für ONTAP 9.12.1 und ONTAP 9.13.1 heruntergeladen werden. Siehe "Unterstützte

Upgrade-Pfade", um festzustellen, ob für Ihren Upgrade-Pfad das Herunterladen eines zwischengeschalteten Softwarepakets erforderlich ist.

- Wenn ein System mit NetApp Volume Encryption auf ONTAP 9.5 oder höher aktualisiert wird, muss das ONTAP Software-Image für nicht eingeschränkte Länder heruntergeladen werden, das NetApp Volume Encryption enthält.

  Wenn das ONTAP Software-Image für eingeschränkte Länder zur Aktualisierung eines Systems mit NetApp Volume Encryption verwendet wird, tritt ein Systemabsturz auf und der Zugriff auf die Volumes geht verloren.

- Sie müssen kein separates Softwarepaket für Ihre Firmware herunterladen. Das Firmware-Update für Ihren Cluster ist im ONTAP Software-Upgrade-Paket enthalten und wird auf das Boot-Gerät jedes Knotens kopiert. Die neue Firmware wird anschließend im Rahmen des Upgrade-Prozesses installiert.

Schritte

1. Die gewünschte ONTAP Software befindet sich im "Software-Downloads" Bereich der NetApp Support Site.

   Für ein ONTAP Select Upgrade ist **ONTAP Select Node Upgrade** auszuwählen.

2. Die Software-Image-Datei (zum Beispiel 97_q_image.tgz) wird an den entsprechenden Speicherort kopiert.

   Je nach Ihrer ONTAP Version ist der Speicherort entweder ein Verzeichnis auf einem HTTP-, HTTPS- oder FTP-Server, von dem das Image an das lokale System bereitgestellt wird, oder ein lokaler Ordner auf dem Speichersystem.

ONTAP Upgrade-Methoden

ONTAP Software-Upgrade-Methoden

Ein automatisiertes Upgrade Ihrer ONTAP Software kann mit System Manager durchgeführt werden. Alternativ ist ein automatisiertes oder manuelles Upgrade über die ONTAP Befehlszeilenschnittstelle (CLI) möglich. Die Methode, die für das Upgrade von ONTAP verwendet wird, hängt von Ihrer Konfiguration, Ihrer aktuellen ONTAP Version und der Anzahl der Knoten in Ihrem Cluster ab. NetApp empfiehlt, für automatisierte Upgrades System Manager zu verwenden, es sei denn, Ihre Konfiguration erfordert eine andere Vorgehensweise. Wenn beispielsweise eine vier Knoten umfassende MetroCluster Konfiguration mit ONTAP 9.3 oder höher vorliegt, sollte für ein automatisiertes Upgrade (auch als automatisiertes unterbrechungsfreies Upgrade oder ANDU bezeichnet) System Manager verwendet werden.

Wenn ein Upgrade auf ONTAP 9.15.1 oder höher über die NetApp Console durchgeführt wird, sind die "Upgrade-Verfahren in der NetApp Console Dokumentation" zu beachten.

Ein Upgrade kann entweder mit dem Rolling-Upgrade-Prozess oder mit dem Batch-Upgrade-Prozess durchgeführt werden. Beide Verfahren sind unterbrechungsfrei.

Bei automatisierten Upgrades installiert ONTAP automatisch das Ziel-ONTAP-Image auf jedem Knoten, validiert die Cluster-Komponenten, um sicherzustellen, dass das Cluster unterbrechungsfrei aktualisiert werden kann, und führt anschließend im Hintergrund ein Batch- oder Rolling-Upgrade durch, abhängig von der Anzahl der Knoten. Bei manuellen Upgrades bestätigt der Administrator manuell, dass jeder Knoten im Cluster

für das Upgrade bereit ist, und führt anschließend die Schritte zur Durchführung eines Rolling-Upgrades aus.

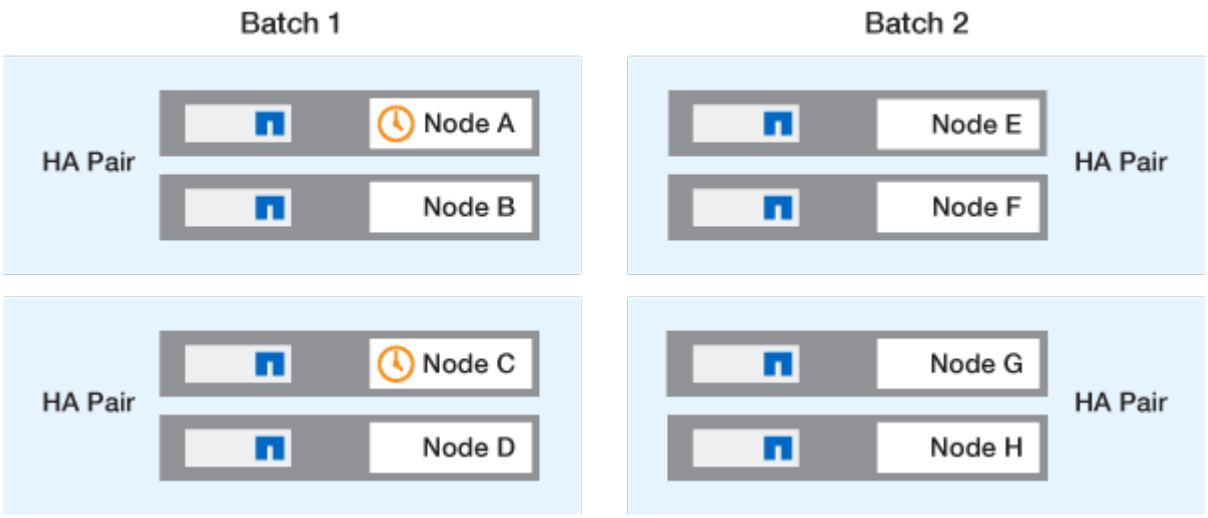
ONTAP Rolling Upgrades

Für Cluster mit weniger als 8 Knoten ist der Rolling-Upgrade-Prozess der Standard. Im Rolling-Upgrade-Prozess wird ein Knoten offline genommen und aktualisiert, während sein Partner dessen Speicher übernimmt. Nach Abschluss des Node-Upgrades gibt der Partnerknoten die Kontrolle an den ursprünglichen Knoten zurück, und der Vorgang wird auf dem Partnerknoten wiederholt. Jedes weitere HA-Paar wird der Reihe nach aktualisiert, bis alle HA-Paare die Zielversion ausführen.

ONTAP Batch-Upgrade

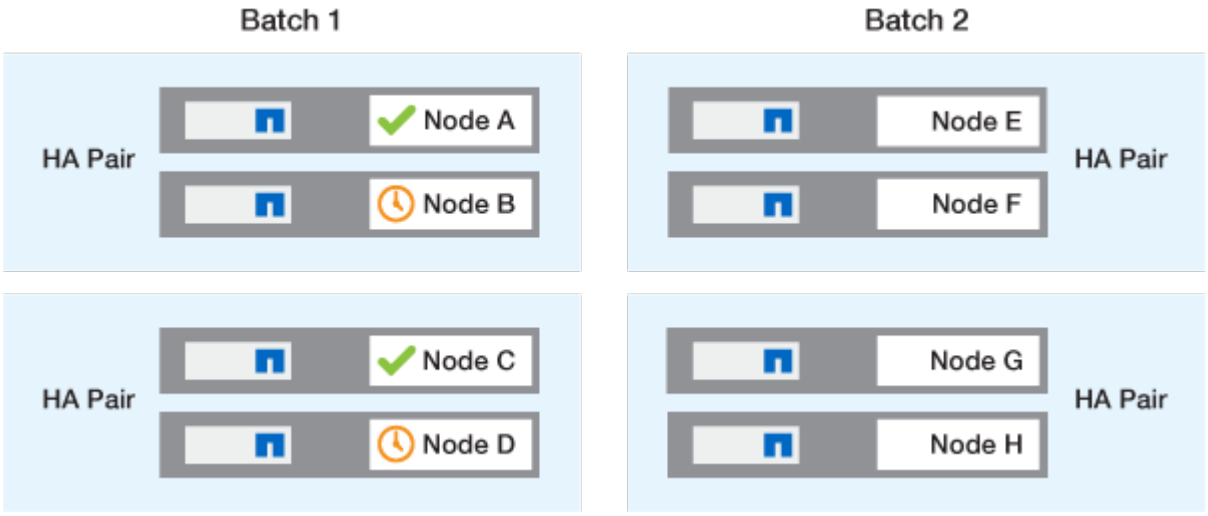
Der Batch-Upgrade-Prozess ist der Standard für Cluster mit 8 oder mehr Knoten. Im Batch-Upgrade-Prozess wird der Cluster in zwei Stapel unterteilt. Jeder Stapel enthält mehrere HA-Paare. Im ersten Stapel wird der erste Knoten jedes HA-Paares gleichzeitig mit dem ersten Knoten aller anderen HA-Paare im Stapel aktualisiert.

Im folgenden Beispiel befinden sich in jedem Batch zwei HA-Paare. Wenn das Batch-Upgrade beginnt, werden Knoten A und Knoten C gleichzeitig aktualisiert.



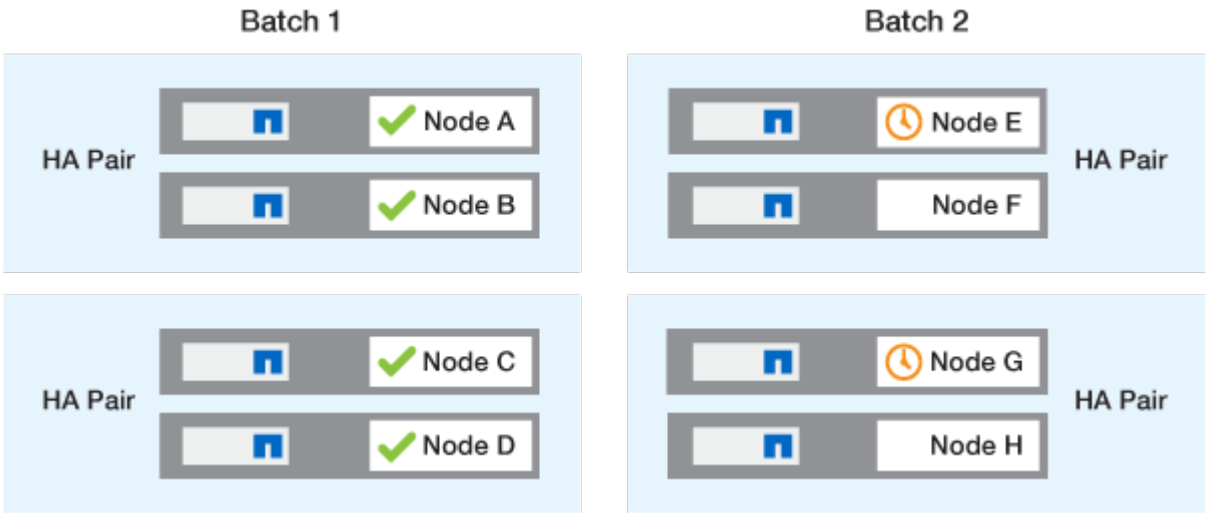
Nach Abschluss des Upgrades der ersten Knoten jedes HA-Paares werden die Partnerknoten in Batch 1 gleichzeitig aktualisiert.

Im folgenden Beispiel werden nach der Aktualisierung von Node A und Node C gleichzeitig Node B und Node D aktualisiert.



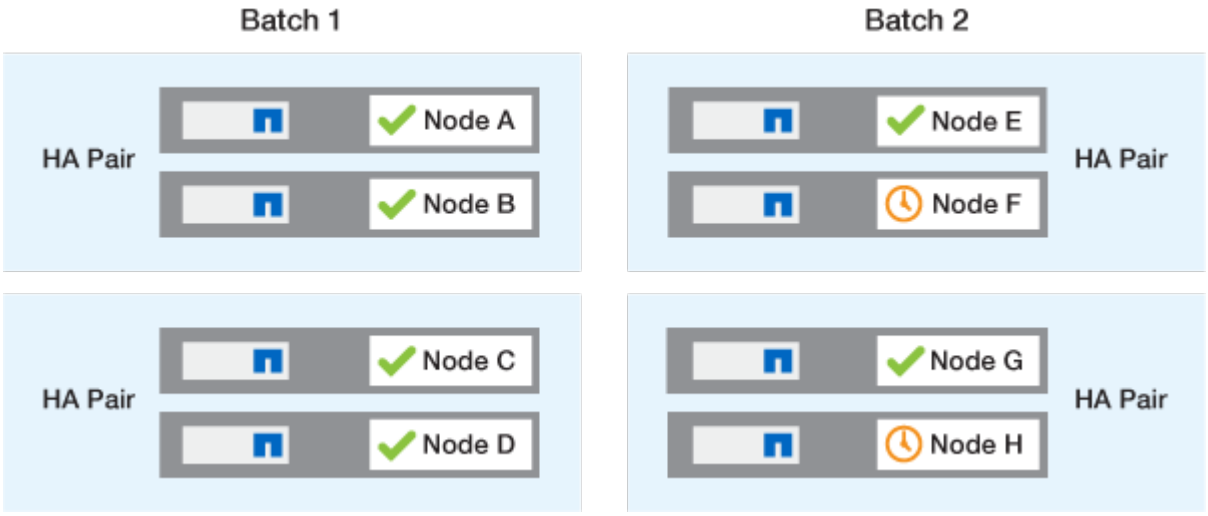
Anschließend wird der Vorgang für die Knoten in Batch 2 wiederholt; der erste Knoten jedes HA-Paares wird gleichzeitig mit dem ersten Knoten aller anderen HA-Paare in der Batch aktualisiert.

Im folgenden Beispiel werden Node E und Node G gleichzeitig aktualisiert.



Nach Abschluss des Upgrades der ersten Knoten jedes HA-Paares werden die Partnerknoten in Batch 2 gleichzeitig aktualisiert.

Im folgenden Beispiel werden Node F und Node H gleichzeitig aktualisiert, um den Batch-Upgrade-Prozess abzuschließen.



Empfohlene ONTAP Upgrade-Methoden basierend auf der Konfiguration

Die von Ihrer Konfiguration unterstützten Upgrade-Methoden sind in der Reihenfolge der empfohlenen Verwendung aufgelistet.

Konfiguration	ONTAP Version	Anzahl der Knoten	Empfohlene Upgrade-Methode
Standard	9.0 oder höher	2 oder mehr	• Automatisiertes unterbrechungsfreies Upgrade mit System Manager • Automatisiertes unterbrechungsfreies Upgrade über die Befehlszeile (CLI)
Standard	9.0 oder höher	Einzel	"Automatisiertes disruptives"
MetroCluster	9.3 oder höher	8	• Automatisiertes unterbrechungsfreies Upgrade über die Befehlszeile (CLI) • Manuelles unterbrechungsfreies Upgrade für 4 oder 8 Node MetroCluster mit der Befehlszeile
MetroCluster	9.3 oder höher	2,4	• Automatisiertes unterbrechungsfreies Upgrade mit System Manager • Automatisiertes unterbrechungsfreies Upgrade über die Befehlszeile (CLI)

Konfiguration	ONTAP Version	Anzahl der Knoten	Empfohlene Upgrade-Methode
MetroCluster	9.2 oder früher	4, 8	Manuelles unterbrechungsfreies Upgrade für 4 oder 8 Node MetroCluster mit der Befehlszeile
MetroCluster	9.2 oder früher	2	Manuelles, unterbrechungsfreies Upgrade für 2-Node MetroCluster mit der Befehlszeile

ANDU mit System Manager ist die empfohlene Upgrade-Methode für alle Patch-Upgrades, unabhängig von der Konfiguration.

Ein manuelles disruptives Upgrade kann auf jeder Konfiguration durchgeführt werden. Allerdings sollte ein unterbrechendes Upgrade nur durchgeführt werden, wenn der Cluster für die Dauer des Upgrades offline genommen werden kann. In einer SAN-Umgebung ist es erforderlich, alle SAN-Clients vor einem unterbrechenden Upgrade herunterzufahren oder anzuhalten. Unterbrechende Upgrades werden mit der ONTAP CLI durchgeführt.

Ein automatisiertes, unterbrechungsfreies ONTAP Upgrade durchführen

Bei einem automatisierten unterbrechungsfreien Upgrade (ANDU) installiert ONTAP automatisch das Ziel-ONTAP-Image auf jedem Knoten, prüft, ob der Cluster erfolgreich aktualisiert werden kann, und führt dann im Hintergrund je nach Anzahl der Knoten im Cluster entweder ein Batch- oder Rolling-Upgrade aus.

Wenn Ihre Konfiguration dies unterstützt, empfiehlt sich die Verwendung von System Manager für ein automatisiertes Upgrade. Wenn Ihre Konfiguration kein automatisiertes Upgrade mit System Manager unterstützt, kann die ONTAP Befehlszeilenschnittstelle (CLI) für ein automatisiertes Upgrade verwendet werden.

Wenn ein Upgrade auf ONTAP 9.15.1 oder höher über die NetApp Console durchgeführt wird, sind die "Upgrade-Verfahren in der NetApp Console Dokumentation" zu beachten.

Die Änderung der Einstellung der `storage failover modify-auto-giveback` Befehlsoption vor dem Start eines ANDU hat keine Auswirkungen auf den Upgrade-Prozess. Der ANDU-Prozess ignoriert jeglichen voreingestellten Wert dieser Option während der für das Update erforderlichen Übernahme/Rückgabe. Beispielsweise unterbricht das Setzen von `-autogiveback` auf „false“ vor Beginn des ANDU die automatische Aktualisierung vor der Rückgabe nicht. Weitere Informationen zu `storage failover modify-auto-giveback` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

- Sie sollten "Vorbereitung auf Ihr Upgrade".
- Das sollten Sie "Das ONTAP Software-Image herunterladen" für Ihre Ziel-ONTAP-Version tun.

Wenn Sie ein "direktes Multi-Hop-Upgrade" durchführen, müssen Sie beide für Ihre spezifische "Upgrade-Pfad" erforderlichen ONTAP Images herunterladen.

- Optional, "Systemfirmware für ein Upgrade mit nur einem Neustart vorab bereitstellen".

  Ab ONTAP 9.17.1 wird, wenn auf dem Boot-Gerät eines Knotens bereits eine neuere BIOS- oder LOADER-Firmware vorhanden ist, bevor ein ANDU durchgeführt wird, die neuere Firmware beim Upgrade-Prozess beibehalten, anstatt sie mit der im ONTAP-Image enthaltenen Version zu überschreiben. Dies ermöglicht, dass sowohl das ONTAP Software-Upgrade als auch das Firmware-Update in einem einzigen Neustartzyklus abgeschlossen werden.

- Für jedes HA-Paar sollte jeder Knoten über einen oder mehrere Ports in derselben Broadcast-Domäne verfügen.

  Wenn Ihr ONTAP Cluster 8 oder mehr Knoten umfasst, wird die Batch-Upgrade-Methode im automatischen unterbrechungsfreien Upgrade verwendet, um die Daten-LIF-Migration vor der SFO-Übernahme präventiv zu erzwingen. Wie LIFs während eines Batch-Upgrades migriert werden, hängt von Ihrer ONTAP Version ab.

Wenn Sie ONTAP ausführen…	LIFs werden migriert…
• 9.15.1 oder höher • 9.14.1P5 • 9.13.1P10 • 9.12.1P13 • 9.11.1P16, P17 • 9.10.1P19	Zu einem Knoten in der anderen Batch-Gruppe. Falls die Migration zur anderen Batch-Gruppe fehlschlägt, werden die LIFs zum HA-Partner des Knotens in derselben Batch-Gruppe migriert.
9.8 bis 9.14.1	Zu einem Knoten in der anderen Batch-Gruppe. Wenn die Netzwerk-Broadcast-Domäne die LIF-Migration zur anderen Batch-Gruppe nicht zulässt, schlägt die LIF-Migration fehl und ANDU pausiert.
9.7 oder früher	An den HA-Partner des zu aktualisierenden Knotens. Falls der Partner keine Ports in derselben Broadcast-Domäne besitzt, schlägt die LIF-Migration fehl und ANDU pausiert.

- Wenn ONTAP in einer MetroCluster FC-Konfiguration aktualisiert wird, sollte der Cluster für die automatische ungeplante Umschaltung aktiviert sein.
- Wenn Sie nicht vorhaben, den Fortschritt des Upgrade-Prozesses zu überwachen, sollten Sie "EMS-Benachrichtigungen über Fehler anfordern, die möglicherweise manuelles Eingreifen erfordern".
- Bei einem Einzelknoten-Cluster ist der im "automatisiertes, unterbrechendes Upgrade" Prozess beschriebene Ablauf zu beachten.

  Upgrades von Einzelknoten-Clustern sind mit Störungen verbunden.

Beispiel 2. Schritte

System Manager

1. Das ONTAP Zielabbild validieren:

Wenn Sie eine MetroCluster Konfiguration aktualisieren, sollte Cluster A validiert und anschließend der Validierungsprozess auf Cluster B wiederholt werden.

a. Je nachdem, welche ONTAP Version verwendet wird, ist einer der folgenden Schritte auszuführen:

Wenn Sie ausführen…	Folgendes ist zu tun…
ONTAP 9.8 oder höher	**Cluster > Übersicht** auswählen.
ONTAP 9.5, 9.6 und 9.7	**Konfiguration** > **Cluster** > **Aktualisieren** auswählen.
ONTAP 9.4 oder früher	**Konfiguration** > **Cluster Update** auswählen.

b. In der rechten Ecke des **Übersicht**-Bereichs auf ⋮ klicken.

c. **ONTAP Update** auswählen.

d. Auf der Registerkarte **Cluster Update** ein neues Image hinzufügen oder ein verfügbares Image auswählen.

Wenn Sie möchten…	Dann…
Ein neues Software-Image aus einem lokalen Ordner hinzufügen Sie sollten bereits "das Image heruntergeladen" eine Verbindung zum lokalen Client hergestellt haben.	i. Unter **Verfügbare Software-Images** auf **Von lokal hinzufügen** klicken. ii. Navigieren Sie zu dem Speicherort, an dem Sie das Software-Image gespeichert haben, wählen Sie das Image aus und klicken Sie anschließend auf **Open**.
Ein neues Software-Image von einem HTTP- oder FTP-Server hinzufügen	i. **Vom Server hinzufügen** auswählen. ii. Im Dialogfeld **Neues Software-Image hinzufügen** ist die URL des HTTP- oder FTP-Servers einzugeben, auf den das ONTAP Software-Image von der NetApp Support Site heruntergeladen wurde. Für anonymes FTP müssen Sie die URL im Format ftp://anonymous@ftpserver angeben. iii. Klicken Sie auf **Add**.
Wählen Sie ein verfügbares Bild	Eines der aufgelisteten Bilder kann ausgewählt werden.

e. Wählen Sie **Validieren**, um die Validierungsprüfungen vor dem Upgrade auszuführen.

Werden während der Validierung Fehler oder Warnungen gefunden, werden diese zusammen mit einer Liste von Korrekturmaßnahmen angezeigt. Alle Fehler müssen behoben werden, bevor mit dem Upgrade fortgefahren werden kann. Es gilt als Best Practice, auch Warnungen zu beheben.

Ab ONTAP 9.19.1 werden Fehler und Warnungen separat angezeigt, damit Sie Probleme, die vor dem Upgrade behoben werden müssen, leichter erkennen können.

2. Klicken Sie auf **Weiter**.
3. Auf **Aktualisieren** klicken.

   Die Validierung wird erneut durchgeführt. Alle verbleibenden Fehler oder Warnungen werden zusammen mit einer Liste der Korrekturmaßnahmen angezeigt. Fehler müssen behoben werden, bevor mit dem Upgrade fortgefahren werden kann. Wenn die Validierung mit Warnungen abgeschlossen wird, können die Warnungen behoben oder **Mit Warnungen aktualisieren** ausgewählt werden.

   > Standardmäßig verwendet ONTAP die "Batch-Upgrade-Prozess" zum Upgrade von Clustern mit acht oder mehr Knoten. Ab ONTAP 9.10.1 besteht die Möglichkeit, bei Bedarf **Jedes HA-Paar einzeln aktualisieren** auszuwählen, um die Standardeinstellung zu überschreiben und das Cluster mithilfe des Rolling-Upgrade-Prozesses jeweils um ein HA-Paar zu aktualisieren.

   Bei MetroCluster Konfigurationen mit mehr als 2 Knoten startet der ONTAP Upgrade-Prozess gleichzeitig auf den HA-Paaren an beiden Standorten. Bei einer 2-Knoten MetroCluster Konfiguration wird das Upgrade zuerst an dem Standort gestartet, an dem das Upgrade nicht initiiert wird. Das Upgrade am verbleibenden Standort beginnt, nachdem das erste Upgrade vollständig abgeschlossen ist.

4. Wenn Ihr Upgrade aufgrund eines Fehlers pausiert, auf die Fehlermeldung klicken, um die Details anzuzeigen, dann den Fehler beheben und "Das Upgrade fortsetzen".

Nachdem Sie fertig sind

Nach erfolgreichem Abschluss des Upgrades startet der Knoten neu, und Sie werden zur Anmeldeseite des System Manager weitergeleitet. Falls der Neustart des Knotens längere Zeit in Anspruch nimmt, empfiehlt sich ein Aktualisieren des Browsers.

CLI

1. Die ONTAP Zielsoftware-Abbilddatei validieren

   > Wenn Sie eine MetroCluster Konfiguration aktualisieren, sollten zuerst die folgenden Schritte auf Cluster A und anschließend die gleichen Schritte auf Cluster B ausgeführt werden.

   a. Das vorherige ONTAP Softwarepaket löschen:

   ```
   cluster image package delete -version <previous_ONTAP_Version>
   ```

   b. Das Ziel-ONTAP Software-Image wird in das Cluster-Paket-Repository geladen:

   ```
   cluster image package get -url location
   ```

   ```
   cluster1::> cluster image package get -url
   http://www.example.com/software/9.13.1/image.tgz

   Package download completed.
   ```

```
Package processing completed.
```

Wenn Sie ein "direktes Multi-Hop-Upgrade" durchführen, muss auch das Softwarepaket für die für Ihr Upgrade erforderliche Zwischenversion von ONTAP geladen werden. Wenn beispielsweise ein Upgrade von 9.8 auf 9.13.1 erfolgt, muss das Softwarepaket für ONTAP 9.12.1 geladen werden, und anschließend wird mit demselben Befehl das Softwarepaket für 9.13.1 geladen.

c. Es sollte sichergestellt sein, dass das Softwarepaket im Cluster-Paket-Repository verfügbar ist:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1             MM/DD/YYYY 10:32:15
```

d. Die automatisierten Vorabprüfungen für das Upgrade werden ausgeführt:

```
cluster image validate -version <package_version_number>
```

Wenn Sie ein "direktes Multi-Hop-Upgrade" durchführen, benötigen Sie für die Verifizierung lediglich das Ziel-ONTAP-Paket. Das Zwischen-Upgrade-Image muss nicht separat validiert werden. Beispielsweise wird bei einem Upgrade von 9.8 auf 9.13.1 das 9.13.1-Paket für die Verifizierung verwendet. Das 9.12.1-Paket muss nicht separat validiert werden.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks
that must be performed after these automated validation checks
have completed...
```

e. Fortschritt der Validierung überwachen:

```
cluster image show-update-progress
```

f. Alle im Rahmen der Validierung identifizierten erforderlichen Aktionen müssen abgeschlossen werden.

Es wird eine Liste aller automatisierten Vorabprüfungen für das Upgrade angezeigt, zusammen mit allen Fehlern und Warnungen, die vor Beginn des Upgrade-Prozesses behoben werden sollten. Alle Fehler müssen behoben werden, bevor mit dem Upgrade fortgefahren werden kann. Es gilt als Best Practice, auch Warnungen zu beheben.

Ab ONTAP 9.19.1 werden Fehler und Warnungen separat angezeigt, damit Sie Probleme, die vor

dem Upgrade behoben werden müssen, leichter erkennen können.

a. Wenn eine MetroCluster Konfiguration aktualisiert wird, sind die oben genannten Schritte auf Cluster B zu wiederholen.

2. Kostenschätzung für ein Software-Upgrade erstellen:

```
cluster image update -version <package_version_number> -estimate
-only
```

Wenn Sie eine MetroCluster Konfiguration aktualisieren, kann dieser Befehl entweder auf Cluster A oder auf Cluster B ausgeführt werden. Es ist nicht erforderlich, ihn auf beiden Clustern auszuführen.

Die Kostenschätzung für das Software-Upgrade enthält Details zu jeder zu aktualisierenden Komponente sowie die geschätzte Dauer des Upgrades.

3. Das Software-Upgrade ausführen:

```
cluster image update -version <package_version_number>
```

- Wenn Sie ein "direktes Multi-Hop-Upgrade" durchführen, verwenden Sie die Ziel ONTAP Version für die package_version_number. Wenn Sie beispielsweise von ONTAP 9.8 auf 9.13.1 aktualisieren, wird 9.13.1 als package_version_number verwendet.
- Standardmäßig verwendet ONTAP die "Batch-Upgrade-Prozess" zum Upgrade von Clustern mit acht oder mehr Knoten. Falls gewünscht, kann der `-force-rolling` Parameter verwendet werden, um den Standardprozess zu überschreiben und das Cluster nacheinander, jeweils ein Knoten, mit dem Rolling-Upgrade-Prozess zu aktualisieren.
- Nach jedem Übernahme- und Rückgabevorgang wartet das Upgrade 8 Minuten, damit sich Clientanwendungen von der während der Übernahme und Rückgabe auftretenden E/A-Pause erholen können. Wenn Ihre Umgebung mehr oder weniger Zeit für die Stabilisierung der Clients benötigt, kann mit dem `-stabilize-minutes` Parameter eine andere Dauer für die Stabilisierung festgelegt werden.
- Bei MetroCluster Konfigurationen mit 4 oder mehr Knoten startet das automatisierte Upgrade gleichzeitig auf den HA-Paaren an beiden Standorten. Bei einer 2-Node-MetroCluster Konfiguration beginnt das Upgrade an dem Standort, an dem das Upgrade nicht initiiert wurde. Das Upgrade am verbleibenden Standort beginnt, nachdem das erste Upgrade vollständig abgeschlossen ist.

