



# **Maßnahmen nach einem ONTAP Upgrade**

## **ONTAP 9**

NetApp  
April 24, 2024

This PDF was generated from [https://docs.netapp.com/de-de/ontap/upgrade/task\\_what\\_to\\_do\\_after\\_upgrade.html](https://docs.netapp.com/de-de/ontap/upgrade/task_what_to_do_after_upgrade.html) on April 24, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- Maßnahmen nach einem ONTAP Upgrade ..... 1
  - Maßnahmen nach einem ONTAP Upgrade ..... 1
  - Überprüfen Sie den Cluster nach dem ONTAP Upgrade ..... 1
  - Überprüfen Sie nach dem ONTAP Upgrade, ob alle LIFS an den Home Ports sind ..... 4
  - Spezielle Konfigurationen ..... 5
  - Aktualisieren Sie das Disk Qualification Package ..... 15

# Maßnahmen nach einem ONTAP Upgrade

## Maßnahmen nach einem ONTAP Upgrade

Nachdem Sie das Upgrade von ONTAP durchgeführt haben, sollten Sie mehrere Aufgaben durchführen, um die Cluster-Bereitschaft zu überprüfen.

1. "Verifizieren Sie Ihr Cluster".

Nach dem Upgrade von ONTAP sollten Sie Ihre Cluster-Version, den Cluster-Zustand und den Storage-Zustand überprüfen. Bei Nutzung einer MetroCluster FC-Konfiguration müssen Sie auch sicherstellen, dass das Cluster für die automatische ungeplante Umschaltung aktiviert ist.

2. "Vergewissern Sie sich, dass alle LIFs an den Home Ports angeschlossen sind".

Während eines Neubootens wurden möglicherweise einige LIFs zu ihren zugewiesenen Failover-Ports migriert. Nach dem Upgrade eines Clusters müssen Sie alle LIFs aktivieren bzw. zurücksetzen, die sich nicht auf den Home-Ports befinden.

3. Verifizieren "Besondere Überlegungen" Spezifisch für Ihr Cluster.

Wenn bestimmte Konfigurationen im Cluster vorhanden sind, müssen Sie nach dem Upgrade möglicherweise weitere Schritte ausführen.

4. "Aktualisieren des Disk Qualification Package (DQP)".

Das DQP wird im Rahmen eines ONTAP-Upgrades nicht aktualisiert.

## Überprüfen Sie den Cluster nach dem ONTAP Upgrade

Überprüfen Sie nach dem Upgrade von ONTAP die Clusterversion, den Clusterstatus und den Storage-Zustand. Überprüfen Sie bei MetroCluster FC-Konfigurationen auch, ob das Cluster für die automatische ungeplante Umschaltung aktiviert ist.

### Überprüfen der Cluster-Version

Nachdem alle HA-Paare aktualisiert wurden, müssen Sie mit dem Befehl `version` überprüfen, ob auf allen Nodes das Ziel-Release ausgeführt wird.

Die Cluster-Version ist die niedrigste Version von ONTAP, die auf einem beliebigen Node im Cluster ausgeführt wird. Wenn die Cluster-Version nicht die ONTAP-Zielversion ist, können Sie ein Cluster-Upgrade durchführen.

1. Vergewissern Sie sich, dass die Cluster-Version die ONTAP-Zielversion ist:

```
version
```

2. Wenn die Cluster-Version nicht das Ziel-ONTAP-Release ist, sollten Sie den Upgrade-Status aller Nodes überprüfen:

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

## Überprüfen des Cluster-Systemzustands

Nach dem Upgrade eines Clusters sollten Sie überprüfen, ob die Nodes ordnungsgemäß sind und berechtigt sind, am Cluster teilzunehmen, und dass sich das Cluster in einem Quorum befindet.