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
```

```
--------------------- ----------
-----------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. Fortschritt der Clusteraktualisierung anzeigen:

```
cluster image show-update-progress
```

Wenn Sie eine 4-Node- oder 8-Node MetroCluster Konfiguration aktualisieren, zeigt der `cluster image show-update-progress` Befehl nur den Fortschritt für den Knoten an, auf dem der Befehl ausgeführt wird. Der Befehl muss auf jedem Knoten ausgeführt werden, um den Fortschritt der einzelnen Knoten anzuzeigen.

5. Es sollte überprüft werden, ob das Upgrade auf jedem Knoten erfolgreich abgeschlossen wurde.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

                                          Estimated
Elapsed
Update Phase         Status                Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed              00:10:00
00:02:07
Data ONTAP updates   completed              01:31:00
01:39:00
Post-update checks   completed              00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. Eine AutoSupport-Benachrichtigung auslösen:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Wenn Ihr Cluster nicht für den Versand von AutoSupport-Nachrichten konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

7. Wenn ein Upgrade einer 2-Node MetroCluster FC Konfiguration durchgeführt wird, sollte überprüft werden, ob der Cluster für die automatische ungeplante Umschaltung aktiviert ist.

   Wenn Sie eine Standardkonfiguration, eine MetroCluster IP-Konfiguration oder eine MetroCluster FC-Konfiguration mit mehr als 2 Knoten aktualisieren, ist dieser Schritt nicht erforderlich.

   a. Es kann überprüft werden, ob die automatische ungeplante Umschaltung aktiviert ist:

      ```
      metrocluster show
      ```

      Wenn die automatische ungeplante Umschaltung aktiviert ist, erscheint die folgende Meldung in der Befehlsausgabe:

      ```
      AUSO Failure Domain    auso-on-cluster-disaster
      ```

   a. Wenn die Anweisung nicht in der Ausgabe erscheint, sollte die automatische ungeplante Umschaltung aktiviert werden:

      ```
      metrocluster modify -auto-switchover-failure-domain auso-on-
      cluster-disaster
      ```

   b. Es sollte überprüft werden, ob die automatische ungeplante Umschaltung aktiviert ist:

      ```
      metrocluster show
      ```

Was kommt als Nächstes?

Wenn Sie Ihre Firmware vorab bereitgestellt haben, kann mit dem `system node firmware bootmedia show` Befehl überprüft werden, ob die vorgesehene Firmware-Version auf jedem Knoten aktiv ist.

Fortsetzung des ONTAP Software Upgrades nach einem Fehler im automatisierten Upgrade-Prozess

Wenn ein automatisiertes ONTAP Software-Upgrade aufgrund eines Fehlers pausiert, sollte der Fehler behoben und das Upgrade anschließend fortgesetzt werden. Nach der Fehlerbehebung besteht die Möglichkeit, den automatisierten Upgrade-Prozess fortzusetzen oder den Upgrade-Prozess manuell abzuschließen. Wenn die Fortsetzung des automatisierten Upgrades gewählt wird, dürfen keine der Upgrade-Schritte manuell durchgeführt werden.

Beispiel 3. Schritte

System Manager

1. Je nachdem, welche ONTAP Version verwendet wird, ist einer der folgenden Schritte auszuführen:

Wenn Sie ausführen…	Dann…
ONTAP 9.8 oder höher	**Cluster** > **Übersicht** auswählen
ONTAP 9.7, 9.6 oder 9.5	**Konfiguration** > **Cluster** > **Aktualisieren** auswählen.
ONTAP 9.4 oder früher	• **Konfiguration** > **Cluster Update** auswählen. • In der rechten Ecke des **Übersicht**-Bereichs auf die drei blauen vertikalen Punkte klicken und **ONTAP Update** auswählen.

2. Das automatisierte Upgrade kann fortgesetzt oder abgebrochen und manuell weitergeführt werden.

Wenn Sie möchten…	Dann…
Automatisierte Aktualisierung fortsetzen	Klicken Sie auf **Fortsetzen**.
Das automatisierte Upgrade abbrechen und manuell fortsetzen	Auf **Abbrechen** klicken.

CLI

1. Upgrade-Fehler anzeigen:

```
cluster image show-update-progress
```

2. Der Fehler wird behoben.
3. Upgrade fortsetzen:

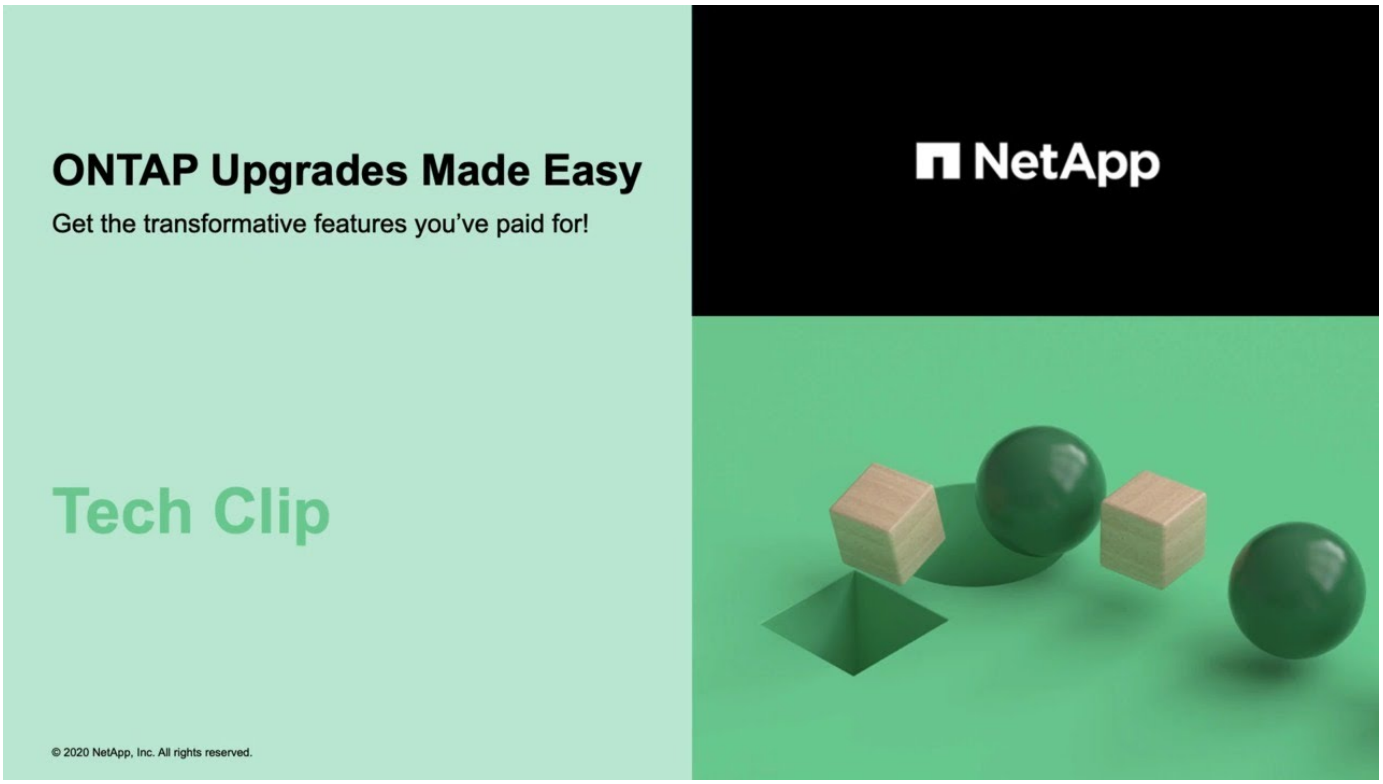
Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Automatisierte Aktualisierung fortsetzen	`cluster image resume-update`
Das automatisierte Upgrade abbrechen und manuell fortsetzen	`cluster image cancel-update`

Nachdem Sie fertig sind

"Prüfungen nach dem Upgrade durchführen".

Video: Upgrades leicht gemacht

Ein Überblick über die vereinfachten ONTAP Upgrade-Funktionen von System Manager in ONTAP 9.8.



Verwandte Informationen

- "Active IQ Digital Advisor starten"
- "Active IQ Digital Advisor Dokumentation"
- "Clusterbild"
- "autosupport invoke"
- "MetroCluster"

Manuelle Upgrades

Das ONTAP Softwarepaket für manuelle Upgrades installieren

Nachdem Sie das ONTAP Softwarepaket für ein manuelles Upgrade heruntergeladen haben, muss es lokal installiert werden, bevor das Upgrade begonnen wird.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein und geben Sie **y** ein, wenn Sie zur Fortsetzung aufgefordert werden: `set -privilege advanced`

   Die erweiterte Eingabeaufforderung (`*>`) erscheint.

2. Das Image wird installiert.

Wenn Sie die folgende Konfiguration haben…	Verwenden Sie diesen Befehl…
• Nicht MetroCluster • 2-Node MetroCluster	`system node image update -node * -package <location> -replace -package true -setdefault true -background true` `<location>` kann je nach ONTAP Version ein Webserver oder ein lokaler Ordner sein. Weitere Informationen zu `system node image update` finden sich in der "ONTAP-Befehlsreferenz". Dieser Befehl installiert das Software-Image gleichzeitig auf allen Knoten. Um das Image nacheinander auf jedem Knoten zu installieren, darf der `-background` Parameter nicht angegeben werden.
• 4-Node MetroCluster • 8-Node MetroCluster Konfiguration	`system node image update -node * -package <location> -replace -package true -background true -setdefault false` Dieser Befehl muss auf beiden Clustern ausgeführt werden. Dieser Befehl verwendet eine erweiterte Abfrage, um das Zielsoftware-Image zu ändern, das als alternatives Image auf jedem Knoten installiert ist.

3. Geben Sie `y` ein, um fortzufahren, wenn Sie dazu aufgefordert werden.
4. Es sollte sichergestellt sein, dass das Software-Image auf jedem Knoten installiert ist.

```
system node image show-update-progress -node *
```

Dieser Befehl zeigt den aktuellen Status der Software-Image-Installation an. Es wird empfohlen, diesen Befehl weiterhin auszuführen, bis alle Knoten einen **Ausführungsstatus** von **Beendet** und einen **Exit-Status** von **Erfolgreich** melden.

Der Befehl zum Aktualisieren des Systemknoten-Images kann fehlschlagen und Fehler- oder Warnmeldungen anzeigen. Nach Behebung aller Fehler oder Warnungen ist eine erneute Ausführung des Befehls möglich.

Dieses Beispiel zeigt einen Zwei-Node-Cluster, in dem das Software-Image auf beiden Knoten erfolgreich installiert wurde:

```
cluster1::*> system node image show-update-progress -node *
```

```
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Standard ONTAP Konfigurationen manuell und unterbrechungsfrei aktualisieren

Die automatisierte Aktualisierung mit System Manager ist die bevorzugte Upgrade-Methode. Wenn System Manager Ihre Konfiguration nicht unterstützt, kann die ONTAP Befehlszeilenschnittstelle (CLI) für ein manuelles unterbrechungsfreies Upgrade verwendet werden. Für das Upgrade eines Clusters mit zwei oder mehr Nodes mittels der manuellen unterbrechungsfreien Methode ist es erforderlich, auf jedem Node eines HA-Paars einen Failover-Vorgang zu initiieren, den „failed“-Node zu aktualisieren, die Rückgabe zu starten und diesen Prozess für jedes HA-Paar im Cluster zu wiederholen.

Bevor Sie beginnen

Die Upgrade-"Vorbereitung"Anforderungen müssen erfüllt sein.

Aktualisierung des ersten Knotens in einem HA-Paar

Sie können den ersten Knoten eines HA-Paares aktualisieren, indem eine Übernahme durch den Partnerknoten eingeleitet wird. Der Partnerknoten stellt die Daten des ersten Knotens bereit, während dieser aktualisiert wird.

Wenn Sie ein größeres Upgrade durchführen, muss der erste zu aktualisierende Knoten derselbe Knoten sein, auf dem Sie die Daten-LIFs für die externe Konnektivität konfiguriert und das erste ONTAP Image installiert haben.

Nach dem Upgrade des ersten Knotens sollte der Partnerknoten so schnell wie möglich aktualisiert werden. Die beiden Knoten sollten sich nicht länger als nötig in einem "gemischte Version" Zustand befinden.

Schritte

1. Der erste Node im Cluster wird aktualisiert, indem eine AutoSupport-Nachricht ausgelöst wird:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Diese AutoSupport Benachrichtigung enthält einen Datensatz des Systemstatus unmittelbar vor dem Update. Es werden nützliche Informationen zur Fehlerbehebung gespeichert, falls ein Problem mit dem Update-Prozess auftritt.

Wenn der Cluster nicht für den Versand von AutoSupport-Nachrichten konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt, wobei bei entsprechender Aufforderung **y** einzugeben ist, um fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

3. Das neue ONTAP Software-Image als Standard-Image festlegen:

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

Der Befehl „system image modify“ verwendet eine erweiterte Abfrage, um das neue ONTAP Software-Image (das als alternatives Image installiert wird) in das Standard-Image für den Node zu ändern.

4. Der Fortschritt des Updates kann überwacht werden:

```
system node upgrade-revert show
```

5. Es sollte überprüft werden, ob das neue ONTAP Software-Image als Standard-Image festgelegt ist:

```
system image show
```

Im folgenden Beispiel ist image2 die neue ONTAP Version und wird als Standardimage auf node0 festgelegt:

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

6. Die automatische Rückgabe auf dem Partner-Node ist zu deaktivieren, falls sie aktiviert ist:

```
storage failover modify -node nodenameB -auto-giveback false
```

Wenn es sich bei dem Cluster um ein Zwei-Node-Cluster handelt, wird eine Meldung angezeigt, die darauf hinweist, dass das Deaktivieren der automatischen Rückgabe verhindert, dass die Management-Cluster-Services im Falle eines alternierenden Ausfallszenarios online gehen. Geben Sie `y` ein, um fortzufahren.

7. Es sollte überprüft werden, ob das automatische Giveback für den Partner des Knotens deaktiviert ist:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. Führen Sie den folgenden Befehl zweimal aus, um festzustellen, ob der zu aktualisierende Node derzeit Clients bedient

```
system node run -node nodenameA -command uptime
```

Der Befehl `uptime` zeigt die Gesamtzahl der Operationen an, die der Knoten seit dem letzten Start für NFS, SMB, FC und iSCSI Clients ausgeführt hat. Für jedes Protokoll muss der Befehl zweimal ausgeführt werden, um festzustellen, ob die Anzahl der Operationen steigt. Wenn sie steigt, bedient der Knoten derzeit Clients für dieses Protokoll. Wenn sie nicht steigt, bedient der Knoten derzeit keine Clients für dieses Protokoll.

> Es empfiehlt sich, jedes Protokoll zu notieren, bei dem die Client-Operationen zunehmen, sodass nach der Aktualisierung des Knotens überprüft werden kann, ob der Client-Datenverkehr wieder aufgenommen wurde.

Das folgende Beispiel zeigt einen Knoten mit NFS-, SMB-, FC- und iSCSI-Operationen. Allerdings bedient der Knoten derzeit nur NFS- und iSCSI-Clients.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Alle Daten-LIFs vom Knoten migrieren:

```
network interface migrate-all -node nodenameA
```

10. Alle migrierten LIFs überprüfen:

```
network interface show
```

Weitere Informationen zu `network interface show` und zu Parametern, mit denen der LIF-Status überprüft werden kann, finden Sie im "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass die Data-LIFs von node0 erfolgreich migriert wurden. Für jede LIF ermöglichen die in diesem Beispiel enthaltenen Felder die Überprüfung des Home-Nodes und Ports der LIF, des aktuellen Nodes und Ports, zu dem die LIF migriert wurde, sowie des Betriebs- und Verwaltungsstatus der LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. Eine Übernahme initiieren:

```
storage failover takeover -ofnode nodenameA
```

Geben Sie den Parameter „-option immediate“ nicht an, da für den zu übernehmenden Knoten ein normaler Übernahmevorgang erforderlich ist, damit der Knoten mit dem neuen Software-Image startet. Wenn die LIFs nicht manuell vom Knoten migriert wurden, migrieren sie automatisch zum HA-Partner des Knotens, sodass keine Serviceunterbrechungen auftreten.

Der erste Knoten startet im Zustand „Warten auf Rückgabe“.



Wenn AutoSupport aktiviert ist, wird eine AutoSupport-Meldung gesendet, die darauf hinweist, dass der Knoten das Cluster-Quorum verlassen hat. Diese Benachrichtigung kann ignoriert und das Update fortgesetzt werden.

12. Es sollte überprüft werden, ob die Übernahme erfolgreich war:

```
storage failover show
```

Möglicherweise werden Fehlermeldungen angezeigt, die auf Versionskonflikte und Probleme mit dem Postfachformat hinweisen. Dies ist ein erwartetes Verhalten und stellt einen vorübergehenden Zustand während eines größeren unterbrechungsfreien Upgrades dar und ist unbedenklich.

Das folgende Beispiel zeigt, dass die Übernahme erfolgreich war. Knoten node0 befindet sich im Zustand „Warten auf Rückgabe“, und sein Partner befindet sich im Zustand „In Übernahme“.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. Mindestens acht Minuten abwarten, bis die folgenden Bedingungen wirksam werden:
    - Client Multipathing (sofern implementiert) ist stabilisiert.
    - Die Clients werden nach einer Unterbrechung einer E/A-Operation, die während einer Übernahme auftritt, wiederhergestellt.

      Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.
14. Die Aggregate an den ersten Knoten zurückgeben:

    ```
    storage failover giveback -ofnode nodenameA
    ```

    Der Giveback-Vorgang gibt zunächst das Root-Aggregat an den Partnerknoten zurück und anschließend, nachdem dieser den Startvorgang abgeschlossen hat, die Nicht-Root-Aggregate sowie alle LIFs, die für die automatische Rücksetzung konfiguriert wurden, zurück. Der neu gestartete Knoten beginnt, Daten für Clients aus jedem Aggregat bereitzustellen, sobald das Aggregat zurückgegeben wurde.
15. Es sollte sichergestellt sein, dass alle Aggregate zurückgegeben wurden:

    ```
    storage failover show-giveback
    ```

    Wenn das Feld „Rückgabestatus“ anzeigt, dass keine Aggregate zurückzugeben sind, wurden alle Aggregate zurückgegeben. Wenn die Rückgabe abgelehnt wird, zeigt der Befehl den Fortschritt der Rückgabe und das Subsystem an, das die Rückgabe abgelehnt hat.
16. Wenn einige Aggregate nicht zurückgegeben wurden, sind die folgenden Schritte auszuführen:

a. Die Vorgehensweise zur Umgehung des Veto-Problems kann herangezogen werden, um zu bestimmen, ob die “veto”-Bedingung behoben oder das Veto außer Kraft gesetzt werden soll.
b. Falls erforderlich sollte die in der Fehlermeldung beschriebene “veto”-Bedingung behoben werden, wobei sichergestellt wird, dass alle identifizierten Operationen ordnungsgemäß beendet werden.
c. Den `storage failover giveback`Befehl erneut ausführen.

   Wenn die “veto”-Bedingung außer Kraft gesetzt werden soll, ist der Parameter -override-vetoes auf true zu setzen.

17. Mindestens acht Minuten abwarten, bis die folgenden Bedingungen wirksam werden:
    - Client Multipathing (sofern implementiert) ist stabilisiert.
    - Clients werden aus der Pause einer E/A-Operation wiederhergestellt, die während der Rückgabe auftritt.

      Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.

18. Überprüfen, ob die Aktualisierung für den Node erfolgreich abgeschlossen wurde:

    a. Zur erweiterten Berechtigungsstufe wechseln:

    ```
    set -privilege advanced
    ```

    b. Es wird geprüft, ob der Aktualisierungsstatus für den Knoten abgeschlossen ist:

    ```
    system node upgrade-revert show -node nodenameA
    ```

    Der Status sollte als abgeschlossen angezeigt werden.

    Wenn der Status nicht vollständig ist, den technischen Support kontaktieren.

    a. Zurück zur Administrator-Privilegstufe:

    ```
    set -privilege admin
    ```

19. Es wird geprüft, ob die Ports des Knotens aktiv sind:

    ```
    network port show -node nodenameA
    ```

    Dieser Befehl muss auf einem Knoten ausgeführt werden, der auf die höhere Version von ONTAP 9 aktualisiert wurde.

    Das folgende Beispiel zeigt, dass alle Ports des Knotens aktiv sind:

    ```
    cluster1::> network port show -node node0
    ```

```
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node0
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

20. Die LIFs werden wieder auf den Knoten zurückgesetzt:

```
network interface revert *
```

Dieser Befehl gibt die LIFs zurück, die vom Knoten migriert wurden.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Es sollte überprüft werden, ob die Data-LIFs des Knotens erfolgreich auf den Knoten zurückgekehrt sind und ob sie aktiv sind:

```
network interface show
```

Das folgende Beispiel zeigt, dass alle vom Knoten gehosteten Daten-LIFs erfolgreich zum Knoten zurückgeführt wurden und ihr Betriebsstatus aktiv ist:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0a
true
            data002      up/up    192.0.2.121/24     node0         e0b
true
            data003      up/up    192.0.2.122/24     node0         e0b
```

```
true
            data004      up/up    192.0.2.123/24     node0          e0a
true
4 entries were displayed.
```

22. Wenn Sie zuvor festgestellt haben, dass dieser Knoten Clients bedient, überprüfen Sie, ob der Knoten für jedes Protokoll, das er zuvor bedient hat, weiterhin Dienste bereitstellt:

```
system node run -node nodenameA -command uptime
```

Die Vorgangszähler werden während des Updates auf Null zurückgesetzt.

Das folgende Beispiel zeigt, dass der aktualisierte Knoten seine NFS- und iSCSI-Clients wieder bedient:

```
cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Die automatische Rückgabe auf dem Partnerknoten wird wieder aktiviert, falls sie zuvor deaktiviert war:

```
storage failover modify -node nodenameB -auto-giveback true
```

Das Update des HA-Partners des Knotens sollte so schnell wie möglich durchgeführt werden. Falls der Aktualisierungsprozess aus irgendeinem Grund unterbrochen werden muss, sollten beide Knoten des HA-Paars dieselbe ONTAP Version ausführen.

Aktualisierung des Partnerknotens in einem HA-Paar

Nach der Aktualisierung des ersten Knotens in einem HA-Paar wird der Partner aktualisiert, indem eine Übernahme auf ihm initiiert wird. Der erste Knoten stellt die Daten des Partners bereit, während der Partnerknoten aktualisiert wird.

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt, wobei bei entsprechender Aufforderung **y** einzugeben ist, um fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) erscheint.

2. Das neue ONTAP Software-Image als Standard-Image festlegen:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

Der Befehl „system image modify“ verwendet eine erweiterte Abfrage, um das neue ONTAP Software-

Image (das als alternatives Image installiert wird) als Standard-Image für den Knoten festzulegen.

3. Der Fortschritt des Updates kann überwacht werden:

```
system node upgrade-revert show
```

4. Es sollte überprüft werden, ob das neue ONTAP Software-Image als Standard-Image festgelegt ist:

```
system image show
```

Im folgenden Beispiel ist `image2` die neue Version von ONTAP und als Standardimage auf dem Knoten festgelegt:

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

5. Die automatische Rückgabe auf dem Partner-Node ist zu deaktivieren, falls sie aktiviert ist:

```
storage failover modify -node nodenameA -auto-giveback false
```

Wenn es sich bei dem Cluster um ein Zwei-Node-Cluster handelt, wird eine Meldung angezeigt, die darauf hinweist, dass das Deaktivieren der automatischen Rückgabe verhindert, dass die Management-Cluster-Services im Falle eines alternierenden Ausfallszenarios online gehen. Geben Sie `y` ein, um fortzufahren.

6. Es sollte überprüft werden, ob die automatische Rückgabe für den Partnerknoten deaktiviert ist:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- -------------
node0    false
```

```
1 entry was displayed.
```

7. Führen Sie den folgenden Befehl zweimal aus, um zu ermitteln, ob der zu aktualisierende Knoten derzeit Clients bedient:

```
system node run -node nodenameB -command uptime
```

Der Befehl `uptime` zeigt die Gesamtzahl der Operationen an, die der Knoten seit dem letzten Start für NFS, SMB, FC und iSCSI Clients ausgeführt hat. Für jedes Protokoll muss der Befehl zweimal ausgeführt werden, um festzustellen, ob die Anzahl der Operationen steigt. Wenn sie steigt, bedient der Knoten derzeit Clients für dieses Protokoll. Wenn sie nicht steigt, bedient der Knoten derzeit keine Clients für dieses Protokoll.



Es empfiehlt sich, jedes Protokoll zu notieren, bei dem die Client-Operationen zunehmen, sodass nach der Aktualisierung des Knotens überprüft werden kann, ob der Client-Datenverkehr wieder aufgenommen wurde.

Das folgende Beispiel zeigt einen Knoten mit NFS-, SMB-, FC- und iSCSI-Operationen. Allerdings bedient der Knoten derzeit nur NFS- und iSCSI-Clients.

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Alle Daten-LIFs vom Knoten migrieren:

```
network interface migrate-all -node nodenameB
```

9. Status aller migrierten LIFs überprüfen:

```
network interface show
```

Weitere Informationen zu `network interface show` und zu Parametern, mit denen der LIF-Status überprüft werden kann, finden Sie im "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass die Data-LIFs von node1 erfolgreich migriert wurden. Für jede LIF ermöglichen die in diesem Beispiel enthaltenen Felder die Überprüfung des Home-Nodes und Ports der LIF, des aktuellen Nodes und Ports, zu dem die LIF migriert wurde, sowie des Betriebs- und Verwaltungsstatus der LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up          up
vs0     data002 node1     e0b       node0     e0b       up          up
vs0     data003 node1     e0b       node0     e0b       up          up
vs0     data004 node1     e0a       node0     e0a       up          up
4 entries were displayed.
```

10. Eine Übernahme initiieren:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

Geben Sie den Parameter „-option immediate“ nicht an, da für den zu übernehmenden Knoten ein normaler Übernahmevorgang erforderlich ist, damit der Knoten mit dem neuen Software-Image startet. Wenn die LIFs nicht manuell vom Knoten migriert wurden, migrieren sie automatisch zum HA-Partner des Knotens, sodass keine Serviceunterbrechungen auftreten.

Es wird eine Warnung angezeigt. Sie müssen `y` eingeben, um fortzufahren.

Der übernommene Knoten startet im Zustand „Warten auf Rückgabe“.

Wenn AutoSupport aktiviert ist, wird eine AutoSupport-Meldung gesendet, die darauf hinweist, dass der Knoten das Cluster-Quorum verlassen hat. Diese Benachrichtigung kann ignoriert und das Update fortgesetzt werden.

11. Es sollte überprüft werden, ob die Übernahme erfolgreich war:

```
storage failover show
```

Das folgende Beispiel zeigt, dass die Übernahme erfolgreich war. Knoten node1 befindet sich im Zustand „Warten auf Rückgabe“, und sein Partner befindet sich im Zustand „In Übernahme“.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
```

```
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. Mindestens acht Minuten abwarten, damit die folgenden Bedingungen wirksam werden: +
    - Client Multipathing (sofern implementiert) ist stabilisiert.
    - Clients werden nach der Unterbrechung der E/A, die während der Übernahme auftritt, wiederhergestellt.

      Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.
13. Die Aggregate an den Partnerknoten zurückgeben:

    ```
    storage failover giveback -ofnode nodenameB
    ```

    Der Rückgabevorgang gibt zunächst das Root-Aggregat an den Partnerknoten zurück und anschließend, nachdem dieser den Startvorgang abgeschlossen hat, die Nicht-Root-Aggregate sowie alle LIFs, die für die automatische Rücksetzung konfiguriert wurden. Der neu gestartete Knoten beginnt, Daten für Clients aus jedem Aggregat bereitzustellen, sobald das Aggregat zurückgegeben wurde.
14. Es wird überprüft, ob alle Aggregate zurückgegeben werden:

    ```
    storage failover show-giveback
    ```

    Wenn das Feld „Rückgabestatus“ anzeigt, dass keine Aggregate zurückzugeben sind, werden alle Aggregate zurückgegeben. Wenn die Rückgabe abgelehnt wird, zeigt der Befehl den Fortschritt der Rückgabe und das Subsystem an, das die Rückgabe abgelehnt hat.
15. Wenn keine Aggregate zurückgegeben werden, sind die folgenden Schritte auszuführen:
    a. Die Vorgehensweise zur Umgehung des Veto-Problems kann herangezogen werden, um zu bestimmen, ob die “veto”-Bedingung behoben oder das Veto außer Kraft gesetzt werden soll.
    b. Falls erforderlich sollte die in der Fehlermeldung beschriebene “veto”-Bedingung behoben werden, wobei sichergestellt wird, dass alle identifizierten Operationen ordnungsgemäß beendet werden.
    c. Den `storage failover giveback`Befehl erneut ausführen.

       Wenn die “veto”-Bedingung außer Kraft gesetzt werden soll, ist der Parameter -override-vetoes auf true zu setzen.
16. Mindestens acht Minuten abwarten, bis die folgenden Bedingungen wirksam werden:
    - Client Multipathing (sofern implementiert) ist stabilisiert.
    - Clients werden aus der Pause einer E/A-Operation wiederhergestellt, die während der Rückgabe auftritt.

      Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.

17. Überprüfen, ob die Aktualisierung für den Node erfolgreich abgeschlossen wurde:

    a. Zur erweiterten Berechtigungsstufe wechseln:

    ```
    set -privilege advanced
    ```

    b. Es wird geprüft, ob der Aktualisierungsstatus für den Knoten abgeschlossen ist:

    ```
    system node upgrade-revert show -node nodenameB
    ```

    Der Status sollte als abgeschlossen angezeigt werden.

    Wenn der Status nicht „Abgeschlossen“ ist, auf dem Knoten den `system node upgrade-revert upgrade` Befehl ausführen. Wenn der Befehl die Aktualisierung nicht abschließt, den technischen Support kontaktieren.

    a. Zurück zur Administrator-Privilegstufe:

    ```
    set -privilege admin
    ```

18. Es wird geprüft, ob die Ports des Knotens aktiv sind:

    ```
    network port show -node nodenameB
    ```

    Dieser Befehl muss auf einem Knoten ausgeführt werden, der auf ONTAP 9.4 aktualisiert wurde.

    Das folgende Beispiel zeigt, dass alle Daten-Ports des Knotens aktiv sind:

    ```
    cluster1::> network port show -node node1
                                                                   Speed
    (Mbps)
    Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
    ------ --------- ------------ ---------------- ----- -------
    ------------
    node1
           e0M       Default      -                up       1500  auto/100
           e0a       Default      -                up       1500  auto/1000
           e0b       Default      -                up       1500  auto/1000
           e1a       Cluster      Cluster          up       9000  auto/10000
           e1b       Cluster      Cluster          up       9000  auto/10000
    5 entries were displayed.
    ```

    Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

19. Die LIFs werden wieder auf den Knoten zurückgesetzt:

```
network interface revert *
```

Dieser Befehl gibt die LIFs zurück, die vom Knoten migriert wurden.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Es sollte überprüft werden, ob die Data-LIFs des Knotens erfolgreich auf den Knoten zurückgekehrt sind und ob sie aktiv sind:

```
network interface show
```

Das folgende Beispiel zeigt, dass alle vom Knoten gehosteten Daten-LIFs erfolgreich auf den Knoten zurückgesetzt wurden und dass ihr Betriebsstatus aktiv ist:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1         e0a
true
            data002      up/up    192.0.2.121/24     node1         e0b
true
            data003      up/up    192.0.2.122/24     node1         e0b
true
            data004      up/up    192.0.2.123/24     node1         e0a
true
4 entries were displayed.
```

21. Wenn Sie zuvor festgestellt haben, dass dieser Knoten Clients bedient, überprüfen Sie, ob der Knoten für jedes Protokoll, das er zuvor bedient hat, weiterhin Dienste bereitstellt:

```
system node run -node nodenameB -command uptime
```

Die Vorgangszähler werden während des Updates auf Null zurückgesetzt.

Das folgende Beispiel zeigt, dass der aktualisierte Knoten seine NFS- und iSCSI-Clients wieder bedient:

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. Wenn dies der letzte Knoten im Cluster war, der aktualisiert wurde, eine AutoSupport-Benachrichtigung auslösen:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Diese AutoSupport Benachrichtigung enthält einen Datensatz des Systemstatus unmittelbar vor dem Update. Es werden nützliche Informationen zur Fehlerbehebung gespeichert, falls ein Problem mit dem Update-Prozess auftritt.

Wenn der Cluster nicht für den Versand von AutoSupport-Nachrichten konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

23. Bestätigen Sie, dass die neue ONTAP Software auf beiden Knoten des HA-Paars ausgeführt wird:

```
set -privilege advanced
```

```
system node image show
```

Im folgenden Beispiel ist image2 die aktualisierte Version von ONTAP und die Standardversion auf beiden Knoten:

```
cluster1::*> system node image show
                 Is      Is                Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. Die automatische Rückgabe auf dem Partnerknoten wird wieder aktiviert, falls sie zuvor deaktiviert war:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Es kann überprüft werden, ob sich der Cluster im Quorum befindet und die Dienste ausgeführt werden, indem die Befehle `cluster show` und `cluster ring show` (erweiterte Berechtigungsstufe) verwendet werden.

    Dieser Schritt ist vor dem Upgrade weiterer HA-Paare erforderlich.

    Weitere Informationen zu `cluster show` und `cluster ring show` finden sich in der "ONTAP-Befehlsreferenz".

26. Zurück zur Administrator-Privilegstufe:

    ```
    set -privilege admin
    ```

27. Alle zusätzlichen HA-Paare aktualisieren.

Verwandte Informationen

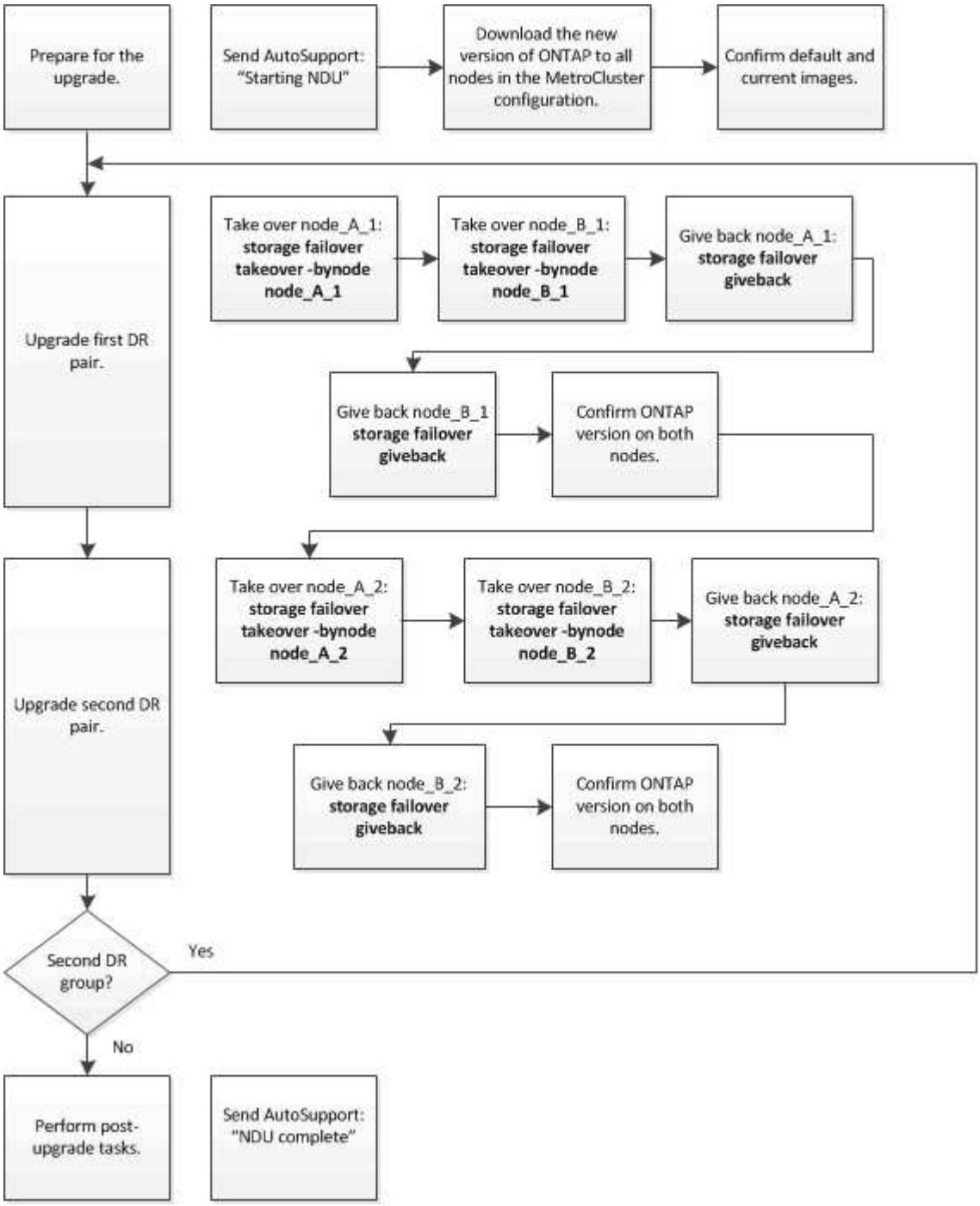
- "autosupport invoke"
- "Systemabbild"
- "Systemknoten"
- "Storage-Failover"
- "Netzwerkschnittstelle"
- "Netzwerkport anzeigen"
- "set -privilege advanced"

Manuelles Upgrade einer ONTAP MetroCluster Konfiguration mit vier oder acht Knoten

Ein manuelles, unterbrechungsfreies Upgrade (NDU) einer vier- oder acht-Knoten MetroCluster Konfiguration umfasst die Vorbereitung des Updates, die gleichzeitige Aktualisierung der DR-Paare in jeder der ein oder zwei DR-Gruppen sowie die Durchführung von Aufgaben nach dem Upgrade.

Über diese Aufgabe

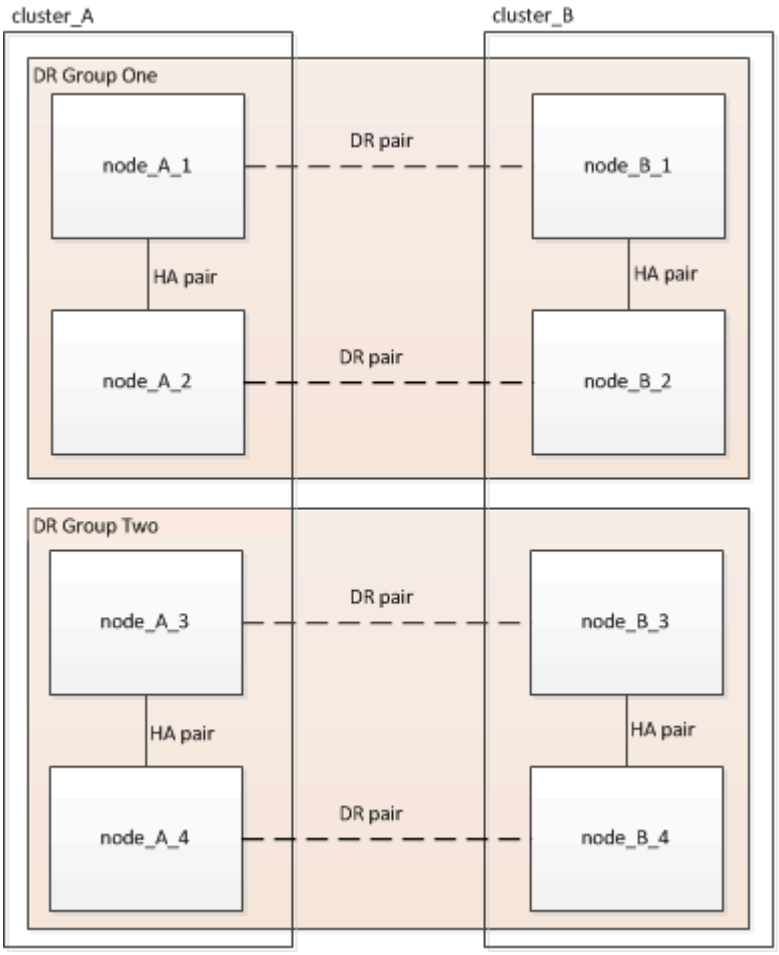
- Für diese Aufgabe muss die ONTAP command line interface (CLI) verwendet werden.
- Diese Aufgabe gilt für die folgenden Konfigurationen:
  - Vier-Knoten MetroCluster FC- oder IP-Konfigurationen mit ONTAP 9.2 oder älter
  - Acht-Knoten MetroCluster FC-Konfigurationen, unabhängig von ONTAP Version
- Wenn eine MetroCluster Konfiguration mit zwei Knoten vorliegt, sollte dieses Verfahren nicht verwendet werden.
- Die folgenden Aufgaben beziehen sich auf die alte und die neue Version von ONTAP.
  - Beim Upgrade ist die alte Version eine frühere Version von ONTAP mit einer niedrigeren Versionsnummer als die neue Version von ONTAP.
  - Beim Downgrade ist die alte Version eine spätere Version von ONTAP mit einer höheren Versionsnummer als die neue Version von ONTAP.
- Für diese Aufgabe wird folgender übergeordneter Arbeitsablauf verwendet:



Unterschiede beim Aktualisieren der ONTAP Software auf einer Acht-Knoten- oder Vier-Knoten MetroCluster Konfiguration

Der MetroCluster Software-Upgrade-Prozess unterscheidet sich, je nachdem, ob in der MetroCluster Konfiguration acht oder vier Knoten vorhanden sind.

Eine MetroCluster Konfiguration besteht aus einer oder zwei DR-Gruppen. Jede DR-Gruppe besteht aus zwei HA-Paaren, jeweils einem HA-Paar pro MetroCluster Cluster. Eine acht-Knoten MetroCluster Konfiguration umfasst zwei DR-Gruppen:



Es wird jeweils eine DR-Gruppe aktualisiert.

Für MetroCluster Konfigurationen mit vier Knoten:

1. Upgrade von DR-Gruppe eins:
   a. Node_A_1 und Node_B_1 aktualisieren.
   b. Knoten_A_2 und Knoten_B_2 aktualisieren.

Für MetroCluster Konfigurationen mit acht Knoten wird das Upgrade-Verfahren für die DR-Gruppe zweimal durchgeführt:

1. Upgrade von DR-Gruppe eins:
   a. Node_A_1 und Node_B_1 aktualisieren.
   b. Knoten_A_2 und Knoten_B_2 aktualisieren.
2. Upgrade DR Gruppe Zwei:
   a. Knoten A_3 und Knoten B_3 aktualisieren.
   b. Knoten_A_4 und Knoten_B_4 aktualisieren.

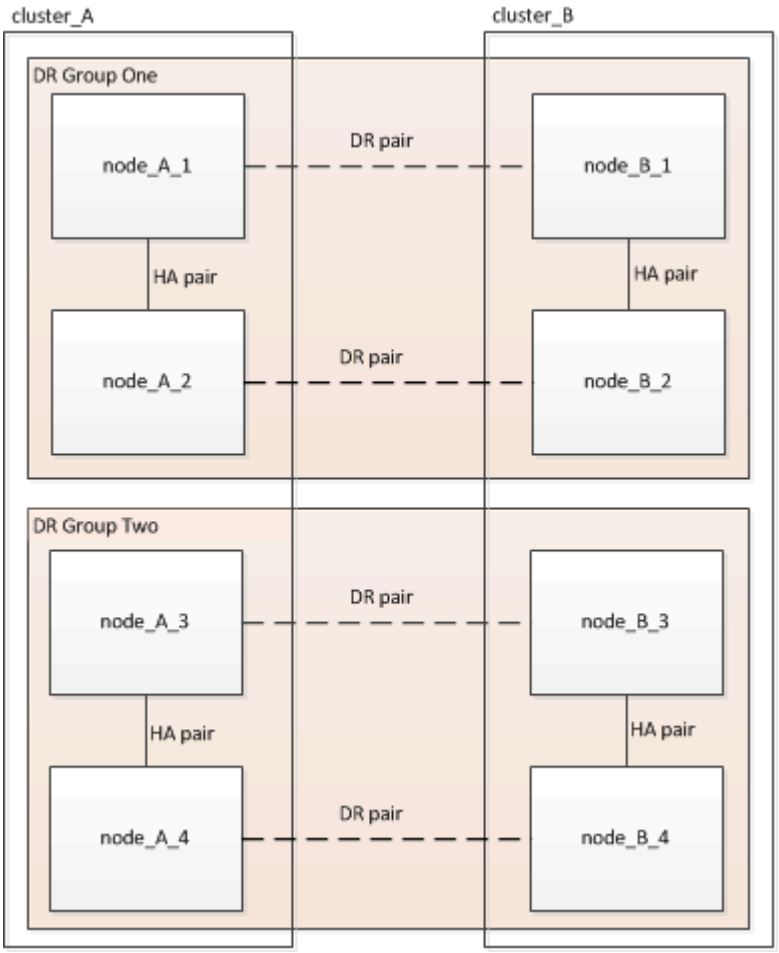
Vorbereitung der Aktualisierung einer MetroCluster DR-Gruppe

Bevor Sie die ONTAP Software auf den Knoten aktualisieren, müssen Sie die DR-Beziehungen zwischen den Knoten ermitteln, eine AutoSupport Nachricht senden, dass Sie ein Upgrade einleiten, und die auf jedem Knoten laufende ONTAP Version bestätigen.

Sie benötigen "heruntergeladen" und "installiert" die Software-Images.

Dieser Vorgang muss für jede DR-Gruppe wiederholt werden. Besteht die MetroCluster Konfiguration aus acht Knoten, gibt es zwei DR-Gruppen. Daher muss dieser Vorgang für jede DR-Gruppe wiederholt werden.

Die in dieser Aufgabe bereitgestellten Beispiele verwenden die in der folgenden Abbildung gezeigten Namen zur Identifizierung der Cluster und Knoten:



Schritte

1. Die DR-Paare in der Konfiguration identifizieren:

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
```

```
4 entries were displayed.

cluster_A::>
```

2. Die Berechtigungsstufe wird von admin auf advanced geändert, wobei bei entsprechender Aufforderung **y** eingegeben wird, um fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

3. Die ONTAP Version auf Cluster_A bestätigen:

```
system image show
```

```
cluster_A::*> system image show
                Is      Is                Install
Node     Image  Default Current Version   Date
-------- ------- ------- ------- -------   -------------------
node_A_1
         image1  true    true    X.X.X     MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1  true    true    X.X.X     MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Die Version auf Cluster_B bestätigen:

```
system image show
```

```
cluster_B::*> system image show
                Is      Is                 Install
Node     Image  Default Current Version    Date
-------- ------- ------- ------- -------    -------------------
node_B_1
         image1  true    true    X.X.X      MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node_B_2
```

```
          image1  true    true    X.X.X      MM/DD/YYYY TIME
          image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. Eine AutoSupport-Benachrichtigung auslösen:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Diese AutoSupport-Benachrichtigung enthält eine Aufzeichnung des Systemstatus vor dem Upgrade. Sie speichert nützliche Informationen zur Fehlerbehebung, falls es während des Upgrade-Prozesses zu Problemen kommt.

Wenn Ihr Cluster nicht für das Senden von AutoSupport-Nachrichten konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

6. Für jeden Knoten im ersten Satz wird das Ziel-ONTAP Software-Image als Standard-Image festgelegt:

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

Dieser Befehl verwendet eine erweiterte Abfrage, um das als alternatives Image installierte Zielsoftware-Image als Standard-Image für den Knoten festzulegen.

7. Es wird geprüft, ob das Ziel-ONTAP Software-Image auf Cluster_A als Standard-Image festgelegt ist:

```
system image show
```

Im folgenden Beispiel ist image2 die neue ONTAP Version und wird auf jedem der Knoten in der ersten Gruppe als Standard-Image festgelegt:

```
cluster_A::*> system image show
                 Is      Is              Install
Node     Image   Default Current Version Date
-------- ------- ------- ------- ------- -------------------
node_A_1
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
node_A_2
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true   false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

a. Es wird überprüft, ob das Ziel-ONTAP Software-Image auf Cluster_B als Standard-Image festgelegt ist:

```
system image show
```

Das folgende Beispiel zeigt, dass die Zielversion auf jedem der Knoten im ersten Satz als Standard-Image festgelegt ist:

```
cluster_B::*> system image show
                  Is      Is              Install
Node     Image    Default Current Version Date
-------- -------  ------- ------- ------- -------------------
node_A_1
         image1   false   true    X.X.X   MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y   MM/YY/YYYY TIME
node_A_2
         image1   false   true    X.X.X   MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

8. Ermitteln, ob die zu aktualisierenden Knoten derzeit für jeden Knoten jeweils zweimal Clients bedienen:

```
system node run -node target-node -command uptime
```

Der Befehl `uptime` zeigt die Gesamtzahl der Operationen an, die der Knoten seit dem letzten Start für NFS, CIFS, FC und iSCSI Clients ausgeführt hat. Für jedes Protokoll muss der Befehl zweimal ausgeführt werden, um festzustellen, ob die Anzahl der Operationen steigt. Wenn sie steigt, bedient der Knoten derzeit Clients für dieses Protokoll. Wenn sie nicht steigt, bedient der Knoten derzeit keine Clients für dieses Protokoll.

Sie sollten sich jedes Protokoll notieren, bei dem die Anzahl der Client-Operationen zunimmt, damit nach dem Upgrade des Knotens überprüft werden kann, ob der Client-Datenverkehr wieder aufgenommen wurde.

Dieses Beispiel zeigt einen Knoten mit NFS-, CIFS-, FC- und iSCSI-Operationen. Allerdings bedient der Knoten derzeit nur NFS- und iSCSI-Clients.

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Aktualisierung des ersten DR-Paares in einer MetroCluster DR-Gruppe

Sie müssen die Übernahme und Rückgabe der Knoten in der richtigen Reihenfolge durchführen, damit die neue Version von ONTAP zur aktuellen Version des Knotens wird.

Alle Knoten müssen die alte Version von ONTAP ausführen.

In dieser Aufgabe werden node_A_1 und node_B_1 aktualisiert.

Wenn die ONTAP Software auf der ersten DR-Gruppe aktualisiert wurde und nun die zweite DR-Gruppe in einer Acht-Knoten MetroCluster Konfiguration aktualisiert wird, werden in diesem Schritt node_A_3 und node_B_3 aktualisiert.

Schritte

1. Alle Daten-LIFs vom Knoten migrieren:

```
network interface migrate-all -node node_A_1
```

```
network interface migrate-all -node node_B_1
```

2. Falls die MetroCluster Tiebreaker-Software aktiviert ist, deaktivieren Sie sie.
3. Für jeden Node im HA-Paar die automatische Rückgabe deaktivieren:

```
storage failover modify -node target-node -auto-giveback false
```

   Dieser Befehl muss für jeden Knoten im HA-Paar wiederholt werden.

4. Überprüfen, ob das automatische Giveback deaktiviert ist:

```
storage failover show -fields auto-giveback
```

   Dieses Beispiel zeigt, dass die automatische Rückgabe auf beiden Knoten deaktiviert wurde:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 false
node_x_2 false
2 entries were displayed.
```

5. Es ist sicherzustellen, dass die I/O-Auslastung für jeden Controller etwa 50 % nicht überschreitet und die CPU-Auslastung pro Controller ebenfalls nicht über ~50 % liegt.
6. Eine Übernahme des Zielknotens auf Cluster_A initiieren:

Der Parameter -option immediate darf nicht angegeben werden, da für den Start der zu übernehmenden Knoten mit dem neuen Software-Image ein normaler Übernahmevorgang erforderlich ist.

a. Übernahme des DR-Partners auf cluster_A (node_A_1):

```
storage failover takeover -ofnode node_A_1
```

Der Knoten startet im Zustand "Warten auf Giveback".

> Wenn AutoSupport aktiviert ist, wird eine AutoSupport-Meldung gesendet, die darauf hinweist, dass die Knoten das Cluster-Quorum verlassen haben. Diese Benachrichtigung kann ignoriert werden und das Upgrade kann fortgesetzt werden.

b. Es sollte überprüft werden, ob die Übernahme erfolgreich war:

```
storage failover show
```

Das folgende Beispiel zeigt, dass die Übernahme erfolgreich war. Node_A_1 befindet sich im Status „Warten auf Rückgabe“ und node_A_2 im Status „In Übernahme“.

```
 cluster_A::> storage failover show
                                Takeover
 Node           Partner        Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_A_1       node_A_2       -        Waiting for giveback (HA
mailboxes)
 node_A_2       node_A_1       false    In takeover
 2 entries were displayed.
```

7. Übernahme des DR-Partners auf cluster_B (node_B_1):

Der Parameter -option immediate darf nicht angegeben werden, da für den Start der zu übernehmenden Knoten mit dem neuen Software-Image ein normaler Übernahmevorgang erforderlich ist.

a. Knoten B1 übernehmen:

```
storage failover takeover -ofnode node_B_1
```

Der Knoten startet im Zustand "Warten auf Giveback".

> Wenn AutoSupport aktiviert ist, wird eine AutoSupport-Meldung gesendet, die darauf hinweist, dass die Knoten das Cluster-Quorum verlassen haben. Diese Benachrichtigung kann ignoriert werden und das Upgrade kann fortgesetzt werden.

b. Es sollte überprüft werden, ob die Übernahme erfolgreich war:

```
storage failover show
```

Das folgende Beispiel zeigt, dass die Übernahme erfolgreich war. Node_B_1 befindet sich im Status „Warten auf Rückgabe“ und node_B_2 im Status „In Übernahme“.

```
cluster_B::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
node_B_2       node_B_1       false    In takeover
2 entries were displayed.
```

8. Mindestens acht Minuten warten, damit die folgenden Bedingungen sichergestellt sind:
   - Client Multipathing (sofern implementiert) ist stabilisiert.
   - Clients werden nach der Unterbrechung der E/A, die während der Übernahme auftritt, wiederhergestellt.

     Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.

9. Die Aggregate werden an die Zielknoten zurückgegeben:

   Nach dem Upgrade der MetroCluster IP-Konfigurationen auf ONTAP 9.5 oder höher befinden sich die Aggregate für kurze Zeit in einem degradierten Zustand, bevor sie sich neu synchronisieren und wieder in einen gespiegelten Zustand zurückkehren.

   a. Die Aggregate werden an den DR-Partner auf Cluster_A zurückgegeben:

   ```
   storage failover giveback -ofnode node_A_1
   ```

   b. Die Aggregate werden an den DR-Partner auf Cluster_B zurückgegeben:

   ```
   storage failover giveback -ofnode node_B_1
   ```

   Die Giveback-Operation gibt zuerst das Root-Aggregat an den Knoten zurück und gibt dann, nachdem der Knoten den Bootvorgang abgeschlossen hat, die Nicht-Root-Aggregate zurück.

10. Es sollte überprüft werden, ob alle Aggregate zurückgegeben wurden, indem auf beiden Clustern der folgende Befehl ausgeführt wird:

```
storage failover show-giveback
```

Wenn das Feld „Rückgabestatus“ anzeigt, dass keine Aggregate zurückzugeben sind, wurden alle Aggregate zurückgegeben. Wenn die Rückgabe abgelehnt wird, zeigt der Befehl den Fortschritt der Rückgabe und das Subsystem an, das die Rückgabe abgelehnt hat.

11. Wenn Aggregate nicht zurückgegeben wurden, ist Folgendes zu tun:
    a. Die Vorgehensweise zur Umgehung des Veto-Problems kann herangezogen werden, um zu bestimmen, ob die “veto”-Bedingung behoben oder das Veto außer Kraft gesetzt werden soll.
    b. Falls erforderlich sollte die in der Fehlermeldung beschriebene “veto”-Bedingung behoben werden, wobei sichergestellt wird, dass alle identifizierten Operationen ordnungsgemäß beendet werden.
    c. Geben Sie den Befehl storage failover giveback erneut ein.

       Wenn die “veto”-Bedingung außer Kraft gesetzt werden soll, ist der Parameter -override-vetoes auf true zu setzen.

12. Mindestens acht Minuten warten, damit die folgenden Bedingungen sichergestellt sind:
    - Client Multipathing (sofern implementiert) ist stabilisiert.
    - Die Clients werden nach der Unterbrechung der E/A, die während der Rückgabe auftritt, wiederhergestellt.

      Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.

13. Die Berechtigungsstufe wird von admin auf advanced geändert, wobei bei entsprechender Aufforderung **y** eingegeben wird, um fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

14. Die Version auf Cluster_A bestätigen:

```
system image show
```

Das folgende Beispiel zeigt, dass das Systemimage2 (Ziel-ONTAP-Image) die Standard- und aktuelle Version auf node_A_1 ist:

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node_A_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
```

```
node_A_2
         image1  false   true     X.X.X   MM/DD/YYYY TIME
         image2  true    false    Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

15. Die Version auf Cluster_B bestätigen:

```
system image show
```

Das folgende Beispiel zeigt, dass das Systemimage2 (Ziel-ONTAP-Image) die Standard- und aktuelle Version auf node_B_1 ist:

```
cluster_B::*> system image show
                 Is      Is                Install
Node     Image   Default Current Version   Date
-------- ------- ------- ------- --------- -------------------
node_B_1
         image1  false   false    X.X.X   MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y   MM/DD/YYYY TIME
node_B_2
         image1  false   true     X.X.X   MM/DD/YYYY TIME
         image2  true    false    Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

Aktualisierung des zweiten DR-Paares in einer MetroCluster DR-Gruppe

Sie müssen die Übernahme und Rückgabe des Knotens in der richtigen Reihenfolge durchführen, damit die neue Version von ONTAP zur aktuellen Version des Knotens wird.

Das erste DR-Paar (node_A_1 und node_B_1) sollte aktualisiert worden sein.

In dieser Aufgabe werden node_A_2 und node_B_2 aktualisiert.

Wenn die ONTAP Software auf der ersten DR-Gruppe aktualisiert wurde und nun die zweite DR-Gruppe in einer Acht-Node MetroCluster Konfiguration aktualisiert wird, werden in dieser Aufgabe node_A_4 und node_B_4 aktualisiert.

Schritte

1. Alle Daten-LIFs vom Knoten migrieren:

```
network interface migrate-all -node node_A_2
```

```
network interface migrate-all -node node_B_2
```

2. Eine Übernahme des Zielknotens auf Cluster_A initiieren:

   Der Parameter -option immediate darf nicht angegeben werden, da für den Start der zu übernehmenden Knoten mit dem neuen Software-Image ein normaler Übernahmevorgang erforderlich ist.

   a. Übernahme des DR-Partners auf Cluster_A:

      ```
      storage failover takeover -ofnode node_A_2 -option allow-version-
      mismatch
      ```

      Die `allow-version-mismatch` Option ist weder für Upgrades von ONTAP 9.0 auf ONTAP 9.1 noch für Patch Upgrades erforderlich.

      Der Knoten startet im Zustand "Warten auf Giveback".

      Wenn AutoSupport aktiviert ist, wird eine AutoSupport-Meldung gesendet, die darauf hinweist, dass die Knoten das Cluster-Quorum verlassen haben. Diese Benachrichtigung kann ignoriert werden und das Upgrade kann fortgesetzt werden.

   b. Es sollte überprüft werden, ob die Übernahme erfolgreich war:

      ```
      storage failover show
      ```

      Das folgende Beispiel zeigt, dass die Übernahme erfolgreich war. Node_A_2 befindet sich im Status „Warten auf Rückgabe“ und node_A_1 im Status „In Übernahme“.

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. Eine Übernahme des Zielknotens auf Cluster_B initiieren:

   Der Parameter -option immediate darf nicht angegeben werden, da für den Start der zu übernehmenden Knoten mit dem neuen Software-Image ein normaler Übernahmevorgang erforderlich ist.

   a. Übernahme des DR-Partners auf cluster_B (node_B_2):

Wenn Sie von … ein Upgrade durchführen	Geben Sie diesen Befehl ein…
ONTAP 9.2 oder ONTAP 9.1	`storage failover takeover -ofnode node_B_2`
ONTAP 9,0	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` Die `allow-version-mismatch` Option ist weder für Upgrades von ONTAP 9.0 auf ONTAP 9.1 noch für Patch Upgrades erforderlich.

Der Knoten startet im Zustand "Warten auf Giveback".

Wenn AutoSupport aktiviert ist, wird eine AutoSupport-Meldung gesendet, die darauf hinweist, dass die Nodes nicht mehr Teil des Cluster-Quorums sind. Diese Benachrichtigung kann ignoriert werden und das Upgrade kann fortgesetzt werden.

b. Es sollte überprüft werden, ob die Übernahme erfolgreich war:

```
storage failover show
```

Das folgende Beispiel zeigt, dass die Übernahme erfolgreich war. Node_B_2 befindet sich im Status „Warten auf Rückgabe“ und node_B_1 im Status „In Übernahme“.