1. Vergewissern Sie sich, dass die Nodes im Cluster online sind und am Cluster teilnehmen können:

```
cluster show
```

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0               true   true
node1               true   true
```

Wenn ein Knoten fehlerhaft oder nicht geeignet ist, überprüfen Sie die EMS-Protokolle auf Fehler und ergreifen Sie Korrekturmaßnahmen.

2. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

3. Überprüfen Sie die Konfigurationsdetails für jeden RDB-Prozess.

- Die Epochen der relationalen Datenbank und Datenbank-Epochen sollten für jeden Node übereinstimmen.
- Der Quorum-Master pro Ring sollte für alle Knoten gleich sein.

Beachten Sie, dass für jeden Ring möglicherweise ein anderer Quorum-Master vorhanden ist.

So zeigen Sie diesen RDB-Prozess an:	Diesen Befehl eingeben...
Managementapplikation	<code>cluster ring show -unitname mgmt</code>
Volume-Standortdatenbank	<code>cluster ring show -unitname vlodb</code>
Virtual Interface Manager	<code>cluster ring show -unitname vifmgr</code>
SAN Management-Daemon	<code>cluster ring show -unitname bcomd</code>

Dieses Beispiel zeigt den Datenbankprozess für den Speicherort des Volumes:

```
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. Wenn Sie in einer SAN-Umgebung arbeiten, vergewissern Sie sich, dass 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
cluster1-01	cluster1-01	in-quorum	true
operational	cluster1-02	in-quorum	true
operational			

2 entries were displayed.

## Verwandte Informationen

["Systemadministration"](#)

## Überprüfen, ob die automatische ungeplante Umschaltung aktiviert ist (nur MetroCluster FC-Konfigurationen)

Wenn sich Ihr Cluster in einer MetroCluster FC-Konfiguration befindet, sollten Sie nach dem Upgrade von ONTAP überprüfen, ob die automatische ungeplante Umschaltung aktiviert ist.

Wenn Sie eine MetroCluster IP-Konfiguration verwenden, überspringen Sie diesen Vorgang.

### Schritte

1. Prüfen, ob die automatische ungeplante Umschaltung aktiviert ist:

```
metrocluster show
```

Wenn die automatische ungeplante Umschaltung aktiviert ist, wird die folgende Anweisung in der

Befehlsausgabe angezeigt:

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

2. Wenn die Anweisung nicht angezeigt wird, aktivieren Sie eine automatische ungeplante Umschaltung:

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

3. Vergewissern Sie sich, dass eine automatische ungeplante Umschaltung aktiviert wurde:

```
metrocluster show
```

### Verwandte Informationen

["Festplatten- und Aggregatmanagement"](#)

## Überprüfen Sie nach dem ONTAP Upgrade, ob alle LIFs an den Home Ports sind

Während des Neubootens im Rahmen des ONTAP Upgrade-Prozesses können einige LIFs von ihren Home Ports in die ihnen zugewiesenen Failover-Ports migriert werden. Nach einem Upgrade müssen Sie alle LIFs, die sich nicht auf ihrem Home-Port befinden, aktivieren und zurücksetzen.

### Schritte

1. Zeigt den Status aller LIFs an:

```
network interface show -fields home-port,curr-port
```

Wenn **Status Admin** auf „Down“ oder **is Home** auf „false“ für alle LIFs gesetzt ist, fahren Sie mit dem nächsten Schritt fort.