```
cluster_B::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. Mindestens acht Minuten warten, damit die folgenden Bedingungen sichergestellt sind:
   - Client Multipathing (sofern implementiert) ist stabilisiert.
   - Clients werden nach der Unterbrechung der E/A, die während der Übernahme auftritt, wiederhergestellt.

     Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.

5. Die Aggregate werden an die Zielknoten zurückgegeben:

   Nach dem Upgrade der MetroCluster IP-Konfigurationen auf ONTAP 9.5 befinden sich die Aggregate für kurze Zeit in einem eingeschränkten Zustand, bevor sie sich neu synchronisieren und wieder in einen gespiegelten Zustand zurückkehren.

   a. Die Aggregate werden an den DR-Partner auf Cluster_A zurückgegeben:

      ```
      storage failover giveback -ofnode node_A_2
      ```

   b. Die Aggregate werden an den DR-Partner auf Cluster_B zurückgegeben:

      ```
      storage failover giveback -ofnode node_B_2
      ```

      Die Giveback-Operation gibt zuerst das Root-Aggregat an den Knoten zurück und gibt dann, nachdem der Knoten den Bootvorgang abgeschlossen hat, die Nicht-Root-Aggregate zurück.

6. Es sollte überprüft werden, ob alle Aggregate zurückgegeben wurden, indem auf beiden Clustern der folgende Befehl ausgeführt wird:

   ```
   storage failover show-giveback
   ```

   Wenn das Feld „Rückgabestatus“ anzeigt, dass keine Aggregate zurückzugeben sind, wurden alle Aggregate zurückgegeben. Wenn die Rückgabe abgelehnt wird, zeigt der Befehl den Fortschritt der Rückgabe und das Subsystem an, das die Rückgabe abgelehnt hat.

7. Wenn Aggregate nicht zurückgegeben wurden, ist Folgendes zu tun:

   a. Die Vorgehensweise zur Umgehung des Veto-Problems kann herangezogen werden, um zu bestimmen, ob die “veto”-Bedingung behoben oder das Veto außer Kraft gesetzt werden soll.

   b. Falls erforderlich sollte die in der Fehlermeldung beschriebene “veto”-Bedingung behoben werden, wobei sichergestellt wird, dass alle identifizierten Operationen ordnungsgemäß beendet werden.

   c. Geben Sie den Befehl storage failover giveback erneut ein.

      Wenn die “veto”-Bedingung außer Kraft gesetzt werden soll, ist der Parameter -override-vetoes auf true zu setzen.

8. Mindestens acht Minuten warten, damit die folgenden Bedingungen sichergestellt sind:

   - Client Multipathing (sofern implementiert) ist stabilisiert.
   - Die Clients werden nach der Unterbrechung der E/A, die während der Rückgabe auftritt, wiederhergestellt.

     Die Wiederherstellungszeit ist client-spezifisch und kann abhängig von den Eigenschaften der Client-Anwendungen länger als acht Minuten dauern.

9. Die Berechtigungsstufe wird von admin auf advanced geändert, wobei bei entsprechender Aufforderung **y** eingegeben wird, um fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) erscheint.

10. Die Version auf Cluster_A bestätigen:

```
system image show
```

Das folgende Beispiel zeigt, dass das Systemimage2 (Ziel-ONTAP-Image) die Standard- und aktuelle Version auf node_A_2 ist:

```
cluster_A::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_A_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_A_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. Die Version auf Cluster_B bestätigen:

```
system image show
```

Das folgende Beispiel zeigt, dass das Systemimage2 (Ziel-ONTAP-Image) die Standard- und aktuelle Version auf node_B_2 ist:

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_B_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_B_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
```

```
4 entries were displayed.

cluster_B::>
```

12. Für jeden Knoten im HA-Paar die automatische Rückgabe aktivieren:

```
storage failover modify -node target-node -auto-giveback true
```

Dieser Befehl muss für jeden Knoten im HA-Paar wiederholt werden.

13. Es sollte überprüft werden, ob das automatische Giveback aktiviert ist:

```
storage failover show -fields auto-giveback
```

Dieses Beispiel zeigt, dass die automatische Rückgabe auf beiden Knoten aktiviert wurde:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

Verwandte Informationen

- "Storage-Failover-Giveback"
- "storage failover modify"
- "storage failover show-giveback"
- "Storage-Failover-Takeover"

Upgrade einer ONTAP Zwei-Knoten MetroCluster Konfiguration

Die Vorgehensweise zum Upgrade einer Zwei-Node-MetroCluster Konfiguration variiert je nach Ihrer ONTAP-Version. Bei Verwendung von ONTAP 9.2 oder einer früheren Version empfiehlt sich dieses Verfahren für ein manuelles unterbrechungsfreies Upgrade, das das Initiieren eines ausgehandelten Switchovers, das Aktualisieren des Clusters am „`failed`“-Standort, das Initiieren des Switchbacks und anschließend das Wiederholen des Prozesses am Cluster des anderen Standorts umfasst.

Wenn Sie eine Zwei-Knoten-MetroCluster-Konfiguration mit ONTAP 9.3 oder höher verwenden, befolgen Sie die CLI-Schritte in "Das ONTAP Image mit automatisiertem, unterbrechungsfreiem ONTAP Upgrade installieren".

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt, wobei bei entsprechender Aufforderung **y** einzugeben

ist, um fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

2. Auf dem zu aktualisierenden Cluster wird das neue ONTAP Software-Image als Standard installiert:

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. Es sollte überprüft werden, ob das Zielsoftware-Image als Standardimage festgelegt ist:

```
system node image show
```

Das folgende Beispiel zeigt, dass `NewImage` als Standardbild festgelegt ist:

```
cluster_B::*> system node image show
                    Is      Is                            Install
Node     Image      Default Current Version               Date
-------- -------    ------- ------- --------------------
-------------------
node_B_1
         OldImage  false   true    X.X.X                 MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                 MM/DD/YYYY TIME
2 entries were displayed.
```

4. Falls das Zielsoftware-Image nicht als Standard-Image festgelegt ist, sollte es geändert werden:

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Es wird sichergestellt, dass sich alle Cluster-SVMs in einem fehlerfreien Zustand befinden:

```
metrocluster vserver show
```

6. Auf dem Cluster, der nicht aktualisiert wird, einen ausgehandelten Switchover initiieren:

```
metrocluster switchover
```

Der Vorgang kann einige Minuten dauern. Mit dem Befehl `metrocluster operation show` kann überprüft werden, ob die Umschaltung abgeschlossen ist.

Im folgenden Beispiel wird ein ausgehandelter Switchover auf dem Remote-Cluster („cluster_A“) durchgeführt. Dies führt dazu, dass der lokale Cluster („cluster_B“) angehalten wird, sodass er aktualisiert werden kann.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Es wird sichergestellt, dass sich alle Cluster-SVMs in einem fehlerfreien Zustand befinden:

```
metrocluster vserver show
```

8. Die Datenaggregate auf dem “überlebenden” Cluster neu synchronisieren:

```
metrocluster heal -phase aggregates
```

Nach dem Upgrade der MetroCluster IP-Konfigurationen auf ONTAP 9.5 oder höher befinden sich die Aggregate für kurze Zeit in einem degradierten Zustand, bevor sie sich neu synchronisieren und wieder in einen gespiegelten Zustand zurückkehren.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Es sollte überprüft werden, ob der Heilungsvorgang erfolgreich abgeschlossen wurde:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
```

```
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Die Root-Aggregate auf dem “surviving” Cluster resynchronisieren:

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Es sollte überprüft werden, ob der Heilungsvorgang erfolgreich abgeschlossen wurde:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. Im angehaltenen Cluster wird der Node über die LOADER-Eingabeaufforderung gebootet:

```
boot_ontap
```

13. Warten Sie, bis der Bootvorgang abgeschlossen ist, und anschließend überprüfen, ob sich alle Cluster SVMs in einem fehlerfreien Zustand befinden:

```
metrocluster vserver show
```

14. Einen Switchback vom “überlebenden” Cluster durchführen:

```
metrocluster switchback
```

15. Es wird überprüft, ob der Rückwechsel erfolgreich abgeschlossen wurde:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Es wird sichergestellt, dass sich alle Cluster-SVMs in einem fehlerfreien Zustand befinden:

```
metrocluster vserver show
```

17. Alle vorherigen Schritte werden auf dem anderen Cluster wiederholt.
18. Es sollte überprüft werden, ob die MetroCluster Konfiguration einwandfrei ist:
    a. Konfiguration prüfen:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

    b. Für detailliertere Ergebnisse kann der Befehl metrocluster check run verwendet werden:

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

d. Den Umschaltvorgang simulieren:

```
metrocluster switchover -simulate
```

e. Die Ergebnisse der Umschaltsimulation werden angezeigt:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

g. Diese Teilschritte sind auch auf dem anderen Cluster durchzuführen.

Nachdem Sie fertig sind

Beliebige Aktionen können ausgeführt werden "Aufgaben nach dem Upgrade".

Verwandte Informationen

"MetroCluster Katastrophenwiederherstellung"

Standard ONTAP Cluster manuell disruptiv aktualisieren

Wenn Sie Ihren Cluster für ein Upgrade auf eine neue ONTAP Version offline nehmen können, kann die disruptive Upgrade-Methode verwendet werden. Diese Methode umfasst mehrere Schritte: Deaktivieren des Storage Failover für jedes HA-Paar, Neustart

jedes Knotens im Cluster und anschließendes erneutes Aktivieren des Storage Failover.

- Sie müssen "herunterladen" und "installieren" das Software-Image verwenden.
- Wenn Sie in einer SAN-Umgebung arbeiten, müssen alle SAN Clients heruntergefahren oder angehalten werden, bis das Upgrade abgeschlossen ist.

  Wenn SAN-Clients vor einem unterbrechenden Upgrade nicht heruntergefahren oder angehalten werden, treten Fehler in den Client-Dateisystemen und Anwendungen auf, die nach Abschluss des Upgrades eine manuelle Wiederherstellung erfordern können.

Bei einem Upgrade mit Unterbrechung ist eine Ausfallzeit erforderlich, da die Speicherausfallsicherung für jedes HA-Paar deaktiviert ist und jeder Node aktualisiert wird. Wenn die Speicherausfallsicherung deaktiviert ist, verhält sich jeder Node wie ein Einzel-Node-Cluster, das heißt, die mit dem Node verbundenen Systemdienste werden für die Dauer des Systemneustarts unterbrochen.

Über diese Aufgabe

Für ein manuelles, unterbrechendes Upgrade muss die ONTAP Befehlszeilenschnittstelle (CLI) verwendet werden.

Schritte

1. Die Berechtigungsstufe wird von admin auf advanced geändert, wobei bei entsprechender Aufforderung **y** eingegeben wird, um fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Eingabeaufforderung (`*>`) erscheint.

2. Das neue ONTAP Software-Image als Standard-Image festlegen:

   ```
   system image modify {-node * -iscurrent false} -isdefault true
   ```

   Dieser Befehl verwendet eine erweiterte Abfrage, um das Ziel ONTAP Software-Image (das als alternatives Image installiert ist) so zu ändern, dass es für jeden Knoten zum Standard-Image wird.

3. Es sollte überprüft werden, ob das neue ONTAP Software-Image als Standard-Image festgelegt ist:

   ```
   system image show
   ```

   Im folgenden Beispiel ist Bild 2 die neue ONTAP Version und als Standardbild auf beiden Knoten festgelegt:

   ```
   cluster1::*> system image show
                    Is      Is                  Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- ---------- -------------------
   node0
   ```

```
          image1  false   true    X.X.X     MM/DD/YYYY TIME
          image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
          image1  false   true    X.X.X     MM/DD/YYYY TIME
          image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

4. Einer der folgenden Schritte kann durchgeführt werden:

Wenn der Cluster aus … besteht	Folgendes ist zu tun…
Ein Knoten	Fahren Sie mit dem nächsten Schritt fort.

Zwei Knoten	a. Cluster-Hochverfügbarkeit deaktivieren:
	`cluster ha modify -configured false`
	Geben Sie `y` ein, um fortzufahren, wenn Sie dazu aufgefordert werden.
	b. Storage-Failover für das HA-Paar deaktivieren:
	`storage failover modify -node * -enabled false`

Mehr als zwei Knoten	Storage-Failover für jedes HA-Paar im Cluster deaktivieren: `storage failover modify -node * -enabled false`

5. Einen Node im Cluster neu starten:

```
system node reboot -node nodename -ignore-quorum-warnings
```

Nicht mehr als ein Node darf gleichzeitig neu gestartet werden.

Der Knoten startet das neue ONTAP Image. Die ONTAP Anmeldeaufforderung erscheint und zeigt damit an, dass der Neustartvorgang abgeschlossen ist.

6. Nachdem der Knoten oder die Knotengruppe mit dem neuen ONTAP Image neu gestartet wurde, ist die Berechtigungsstufe auf „Erweitert“ zu setzen:

```
set -privilege advanced
```

y eingeben, wenn zur Fortsetzung aufgefordert wird

7. Bestätigen Sie, dass die neue Software ausgeführt wird:

```
system node image show
```

Im folgenden Beispiel ist image1 die neue ONTAP Version und als aktuelle Version auf node0 festgelegt:

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

8. Es sollte überprüft werden, ob das Upgrade erfolgreich abgeschlossen wurde:

   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

   b. Es sollte überprüft werden, ob der Upgrade-Status für jeden Node abgeschlossen ist:

   ```
   system node upgrade-revert show -node nodename
   ```

   Der Status sollte als abgeschlossen angezeigt werden.

   Wenn der Status nicht vollständig ist, "Den NetApp Support kontaktieren" sofort.

   a. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

9. Schritte 5 bis 8 sind für jeden weiteren Node zu wiederholen.
10. Besteht der Cluster aus zwei oder mehr Knoten, wird das Storage-Failover für jedes HA-Paar im Cluster

aktiviert:

```
storage failover modify -node * -enabled true
```

11. Besteht der Cluster nur aus zwei Knoten, kann die Cluster-High Availability aktiviert werden:

```
cluster ha modify -configured true
```

Verwandte Informationen

- "storage failover modify"

Überprüfungen nach dem Upgrade

ONTAP Verifizierungsworkflow nach dem Upgrade

Nach dem Upgrade von ONTAP sind mehrere Aufgaben erforderlich, um die Einsatzbereitschaft Ihres Clusters zu überprüfen.

1 Ihr Cluster wird überprüft.

Nach dem Upgrade von ONTAP sollten Sie "Clusterversion, Clusterzustand und Speicherzustand überprüfen". Wenn Sie eine MetroCluster FC-Konfiguration verwenden, ist außerdem zu überprüfen, ob der Cluster für die automatische ungeplante Umschaltung aktiviert ist.

2 Es wird überprüft, ob alle LIFs auf den Home-Ports sind.

Während eines Neustarts wurden möglicherweise einige LIFs auf ihre zugewiesenen Failover-Ports migriert. Nach dem Upgrade eines Clusters ist es erforderlich, "Alle LIFs, die sich nicht auf ihren Heimatports befinden, aktivieren und zurücksetzen".

3 Spezielle, für Ihren Cluster geltende Besonderheiten sind zu berücksichtigen.

Falls bestimmte Konfigurationen in Ihrem Cluster vorhanden sind, müssen Sie möglicherweise "Nach dem Upgrade sind zusätzliche Schritte erforderlich.".

4 Das Disk Qualification Package (DQP) wird aktualisiert.

Die DQP wird nicht im Rahmen eines ONTAP Upgrades aktualisiert. Nach dem Upgrade ist "das DQP aktualisieren" erforderlich.

Cluster nach einem ONTAP Upgrade überprüfen

Nach dem Upgrade von ONTAP sollten die Clusterversion, der Clusterzustand und der Speicherzustand überprüft werden. Für MetroCluster FC Konfigurationen ist außerdem zu prüfen, ob der Cluster für die automatische ungeplante Umschaltung aktiviert ist.

Clusterversion überprüfen

Nachdem alle HA-Paare aktualisiert wurden, kann mit dem Befehl version überprüft werden, ob auf allen Knoten die Zielversion ausgeführt wird.

Die Clusterversion ist die niedrigste Version von ONTAP, die auf einem beliebigen Knoten im Cluster ausgeführt wird. Wenn die Clusterversion nicht der Ziel-ONTAP-Version entspricht, kann Ihr Cluster aktualisiert werden.

1. Wechsel zum erweiterten Berechtigungslevel:

```
set -privilege advanced
```

2. Es sollte sichergestellt werden, dass die Clusterversion der Ziel-ONTAP-Version entspricht:

```
system node image show -version
```

3. Wenn die Clusterversion nicht der Zielversion ONTAP entspricht, ist der Aktualisierungsstatus aller Knoten zu überprüfen:

```
system node upgrade-revert show
```

Clusterzustand überprüfen

Nach der Aktualisierung eines Clusters ist zu überprüfen, ob die Knoten fehlerfrei funktionieren und zur Teilnahme am Cluster berechtigt sind und ob sich der Cluster im Quorum befindet.

1. Es sollte sichergestellt werden, dass die Knoten im Cluster online sind und zur Teilnahme am Cluster berechtigt sind:

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

   Wenn ein Knoten fehlerhaft oder nicht geeignet ist, sollten die EMS-Protokolle auf Fehler überprüft und Korrekturmaßnahme ergriffen werden.

2. Die Konfigurationsdetails für jeden RDB-Prozess werden überprüft.

   - Die relationalen Datenbank-Epochen und die Datenbank-Epochen sollten für jeden Knoten übereinstimmen.

- Das primäre Quorum pro Ring sollte für alle Knoten gleich sein.

  Beachten Sie, dass jeder Ring ein anderes Quorum-Primary haben kann.

Um diesen RDB-Prozess anzuzeigen…	Geben Sie diesen Befehl ein…
Verwaltungsanwendung	`cluster ring show -unitname mgmt`
Volume-Standortdatenbank	`cluster ring show -unitname vldb`
Manager für virtuelle Schnittstellen	`cluster ring show -unitname vifmgr`
SAN Management-Daemon	`cluster ring show -unitname bcomd`

  Weitere Informationen zu `cluster ring show` finden sich in der "ONTAP-Befehlsreferenz".

  Dieses Beispiel zeigt den Volume Location Database-Prozess:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

3. Wenn Sie in einer SAN-Umgebung arbeiten, überprüfen Sie, ob sich jeder Knoten in einem SAN-Quorum befindet:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

4. Die Berechtigungsstufe wird auf Administrator zurückgesetzt:

```
set -privilege admin
```

Verwandte Informationen

"Systemadministration"

Überprüfen, ob die automatische ungeplante Umschaltung aktiviert ist (MetroCluster FC-Konfigurationen nur)

Wenn Ihr Cluster in einer MetroCluster FC Konfiguration betrieben wird, sollte nach dem Upgrade von ONTAP überprüft werden, ob der automatische ungeplante Switchover aktiviert ist.

Wenn Sie eine MetroCluster IP-Konfiguration verwenden, kann dieses Verfahren übersprungen werden.

Schritte

1. Es kann überprüft werden, ob die automatische ungeplante Umschaltung aktiviert ist:

   ```
   metrocluster show
   ```

   Wenn die automatische ungeplante Umschaltung aktiviert ist, erscheint die folgende Meldung in der Befehlsausgabe:

   ```
   AUSO Failure Domain  auso-on-cluster-disaster
   ```

2. Falls die Meldung nicht angezeigt wird, kann eine automatische ungeplante Umschaltung aktiviert werden:

   ```
   metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
   disaster
   ```

3. Es sollte überprüft werden, ob eine automatische ungeplante Umschaltung aktiviert ist:

   ```
   metrocluster show
   ```

Verwandte Informationen

"Festplatten- und Aggregatverwaltung"

LIFs nach einem ONTAP Upgrade wieder aktivieren und auf ihre Home-Ports zurücksetzen

Beim Neustart im Rahmen des ONTAP Upgrade-Prozesses werden einige LIFs möglicherweise von ihren Home-Ports auf ihre zugewiesenen Failover-Ports migriert. Nach einem Upgrade ist es erforderlich, alle LIFs, die sich nicht auf ihren Home-Ports befinden, zu aktivieren und auf ihre Home-Ports zurückzusetzen.

Schritte

1. Status aller LIFs anzeigen:

```
network interface show -fields home-port,curr-port
```

Wenn **Status Admin** für einen LIF den Wert „down“ oder **Is home** den Wert „false“ hat, mit dem nächsten Schritt fortfahren.

2. Die Daten-LIFs aktivieren:

```
network interface modify {-role data} -status-admin up
```

3. LIFs auf ihre Home-Ports zurückführen:

```
network interface revert *
```

4. Es sollte sichergestellt werden, dass sich alle LIFs in ihren Home-Ports befinden:

```
network interface show
```

Dieses Beispiel zeigt, dass sich alle LIFs für SVM vs0 auf ihren Home-Ports befinden.

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network         Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask    Node     Port    Home
-------- ---------- ---------- --------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24  node0    e0e     true
         data002    up/up      192.0.2.121/24  node0    e0f     true
         data003    up/up      192.0.2.122/24  node0    e2a     true
         data004    up/up      192.0.2.123/24  node0    e2b     true
         data005    up/up      192.0.2.124/24  node1    e0e     true
         data006    up/up      192.0.2.125/24  node1    e0f     true
         data007    up/up      192.0.2.126/24  node1    e2a     true
         data008    up/up      192.0.2.127/24  node1    e2b     true
8 entries were displayed.
```

Verwandte Informationen

- "Netzwerkschnittstelle"

Spezielle Konfigurationen

Prüfungen nach dem Upgrade für spezifische ONTAP Konfigurationen

Wenn Ihr Cluster mit einer der folgenden Funktionen konfiguriert ist, könnten nach dem Upgrade Ihrer ONTAP Software zusätzliche Schritte erforderlich sein.

Stellen Sie sich die Frage …	Wenn Ihre Antwort ja lautet, ist Folgendes zu tun…
Wurde von ONTAP 9.7 oder früher auf ONTAP 9.8 oder später ein Upgrade durchgeführt?	Netzwerkkonfiguration überprüfen Den EMS LIF-Service aus Netzwerkservice-Richtlinien entfernen, die keine Erreichbarkeit des EMS-Ziels bieten
Befindet sich mein Cluster in einer MetroCluster Konfiguration?	Netzwerk- und Speicherstatus überprüfen
Liegt eine SAN Konfiguration vor?	SAN-Konfiguration überprüfen
Wurde von ONTAP 9.3 oder einer früheren Version ein Upgrade durchgeführt und wird NetApp Storage Encryption verwendet?	KMIP Serververbindungen neu konfigurieren
Habe ich Load-Sharing Mirror?	Verschobene Load-Sharing-Spiegelquell-Volumes verlagern
Habe ich Benutzerkonten für den Zugriff auf den Service Processor (SP), die vor ONTAP 9.9.1 erstellt wurden?	Die Änderung der Konten, die auf den Serviceprozessor zugreifen können, überprüfen.

Nach einem Upgrade sollte die ONTAP Netzwerkkonfiguration überprüft werden.

Nach dem Upgrade von ONTAP 9.7x oder älter auf ONTAP 9.8 oder neuer sollte die Netzwerkkonfiguration überprüft werden. Nach dem Upgrade überwacht ONTAP automatisch die Erreichbarkeit von Layer 2.

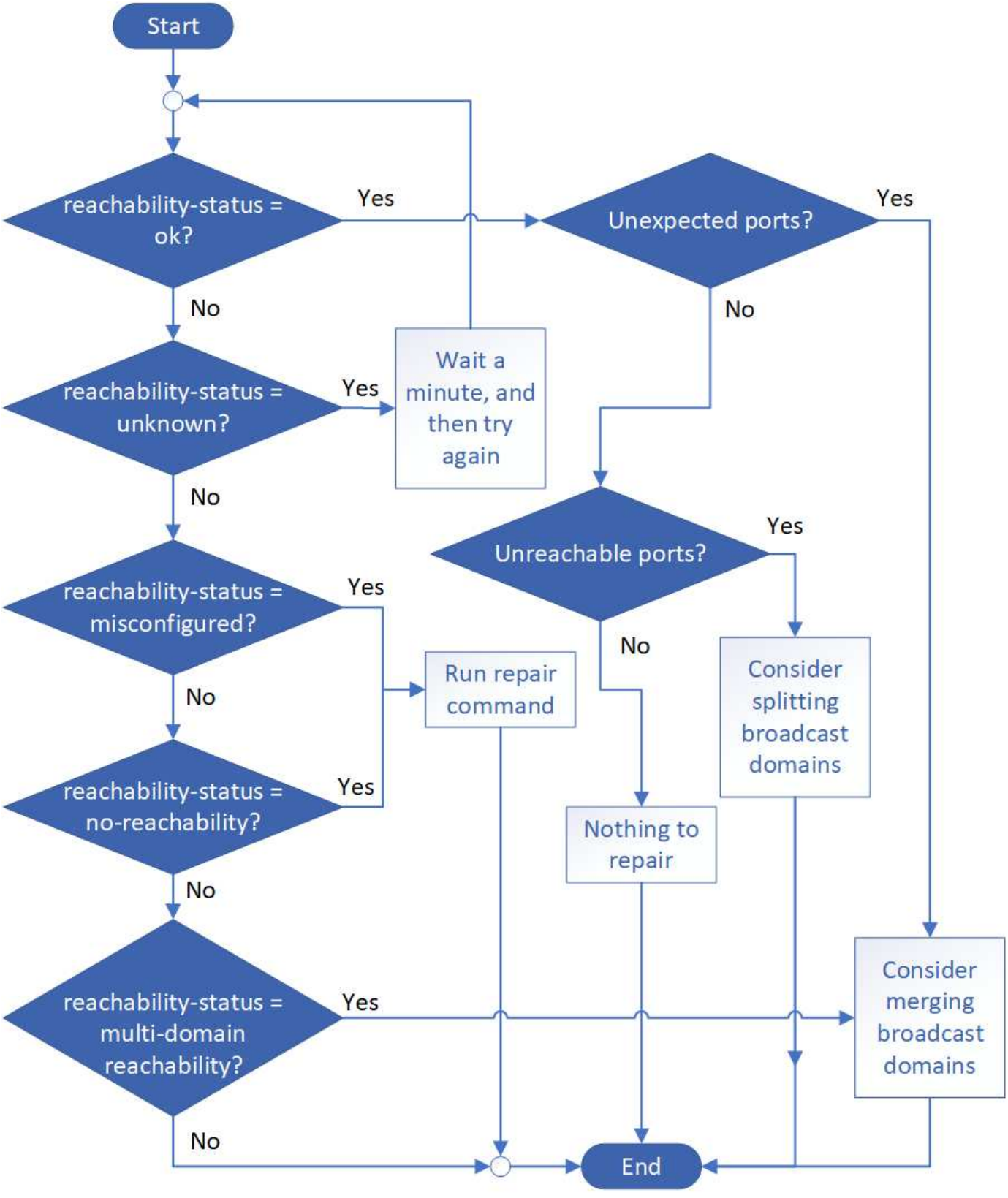
Schritt

1. Es wird überprüft, ob jeder Port die erwartete Broadcast-Domäne erreichen kann:

   ```
   network port reachability show -detail
   ```

   Weitere Informationen zu `network port reachability show` finden sich in der "ONTAP-Befehlsreferenz".

Die Befehlsausgabe enthält die Ergebnisse der Erreichbarkeitsprüfung. Die folgende Entscheidungsstruktur und Tabelle bieten eine Übersicht über die Ergebnisse (Erreichbarkeitsstatus) und ermöglichen eine Einschätzung, ob und welche weiteren Schritte erforderlich sind.



Erreichbarkeitsstatus	Beschreibung

OK	Der Port verfügt über Layer-2-Erreichbarkeit zu seiner zugewiesenen Broadcast-Domäne. Wenn der Erreichbarkeitsstatus „ok“ ist, aber „unerwartete Ports“ vorhanden sind, kann das Zusammenführen einer oder mehrerer Broadcast-Domänen in Betracht gezogen werden. Weitere Informationen finden sich unter "Zusammenführen von Broadcast-Domänen". Wenn der Erreichbarkeitsstatus „ok“ ist, aber „nicht erreichbare Ports“ vorhanden sind, kann das Aufteilen einer oder mehrerer Broadcast-Domänen in Erwägung gezogen werden. Weitere Informationen finden sich unter "Aufgeteilte Broadcast-Domänen". Wenn der Erreichbarkeitsstatus "ok" ist und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist Ihre Konfiguration korrekt.
Fehlkonfigurierte Erreichbarkeit	Der Port hat keine Layer-2-Erreichbarkeit zu seiner zugewiesenen Broadcast-Domäne, jedoch hat der Port Layer-2-Erreichbarkeit zu einer anderen Broadcast-Domäne. Die Port-Erreichbarkeit kann wiederhergestellt werden. Bei Ausführung des folgenden Befehls weist das System den Port der Broadcast-Domäne zu, zu der er erreichbar ist: `network port reachability repair -node -port` Weitere Informationen finden sich unter "Reparatur der Port-Erreichbarkeit". Weitere Informationen zu `network port reachability repair` finden sich in der "ONTAP-Befehlsreferenz".
Unerreichbarkeit	Der Port hat keine Layer-2-Erreichbarkeit zu einer bestehenden Broadcast-Domäne. Die Port-Erreichbarkeit kann wiederhergestellt werden. Beim Ausführen des folgenden Befehls weist das System den Port einer neu automatisch erstellten Broadcast-Domäne im Default-IPspace zu: `network port reachability repair -node -port` Weitere Informationen finden sich unter "Reparatur der Port-Erreichbarkeit".
Erreichbarkeit über mehrere Domänen hinweg	Der Port ist über Layer 2 zu seiner zugewiesenen Broadcast-Domäne erreichbar; er ist jedoch auch über Layer 2 zu mindestens einer weiteren Broadcast-Domäne erreichbar. Die physische Konnektivität und die Switch-Konfiguration sollten überprüft werden, um festzustellen, ob sie fehlerhaft sind oder ob die dem Port zugewiesene Broadcast-Domäne mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss. Weitere Informationen finden Sie unter "Zusammenführen von Broadcast-Domänen" oder "Reparatur der Port-Erreichbarkeit".
unbekannt	Wenn der Erreichbarkeitsstatus „unbekannt“ ist, einige Minuten abwarten und den Befehl erneut ausführen.

Nach der Reparatur eines Ports müssen verschobene LIFs und VLANs überprüft und behoben werden. Wenn der Port Teil einer Schnittstellengruppe war, ist es außerdem erforderlich, nachzuvollziehen, was mit dieser Schnittstellengruppe geschehen ist. Weitere Informationen finden sich unter "Reparatur der Port-Erreichbarkeit".

Entfernen des EMS LIF Service aus den Netzwerkrichtlinien nach dem Upgrade von ONTAP

Wenn Sie vor dem Upgrade von ONTAP 9.7 oder früher auf ONTAP 9.8 oder später Event Management System (EMS)-Nachrichten eingerichtet haben, werden Ihre EMS-Nachrichten nach dem Upgrade möglicherweise nicht zugestellt.

Während des Upgrades `management-ems`, das der EMS-LIF-Dienst ist, wird dieser allen bestehenden Dienstrichtlinien in den administrativen SVMs hinzugefügt. Dadurch können EMS-Meldungen von jedem der den Dienstrichtlinien zugeordneten LIFs gesendet werden. Wenn der ausgewählte LIF keine Erreichbarkeit zum Ziel der Ereignisbenachrichtigung hat, wird die Nachricht nicht zugestellt.

Um dies zu verhindern, sollte nach dem Upgrade der EMS LIF Dienst aus den Netzwerkservice-Richtlinien entfernt werden, die keine Erreichbarkeit zum Ziel bieten.

"Weitere Informationen zu ONTAP LIFs und Servicerichtlinien".

Schritte

1. Die LIFs und die zugehörigen Netzwerkservice-Richtlinien, über die EMS-Nachrichten gesendet werden können, lassen sich identifizieren:

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------   ------------------
cluster-1      cluster_mgmt   default-management
cluster-1      node1-mgmt     default-management
cluster-1      node2-mgmt     default-management
cluster-1      inter_cluster  default-intercluster
4 entries were displayed.
```

2. Jede LIF auf Konnektivität zum EMS-Ziel überprüfen:

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

Dies ist auf jedem Knoten auszuführen.

Beispiele

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
```

```
no answer from 10.10.10.10
```

3. Erweiterte Berechtigungsstufe eingeben:

```
set advanced
```

4. Für die LIFs, die keine Erreichbarkeit haben, den `management-ems`LIF-Service aus den entsprechenden Service-Richtlinien entfernen:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

Weitere Informationen zu `network interface service-policy remove-service` finden sich in der "ONTAP-Befehlsreferenz".

5. Es sollte sichergestellt sein, dass die management-ems LIF nun nur noch mit den LIFs verknüpft ist, die die Erreichbarkeit des EMS-Ziels bereitstellen:

```
network interface show -fields service-policy -services management-ems
```

Netzwerk- und Speicherstatus von MetroCluster nach einem ONTAP Upgrade überprüfen

Nach dem Upgrade eines ONTAP Clusters in einer MetroCluster Konfiguration empfiehlt sich die Überprüfung des Status der LIFs, Aggregate und Volumes für jedes Cluster.

1. Der LIF-Status kann überprüft werden:

```
network interface show
```

Im Normalbetrieb müssen die LIFs für Quell-SVMs den Administratorstatus „Aktiv“ aufweisen und sich auf ihren jeweiligen Heimatknoten befinden. Die LIFs für Ziel-SVMs müssen weder aktiv sein noch sich auf ihren Heimatknoten befinden. Im Switchover haben alle LIFs den Administratorstatus „Aktiv“, müssen sich jedoch nicht auf ihren Heimatknoten befinden.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
```

```
                        up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                        up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                        up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

2. Der Zustand der Aggregate kann überprüft werden:

```
storage aggregate show -state !online
```

Dieser Befehl zeigt alle Aggregate an, die nicht online sind. Im Normalbetrieb müssen alle Aggregate am lokalen Standort online sein. Befindet sich die MetroCluster Konfiguration im Switchover, dürfen die Root-Aggregate am Disaster-Recovery-Standort offline sein.

Dieses Beispiel zeigt einen Cluster im Normalbetrieb:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

Dieses Beispiel zeigt einen Cluster im Switchover, in dem die Root-Aggregate am Disaster-Recovery-Standort offline sind:

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
               0B        0B    0% offline      0 cluster2-01
```

```
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. Den Zustand der Volumes überprüfen:

```
volume show -state !online
```

Dieser Befehl zeigt alle Volumes an, die *nicht* online sind.

Wenn sich die MetroCluster Konfiguration im Normalbetrieb befindet (sie befindet sich nicht im Switchover-Zustand), sollte die Ausgabe alle Volumes anzeigen, die den sekundären SVMs des Clusters gehören (diejenigen, deren SVM-Name mit "-mc" ergänzt wird).

Diese Volumes werden nur im Falle einer Umschaltung online verfügbar.

Dieses Beispiel zeigt einen Cluster im Normalbetrieb, bei dem die Volumes am Disaster Recovery-Standort nicht online sind.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
```

```
5 entries were displayed.
```

4. Es wird überprüft, ob keine inkonsistenten Volumes vorhanden sind:

```
volume show -is-inconsistent true
```

Siehe die "NetApp Knowledge Base: Volumen zeigt WAFL als inkonsistent" Hinweise zum Umgang mit den uneinheitlichen Volumen.

Die SAN-Konfiguration nach einem ONTAP Upgrade überprüfen

Nach einem ONTAP Upgrade in einer SAN-Umgebung ist zu überprüfen, ob jeder Initiator, der vor dem Upgrade mit einem LIF verbunden war, erfolgreich wieder mit dem LIF verbunden ist.

1. Es sollte sichergestellt werden, dass jeder Initiator mit dem richtigen LIF verbunden ist.

   Die Liste der Initiatoren sollte mit der Liste verglichen werden, die während der Upgrade-Vorbereitung erstellt wurde. Bei Verwendung von ONTAP 9.11.1 oder höher empfiehlt sich System Manager zur Anzeige des Verbindungsstatus, da dieser eine deutlich übersichtlichere Darstellung als die CLI bietet.

System Manager

a. Im System Manager auf **Hosts > SAN Initiatorgruppen** klicken.

   Auf der Seite wird eine Liste der Initiatorgruppen (Initiatorgruppen) angezeigt. Wenn die Liste lang ist, können zusätzliche Seiten der Liste angezeigt werden, indem auf die Seitenzahlen in der unteren rechten Ecke der Seite geklickt wird.

   Die Spalten zeigen verschiedene Informationen zu den Initiatorgruppen an. Ab Version 9.11.1 wird auch der Verbindungsstatus der Initiatorgruppe angezeigt. Durch das Überfahren der Statusmeldungen mit dem Mauszeiger werden Details angezeigt.

CLI

- Liste der iSCSI-Initiatoren:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- Liste der FC-Initiatoren:

```
fcp initiator show -fields igroup,wwpn,lif
```

KMIP-Server nach einem Upgrade von ONTAP 9.2 oder früher neu konfigurieren

Nach dem Upgrade von ONTAP 9.2 oder früher auf ONTAP 9.3 oder später ist es erforderlich, alle externen Key Management (KMIP) Server-Verbindungen neu zu

konfigurieren.

Schritte

1. Konfiguration der Key Manager-Konnektivität:

```
security key-manager setup
```

2. Fügen Sie Ihre KMIP-Server hinzu:

```
security key-manager add -address <key_management_server_ip_address>
```

3. Es sollte überprüft werden, ob die KMIP Server verbunden sind:

```
security key-manager show -status
```

4. Abfrage der Schlüsselserver:

```
security key-manager query
```

5. Einen neuen Authentifizierungsschlüssel und eine neue Passphrase erstellen:

```
security key-manager create-key -prompt-for-key true
```

   Eine Passphrase mit mindestens 32 Zeichen festlegen.

6. Den neuen Authentifizierungsschlüssel abfragen:

```
security key-manager query
```

7. Weisen Sie Ihren selbstverschlüsselnden Festplatten (SEDs) den neuen Authentifizierungsschlüssel zu:

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```

   Verwenden Sie den neuen Authentifizierungsschlüssel aus Ihrer Abfrage.

8. Weisen Sie den SEDs gegebenenfalls einen FIPS-Schlüssel zu:

```
storage encryption disk modify -disk <disk_id> -fips-key-id
<fips_authentication_key_id>
```

Wenn Ihre Sicherheitskonfiguration die Verwendung unterschiedlicher Schlüssel für die Authentifizierung von Daten und die FIPS 140-2 Authentifizierung erfordert, sollte für jeden Zweck ein separater Schlüssel erstellt werden. Andernfalls kann derselbe Authentifizierungsschlüssel für beide verwendet werden.

Verwandte Informationen

- "security key-manager setup"
- "Speicherverschlüsselung Festplatte ändern"

Verschobene Load-Sharing Mirror-Quell-Volumes nach einem ONTAP Upgrade neu zuordnen

Nach dem Upgrade von ONTAP ist es erforderlich, die Load-Sharing-Mirror-Quell-Volumes wieder an ihre Speicherorte vor dem Upgrade zu verschieben.

Schritte

1. Den Zielort, an den das Load-Sharing Mirror-Quellvolume verschoben wird, anhand des zuvor erstellten Datensatzes für das Load-Sharing Mirror-Quellvolume bestimmen.
2. Das Load-Sharing-Mirror-Quellvolume wird an seinen ursprünglichen Speicherort zurück verschoben:

```
volume move start
```

Wie ONTAP Upgrades die Benutzerkonten des Serviceprozessors ändern

Wenn in ONTAP 9.8 oder früher Benutzerkonten erstellt wurden, die mit einer Nicht-Administratorrolle auf den Service Processor (SP) zugreifen können, und ein Upgrade auf ONTAP 9.9.1 oder höher erfolgt, wird jeder Nicht-Administratorwert im `-role` Parameter in `admin` geändert.

Weitere Informationen finden sich unter "Konten, die auf den SP zugreifen können".

Das Disk Qualification Package nach einem ONTAP Upgrade aktualisieren

Nach dem Upgrade Ihrer ONTAP Software sollten das ONTAP Disk Qualification Package (DQP) heruntergeladen und installiert werden. Die DQP wird im Rahmen eines ONTAP Upgrades nicht aktualisiert.

Das DQP enthält die erforderlichen Parameter für die Interaktion von ONTAP mit allen neu qualifizierten Laufwerken. Wenn Ihre Version des DQP keine Informationen für ein neu qualifiziertes Laufwerk enthält, verfügt ONTAP nicht über die Informationen, um das Laufwerk korrekt zu konfigurieren.

Es empfiehlt sich, den DQP vierteljährlich zu aktualisieren. Der DQP sollte auch aus folgenden Gründen aktualisiert werden:

- Immer wenn einem Knoten in Ihrem Cluster ein neuer Laufwerkstyp oder eine neue Laufwerksgröße hinzugefügt wird

  Wenn Sie beispielsweise bereits 1-TB-Festplatten besitzen und 2-TB-Festplatten hinzufügen, müssen Sie auf das neueste DQP-Update prüfen.

- Immer wenn Sie die Festplatten-Firmware aktualisieren

- Sobald neuere Festplatten-Firmware oder DQP-Dateien verfügbar sind

Verwandte Informationen

- "NetApp Downloads: Datenträgerqualifizierungspaket"
- "NetApp Downloads: Festplatten-Firmware"

Firmware, System- und Sicherheitsupdates

Wie ONTAP automatische Updates für die Installation plant

Alle berechtigten Knoten innerhalb desselben Clusters werden für automatische Updates zusammengefasst. Der Zeitraum, in dem die berechtigten Knoten für automatische Updates eingeplant werden, variiert je nach Prioritätsstufe des Updates und dem Prozentsatz der Systeme in Ihrer Umgebung, die das Update benötigen.

Wenn beispielsweise 10 % oder weniger Ihrer gesamten Systeme für ein Update ohne Priorität in Frage kommen, wird das Update innerhalb einer Woche für alle berechtigten Systeme eingeplant. Wenn jedoch 76 % oder mehr Ihrer gesamten Systeme für ein Update ohne Priorität in Frage kommen, wird das Update über einen Zeitraum von acht Wochen gestaffelt auf die berechtigten Systeme verteilt. Diese gestaffelte Installation trägt dazu bei, Risiken für Ihre gesamte Umgebung zu minimieren, falls bei einem Update ein Problem auftritt, das behoben werden muss.

Der prozentuale Anteil Ihrer gesamten Systeme, die wöchentlich für automatische Updates vorgesehen sind, stellt sich wie folgt dar:

Für wichtige Aktualisierungen

Prozentsatz der Systeme, die ein Update benötigen	% der Aktualisierungen, die in Woche 1 erfolgen	% der Aktualisierungen, die in Woche 2 erfolgen
50 % oder weniger	100%	
50-100%	30%	70%

Für Updates mit hoher Priorität

Prozentsatz der Systeme, die ein Update benötigen	% der Aktualisierungen pro Woche			
	Woche 1	**Woche 2**	**Woche 3**	**Woche 4**
25% oder weniger	100%			
26-50%	30%	70%		
50-100%	10%	20%	30%	40%

Für Updates mit normaler Priorität

Prozentsatz der Systeme, die ein Update benötigen	% der Aktualisierungen pro Woche							
	Woche 1	**Woche 2**	**Woche 3**	**Woche 4**	**Woche 5**	**Woche 6**	**Woche 7**	**Woche 8**
10% oder weniger	100%							
11-20%	30%	70%						
21-50%	10%	20%	30%	40%				
51-75%	5%	10%	15%	20%	20%	30%		
76-100%	5%	5%	10%	10%	15%	15%	20%	20%

Automatische Updates in ONTAP aktivieren

Verwenden Sie den System Manager, um automatische Updates zu aktivieren und ONTAP zu erlauben, Firmware-, System- und Sicherheitsupdates ohne Ihr Zutun herunterzuladen und zu installieren.

Sie können die ONTAP CLI ausschließlich zur Verwaltung von SP/BMC Firmware-Updates verwenden.

- Weitere Informationen zu "Verwaltung von ONTAP SP/BMC Firmware-Updates".
- Erfahren Sie mehr über die Unterschiede zwischen der Verwaltung automatischer Updates mit System Manager und CLI im Knowledge Base Artikel: "Warum zeigen GUI und CLI unterschiedliche Status für die ONTAP-Konfiguration automatischer Updates an?".

Die Verfügbarkeit automatischer Updates für die einzelnen Systemkomponenten hängt von Ihrer ONTAP Version ab.

ONTAP Version	Verfügbare automatische Updates
9.16.1 und später	• Autonomer Ransomware-Schutz mit künstlicher Intelligenz (ARP/AI) • ONTAP Zeitzonendatenbank • Speicher-Firmware für Speichergeräte, Festplatten und Festplattengehäuse • SP/BMC Firmware für Serviceprozessoren und BMC Module • Disk Qualification Package (DQP)
9.13.1 und später	• ONTAP Zeitzonendatenbank • Speicher-Firmware für Speichergeräte, Festplatten und Festplattengehäuse • SP/BMC Firmware für Serviceprozessoren und BMC Module • Disk Qualification Package (DQP)
9.10.1 und später	• Speicher-Firmware für Speichergeräte, Festplatten und Festplattengehäuse • SP/BMC Firmware für Serviceprozessoren und BMC Module • Disk Qualification Package (DQP)

Falls für Ihre Version von ONTAP kein automatisches Update verfügbar ist oder Sie automatische Updates nicht aktiviert haben, können Firmware-, Zeitzonendatenbank- und Sicherheitsupdates manuell durchgeführt werden.

Über diese Aufgabe

Die Aktivierung automatischer Updates erfordert, dass Sie die Bedingungen einer EULA akzeptieren und das Standard-Updateverhalten für jede Systemkomponente entsprechend Ihrer Umgebung bestätigen oder konfigurieren.

Für Cluster, die in ONTAP 9.16.1 oder früher erstellt und dann auf 9.16.1 oder später aktualisiert wurden:

- Wenn die automatische Update-Funktionalität vor dem Upgrade aktiviert ist, werden die Standardeinstellungen für Systemkomponenten-Updates nach einem Upgrade nicht geändert.
- Wenn automatische Updates vor dem Upgrade nicht aktiviert sind, werden die Standardeinstellungen für Systemkomponenten-Updates in ONTAP 9.16.1 und später angewendet.

Die Standardeinstellungen für automatische Systemkomponentenaktualisierungen sind je nach ONTAP Version entweder auf automatische Aktualisierung oder auf die Anzeige von Benachrichtigungen eingestellt. Vor Abschluss des Vorgangs sollte bestätigt werden, dass diese Einstellungen für Ihre Umgebung korrekt sind.

Dies "Video" ist eine kurze Übersicht über die Verwendung des automatischen Aktualisierungsprozesses.

Bevor Sie beginnen

- Sie benötigen eine gültige Supportberechtigung. Dies lässt sich auf der Seite link:https://mysupport.netapp.com/site/<strong class=""NetApp Support-Website"^">Systemdetails prüfen.
- Um automatische Updates zu aktivieren, muss zunächst AutoSupport mit HTTPS aktiviert werden. Wenn AutoSupport in Ihrem Cluster nicht aktiviert ist oder wenn AutoSupport in Ihrem Cluster mit einem anderen Transportprotokoll aktiviert ist, kann es im Rahmen dieses Vorgangs mit HTTPS aktiviert werden.

> AutoSupport OnDemand ist standardmäßig aktiviert und funktionsfähig, wenn es so konfiguriert ist, dass Nachrichten über das HTTPS-Transportprotokoll an den technischen Support gesendet werden.

- Ab ONTAP 9.10.1 ist bei aktivierten automatischen Updates sicherzustellen, dass eine HTTPS-Verbindung zu den folgenden zusätzlichen URLs besteht:
  - https://support-sg-naeast.netapp.com
  - https://support-sg-nawest.netapp.com

Beispiel 4. Schritte

System Manager – ONTAP 9.16.1 und höher

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Wählen Sie unter **Software updates** die Option **Enable**.
3. Unter **Automatische Update-Einstellungen** wählen Sie die Aktion aus, die für jeden Update-Typ durchgeführt werden soll.

   Automatisch aktualisieren ist standardmäßig für alle Optionen ausgewählt. Sie können die Standardauswahl ändern in **Benachrichtigungen anzeigen** oder **Aktualisierungen automatisch verwerfen**.

4. Wählen Sie **Ich akzeptiere das aktuelle und alle zukünftigen Updates** und anschließend **Speichern**.

System Manager – ONTAP 9.15.1 und früher

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Wählen Sie unter **Automatische Aktualisierung** ⋮ und dann **Aktivieren** aus.

   Automatisch aktualisieren ist standardmäßig für alle Optionen ausgewählt. Sie können die Standardauswahl ändern in **Benachrichtigungen anzeigen** oder **Aktualisierungen automatisch verwerfen**.

3. Wählen Sie **Ich akzeptiere aktuelle und alle zukünftigen Aktualisierungen** und anschließend **Speichern**.

CLI

Sie können die ONTAP CLI nur zur Verwaltung von SP/BMC-Firmware-Updates verwenden

1. Automatische Firmware-Updates aktivieren:

```
system service-processor image modify -node <node_name> -autoupdate
true
```

Verwandte Informationen

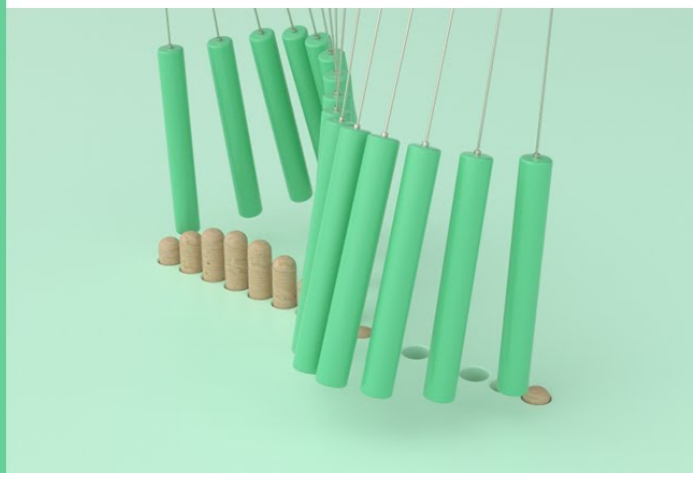
- "Firmware-Updates manuell durchführen"
- "Knowledge Base Artikel, Aktualisierung der Zeitzoneninformationen in ONTAP 9"
- "Manuelle Durchführung von Sicherheitsupdates"
- "Vorbereitung auf die Verwendung von AutoSupport"
- "Fehlerbehebung bei der AutoSupport-Nachrichtenzustellung über HTTPS"

Video: Automatisches Firmware-Update

Die automatische Firmware Update Funktion ist ab ONTAP 9.10.1 verfügbar.

Automatic Firmware Update feature is available starting in ONTAP 9.10.1

By Jim Svesnik,
Quality Assurance Engineer



Ändern von automatischen Updates in ONTAP

Wenn die automatische Update-Funktion aktiviert und die Standardeinstellungen für Systemkomponenten konfiguriert sind, kann ONTAP alle empfohlenen Updates automatisch erkennen, herunterladen und installieren. Wenn empfohlene Updates vor der Installation angezeigt oder Empfehlungen automatisch ausgeblendet werden sollen, lässt sich das Standardverhalten entsprechend anpassen.

Beispiel 5. Schritte

ONTAP 9.16.1 und höher

1. Im System Manager unter **Cluster > Einstellungen** navigieren.
2. Im Abschnitt **Software updates** → auswählen.
3. Die Registerkarte **Alle anderen Updates** auswählen und auf **Automatische Update-Einstellungen bearbeiten** klicken.
4. Die Standardaktionen, die für jeden Aktualisierungstyp durchgeführt werden, können festgelegt werden.

   Sie können für jeden Aktualisierungstyp festlegen, ob automatische Aktualisierungen, Benachrichtigungen angezeigt oder Aktualisierungen automatisch abgelehnt werden.

   ⓘ Die ONTAP Zeitzonendatenbank wird durch den Aktualisierungstyp **Systemdateien** gesteuert.

5. Die Allgemeinen Geschäftsbedingungen akzeptieren und **Speichern** auswählen.

ONTAP 9.15.1 und früher

1. Im System Manager auf **Cluster > Einstellungen** klicken.
2. Im Abschnitt **Automatische Aktualisierung** auf ⋮ klicken, um eine Liste der Aktionen anzuzeigen.
3. **Einstellungen für automatische Updates bearbeiten** auswählen.
4. Die Standardaktionen, die für jeden Aktualisierungstyp durchgeführt werden, können festgelegt werden.

   Für jeden Aktualisierungstyp kann festgelegt werden, ob automatisch aktualisiert, Benachrichtigungen angezeigt oder Aktualisierungen automatisch verworfen werden.

   ⓘ Die ONTAP Zeitzonen Datenbank wird durch den Aktualisierungstyp SYSTEM FILES gesteuert.

Verwaltung empfohlener automatischer Updates in ONTAP

Das automatische Update-Protokoll zeigt eine Liste mit Update-Empfehlungen und Details zu jeder einzelnen an, darunter Beschreibung, Kategorie, geplanter Installationszeitpunkt, Status und eventuelle Fehler. Das Protokoll kann eingesehen werden, anschließend lässt sich festlegen, welche Aktion für jede Empfehlung ausgeführt werden soll.

Schritte

1. Liste der Empfehlungen anzeigen:

Ansicht aus den Cluster Einstellungen	Ansicht aus dem Aktualisieren-Tab
a. **Cluster > Einstellungen** auswählen. b. Je nach Ihrer ONTAP-Version ist eine der folgenden Optionen zu wählen: ◦ Für ONTAP 9.15.1 und früher im Abschnitt **Automatische Aktualisierung** auf ⋮ klicken, dann die Option auswählen, um alle Aktualisierungen anzuzeigen. ◦ Für ONTAP 9.16.1 und höher im Abschnitt **Software updates** → auswählen. In der rechten Ecke des Bereichs **All other updates** auf **More** ⋮ klicken und dann die Option zum Anzeigen aller Updates wählen.	a. **Cluster > Übersicht** auswählen. b. Im Abschnitt **Übersicht** auf **Mehr** ⋮ klicken, dann auf **ONTAP Update**. c. Je nach Ihrer Version von ONTAP ist Folgendes zu tun: ◦ Für ONTAP 9.15.1 und frühere Versionen auf **Firmware Update** klicken. ◦ Für ONTAP 9.16.1 und höher auf **Alle anderen Updates** klicken. d. Auf der Update-Seite auf **Mehr** ⋮ klicken, dann die Option auswählen, alle Updates anzuzeigen.

2. Klicken Sie ⋮ neben der Beschreibung, um eine Liste von Aktionen anzuzeigen, die Sie für die Empfehlung ausführen können.

   Je nach Status der Empfehlung ist eine der folgenden Aktionen möglich:

Wenn sich das Update in diesem Zustand befindet…	Sie können…

Ist noch nicht terminiert	**Update**: Startet den Aktualisierungsprozess. **Zeitplan**: Ermöglicht das Festlegen eines Datums für den Beginn des Aktualisierungsprozesses. **Verwerfen**: Entfernt die Empfehlung aus der Liste.
Wurde geplant	**Update**: Startet den Aktualisierungsprozess. **Zeitplan bearbeiten**: Ermöglicht die Änderung des geplanten Datums für den Beginn des Aktualisierungsprozesses. **Termin stornieren**: Hebt das geplante Datum auf.
Wurde entlassen	**Wiederherstellen**: Die Empfehlung wird wieder in die Liste aufgenommen.
Wird angewendet oder wird heruntergeladen	**Abbrechen**: Das Update wird abgebrochen.

ONTAP Firmware manuell aktualisieren

Ab ONTAP 9.9.1, wenn Sie bei "Digital Advisor" registriert sind, können Sie im System Manager Benachrichtigungen erhalten, die Sie darüber informieren, wenn Firmware-Updates für unterstützte Geräte wie Festplatten, Festplattengehäuse, den Serviceprozessor (SP) oder den Baseboard Management Controller (BMC) im Cluster ausstehen.

Wenn Sie ONTAP 9.8 verwenden oder nicht bei Digital Advisor registriert sind, navigieren Sie zur NetApp Support-Website, um Firmware-Updates herunterzuladen.

Bevor Sie beginnen

Für eine reibungslose Firmware-Aktualisierung empfiehlt sich ein Neustart von SP oder BMC vor Beginn des Updates. Der Neustart erfolgt mit dem `system service-processor reboot-sp -node node_name` Befehl. Weitere Informationen zu `system service-processor reboot-sp` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

Befolgen Sie das entsprechende Verfahren basierend auf Ihrer Version von ONTAP und falls Sie bei Digital Advisor registriert sind.

ONTAP 9.16.1 und höher mit Digital Advisor

Schritte

1. Im System Manager zur **Dashboard** wechseln.

   Im Abschnitt **Health** wird eine Meldung angezeigt, wenn empfohlene Firmware-Updates für das Cluster verfügbar sind.

2. Klicken Sie auf die Warnmeldung.
3. Neben den Sicherheitsupdates in der Liste der empfohlenen Updates die Option **Aktionen** auswählen.
4. **Aktualisieren** installiert das Update sofort, **Planen** legt die Installation für einen späteren Zeitpunkt

fest.

Wenn das Update bereits geplant ist, besteht die Möglichkeit, es **zu bearbeiten** oder **zu stornieren**.

ONTAP 9.9.1 bis 9.15.1 mit Digital Advisor

1. Im System Manager zur **Dashboard** wechseln.

   Im Abschnitt **Health** wird eine Meldung angezeigt, wenn empfohlene Firmware-Updates für das Cluster verfügbar sind.

2. Klicken Sie auf die Warnmeldung.

   Auf der Seite **Update** wird die Registerkarte **Firmware Update** angezeigt.

3. Auf **Download von der NetApp Support Site** klicken, um das gewünschte Firmware-Update durchzuführen.

   Die NetApp Support Site wird angezeigt.

4. Melden Sie sich auf der NetApp Support Site an und laden Sie das für das Update benötigte Firmware-Image-Paket herunter.
5. Die Dateien werden auf einen HTTP- oder FTP-Server im Netzwerk oder in einen lokalen Ordner kopiert.
6. Im System Manager auf **Cluster > Übersicht** klicken.
7. In der rechten Ecke des **Übersicht**-Bereichs auf **Mehr** ⋮ klicken und **ONTAP Update** auswählen.
8. **Firmware Update** auswählen.
9. Je nach Ihrer Version von ONTAP ist Folgendes zu tun:

ONTAP 9.9.1 und 9.10.0	ONTAP 9.10.1 und höher
a. **Vom Server** oder **Lokaler Client** auswählen b. Geben Sie die Server-URL oder den Dateispeicherort an.	a. In der Liste der empfohlenen Updates die Option **Aktionen** auswählen. b. **Aktualisieren** installiert das Update sofort, **Planen** legt die Installation für einen späteren Zeitpunkt fest. Wenn das Update bereits geplant ist, besteht die Möglichkeit, es **zu bearbeiten** oder **zu stornieren**. c. Die Schaltfläche **Firmware aktualisieren** auswählen.

ONTAP 9.8 und höher ohne Digital Advisor

1. Navigieren Sie zu "NetApp Support Site" und melden Sie sich an.
2. Wählen Sie das Firmware-Paket aus, das Sie zum Aktualisieren der Cluster-Firmware verwenden möchten.
3. Die Dateien werden auf einen HTTP- oder FTP-Server im Netzwerk oder in einen lokalen Ordner kopiert.
4. Im System Manager auf **Cluster > Übersicht** klicken.

5. In der rechten Ecke des **Übersicht**-Bereichs auf **Mehr** ⋮ klicken und **ONTAP Update** oder **Software updates** auswählen (abhängig von Ihrer Version).
6. Je nach Ihrer Version von ONTAP ist Folgendes zu tun:
   - Für ONTAP 9.15.1 und frühere Versionen auf **Firmware Update** klicken.
   - Für ONTAP 9.16.1 und höher auf **Alle anderen Updates** klicken.
7. Je nach Ihrer Version von ONTAP ist Folgendes zu tun:

ONTAP 9.8, 9.9.1 und 9.10.0	ONTAP 9.10.1 und höher
1. **Vom Server** oder **Lokaler Client** auswählen 2. Geben Sie die Server-URL oder den Dateispeicherort an.	1. In der Liste der empfohlenen Updates die Option **Aktionen** auswählen. 2. **Aktualisieren** installiert das Update sofort, **Planen** legt die Installation für einen späteren Zeitpunkt fest. Wenn das Update bereits geplant ist, besteht die Möglichkeit, es **zu bearbeiten** oder **zu stornieren**. 3. Die Schaltfläche **Firmware aktualisieren** auswählen.

Nachdem Sie fertig sind

Sie können Updates unter **Firmware Update Summary** überwachen oder überprüfen. Um Updates anzuzeigen, die verworfen wurden oder deren Installation fehlgeschlagen ist, gibt es je nach Ihrer Version von ONTAP folgende Möglichkeiten:

- Für ONTAP 9.15.1 und frühere Versionen auf **Cluster > Einstellungen > Automatisches Update > Alle automatischen Updates anzeigen** klicken
- Für ONTAP 9.16.1 und höher unter **Cluster > Einstellungen > Softwareupdates** klicken. In der rechten Ecke des Bereichs **Alle anderen Updates** auf **Mehr** ⋮ klicken und **Alle automatischen Updates anzeigen** auswählen.

System-Firmware vor einem ONTAP Software Upgrade vorbereiten

Ab ONTAP 9.17.1 bleibt, wenn auf dem Boot-Gerät eines Knotens bereits eine neuere BIOS- oder LOADER-Firmware vorhanden ist, bevor ein automatisiertes unterbrechungsfreies Upgrade (ANDU) durchgeführt wird, die neuere Firmware erhalten, anstatt sie durch die im ONTAP Image enthaltene Version zu überschreiben. Dadurch können sowohl das ONTAP Software-Upgrade als auch das Firmware-Update in einem einzigen Neustartzyklus abgeschlossen werden.

In ONTAP 9.16.1 und früher installiert ein ANDU immer die im Ziel-ONTAP-Image enthaltene BIOS- und LOADER-Firmware, unabhängig davon, welche Firmware-Version bereits auf dem Boot-Gerät vorhanden ist. Wenn ein neueres BIOS- oder LOADER-Service-Image unabhängig heruntergeladen wurde, ist nach dem ONTAP Upgrade ein separater Übernahme- und Rückgabevorgang erforderlich, um die neuere Firmware zu aktivieren.

Ab ONTAP 9.17.1 vergleicht ONTAP die BIOS- und LOADER-Firmware-Versionen auf dem Boot-Gerät jedes

Knotens mit den im Ziel-ONTAP-Image enthaltenen Versionen. Ist auf dem Boot-Gerät bereits eine neuere Version als die mitgelieferte vorhanden, wird die mitgelieferte Firmware nicht installiert. Die vorhandene neuere Firmware bleibt erhalten. Ist die mitgelieferte Version gleich oder neuer als die auf dem Boot-Gerät vorhandene, wird die mitgelieferte Firmware installiert.

Nach dem Neustart des Knotens im Rahmen des normalen ANDU-Workflows wird die Firmware auf dem Boot-Gerät aktiviert, sodass sowohl das ONTAP Upgrade als auch das Firmware-Update in einem einzigen Neustart abgeschlossen werden.

Bevor Sie beginnen

- Alle Knoten im Cluster müssen ONTAP 9.17.1 oder höher ausführen.
- Sie müssen das neuere BIOS- oder LOADER-Service-Image von der "NetApp Support Site" heruntergeladen haben.

  Für das Herunterladen der Firmware auf das Boot-Gerät eines Knotens ist ein erweitertes Berechtigungsniveau erforderlich.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Das neuere Service-Image wird auf das Boot-Gerät jedes Knotens heruntergeladen:

   ```
   system node firmware download -node <node_name> -package
   ```

   Dieser Schritt ist für jeden Knoten im Cluster zu wiederholen, der die neuere Firmware erhalten soll.

3. Zurück zu Administratorrechten:

   ```
   set -privilege admin
   ```

4. Die aktuell auf dem Boot-Gerät jedes Knotens vorhandene Firmware-Version kann überprüft werden:

   ```
   system node firmware bootmedia show
   ```

   Die vorab bereitgestellte Firmware-Version sollte höher sein als die in Ihrem Ziel ONTAP Image enthaltene Version.

Was kommt als Nächstes?

- Nachdem Sie Ihre Firmware vorbereitet haben, sind Sie bereit, "Ein automatisiertes ONTAP Upgrade durchführen".

  Während des Upgrades erkennt ONTAP, dass das Boot-Gerät bereits neuere BIOS- und LOADER-Firmware enthält und behält diese bei. Die mitgelieferte Firmware wird nicht auf Knoten installiert, auf denen bereits eine höhere Version vorhanden ist.

ONTAP zurücksetzen

Wann Sie den technischen Support für eine ONTAP Rücksetzung kontaktieren sollten

Sie sollten sich in den folgenden Situationen an den technischen Support wenden, bevor Sie versuchen, einen ONTAP Cluster zurückzusetzen:

- Eine Produktionsumgebung

  Ein Produktionscluster sollte nicht ohne Unterstützung des technischen Supports zurückgesetzt werden.

- Sie haben Volumes in ONTAP 9.5 oder einer späteren Version erstellt und müssen auf eine frühere Version zurückkehren.

  Volumes, die adaptive Komprimierung verwenden, müssen vor dem Zurücksetzen dekomprimiert werden.

Sie können neue oder Testcluster ohne Unterstützung zurücksetzen. Wenn beim Versuch, einen Cluster eigenständig zurückzusetzen, eines der folgenden Probleme auftritt, sollte der technische Support kontaktiert werden:

- Der Rücksetzvorgang schlägt fehl oder kann nicht abgeschlossen werden.
- Der Rücksetzvorgang wird abgeschlossen, aber der Cluster ist in einer Produktionsumgebung nicht verwendbar.
- Der Rücksetzvorgang wird abgeschlossen und der Cluster geht in die Produktion, aber Sie sind mit seinem Verhalten nicht zufrieden.

Unterstützte ONTAP Revert-Pfade

Sie können Ihre ONTAP Software nur direkt auf eine Version zurücksetzen, die eine Version älter ist als Ihre aktuelle ONTAP Version. Wenn Sie beispielsweise Version 9.15.1 verwenden, ist ein direktes Zurücksetzen auf 9.13.1 nicht möglich. Zuerst muss auf 9.14.1 zurückgesetzt werden, danach erfolgt ein separates Zurücksetzen von 9.14.1 auf 9.13.1.

Die Rückkehr zu ONTAP 9.4 oder einer früheren Version wird nicht unterstützt. Ein Zurücksetzen auf nicht unterstützte ONTAP Versionen sollte vermieden werden.

Sie können den `system image show` Befehl verwenden, um die auf jedem Knoten ausgeführte ONTAP-Version zu ermitteln.

Die folgenden unterstützten Wiederherstellungspfade beziehen sich nur auf lokale ONTAP Versionen. Informationen zur Wiederherstellung von ONTAP in der Cloud sind unter "Zurücksetzen oder Herabstufen von Cloud Volumes ONTAP" zu finden.

"AFX Storage-Systeme"Das Zurücksetzen der ONTAP Software wird nicht unterstützt.

Sie können von… zurückkehren.	Zu…
ONTAP 9.20.1	ONTAP 9.19.1

Sie können von… zurückkehren.	Zu…
ONTAP 9.19.1	ONTAP 9.18.1
ONTAP 9.18.1	ONTAP 9.17.1
ONTAP 9.17.1	ONTAP 9.16.1
ONTAP 9.16.1	ONTAP 9.15.1
ONTAP 9.15.1	ONTAP 9.14.1
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5

ONTAP Revert-Probleme und Einschränkungen

Vor dem Zurücksetzen eines ONTAP Clusters sind die möglichen Probleme und Einschränkungen zu berücksichtigen.

- Die Rückführung ist störend.

  Während der Wiederherstellung darf kein Clientzugriff erfolgen. Bei der Wiederherstellung eines Produktionsclusters sollte diese Unterbrechung in der Planung berücksichtigt werden.

- Die Rücksetzung betrifft alle Knoten im Cluster.

  Die Rücksetzung betrifft alle Knoten im Cluster, allerdings muss die Rücksetzung auf jedem HA-Paar durchgeführt und abgeschlossen werden, bevor andere HA-Paare rückgesetzt werden.

  "AFX Storage-Systeme" Die Rücksetzung wird nicht unterstützt.

- Die Rücksetzung ist abgeschlossen, wenn auf allen Knoten die neue Zielversion ausgeführt wird.

  Befindet sich der Cluster in einem gemischten Versionszustand, sollten keine Befehle eingegeben werden, die den Clusterbetrieb oder die Konfiguration verändern, es sei denn, dies ist zur Erfüllung der Reversionsanforderungen erforderlich; Überwachungsvorgänge sind zulässig.

  Wenn Sie einige, aber nicht alle Knoten zurückgesetzt haben, sollte der Cluster nicht auf die Quellversion zurückaktualisiert werden.

- Wenn ein Knoten zurückgesetzt wird, werden die zwischengespeicherten Daten in einem Flash Cache Modul gelöscht.

Da im Flash Cache-Modul keine zwischengespeicherten Daten vorhanden sind, bedient der Knoten anfängliche Leseanfragen von der Festplatte, was in diesem Zeitraum zu einer verringerten Leseleistung führt. Der Knoten füllt den Cache wieder auf, während er Leseanfragen bearbeitet.

- Eine LUN, die auf Band gesichert wurde, während ONTAP 9.x ausgeführt wurde, kann nur auf 9.x und spätere Versionen wiederhergestellt werden und nicht auf eine frühere Version.
- Wenn Ihre aktuelle Version von ONTAP die In-Band ACP (IBACP)-Funktionalität unterstützt und Sie auf eine Version von ONTAP zurückkehren, die IBACP nicht unterstützt, wird der alternative Pfad zu Ihrem Disk Shelf deaktiviert.
- Wenn LDAP von einer Ihrer Storage Virtual Machines (SVMs) verwendet wird, muss die LDAP-Weiterleitung vor der Rückkehr auf eine frühere Version deaktiviert werden.
- In MetroCluster IP-Systemen mit Switches, die MetroCluster-konform, aber nicht MetroCluster-validiert sind, ist die Rückkehr von ONTAP 9.7 auf 9.6 disruptiv, da es keine Unterstützung für Systeme mit ONTAP 9.6 und älteren Versionen gibt.
- Bevor ein Knoten auf ONTAP 9.13.1 oder eine frühere Version zurückgesetzt wird, ist zunächst ein verschlüsseltes SVM-Root-Volume in ein nicht verschlüsseltes Volume zu konvertieren.

  Wenn versucht wird, auf eine ONTAP Version zurückzukehren, die die Verschlüsselung des SVM-Root-Volumes nicht unterstützt, gibt das System eine Warnung aus und blockiert die Rückkehr.

- Wenn NFS über TLS in ONTAP 9.19.1 oder höher aktiviert ist, müssen alle NFS over TLS-Konfigurationsinstanzen deaktiviert werden, bevor auf eine frühere Version von ONTAP zurückgegangen werden kann. NFS over TLS wird erst ab ONTAP 9.19.1 unterstützt.

Überprüfung der Ressourcen vor dem Zurücksetzen eines ONTAP Cluster

Bevor Sie einen ONTAP Cluster zurücksetzen, sollte die Hardwareunterstützung bestätigt und die verfügbaren Ressourcen geprüft werden, um mögliche Probleme zu verstehen oder zu lösen.

1. Prüfen Sie "ONTAP 9 Versionshinweise" für die Zielversion.

   Im Abschnitt „Wichtige Hinweise“ werden mögliche Probleme beschrieben, derer Sie sich vor einem Downgrade oder einer Rückkehr zur vorherigen Version bewusst sein sollten.

2. Bestätigen Sie, dass Ihre Hardwareplattform in der Zielversion unterstützt ist.

   "NetApp Hardware Universe"

3. Es sollte bestätigt werden, dass Ihr Cluster und Ihre Management-Switches in der Zielversion unterstützt sind.

   Es ist zu überprüfen, ob die Softwareversionen von NX-OS (Cluster-Netzwerk-Switches), IOS (Management-Netzwerk-Switches) und der Referenzkonfigurationsdatei (RCF) mit der Version von ONTAP, auf die zurückgesetzt wird, kompatibel sind.

   "NetApp Downloads: Cisco Ethernet Switch"

4. Wenn Ihr Cluster für SAN konfiguriert ist, sollte bestätigt werden, dass die SAN-Konfiguration vollständig unterstützt ist.

   Alle SAN-Komponenten, einschließlich der Ziel-ONTAP Softwareversion, des Host-Betriebssystems und

der Patches, der erforderlichen Host Utilities Software sowie der Adaptertreiber und Firmware, sollten unterstützt werden.

"NetApp Interoperabilitätsmatrix-Tool"

Überprüfung der Systembereitschaft vor dem Zurücksetzen eines ONTAP Clusters

Vor dem Zurücksetzen eines ONTAP Clusters empfiehlt sich die Überprüfung des Clusterzustands, des Speicherzustands und der Systemzeit. Zudem sollte überprüft werden, dass keine Jobs auf dem Cluster laufen.

Clusterzustand überprüfen

Bevor ein ONTAP Cluster zurückgesetzt wird, sollte überprüft werden, ob die Knoten fehlerfrei sind und zur Teilnahme am Cluster berechtigt sind sowie ob sich der Cluster im Quorum befindet.

Schritte

1. Es sollte sichergestellt werden, dass die Knoten im Cluster online sind und zur Teilnahme am Cluster berechtigt sind:

   ```
   cluster show
   ```

   In diesem Beispiel sind alle Knoten fehlerfrei und zur Teilnahme am Cluster berechtigt.

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   Wenn ein Knoten fehlerhaft oder nicht geeignet ist, sollten die EMS-Protokolle auf Fehler überprüft und Korrekturmaßnahme ergriffen werden.

2. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

   Geben Sie `y` ein, um fortzufahren.

3. Die Konfigurationsdetails für jeden RDB-Prozess werden überprüft.

   - Die relationalen Datenbank-Epochen und die Datenbank-Epochen sollten für jeden Knoten übereinstimmen.
   - Das primäre Quorum pro Ring sollte für alle Knoten gleich sein.

     Beachten Sie, dass jeder Ring ein anderes Quorum-Primary haben kann.

Um diesen RDB-Prozess anzuzeigen…	Geben Sie diesen Befehl ein…
Verwaltungsanwendung	`cluster ring show -unitname mgmt`
Volume-Standortdatenbank	`cluster ring show -unitname vldb`
Manager für virtuelle Schnittstellen	`cluster ring show -unitname vifmgr`
SAN Management-Daemon	`cluster ring show -unitname bcomd`

Dieses Beispiel zeigt den Volume Location Database-Prozess:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

5. Wenn Sie in einer SAN-Umgebung arbeiten, überprüfen Sie, ob sich jeder Knoten in einem SAN-Quorum befindet:

```
event log show  -severity informational -message-name scsiblade.*
```

Die aktuellste scsi-blade-Ereignismeldung für jeden Knoten sollte anzeigen, dass sich das scsi-blade im Quorum befindet.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
```

```
scsi-blade ...
MM/DD/YYYY TIME   node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Verwandte Informationen

"Systemadministration"

Speicherzustand überprüfen

Bevor Sie einen ONTAP Cluster zurücksetzen, sollte der Status Ihrer Festplatten, Aggregate und Volumes überprüft werden.

Schritte

1. Festplattenstatus überprüfen:

Zur Überprüfung, ob…	Folgendes ist zu tun…
Defekte Festplatten	a. Alle defekten Datenträger anzeigen: `storage disk show -state broken` b. Beschädigte Datenträger entfernen oder ersetzen.
Festplatten, die sich in Wartung oder Wiederherstellung befinden	a. Alle Datenträger im Wartungs-, Ausstehend- oder Wiederherstellungsstatus anzeigen: `storage disk show -state maintenance`
pending	reconstructing ---- .. Es sollte abgewartet werden, bis die Wartungs- oder Wiederherstellungsarbeiten abgeschlossen sind, bevor fortgefahren wird.

2. Es sollte sichergestellt werden, dass alle Speicheraggregate online sind, indem der Status des physischen und logischen Speichers, einschließlich der Speicheraggregate, angezeigt wird: +

```
storage aggregate show -state !online
```

Dieser Befehl zeigt die Aggregate an, die nicht online sind. Alle Aggregate müssen vor und nach einer größeren Aktualisierung oder Rücksetzung online sein.

```
cluster1::> storage aggregate show -state !online
```

```
There are no entries matching your query.
```

3. Es kann überprüft werden, ob alle Volumes online sind, indem alle Volumes angezeigt werden, die *nicht* online sind:

   ```
   volume show -state !online
   ```

   Alle Volumes müssen vor und nach einer größeren Aktualisierung oder Rücksetzung online sein.

   ```
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Es wird überprüft, ob keine inkonsistenten Volumes vorhanden sind:

   ```
   volume show -is-inconsistent true
   ```

   Siehe die "NetApp Knowledge Base: Volumen zeigt WAFL als inkonsistent" Hinweise zum Umgang mit den uneinheitlichen Volumen.

Verwandte Informationen

"Festplatten- und Aggregatverwaltung"

Systemzeit überprüfen

Bevor ein ONTAP Cluster zurückgesetzt wird, sollte überprüft werden, ob NTP konfiguriert ist und die Zeit im gesamten Cluster synchronisiert ist.

Schritte

1. Es sollte überprüft werden, ob der Cluster mit einem NTP-Server verbunden ist:

   ```
   cluster time-service ntp server show
   ```

2. Es sollte sichergestellt sein, dass jeder Knoten das gleiche Datum und die gleiche Uhrzeit hat:

   ```
   cluster date show
   ```

   ```
   cluster1::> cluster date show
   Node      Date                Timezone
   --------- ------------------- -------------------------
   node0     4/6/2013 20:54:38   GMT
   node1     4/6/2013 20:54:38   GMT
   node2     4/6/2013 20:54:38   GMT
   ```

```
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

Es sollte sichergestellt sein, dass keine Jobs ausgeführt werden.

Bevor Sie einen ONTAP Cluster zurücksetzen, sollte der Status der Cluster-Jobs überprüft werden. Wenn Aggregate-, Volume-, NDMP- (Dump- oder Restore-) oder Snapshot-Jobs (wie Erstellen, Löschen, Verschieben, Ändern, Replizieren und Mounten) ausgeführt werden oder in der Warteschlange stehen, sollten die Jobs erfolgreich abgeschlossen werden oder die Einträge in der Warteschlange gestoppt werden.

Schritte

1. Die Liste aller laufenden oder in der Warteschlange befindlichen Aggregate-, Volume- oder Snapshot-Jobs kann eingesehen werden:

   ```
   job show
   ```

   In diesem Beispiel befinden sich zwei Aufträge in der Warteschlange:

   ```
   cluster1::> job show
                             Owning
   Job ID Name               Vserver    Node           State
   ------ ------------------ ---------- -------------- ----------
   8629   Vol Reaper         cluster1   -              Queued
          Description: Vol Reaper Job
   8630   Certificate Expiry Check
                             cluster1   -              Queued
          Description: Certificate Expiry Check
   ```

2. Alle laufenden oder in der Warteschlange befindlichen Aggregate-, Volume- oder Snapshot-Jobs löschen:

   ```
   job delete -id <job_id>
   ```

3. Es sollte sichergestellt sein, dass keine Aggregate-, Volume- oder Snapshot-Jobs ausgeführt werden oder in der Warteschlange stehen:

   ```
   job show
   ```

   In diesem Beispiel wurden alle laufenden und in der Warteschlange befindlichen Jobs gelöscht:

   ```
   cluster1::> job show
                             Owning
   Job ID Name               Vserver    Node           State
   ------ ------------------ ---------- -------------- ----------
   ```

```
9944   SnapMirrorDaemon_7_2147484678
                           cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                           cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

Überprüfung des Status des Schlüsselmanagers vor dem Zurücksetzen

Vor der Rückkehr von ONTAP 9.20.1 zu einer früheren ONTAP Version ist zu prüfen, ob sich die Key Manager-Konfigurationen für die Zielversion in einem gültigen Zustand befinden.

Schritte

1. Status des Schlüsselmanagers anzeigen:

```
security key-manager keystore show
```

2. Falls eine Konfiguration vorhanden ist `inactive`, muss sie vor dem Fortfahren mit dem Zurücksetzen gelöscht werden:

```
security key-manager keystore delete -vserver <svm_name>
```

3. Prüfung, ob noch ein Key Manager Job ausgeführt wird:

```
job show -name *keymanager*
```

4. Wenn ein Schlüsselmanager-Job noch initialisiert wird, ist vor dem Start der Revertierung dessen Abschluss abzuwarten.

> Aktive Keystore-Konfigurationen sind Teil des Standard-Revert-Prozesses. Das Hauptproblem bei der Revertierung sind inaktive Keystore-Einträge oder laufende key-manager Jobs, die durch den ONTAP 9.20.1 key-manager Workflow eingeführt wurden.

Verwandte Informationen

- "Speicherdatenträger anzeigen"

ONTAP versionsspezifische Prüfungen vor dem Zurücksetzen durchführen

Voraussetzungen vor der Rückkehr zu Ihrer ONTAP Version

Je nach Ihrer ONTAP Version sind möglicherweise zusätzliche vorbereitende Aufgaben erforderlich, bevor der Wiederherstellungsprozess gestartet werden kann.

Wenn Sie von … zurückkehren	Vor Beginn des Wiederherstellungsprozesses ist Folgendes zu beachten…
Jede ONTAP 9 Version	• "SMB-Sitzungen beenden, die nicht durchgehend verfügbar sind". • "Überprüfung der Rückführungsanforderungen für SnapMirror und SnapVault Beziehungen". • "Es sollte sichergestellt werden, dass die deduplizierten Volumes über ausreichend freien Speicherplatz verfügen.". • "Snapshots vorbereiten". • "Legen Sie den Autocommit-Zeitraum für SnapLock Volumes auf Stunden fest". • Wenn Sie eine MetroCluster Konfiguration haben, "Automatische ungeplante Umschaltung deaktivieren". • "Auf Warnungen des autonomen Ransomware-Schutzes bezüglich ungewöhnlicher Aktivität reagieren".
ONTAP 9.20.1	• Wenn für eine LUN in der Vergangenheit mehr als 182 Registrierungen für persistente SCSI-3-Reservierungen vorlagen, "Alle Registrierungen für persistente Reservierungen auf den betroffenen LUNs entfernen". • Wenn Sie über SNMPv3-Benutzer verfügen, die die SHA-512-Authentifizierung verwenden, "löschen und mit einem unterstützten Authentifizierungsprotokoll neu erstellen".
ONTAP 9.19.1	• Wenn Sie SVMs mit Aktiv/Aktiv Multipathing-Konfigurationen haben, ist Folgendes zu beachten "Die SVMs löschen". • Wenn Sie die Standardeinstellungen einer in ONTAP 9.19.1 oder höher erstellten QoS-Richtliniengruppe geändert haben, "zurücksetzen". • Wenn Sie die Volumes auf ONTAP 9.19.1 aktualisiert und einem Benutzer einen zweiten S3-Zugriffsschlüssel hinzugefügt haben, muss "Diese Schlüssel entfernen".
ONTAP 9.18.1	• Wenn die automatische Aktivierung für ARP/AI im Rahmen eines ONTAP 9.18.1 Upgrades eingestellt wurde, ist es erforderlich, "deaktivieren".
ONTAP 9.17.1	• Wenn Sie die ONTAP ARP/AI Funktion für SAN aktiviert haben, "deaktivieren".

Wenn Sie von … zurückkehren	Vor Beginn des Wiederherstellungsprozesses ist Folgendes zu beachten…
ONTAP 9.16.1	• Wenn Sie TLS für NVMe/TCP-Verbindungen konfiguriert haben, "Die TLS-Konfiguration auf den NVMe-Hosts deaktivieren". • Wenn Sie die erweiterte Qtree-Leistungsüberwachung aktiviert haben, "deaktivieren". • Wenn Sie CORS verwenden, um auf Ihre ONTAP s3 Buckets zuzugreifen, "Die CORS-Konfiguration entfernen".
ONTAP 9.14.1	Wenn Sie Trunking für Clientverbindungen aktiviert haben, "Trunking auf allen NFSv4.1 Servern deaktivieren".
ONTAP 9.12.1	• Wenn Sie den S3-Clientzugriff für NAS-Daten konfiguriert haben, "Die S3 NAS-Bucket-Konfiguration wird entfernt." • Wenn Sie das NVMe-Protokoll verwenden und die In-Band Authentifizierung konfiguriert haben, "In-Band Authentifizierung deaktivieren". • Wenn Sie eine MetroCluster Konfiguration haben, "IPsec deaktivieren".
ONTAP 9.11.1	Wenn Sie den autonomen Ransomware-Schutz (ARP) konfiguriert haben, "Die ARP-Lizenzierung prüfen.".
ONTAP 9.6	Wenn Sie SnapMirror synchron Beziehungen haben, "Die Beziehungen für das Zurücksetzen vorbereiten".

Jede ONTAP 9 Version

Bestimmte SMB-Sitzungen müssen beendet werden, bevor ONTAP zurückgesetzt wird

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, sollten alle SMB-Sitzungen identifiziert und ordnungsgemäß beendet werden, die nicht kontinuierlich verfügbar sind.

Kontinuierlich verfügbare SMB-Freigaben, auf die Hyper-V- oder Microsoft SQL Server Clients über das SMB 3.0-Protokoll zugreifen, müssen vor einem Upgrade oder Downgrade nicht beendet werden.

Schritte

1. Alle bestehenden SMB-Sitzungen, die nicht kontinuierlich verfügbar sind, identifizieren:

```
vserver cifs session show -continuously-available No -instance
```

Dieser Befehl zeigt detaillierte Informationen zu allen SMB-Sitzungen an, die keine kontinuierliche Verfügbarkeit aufweisen. Diese sollten vor dem Fortfahren mit dem ONTAP Downgrade beendet werden.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
           Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. Ermitteln Sie gegebenenfalls die Dateien, die für jede identifizierte SMB-Sitzung geöffnet sind:

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

Informationen zum Zurücksetzen von ONTAP SMB-Clustern

Wenn Sie planen, den Cluster auf eine ONTAP Version zurückzusetzen, die keine lokalen Benutzer und Gruppen unterstützt und lokale Benutzer und Gruppen zur Verwaltung von Dateizugriff oder Benutzerrechten verwendet werden, sind bestimmte Aspekte zu beachten.

- Aus Sicherheitsgründen werden Informationen über konfigurierte lokale Benutzer, Gruppen und Berechtigungen nicht gelöscht, wenn ONTAP auf eine Version zurückgesetzt wird, die die Funktionalität lokaler Benutzer und Gruppen nicht unterstützt.
- Bei der Rückkehr zu einer früheren Hauptversion von ONTAP verwendet ONTAP während der Authentifizierung und der Erstellung von Anmeldeinformationen keine lokalen Benutzer und Gruppen.
- Lokale Benutzer und Gruppen werden nicht aus den Datei- und Ordner-ACLs entfernt.
- Dateizugriffsanfragen, die davon abhängen, dass der Zugriff aufgrund von Berechtigungen lokaler Benutzer oder Gruppen gewährt wird, werden abgelehnt.

  Um den Zugriff zu ermöglichen, müssen die Dateiberechtigungen so umkonfiguriert werden, dass der Zugriff auf Domänenobjekten anstatt auf lokalen Benutzer- und Gruppenobjekten basiert.

ONTAP Rücksetzanforderungen für SnapMirror und SnapVault Beziehungen

Der `system node revert-to` Befehl benachrichtigt Sie über alle SnapMirror und SnapVault Beziehungen, die für den Abschluss des Wiederherstellungsprozesses gelöscht oder neu konfiguriert werden müssen. Allerdings sollten diese Anforderungen vor Beginn der Wiederherstellung bekannt sein.

- Alle SnapVault- und Datenschutz-Spiegelbeziehungen müssen stillgelegt und anschließend getrennt werden.

  Nach Abschluss der Rücksetzung können Sie diese Beziehungen erneut synchronisieren und fortsetzen, sofern ein gemeinsamer Snapshot vorhanden ist.

- SnapVault-Beziehungen dürfen die folgenden SnapMirror-Richtlinientypen nicht enthalten:
  - async-mirror

    Alle Beziehungen, die diesen Richtlinientyp verwenden, müssen gelöscht werden.

  - MirrorAndVault

    Falls eine dieser Beziehungen besteht, sollte die SnapMirror Richtlinie auf mirror-vault geändert werden.

- Alle Load Sharing Mirror-Beziehungen und Ziel-Volumes müssen gelöscht werden.
- SnapMirror-Beziehungen mit FlexClone-Zielvolumes müssen gelöscht werden.
- Die Netzwerkkomprimierung muss für jede SnapMirror Richtlinie deaktiviert werden.
- Die Regel all_source_snapshot muss aus allen async-mirror Typ SnapMirror Richtlinien entfernt werden.

> Die Einzeldatei SnapRestore (SFSR) und Partial File Snapshot Restore (PFSR) Operationen sind auf dem Root-Volume veraltet.

- Alle aktuell laufenden Wiederherstellungsvorgänge für einzelne Dateien und Snapshots müssen abgeschlossen sein, bevor die Rücksetzung fortgesetzt werden kann.

  Sie können entweder warten, bis der Wiederherstellungsvorgang abgeschlossen ist, oder ihn abbrechen.

- Alle unvollständigen Wiederherstellungsvorgänge einzelner Dateien und Snapshots müssen mit dem `snapmirror restore` Befehl entfernt werden.

  Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Freier Speicherplatz für deduplizierte Volumes sollte vor dem Zurücksetzen von ONTAP überprüft werden

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, muss sichergestellt sein, dass die Volumes über ausreichend freien Speicherplatz für den Rücksetzungsvorgang verfügen.

Das Volumen muss ausreichend Platz bieten, um die durch die Inline-Erkennung von Nullblöcken erzielten Einsparungen aufzunehmen. Siehe "NetApp Knowledge Base: Wie sich Speicherplatzeinsparungen durch Deduplizierung, Komprimierung und Kompaktierung in ONTAP 9 anzeigen lassen".

Wenn sowohl Deduplizierung als auch Datenkomprimierung auf einem Volume aktiviert wurden, dessen Zustand zurückgesetzt werden soll, muss die Datenkomprimierung vor der Deduplizierung zurückgesetzt werden.

Schritte

1. Den Fortschritt der Effizienzmaßnahmen, die auf den Volumes ausgeführt werden, anzeigen:

   ```
   volume efficiency show -fields vserver,volume,progress
   ```

2. Alle aktiven und in der Warteschlange befindlichen Deduplizierungsvorgänge anhalten:

   ```
   volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
   ```

3. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

4. Die Effizienzmetadaten eines Volumes auf die Zielversion von ONTAP herabstufen:

   ```
   volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
   -version <version>
   ```

   Das folgende Beispiel setzt die Effizienz-Metadaten auf dem Volume VolA auf ONTAP 9.x zurück.

   ```
   volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
   ```

Der Befehl „volume efficiency revert-to“ setzt die Volumes zurück, die sich auf dem Knoten befinden, auf dem dieser Befehl ausgeführt wird. Mit diesem Befehl werden keine Volumes über Knoten hinweg zurückgesetzt.

5. Der Fortschritt der Herabstufung kann überwacht werden:

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. Falls die Rücksetzung fehlschlägt, kann die Instanz angezeigt werden, um den Grund für das Scheitern der Rücksetzung zu ermitteln.

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. Nach Abschluss des Rückgängigmachungsvorgangs wird zur Administratorberechtigungsstufe zurückgekehrt:

```
set -privilege admin
```

Weitere Informationen zu "Logische Speicherverwaltung".

Vor dem Zurücksetzen eines ONTAP Cluster ist es ratsam, Snapshot-Kopien zu erstellen.

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, müssen alle Snapshot-Richtlinien deaktiviert und alle Snapshots gelöscht werden, die nach dem Upgrade auf die aktuelle Version erstellt wurden.

Wenn Sie in einer SnapMirror-Umgebung einen Reset durchführen, müssen zuvor die folgenden Spiegelbeziehungen gelöscht worden sein:

- Alle lastverteilenden Spiegelbeziehungen

  Weitere Informationen zum Löschen von Lastverteilungsbeziehungen sind unter "Entfernen einer Load-Sharing Mirror-Beziehung" zu finden.

Schritte

1. Snapshot-Richtlinien für alle Daten-SVMs deaktivieren:

```
volume snapshot policy modify -vserver * -enabled false
```

2. Snapshot-Richtlinien für die Aggregate jedes Knotens deaktivieren:
   a. Die Aggregate des Knotens identifizieren:

```
run -node <nodename> -command aggr status
```

b. Die Snapshot-Richtlinie für jedes Aggregat wird deaktiviert:

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

c. Wiederholen Sie diesen Schritt für jeden verbleibenden Node.

3. Snapshot-Richtlinien für das Root-Volume jedes Knotens deaktivieren:

a. Das Root-Volume des Node identifizieren:

```
run -node <node_name> -command vol status
```

Das Root-Volume wird durch das Wort „root“ in der Spalte **Optionen** der `vol status` Befehlsausgabe identifiziert.

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

a. Die Snapshot-Richtlinie auf dem Root-Volume wird deaktiviert:

```
run -node <node_name> vol options root_volume_name nosnap on
```

b. Wiederholen Sie diesen Schritt für jeden verbleibenden Node.

4. Alle Snapshots, die nach dem Upgrade auf die aktuelle Version erstellt wurden, löschen:

a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

b. Snapshots deaktivieren:

```
snapshot policy modify -vserver * -enabled false
```

c. Die neueren Snapshots des Knotens löschen:

```
volume snapshot prepare-for-revert -node <node_name>
```

Dieser Befehl löscht die neueren Snapshots auf jedem Datenvolume, Root-Aggregat und Root-Volume.

Falls Snapshots nicht gelöscht werden können, schlägt der Befehl fehl und Sie werden über die erforderlichen Aktionen informiert, die Sie vor dem Löschen der Snapshots durchführen müssen. Die erforderlichen Aktionen müssen abgeschlossen und anschließend der `volume snapshot prepare-for-revert` Befehl erneut ausgeführt werden, bevor mit dem nächsten Schritt fortgefahren wird.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all snapshots that have the format
used by the current version of ONTAP. It will fail if any snapshot
policies are enabled, or
         if any snapshots have an owner. Continue? {y|n}: y
```

a. Es sollte überprüft werden, ob die Snapshots gelöscht wurden:

```
volume snapshot show -node nodename
```

b. Falls noch neuere Snapshots vorhanden sind, diese zwangsweise löschen:

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
-constituent true} -ignore-owners -force
```

c. Diese Schritte sind für jeden verbleibenden Knoten zu wiederholen.

d. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Diese Schritte sind auf beiden Clustern in der MetroCluster Konfiguration durchzuführen.

Autocommit-Zeiträume für SnapLock Volumes vor dem Zurücksetzen von ONTAP festlegen

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, muss der Wert des Autocommit-Zeitraums für SnapLock Volumes in Stunden und nicht in Tagen festgelegt sein. Es empfiehlt sich, den Autocommit-Wert für die SnapLock Volumes zu überprüfen und ihn gegebenenfalls von Tagen auf Stunden zu ändern.

Schritte

1. Es wird überprüft, ob im Cluster SnapLock Volumes vorhanden sind, die nicht unterstützte Autocommit-Zeiträume haben:

```
volume snaplock show -autocommit-period *days
```

2. Nicht unterstützte Autocommit-Zeiträume auf Stunden ändern

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

Deaktivierung der automatischen ungeplanten Umschaltung vor einem ONTAP MetroCluster Revert

Vor dem Zurücksetzen einer MetroCluster Konfiguration, auf der eine beliebige Version von ONTAP 9 ausgeführt wird, muss die automatische ungeplante Umschaltung (AUSO) deaktiviert werden.

Schritt

1. In beiden Clustern in MetroCluster die automatische ungeplante Umschaltung deaktivieren:

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

Verwandte Informationen

"MetroCluster Management und Katastrophenwiederherstellung"

Behebung von ARP-Aktivitätswarnungen vor einem ONTAP Revert

Bevor Sie auf ONTAP 9.17.1 oder eine frühere Version zurückkehren, sollten Sie auf alle von Autonomous Ransomware Protection gemeldeten Warnungen vor ungewöhnlichen Aktivitäten reagieren und alle zugehörigen Autonomous Ransomware Protection Snapshots löschen.

Bevor Sie beginnen

Zum Löschen von Snapshots der Autonomous Ransomware Protection sind „Advanced“-Berechtigungen erforderlich.

Schritte

1. Auf alle von "Autonomous Ransomware Protection" gemeldeten Warnungen zu ungewöhnlichen Aktivitäten reagieren und mögliche Probleme beheben.
2. Bestätigen Sie die Behebung dieser Probleme, bevor Sie die vorherigen Schritte rückgängig machen, indem Sie **Aktualisieren und verdächtige Dateitypen löschen** auswählen, um Ihre Entscheidung zu speichern und die normale Überwachung von Autonomous Ransomware Protection fortzusetzen.
3. Alle mit den Warnungen verknüpften Autonomous Ransomware Protection Snapshots werden durch Ausführen des folgenden Befehls aufgelistet:

```
volume snapshot snapshot show -fs-version 9.18
```

4. Alle mit den Warnungen verknüpften Autonomous Ransomware Protection Snapshots löschen:

> Dieser Befehl löscht alle Snapshots, die das von der aktuellen Version von ONTAP verwendete Format haben, möglicherweise nicht nur Snapshots von Autonomous Ransomware Protection. Es sollte sichergestellt werden, dass alle erforderlichen Maßnahmen für alle zu entfernenden Snapshots getroffen wurden, bevor dieser Befehl

ausgeführt wird.

```
volume snapshot prepare-for-revert -node <node_name>
```

ONTAP 9.20.1

Deaktivierung von FC-SP-3 auf FC LIFs vor dem Zurücksetzen von ONTAP 9.20.1

Ab ONTAP 9.20.1 unterstützt ONTAP die Authentifizierung und Verschlüsselung mit Fibre Channel Security Protocol 3 (FC-SP-3) unter Verwendung sicherer Broadcom Host-Bus-Adapter (HBAs) mit AFF und FAS Systemen. Wenn FC- oder NVMe/FC-Netzwerkschnittstellen (LIFs) auf Ihrem ONTAP System für FC-SP-3 aktiviert sind, müssen Sie FC-SP-3 deaktivieren, bevor Sie zu ONTAP 9.19.1 zurückkehren.

Schritte

1. Überprüfung der FC-SP-3 Konfiguration auf Ihren LIFs:

```
network interface show -fields fc-transport-security
```

2. Wenn der Status des Feldes **transport-security-state** nicht verfügbar ist, sind keine weiteren Maßnahmen erforderlich. Wenn der Status **mandatory** oder **preferred** ist, ist er in **disabled** zu ändern:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -fc
-transport-security disabled
```

3. Prüfung, ob FC-SP-3 auf den zuvor aktivierten LIFs deaktiviert ist:

```
network interface show -fields fc-transport-security
```

Entfernen von Registrierungen für persistente Reservierungen für eine Rücksetzung auf ONTAP 9.20.1

ONTAP Versionen vor 9.20.1 unterstützen maximal 182 Registrierungen persistenter Reservierungen pro LUN. Ab ONTAP 9.20.1 erhöht sich dieses Limit auf 256. Wenn eine LUN in der Vergangenheit mehr als 182 Registrierungen aufgewiesen hat, blockiert ONTAP die Revertierung unabhängig von der aktuellen Anzahl der Registrierungen. Vor einer Revertierung von 9.20.1 auf 9.19.1 ist die Identifizierung und Entfernung der Registrierungen persistenter Reservierungen auf den betroffenen LUNs erforderlich.

Das Entfernen von Registrierungen für persistente Reservierungen kann in Clusterumgebungen eine Neukonfiguration auf Host-Seite erfordern. Je nach Host-Betriebssystem und Clustering-Software kann es erforderlich sein, Clusterressourcen offline zu nehmen, betroffene LUNs aus der Clusterverwaltung zu entfernen und den Clusterzugriff nach dem Revert erneut herzustellen. Die Dokumentation der Clustering-Lösung sollte überprüft und der Recovery-Workflow vor einem Revert in einer Testumgebung validiert werden.

Schritte

1. Es ist zu prüfen, ob LUNs in der Vergangenheit mehr als 182 Registrierungen für persistente Reservierungen aufwiesen:

```
lun show -field persistent-reservation-scale-tier
```

   Ein Wert über 182 im Feld „persistent-reservation-scale-tier“ bedeutet, dass die LUN zusätzliche persistente Reservierungsmetadaten zugewiesen hat. Dies blockiert eine Reversion, unabhängig von der aktuellen Anzahl der Registrierungen.

2. Für jede betroffene LUN folgt die Anzeige der aktuellen Anzahl aktiver Registrierungen:

```
lun persistent-reservation show -vserver <vserver_name> -path <lun_path>
```

3. Die Registrierungen für persistente Reservierungen sind auf allen betroffenen LUNs zu entfernen.

   Die Vorabprüfung für das Revert ausführen. Wenn diese Bedingung erkannt wird, enthält die Ausgabe der Vorabprüfung die erforderlichen spezifischen Bereinigungsbefehle.

Vor der Rückkehr von ONTAP 9.20.1 sollten SHA-512-SNMPv3-Benutzer entfernt werden.

Ab ONTAP 9.20.1 können SNMPv3-Benutzer erstellt werden, die die SHA-512 Authentifizierung verwenden. ONTAP Versionen vor 9.20.1 unterstützen die SHA-512 Authentifizierung nicht, daher blockiert ONTAP das Zurücksetzen, wenn SNMPv3-Benutzer mit SHA-512 Authentifizierung vorhanden sind. Vor dem Zurücksetzen müssen diese Benutzer gelöscht und mit einem unterstützten Authentifizierungsprotokoll neu erstellt werden.

Schritte

1. SNMPv3-Benutzer, die die SHA-512-Authentifizierung verwenden:

```
security snmpusers -authmethod usm -authprotocol sha512
```

2. Löschen der einzelnen SHA-512-Benutzer:

```
security login delete -vserver <vserver_name> -user-or-group-name
<user_name> -application snmp -authentication-method usm
```

3. Falls Sie die Benutzer weiterhin benötigen, ist eine Neuerstellung mit einem unterstützten Authentifizierungsprotokoll wie `sha` oder `sha2-256` erforderlich:

```
security login create -vserver <vserver_name> -user-or-group-name
<user_name> -application snmp -authentication-method usm
```

Wenn der Benutzer einen Switch überwacht, ist der `-remote-switch-ipaddress`Parameter mit der IP-Adresse des Switches anzugeben:

```
security login create -user-or-group-name <user_name> -application snmp
-authentication-method usm -remote-switch-ipaddress <switch_ip_address>
```

Weitere Informationen zu "Konfigurieren von SNMPv3-Benutzern".

4. Falls Ethernet-Switches die gelöschten SHA-512-Benutzer für die Überwachung verwendet haben, muss jeder Switch so aktualisiert werden, dass er den neu erstellten Benutzer verwendet:

```
system switch ethernet modify -device <switch_name> -snmp-version SNMPv3
-community-or-username <snmp_user_name>
```

Weitere Informationen zu `system switch ethernet modify` finden sich in der "ONTAP-Befehlsreferenz".

Weitere Informationen zu SNMPv3 für den Ethernet Switch Systemstatus Monitor (CSHM), einschließlich Informationen zur Konfiguration der Ethernet Switches, enthält "SNMPv3 für die Zustandsüberwachung von Ethernet-Switches konfigurieren".

ONTAP 9.19.1

Aktiv/Aktiv SVMs müssen gelöscht werden, bevor von ONTAP 9.19.1 zurückgekehrt wird.

SAN Aktiv/Aktiv Multipathing wird in ONTAP 9.18.1 und früher nicht unterstützt. Vor dem Zurücksetzen von ONTAP 9.19.1 müssen alle Storage Virtual Machines (SVMs) mit Aktiv/Aktiv Konfigurationen gelöscht werden.

Schritte

1. Alle SVMs identifizieren, bei denen die Option san-multipathing für Aktiv/Aktiv oder Aktiv/Aktiv-nur-SCSI konfiguriert ist:

```
vserver show
```

2. Alle SVMs, die für Aktiv/Aktiv oder Aktiv/Aktiv-SCSI-Only-Multipathing konfiguriert sind, löschen:

```
vserver delete -vserver <SVM>
```

3. Es wird überprüft, ob die SVMs gelöscht wurden:

```
vserver show
```

Verwandte Informationen

Weitere Informationen zu "SAN Aktiv/Aktiv Multipathing-Unterstützung" in ONTAP 9.19.1 und späteren Versionen.

Ändern von QoS-Richtliniengruppen vor der Rückkehr von ONTAP 9.19.1

Adaptive und nicht-adaptive QoS-Richtliniengruppen werden standardmäßig automatisch aktiviert, um den Durchsatz einer Arbeitslast für eine Dauer von 1 Sekunde um 50 % zu erhöhen, um kurzfristigen Anforderungen nach höherer Leistung zu entsprechen. Ab ONTAP 9.19.1 können Sie diese Standardeinstellungen ändern. In ONTAP 9.18.1 und früher können diese Einstellungen nicht geändert werden. Wenn Sie die Standardeinstellungen einer in ONTAP 9.19.1 oder später erstellten QoS-Policy-Gruppe geändert haben, müssen Sie diese zurücksetzen, bevor Sie von ONTAP 9.19.1 auf ONTAP 9.18.1 zurückkehren können.

Schritte

1. Prüfen Sie, ob QoS-Richtliniengruppen für die automatische Erhöhung des Durchsatzlimits aktiviert sind:

```
qos policy-group show – instance
```

2. Wenn Richtliniengruppen mit `burst-percent`, `burst-iops` und `burst-duration` konfiguriert sind, setzen Sie diese Optionen auf 0.

```
qos policy-group modify -policy-group <policy-group> -burst-percent 0
-burst-iops 0 -burst-duration 0
```

Entfernen Sie die zweiten S3-Zugriffsschlüssel, bevor Sie von ONTAP 9.19.1 zurückkehren.

Wenn Sie auf ONTAP 9.19.1 aktualisiert und einem Benutzer einen zweiten S3-Zugriffsschlüssel hinzugefügt haben, müssen diese Schlüssel entfernt werden, bevor Sie zu einer früheren ONTAP-Version zurückkehren können.

Schritte

1. "S3-Zugriffsschlüssel anzeigen" um festzustellen, ob für S3-Benutzer zweite Zugriffsschlüssel hinzugefügt wurden.
2. "Entfernen Sie die zweiten Zugriffsschlüssel" für alle S3-Nutzer.

ONTAP 9.18.1

Automatische ARP-Aktivierung vor dem Zurücksetzen von ONTAP 9.18.1 deaktivieren

Wenn Volumes auf ONTAP 9.18.1 oder höher aktualisiert wurden, könnte die automatische Aktivierung von ONTAP ARP/AI nach einer kurzen Karenzzeit (12 Stunden) für Ihre Volumes eingerichtet worden sein. Es wird empfohlen, diese automatische Aktivierungseinstellung auf Volumes, die auf ONTAP 9.18.1 oder höher aktualisiert wurden, zu deaktivieren, bevor auf ONTAP 9.17.1 oder eine frühere Version zurückgekehrt wird.

Schritte

1. Ermitteln Sie, ob die automatische Aktivierungsoption auf Volumes aktiviert wurde, die auf ONTAP 9.18.1 oder höher aktualisiert wurden:

```
security anti-ransomware auto-enable show
```

2. Deaktivieren Sie die automatische Aktivierungsoption für den Ransomware-Schutz auf allen Volumes auf der SVM:

```
security anti-ransomware volume disable -volume * -auto-enabled-volumes
-only true
```

ONTAP 9.17.1

Deaktivierung von ARP auf SAN-Volumes vor dem Revert von ONTAP 9.17.1

Die ONTAP ARP/AI-Funktion für SAN-Volumes wird in ONTAP 9.16.1 und früher nicht unterstützt. Es wird empfohlen, ARP/AI auf SAN-Volumes zu deaktivieren, bevor auf ONTAP 9.16.1 oder eine frühere Version zurückgesetzt wird, um zu verhindern, dass die Funktion aktiv bleibt und CPU- sowie Festplattenressourcen nutzt, ohne in der zurückgesetzten Version eine tatsächliche Erkennung durchzuführen.

Beispiel 6. Schritte

System Manager

1. **Speicher > Volumes** auswählen und dann den Namen des Volumes auswählen.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Aktiviert auf Deaktiviert zu wechseln.

CLI

1. Ransomware-Schutz auf einem Volume deaktivieren:

```
security anti-ransomware volume disable -volume <vol_name> -vserver
<svm_name>
```

ONTAP 9.16.1

TLS auf NVMe-Hosts vor dem Zurücksetzen von ONTAP 9.16.1 deaktivieren

Wenn auf einem NVMe-Host ein sicherer TLS-Kanal für NVMe/TCP-Verbindungen konfiguriert ist, muss dieser deaktiviert werden, bevor der Cluster von ONTAP 9.16.1 zurückgesetzt wird.

Schritte

1. Die TLS-Sicherheitskanalkonfiguration wird vom Host entfernt:

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

   Dieser Befehl entfernt den Host aus dem Subsystem und erstellt den Host anschließend ohne die TLS-Konfiguration im Subsystem neu.

2. Es sollte überprüft werden, ob der sichere TLS-Kanal vom Host entfernt wurde:

```
vserver nvme subsystem host show
```

Deaktivieren der erweiterten qtree-Performanceüberwachung vor einem ONTAP Revert

Ab ONTAP 9.16.1 kann über die ONTAP REST API auf die erweiterten Qtree-Überwachungsfunktionen zugegriffen werden, die Latenzmetriken und historische Statistiken umfassen. Wenn die erweiterte Qtree-Überwachung auf einem Qtree aktiviert ist, muss `ext_performance_monitoring.enabled` vor dem Zurücksetzen von Version 9.16.1 auf false gesetzt werden.

Sie arbeiten mit der `ext_performance_monitoring.enabled` Einstellung, indem Sie den `/api/storage/qtrees` Endpoint verwenden. Verwenden Sie GET, um den aktuellen Wert abzurufen, POST, um ihn beim Erstellen eines neuen qtree festzulegen, und PATCH, um ihn bei einem bestehenden qtree zu ändern.

Weitere Informationen zu "Wiederherstellung von Clustern mit erweiterter Qtree-Leistungsüberwachung".

CORS-Konfiguration vor dem Zurücksetzen von ONTAP 9.16.1 entfernen

Wenn Sie Cross-Origin Resource Sharing (CORS) für den Zugriff auf ONTAP S3 Buckets verwenden, muss dies entfernt werden, bevor Sie von ONTAP 9.16.1 zurückkehren.

Weitere Informationen zu "Zurücksetzen von ONTAP Clustern mit CORS".

ONTAP 9.14.1

NFSv4.1 Session Trunking vor dem Zurücksetzen von ONTAP 9.14.1 deaktivieren

Wenn Trunking für Clientverbindungen aktiviert wurde, muss Trunking auf allen NFSv4.1-Servern deaktiviert werden, bevor ein Wechsel von ONTAP 9.14.1 erfolgt.

Wenn Sie den `revert-to` Befehl eingeben, erscheint eine Warnmeldung, in der empfohlen wird, Trunking zu deaktivieren, bevor Sie fortfahren.

Nach dem Downgrade auf ONTAP 9.13.1 nutzen Clients mit trunked Verbindungen eine einzelne Verbindung. Ihr Datendurchsatz wird beeinträchtigt, es kommt jedoch zu keiner Unterbrechung. Das Rückkehrverhalten entspricht der Änderung der NFSv4.1 trunking Option für die SVM von aktiviert auf deaktiviert.

Schritte

1. Trunking auf dem NFSv4.1 Server deaktivieren:

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. Es sollte überprüft werden, ob NFS wie gewünscht konfiguriert ist:

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12.1

Die S3 NAS-Bucket-Konfiguration sollte entfernt werden, bevor von ONTAP 9.12.1 zurückgekehrt wird.

Wenn der S3-Clientzugriff für NAS-Daten konfiguriert wurde, empfiehlt sich die Verwendung der ONTAP Befehlszeilenschnittstelle (CLI), um die NAS-Bucket-Konfiguration sowie alle Namenszuordnungen (S3-Benutzer zu Windows- oder Unix-Benutzern) zu entfernen, bevor von ONTAP 9.12.1 zurückgekehrt wird.

Über diese Aufgabe

Die folgenden Aufgaben werden während des Rücksetzungsprozesses im Hintergrund abgeschlossen.

- Alle unvollständig erstellten Singleton-Objekte (also alle Einträge in versteckten Verzeichnissen) entfernen.
- Alle versteckten Verzeichnisse entfernen; möglicherweise existiert für jedes Volume, das vom Stammverzeichnis des aus dem S3 NAS-Bucket gemappten Exports aus zugänglich ist, ein solches Verzeichnis.
- Die Upload-Tabelle wird entfernt.
- Alle default-unix-user- und default-windows-user-Werte für alle konfigurierten S3-Server löschen.

Schritte

1. S3 NAS-Bucket-Konfiguration entfernen:

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket
<s3_nas_bucket_name>
```

   Weitere Informationen zu `vserver object-store-server bucket delete` finden sich in der "ONTAP-Befehlsreferenz".

2. Namenszuordnungen für UNIX entfernen:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

   Weitere Informationen zu `vserver name-mapping delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Namenszuordnungen für Windows entfernen:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. Die S3-Protokolle aus der SVM entfernen:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Weitere Informationen zu `vserver remove-protocols` finden sich in der "ONTAP-Befehlsreferenz".

NVMe In-Band-Authentifizierung vor der Rückkehr von ONTAP 9.12.1 deaktivieren

Wenn Sie das NVME-Protokoll verwenden, muss die In-Band Authentifizierung deaktiviert werden, bevor Sie Ihren Cluster von ONTAP 9.12.1 zurücksetzen. Wenn die In-Band Authentifizierung mit DH-HMAC-CHAP nicht deaktiviert ist, schlägt das Zurücksetzen fehl.

Schritte

1. Den Host aus dem Subsystem entfernen, um die DH-HMAC-CHAP Authentifizierung zu deaktivieren:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Es sollte überprüft werden, ob das DH-HMAC-CHAP Authentifizierungsprotokoll vom Host entfernt ist:

```
vserver nvme subsystem host show
```

3. Den Host ohne Authentifizierung wieder dem Subsystem hinzufügen:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Deaktivierung von IPsec in MetroCluster vor der Rückkehr von ONTAP 9.12.1

Bevor eine MetroCluster Konfiguration von ONTAP 9.12.1 zurückgesetzt wird, muss IPsec deaktiviert werden.

Vor dem Zurücksetzen wird geprüft, ob innerhalb der MetroCluster Konfiguration IPsec-Konfigurationen vorhanden sind. Alle vorhandenen IPsec-Konfigurationen müssen entfernt und IPsec muss deaktiviert werden, bevor mit dem Zurücksetzen fortgefahren werden kann. Das Zurücksetzen von ONTAP ist blockiert, wenn IPsec aktiviert ist, selbst wenn keine Benutzerrichtlinien konfiguriert wurden.

ONTAP 9.11.1

Prüfung der ARP-Lizenzierung vor dem Revert von ONTAP 9.11.1

Wenn Sie Autonomous Ransomware Protection (ARP) konfiguriert haben und von ONTAP 9.11.1 auf ONTAP 9.10.1 zurückkehren, kann es zu Warnmeldungen und einer eingeschränkten ARP-Funktionalität kommen.

In ONTAP 9.11.1 wurde die Anti-ransomware-Lizenz anstelle der Multi-Tenant Key Management (MTKM) Lizenz eingeführt. Wenn Ihr System über die Anti_ransomware-Lizenz, aber nicht über die MT_EK_MGMT-Lizenz verfügt, erscheint beim Zurücksetzen eine Warnung, dass ARP auf neuen Volumes nach dem Zurücksetzen nicht aktiviert werden kann.

Die Volumes mit bestehendem Schutz funktionieren nach dem Zurücksetzen weiterhin normal, und der ARP-Status kann über die ONTAP CLI angezeigt werden. System Manager kann den ARP-Status ohne die MTKM-Lizenz nicht anzeigen.

Wenn ARP nach der Rückkehr zu ONTAP 9.10.1 weiterhin funktionieren soll, muss die MTKM-Lizenz vor der Rückkehr installiert sein."Informationen zur ARP-Lizenzierung."

ONTAP 9.6

Vorbereitung synchroner SnapMirror Beziehungen für einen ONTAP 9.6 Revert

Vor dem Zurücksetzen von ONTAP 9.6 auf ONTAP 9.5 sind die Überlegungen zu SnapMirror synchronen Beziehungen zu beachten.

Vor dem Zurücksetzen sind die folgenden Schritte erforderlich, wenn SnapMirror synchron Beziehungen bestehen:

- Es müssen alle SnapMirror synchronen Beziehungen gelöscht werden, in denen das Quellvolume Daten über NFSv4 oder SMB bereitstellt.

  ONTAP 9.5 unterstützt NFSv4 und SMB nicht.

- Alle SnapMirror synchronen Beziehungen in einer Mirror-Mirror-Kaskadenbereitstellung müssen gelöscht werden.

  Eine Spiegel Spiegel Kaskadenbereitstellung wird für SnapMirror synchron Beziehungen in ONTAP 9.5 nicht unterstützt.

- Wenn die gemeinsamen Snapshots in ONTAP 9.5 während des Rücksetzens nicht verfügbar sind, muss die SnapMirror synchron Beziehung nach dem Rücksetzen initialisiert werden.

  Nach zwei Stunden nach dem Upgrade auf ONTAP 9.6 werden die gemeinsamen Snapshots von ONTAP 9.5 automatisch durch die gemeinsamen Snapshots in ONTAP 9.6 ersetzt. Daher kann die SnapMirror synchron Beziehung nach dem Zurücksetzen nicht erneut synchronisiert werden, wenn die gemeinsamen Snapshots von ONTAP 9.5 nicht verfügbar sind.

Das ONTAP Software-Image herunterladen und installieren

Bevor Sie Ihre aktuelle ONTAP Software zurücksetzen, muss die Zielsoftwareversion von der NetApp Support-Website heruntergeladen und anschließend installiert werden.

Das ONTAP Software-Image herunterladen

Software-Images sind spezifisch für Plattformmodelle. Das korrekte Image für Ihren Cluster muss bezogen werden. Software-Images, Firmware-Versionsinformationen und die neueste Firmware für Ihr Plattformmodell sind auf der NetApp Support Site verfügbar. Software-Images enthalten die neueste Version der System-Firmware, die zum Zeitpunkt der Veröffentlichung einer bestimmten Version von ONTAP verfügbar war.

> Wenn Sie ein System mit NetApp Volume Encryption von ONTAP 9.5 oder höher zurücksetzen, muss das ONTAP Software-Image für nicht eingeschränkte Länder heruntergeladen werden, das NetApp Volume Encryption enthält. Wird das ONTAP Software-Image für eingeschränkte Länder verwendet, um ein System mit NetApp Volume Encryption zurückzusetzen, führt dies zu einem Systemabsturz und der Zugriff auf die Volumes geht verloren.

Schritte

1. Die gewünschte ONTAP Software befindet sich im "Software-Downloads" Bereich der NetApp Support Site.
2. Das Software-Image (zum Beispiel `97_q_image.tgz`) von der NetApp Support Site kopieren

   Sie können das Bild in das Verzeichnis auf dem HTTP-Server oder FTP-Server kopieren, von dem das Bild bereitgestellt wird, oder in einen lokalen Ordner.

Das ONTAP Software-Image installieren

Nachdem das gewünschte ONTAP Software-Image von der NetApp Support-Website heruntergeladen wurde, erfolgt die Installation auf den Cluster-Nodes.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

   Die erweiterte Eingabeaufforderung (`*>`) erscheint.

2. Geben Sie `y` ein, um fortzufahren, wenn Sie dazu aufgefordert werden.
3. Das Software-Image installieren:
   - Für Standardkonfigurationen oder eine Zwei-Node MetroCluster Konfiguration ist folgender Befehl einzugeben:

     ```
     system node image update -node * -package
     <http://example.com/downloads/image.tgz> -replace-package true
     -replace {image1|image2} -background true -setdefault true
     ```

     Dieser Befehl lädt das Software-Image herunter und installiert es gleichzeitig auf allen Knoten. Um das Image auf jedem Knoten einzeln herunterzuladen und zu installieren, darf der `-background` Parameter nicht angegeben werden. Dieser Befehl verwendet außerdem eine erweiterte Abfrage, um das Ziel-Software-Image, das als alternatives Image installiert ist, als Standard-Image für den Knoten festzulegen.

◦ Für eine Vier-Node- oder Acht-Node-MetroCluster Konfiguration ist auf beiden Clustern folgender Befehl einzugeben:

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault false
```

Dieser Befehl lädt das Software-Image herunter und installiert es gleichzeitig auf allen Knoten. Um das Image auf jedem Knoten einzeln herunterzuladen und zu installieren, darf der `-background` Parameter nicht angegeben werden. Dieser Befehl verwendet außerdem eine erweiterte Abfrage, um das Ziel-Software-Image zu ändern, das als alternatives Image auf jedem Knoten installiert wird.

4. Geben Sie `y` ein, um fortzufahren, wenn Sie dazu aufgefordert werden.
5. Es sollte sichergestellt sein, dass das Software-Image auf jedem Node heruntergeladen und installiert ist:

```
system node image show-update-progress -node *
```

Dieser Befehl zeigt den aktuellen Status des Software-Image-Downloads und der Installation an. Dieser Befehl sollte weiterhin ausgeführt werden, bis alle Knoten einen **Ausführungsstatus** von „Beendet“ und einen **Exit-Status** von „Erfolgreich“ melden.

Der Befehl zum Aktualisieren des Systemknoten-Images kann fehlschlagen und Fehler- oder Warnmeldungen anzeigen. Nach Behebung aller Fehler oder Warnungen ist eine erneute Ausführung des Befehls möglich.

Dieses Beispiel zeigt einen Zwei-Node-Cluster, in dem das Software-Image erfolgreich auf beiden Knoten heruntergeladen und installiert wurde:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Verwandte Informationen

- "Aktualisierung des System-Node-Images"

Ein ONTAP Cluster zurücksetzen

Das Zurücksetzen eines ONTAP Clusters ist mit Unterbrechungen verbunden. Der Cluster muss für die Dauer des Zurücksetzens offline genommen werden. Ein produktiver Cluster sollte nicht ohne Unterstützung des technischen Supports zurückgesetzt werden.

Um einen neuen oder Test-Cluster zurückzusetzen, müssen Storage-Failover und Daten-LIFs deaktiviert und die Voraussetzungen für die Rücksetzung erfüllt werden; anschließend sind die Cluster- und Dateisystemkonfiguration auf jedem Node im Cluster zurückzusetzen.

Bevor Sie beginnen.

- Sie sollten die "Vorabüberprüfungen vor dem Zurücksetzen" abgeschlossen haben.
- Sie sollten die erforderlichen "Vorabprüfungen für Ihre spezifische ONTAP Version" abgeschlossen haben.
- Sie sollten "das Ziel-ONTAP Software-Image heruntergeladen und installiert" haben.

Schritt 1: Cluster für die Rücksetzung vorbereiten

Bevor Sie einen Ihrer Clusterknoten zurücksetzen, sollte überprüft werden, ob Ihr Ziel-ONTAP-Image installiert ist, und alle Daten-LIFs im Cluster sollten deaktiviert werden.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

   y eingeben, wenn zur Fortsetzung aufgefordert wird.

2. Es sollte überprüft werden, ob die Ziel ONTAP Software installiert ist:

   ```
   system image show
   ```

   Das folgende Beispiel zeigt, dass Version 9.13.1 als alternatives Image auf beiden Knoten installiert ist:

   ```
   cluster1::*> system image show
                    Is      Is                    Install
   Node     Image   Default Current Version    Date
   -------- ------- ------- ------- --------   -------------------
   node0
            image1  true    true    9.14.1      MM/DD/YYYY TIME
            image2  false   false   9.13.1      MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1      MM/DD/YYYY TIME
            image2  false   false   9.13.1      MM/DD/YYYY TIME
   ```

```
4 entries were displayed.
```

3. Alle Daten-LIFs im Cluster deaktivieren:

```
network interface modify {-role data} -status-admin down
```

4. Feststellen, ob zwischen Clustern FlexCache Beziehungen bestehen:

```
flexcache origin show-caches -relationship-type inter-cluster
```

5. Falls Intercluster-Flexcaches vorhanden sind, werden die Data-LIFs auf dem Cache-Cluster deaktiviert:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -status
-admin down
```

Schritt 2: Cluster-Nodes zurücksetzen

Um Ihren Cluster zurückzusetzen, muss zuerst der erste Node eines HA-Paares und anschließend der Partner-Node zurückgesetzt werden. Dieser Vorgang wird für jedes HA-Paar im Cluster wiederholt, bis alle Nodes zurückgesetzt sind. Wenn eine MetroCluster Konfiguration vorliegt, sind diese Schritte für beide Cluster in der Konfiguration zu wiederholen.

4 oder mehr Knoten

Schritte

1. Melden Sie sich bei dem Node an, den Sie zurücksetzen möchten.

   Um einen Node zurückzusetzen, muss eine Anmeldung am Cluster über die Node-Management-LIF des Nodes erfolgen.

2. Speicherausfallsicherung für die Knoten im HA-Paar deaktivieren:

   ```
   storage failover modify -node <nodename> -enabled false
   ```

   Sie müssen das Speicher-Failover nur einmal für das HA-Paar deaktivieren. Wenn das Speicher-Failover für einen Knoten deaktiviert wird, ist es auch auf dem Partnerknoten deaktiviert.

3. Das Ziel-ONTAP-Software-Image des Knotens wird als Standard-Image festgelegt:

   ```
   system image modify -node <nodename> -image <target_image>
   -isdefault true
   ```

4. Es sollte überprüft werden, dass das Ziel ONTAP Software Image als Standard-Image für den Knoten festgelegt ist, der zurückgesetzt wird:

```
system image show
```

Das folgende Beispiel zeigt, dass Version 9.13.1 als Standardimage auf node0 festgelegt ist:

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   false   true    9.14.1       MM/DD/YYYY TIME
         image2   true    false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

5. Es sollte überprüft werden, ob der Knoten für die Rücksetzung bereit ist:

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

Der `check-only`Parameter kennzeichnet alle Vorbedingungen, die vor dem Zurücksetzen erfüllt sein müssen, wie das Deaktivieren der Snapshot-Richtlinie oder das Löschen von Snapshots, die nach dem Upgrade auf die neuere Version von ONTAP erstellt wurden.

Die `-version` Option bezieht sich auf die ONTAP Version, auf die Sie zurücksetzen. Wenn Sie beispielsweise von 9.14.1 auf 9.13.1 zurücksetzen, ist der korrekte Wert der `-version` Option 9.13.1.

6. Die Clusterkonfiguration des Knotens zurücksetzen:

```
system node revert-to -node <nodename> -version 9.x
```

Die Clusterkonfiguration wird zurückgesetzt, und anschließend erfolgt die Abmeldung aus der Clustershell.

7. Warten Sie auf die Anmeldeaufforderung; dann **Nein** eingeben, wenn gefragt wird, ob eine Anmeldung an der Systemshell erfolgen soll.

Es kann bis zu 30 Minuten oder länger dauern, bis die Anmeldeaufforderung erscheint.

8. Anmeldung an der Clustershell mit admin.
9. Zum Nodeshell wechseln:

```
run -node <nodename>
```

Nach erneuter Anmeldung an der Clustershell kann es einige Minuten dauern, bis der nodeshell-Befehl akzeptiert wird. Falls der Befehl fehlschlägt, empfiehlt es sich, einige Minuten zu warten und es dann erneut zu versuchen.

10. Die Dateisystemkonfiguration des Knotens wird zurückgesetzt:

```
revert_to 9.x
```

Dieser Befehl prüft, ob die Dateisystemkonfiguration des Knotens zur Wiederherstellung bereit ist, und stellt sie anschließend wieder her. Wenn Vorbedingungen festgestellt werden, müssen diese behoben werden und anschließend der `revert_to` Befehl erneut ausgeführt werden.



Die Überwachung des Revert-Prozesses über eine Systemkonsole liefert detailliertere Informationen als in NodeShell.

Wenn AUTOBOOT auf „true“ gesetzt ist, startet der Knoten nach Abschluss des Befehls in ONTAP neu.

Wenn AUTOBOOT auf „false“ gesetzt ist, wird nach Abschluss des Befehls die LOADER-Eingabeaufforderung angezeigt. `yes` eingeben, um die Änderung rückgängig zu machen; anschließend `boot_ontap` verwenden, um den Knoten manuell neu zu starten.

11. Nachdem der Knoten neu gestartet wurde, ist zu bestätigen, dass die neue Software ausgeführt wird:

```
system node image show
```

Im folgenden Beispiel ist image1 die neue ONTAP Version und als aktuelle Version auf node0 festgelegt:

```
cluster1::*> system node image show
                 Is      Is                  Install
Node     Image   Default Current Version     Date
-------- ------- ------- ------- --------    -------------------
node0
         image1  true    true    X.X.X        MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X       MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

12. Es sollte überprüft werden, ob der Wiederherstellungsstatus für den Knoten abgeschlossen ist:

```
system node upgrade-revert show -node <nodename>
```

Der Status sollte als „abgeschlossen“, „nicht erforderlich“ oder „es wurden keine Tabelleneinträge zurückgegeben“ aufgeführt sein.

13. Diese Schritte sind am anderen Knoten des HA-Paares zu wiederholen, anschließend für jedes weitere HA-Paar.

    Wenn Sie eine MetroCluster Konfiguration haben, müssen diese Schritte auf beiden Clustern in der Konfiguration wiederholt werden.

14. Nachdem alle Knoten zurückgesetzt wurden, wird die Hochverfügbarkeit für den Cluster wieder aktiviert:

```
storage failover modify -node* -enabled true
```

2-Node Cluster

1. Melden Sie sich bei dem Node an, den Sie zurücksetzen möchten.

   Um einen Node zurückzusetzen, muss eine Anmeldung am Cluster über die Node-Management-LIF des Nodes erfolgen.

2. Cluster-High Availability (HA) deaktivieren:

```
cluster ha modify -configured false
```

3. Storage-Failover deaktivieren:

```
storage failover modify -node <nodename> -enabled false
```

   Sie müssen das Speicher-Failover nur einmal für das HA-Paar deaktivieren. Wenn das Speicher-Failover für einen Knoten deaktiviert wird, ist es auch auf dem Partnerknoten deaktiviert.

4. Das Ziel-ONTAP-Software-Image des Knotens wird als Standard-Image festgelegt:

```
system image modify -node <nodename> -image <target_image>
-isdefault true
```

5. Es sollte überprüft werden, dass das Ziel ONTAP Software Image als Standard-Image für den Knoten festgelegt ist, der zurückgesetzt wird:

```
system image show
```

   Das folgende Beispiel zeigt, dass Version 9.13.1 als Standardimage auf node0 festgelegt ist:

```
cluster1::*> system image show
                Is      Is                  Install
```

```
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  false   true    9.14.1      MM/DD/YYYY TIME
         image2  true    false   9.13.1      MM/DD/YYYY TIME
node1
         image1  true    true    9.14.1      MM/DD/YYYY TIME
         image2  false   false   9.13.1      MM/DD/YYYY TIME
4 entries were displayed.
```

6. Es wird geprüft, ob der Knoten aktuell Epsilon enthält:

```
cluster show -node <nodename>
```

Das folgende Beispiel zeigt, dass der Knoten Epsilon enthält:

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

a. Wenn der Knoten Epsilon enthält, wird Epsilon auf dem Knoten als falsch markiert, sodass Epsilon an den Partnerknoten übertragen werden kann:

```
cluster modify -node <nodename> -epsilon false
```

b. Epsilon wird auf den Partnerknoten übertragen, indem Epsilon auf dem Partnerknoten als „true“ markiert wird:

```
cluster modify -node <node_partner_name> -epsilon true
```

7. Es sollte überprüft werden, ob der Knoten für die Rücksetzung bereit ist:

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

Der `check-only`Parameter kennzeichnet alle Bedingungen, die vor dem Zurücksetzen erfüllt sein müssen, wie das Deaktivieren der Snapshot-Richtlinie oder das Löschen von Snapshots, die nach dem Upgrade auf die neuere Version von ONTAP erstellt wurden.

Die `-version` Option bezieht sich auf die ONTAP Version, auf die Sie zurücksetzen. Nur die ersten beiden Werte der ONTAP Version sind erforderlich. Wenn Sie beispielsweise von 9.14.1 auf 9.13.1 zurücksetzen, ist der korrekte Wert der `-version` Option 9.13.

Die Clusterkonfiguration wird zurückgesetzt, und anschließend erfolgt die Abmeldung aus der Clustershell.

8. Die Clusterkonfiguration des Knotens zurücksetzen:

```
system node revert-to -node <nodename> -version 9.x
```

9. Warten Sie auf die Anmeldeaufforderung, dann `No` eingeben, wenn Sie gefragt werden, ob Sie sich in der Systemshell anmelden möchten.

   Es kann bis zu 30 Minuten oder länger dauern, bis die Anmeldeaufforderung erscheint.

10. Anmeldung an der Clustershell mit admin.
11. Zum Nodeshell wechseln:

```
run -node <nodename>
```

   Nach erneuter Anmeldung an der Clustershell kann es einige Minuten dauern, bis der nodeshell-Befehl akzeptiert wird. Falls der Befehl fehlschlägt, empfiehlt es sich, einige Minuten zu warten und es dann erneut zu versuchen.

12. Die Dateisystemkonfiguration des Knotens wird zurückgesetzt:

```
revert_to 9.x
```

   Dieser Befehl prüft, ob die Dateisystemkonfiguration des Knotens zur Wiederherstellung bereit ist, und stellt sie anschließend wieder her. Wenn Vorbedingungen festgestellt werden, müssen diese behoben werden und anschließend der `revert_to` Befehl erneut ausgeführt werden.

   > Die Überwachung des Revert-Prozesses über eine Systemkonsole liefert detailliertere Informationen als in NodeShell.

   Wenn AUTOBOOT auf „true“ gesetzt ist, startet der Knoten nach Abschluss des Befehls in ONTAP neu.

   Wenn AUTOBOOT auf „false“ gesetzt ist, wird nach Abschluss des Befehls die LOADER-Eingabeaufforderung angezeigt. `yes` eingeben, um die Änderung rückgängig zu machen; anschließend `boot_ontap` verwenden, um den Knoten manuell neu zu starten.

13. Nachdem der Knoten neu gestartet wurde, ist zu bestätigen, dass die neue Software ausgeführt wird:

```
system node image show
```

Im folgenden Beispiel ist image1 die neue ONTAP Version und als aktuelle Version auf node0 festgelegt:

```
cluster1::*> system node image show
                 Is      Is                  Install
Node     Image   Default Current Version     Date
-------- ------- ------- ------- --------    -------------------
node0
         image1  true    true    X.X.X        MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X       MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

14. Es wird geprüft, ob der Rücksetzungsstatus für den Knoten abgeschlossen ist:

```
system node upgrade-revert show -node <nodename>
```

Der Status sollte als „abgeschlossen“, „nicht erforderlich“ oder „es wurden keine Tabelleneinträge zurückgegeben“ aufgeführt sein.

15. Diese Schritte sind am anderen Knoten des HA-Paares ebenfalls auszuführen.
16. Nachdem beide Knoten zurückgesetzt wurden, wird HA für den Cluster wieder aktiviert:

```
cluster ha modify -configured true
```

Durch die erneute Aktivierung von Cluster HA kann die `storage failover auto-giveback` Einstellung wieder auf „true“ zurückgesetzt werden.

17. Speicherausfallsicherung auf beiden Knoten wieder aktivieren:

```
storage failover modify -node <nodename> -enabled true
```

18. Die `storage failover auto-giveback` Einstellung auf beiden Knoten überprüfen:

```
storage failover show -node <nodename>
```

Falls für Ihre Umgebung eine andere Einstellung erforderlich ist, kann dies mit dem `storage failover modify -node <nodename> -auto-giveback <true|false>` Befehl angepasst werden.

Verwandte Informationen

- "storage failover modify"
- "NetApp Knowledge Base: Warum ist die automatische Rückgabe nach der erneuten Aktivierung der Speicherausfallsicherungseinstellung aktiviert?"

Was nach einer ONTAP Rücksetzung zu tun ist

Cluster- und Speicherzustand nach einer ONTAP Rücksetzung überprüfen

Nach dem Zurücksetzen eines ONTAP Clusters sollte überprüft werden, ob die Knoten fehlerfrei funktionieren und zur Teilnahme am Cluster berechtigt sind sowie ob der Cluster ein Quorum aufweist. Auch der Status der Festplatten, Aggregate und Volumes sollte überprüft werden.

Clusterzustand überprüfen

Schritte

1. Es sollte sichergestellt werden, dass die Knoten im Cluster online sind und zur Teilnahme am Cluster berechtigt sind:

   ```
   cluster show
   ```

   In diesem Beispiel ist der Cluster fehlerfrei und alle Knoten sind zur Teilnahme am Cluster berechtigt.

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   Wenn ein Knoten fehlerhaft oder nicht geeignet ist, sollten die EMS-Protokolle auf Fehler überprüft und Korrekturmaßnahme ergriffen werden.

2. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

   Geben Sie `y` ein, um fortzufahren.

3. Die Konfigurationsdetails für jeden RDB-Prozess werden überprüft.

   - Die relationalen Datenbank-Epochen und die Datenbank-Epochen sollten für jeden Knoten übereinstimmen.
   - Das primäre Quorum pro Ring sollte für alle Knoten gleich sein.

     Beachten Sie, dass jeder Ring ein anderes Quorum-Primary haben kann.

Um diesen RDB-Prozess anzuzeigen…	Geben Sie diesen Befehl ein…
Verwaltungsanwendung	`cluster ring show -unitname mgmt`
Volume-Standortdatenbank	`cluster ring show -unitname vldb`
Manager für virtuelle Schnittstellen	`cluster ring show -unitname vifmgr`
SAN Management-Daemon	`cluster ring show -unitname bcomd`

Dieses Beispiel zeigt den Volume Location Database-Prozess:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

5. Wenn Sie in einer SAN-Umgebung arbeiten, überprüfen Sie, ob sich jeder Knoten in einem SAN-Quorum befindet:

```
event log show  -severity informational -message-name scsiblade.*
```

Die aktuellste scsi-blade-Ereignismeldung für jeden Knoten sollte anzeigen, dass sich das scsi-blade im Quorum befindet.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
```

```
scsi-blade ...
MM/DD/YYYY TIME   node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Verwandte Informationen

"Systemadministration"

Speicherzustand überprüfen

Nach dem Zurücksetzen oder Downgrade eines Clusters empfiehlt sich eine Überprüfung des Status der Festplatten, Aggregate und Volumes.

Schritte

1. Festplattenstatus überprüfen:

Zur Überprüfung, ob…	Folgendes ist zu tun…
Defekte Festplatten	a. Alle defekten Datenträger anzeigen: `storage disk show -state broken` b. Beschädigte Datenträger entfernen oder ersetzen.
Festplatten, die sich in Wartung oder Wiederherstellung befinden	a. Alle Datenträger im Wartungs-, Ausstehend- oder Wiederherstellungsstatus anzeigen: `storage disk show -state maintenance`
pending	reconstructing ---- .. Es sollte abgewartet werden, bis die Wartungs- oder Wiederherstellungsarbeiten abgeschlossen sind, bevor fortgefahren wird.

2. Es sollte überprüft werden, ob alle Speicheraggregate online sind, indem der Status des physischen und logischen Speichers, einschließlich der Speicheraggregate, angezeigt wird:

```
storage aggregate show -state !online
```

Dieser Befehl zeigt die Aggregate an, die nicht online sind. Alle Aggregate müssen vor und nach einer größeren Aktualisierung oder Rücksetzung online sein.

```
cluster1::> storage aggregate show -state !online
```

```
There are no entries matching your query.
```

3. Es kann überprüft werden, ob alle Volumes online sind, indem alle Volumes angezeigt werden, die *nicht* online sind:

   ```
   volume show -state !online
   ```

   Alle Volumes müssen vor und nach einer größeren Aktualisierung oder Rücksetzung online sein.

   ```
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Es wird überprüft, ob keine inkonsistenten Volumes vorhanden sind:

   ```
   volume show -is-inconsistent true
   ```

   Siehe die "NetApp Knowledge Base: Volumen zeigt WAFL als inkonsistent" Hinweise zum Umgang mit den uneinheitlichen Volumen.

Clientzugriff (SMB und NFS) überprüfen

Für die konfigurierten Protokolle sollte der Zugriff von SMB- und NFS-Clients getestet werden, um zu überprüfen, ob der Cluster erreichbar ist.

Verwandte Informationen

- "Festplatten- und Aggregatverwaltung"
- "Speicherdatenträger anzeigen"

Aktivierung der automatischen Umschaltung nach einer ONTAP MetroCluster Rücksetzung

Nach dem Zurücksetzen einer ONTAP MetroCluster Konfiguration muss die automatische ungeplante Umschaltung aktiviert werden, damit die MetroCluster Konfiguration voll funktionsfähig ist.

Schritte

1. Automatische ungeplante Umschaltung aktivieren:

   ```
   metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
   disaster
   ```

2. Die MetroCluster Konfiguration validieren:

   ```
   metrocluster check run
   ```

LIFs nach einer ONTAP Umstellung auf die Home-Ports aktivieren und zurücksetzen

Während eines Neustarts wurden möglicherweise einige LIFs auf ihre zugewiesenen Failover-Ports migriert. Nach dem Zurücksetzen eines ONTAP Clusters müssen alle LIFs, die sich nicht auf ihren Home-Ports befinden, aktiviert und zurückgesetzt werden.

Der Befehl `network interface revert` setzt eine LIF, die sich aktuell nicht an ihrem Home-Port befindet, wieder auf ihren Home-Port zurück, sofern dieser funktionsfähig ist. Der Home-Port einer LIF wird bei deren Erstellung festgelegt; der Home-Port einer LIF kann mit dem Befehl `network interface show` ermittelt werden.

Schritte

1. Status aller LIFs anzeigen:

```
network interface show
```

Dieses Beispiel zeigt den Status aller LIFs für eine Storage Virtual Machine (SVM).

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

Wenn LIFs mit dem Status Admin „down“ oder mit dem Status „Is home“ „false“ angezeigt werden, erfolgt der nächste Schritt.

2. Die Daten-LIFs aktivieren:

```
network interface modify {-role data} -status-admin up
```

3. LIFs auf ihre Home-Ports zurückführen:

```
network interface revert *
```

4. Es sollte sichergestellt werden, dass sich alle LIFs in ihren Home-Ports befinden:

```
network interface show
```

Dieses Beispiel zeigt, dass sich alle LIFs für SVM vs0 auf ihren Home-Ports befinden.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0          e0e
true
            data002      up/up    192.0.2.121/24     node0          e0f
true
            data003      up/up    192.0.2.122/24     node0          e2a
true
            data004      up/up    192.0.2.123/24     node0          e2b
true
            data005      up/up    192.0.2.124/24     node1          e0e
true
            data006      up/up    192.0.2.125/24     node1          e0f
true
            data007      up/up    192.0.2.126/24     node1          e2a
true
            data008      up/up    192.0.2.127/24     node1          e2b
true
8 entries were displayed.
```

Verwandte Informationen

- "Netzwerkschnittstelle"

Snapshot-Richtlinien nach einem ONTAP Revert aktivieren

Nach der Rückkehr zu einer früheren Version von ONTAP müssen Snapshot-Richtlinien aktiviert werden, damit Snapshots wieder erstellt werden.

Sie reaktivieren die Snapshot-Zeitpläne, die Sie deaktiviert hatten, bevor Sie auf eine frühere Version von ONTAP zurückgekehrt sind.

Schritte

1. Snapshot-Richtlinien für alle Daten-SVMs aktivieren:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. Für jeden Node wird die Snapshot-Richtlinie des Root-Volumes aktiviert:

```
run -node <node_name> vol options <volume_name> nosnap off
```

IPv6-Firewall-Einträge nach einer ONTAP Rücksetzung überprüfen

Bei einem Downgrade von einer beliebigen Version von ONTAP 9 können die Standard-IPv6-Firewall-Einträge für einige Dienste in den Firewall-Richtlinien fehlen. Es ist zu überprüfen, ob die erforderlichen Firewall-Einträge in Ihrem System wiederhergestellt wurden.

Schritte

1. Es sollte überprüft werden, ob alle Firewall-Richtlinien korrekt sind, indem sie mit den Standardrichtlinien verglichen werden:

```
system services firewall policy show
```

Das folgende Beispiel zeigt die Standardrichtlinien:

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
```

```
                    rsh         allow  0.0.0.0/0
                    snmp        allow  0.0.0.0/0
                    ssh         allow  0.0.0.0/0
                    telnet      allow  0.0.0.0/0
data
                    dns         allow  0.0.0.0/0, ::/0
                    http        deny   0.0.0.0/0, ::/0
                    https       deny   0.0.0.0/0, ::/0
                    ndmp        allow  0.0.0.0/0, ::/0
                    ntp         deny   0.0.0.0/0, ::/0
                    rsh         deny   0.0.0.0/0, ::/0
.
.
.
```

2. Fehlende Standard-IPv6-Firewall-Einträge können manuell hinzugefügt werden, indem eine neue Firewall-Richtlinie erstellt wird:

```
system services firewall policy create -policy <policy_name> -service
ssh -action allow -ip-list <ip_list>
```

3. Die neue Richtlinie wird auf den LIF angewendet, um den Zugriff auf einen Netzwerkservice zu ermöglichen:

```
network interface modify -vserve <svm_name> -lif <lif_name> -firewall
-policy <policy_name>
```

Überprüfung der Benutzerkonten des Serviceprozessors nach der Rückkehr zu ONTAP 9.8

In ONTAP 9.9.1 und höher wird der `-role` Parameter für Benutzerkonten in `admin` geändert. Wenn Benutzerkonten in ONTAP 9.8 oder früher erstellt, auf ONTAP 9.9.1 oder höher aktualisiert und anschließend wieder auf ONTAP 9.8 zurückgesetzt wurden, wird der `-role` Parameter auf seinen ursprünglichen Wert zurückgesetzt. Es sollte überprüft werden, ob die geänderten Werte zulässig sind.

Während des Zurücksetzens wird, falls die Rolle für einen SP-Benutzer gelöscht wurde, die EMS-Meldung "rbac.spuser.role.notfound" protokolliert.

Weitere Informationen finden sich unter "Konten, die auf den SP zugreifen können".

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.