2. Aktivieren der Daten-LIFs:

```
network interface modify {-role data} -status-admin up
```

3. Zurücksetzen von LIFs auf ihre Home Ports:

```
network interface revert *
```

4. Vergewissern Sie sich, dass sich alle LIFs in ihren Home-Ports befinden:

```
network interface show
```

Dieses Beispiel zeigt, dass alle LIFs für SVM vs0 sich auf ihren Home-Ports befinden.

```
cluster1::> network interface show -vserver vs0
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is 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.

## Spezielle Konfigurationen

### Besondere Überlegungen nach einem ONTAP Upgrade

Wenn das Cluster mit einer der folgenden Funktionen konfiguriert ist, müssen Sie nach dem Upgrade der ONTAP Software möglicherweise weitere Schritte ausführen.

Fragen Sie sich...	Wenn Ihre Antwort ja lautet, dann tun Sie das...
Habe ich ein Upgrade von ONTAP 9.7 oder früher auf ONTAP 9.8 oder höher durchgeführt?	<a href="#">Überprüfen Sie die Netzwerkkonfiguration</a>  <a href="#">Entfernen Sie den EMS-LIF-Dienst aus den Netzwerkdienstpolicies, die dem EMS-Ziel keine Erreichbarkeit bieten</a>
Befindet sich mein Cluster in einer MetroCluster Konfiguration?	<a href="#">Überprüfen Sie den Netzwerk- und Storage-Status</a>
Habe ich eine SAN-Konfiguration?	<a href="#">Überprüfen Sie Ihre SAN-Konfiguration</a>
Habe ich ein Upgrade von ONTAP 9.3 oder einer früheren Version durchgeführt und verwende ich NetApp-Speicherverschlüsselung?	<a href="#">Neukonfigurieren der KMIP-Serververbindungen</a>
Gibt es Spiegelungen zur Lastverteilung?	<a href="#">Verschiebung von Quell-Volumes mit verschobenen Load-Sharing-Spiegeln</a>
Gibt es Benutzerkonten für Service-Prozessor (SP)-Zugriff, die vor ONTAP 9.9 erstellt wurden?	<a href="#">Überprüfen Sie die Änderungen an Konten, die auf den Service Processor zugreifen können</a>

## Überprüfen Sie Ihre Netzwerkkonfiguration nach einem ONTAP Upgrade von ONTAP 9.7x oder früher

Nach dem Upgrade von ONTAP 9.7x oder einer früheren Version auf ONTAP 9.8 oder höher sollten Sie Ihre Netzwerkkonfiguration überprüfen. Nach dem Upgrade überwacht ONTAP automatisch die Erreichbarkeit von Ebene 2.

### Schritt

1. Überprüfen Sie, ob jeder Port die erwartete Broadcast-Domäne erreicht:

```
network port reachability show -detail
```

Die Befehlsausgabe enthält Ergebnisse zur Wiederherstellung. Verwenden Sie die folgende Entscheidungsstruktur und Tabelle, um die Ergebnisse der Nachachbarkeit (Status der Erreichbarkeit) zu verstehen und zu bestimmen, welche, wenn überhaupt, als Nächstes zu tun.





Erreichbarkeit-Status	Beschreibung
-----------------------	--------------

ok	<p>Der Port verfügt über eine Layer 2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne.</p> <p>Wenn der Status der Erreichbarkeit „ok“ ist, aber es „unerwartete Ports“ gibt, sollten Sie eine oder mehrere Broadcast-Domänen zusammenführen. Weitere Informationen finden Sie unter <a href="#">"Broadcast-Domänen zusammenführen"</a>.</p> <p>Wenn der Status „Erreichbarkeit“ „ok“ lautet, aber „nicht erreichbare Ports“ vorhanden sind, sollten Sie eine oder mehrere Broadcast-Domänen aufteilen. Weitere Informationen finden Sie unter <a href="#">"Teilen von Broadcast-Domänen auf"</a>.</p> <p>Wenn der Status „Erreichbarkeit“ „ok“ lautet und keine unerwarteten oder nicht erreichbaren Ports vorhanden sind, ist die Konfiguration korrekt.</p>
Falsch konfigurierte Erreichbarkeit	<p>Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit seiner zugewiesenen Broadcast-Domäne; der Port besitzt jedoch Layer 2-Erreichbarkeit zu einer anderen Broadcast-Domäne.</p> <p>Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port der Broadcast-Domäne zu, der sie nachzuweisen kann:</p> <pre>network port reachability repair -node -port</pre> <p>Weitere Informationen finden Sie unter <a href="#">"Port-Erreichbarkeit reparieren"</a>.</p>
Keine Erreichbarkeit	<p>Der Port verfügt nicht über eine Ebene 2-Erreichbarkeit für eine vorhandene Broadcast-Domäne.</p> <p>Sie können die Anschlussfähigkeit reparieren. Wenn Sie den folgenden Befehl ausführen, weist das System den Port einer neuen automatisch erstellten Broadcast-Domäne im Standard-IPspace zu:</p> <pre>network port reachability repair -node -port</pre> <p>Weitere Informationen finden Sie unter <a href="#">"Port-Erreichbarkeit reparieren"</a>.</p>
Multi-Domain-Erreichbarkeit	<p>Der Port verfügt über eine Layer-2-Erreichbarkeit für seine zugewiesene Broadcast-Domäne; er verfügt jedoch auch über eine Layer-2-Erreichbarkeit von mindestens einer anderen Broadcast-Domäne.</p> <p>Überprüfen Sie die physische Konnektivität und die Switch-Konfiguration, um festzustellen, ob sie falsch ist oder ob die zugewiesene Broadcast-Domain des Ports mit einer oder mehreren Broadcast-Domänen zusammengeführt werden muss.</p> <p>Weitere Informationen finden Sie unter <a href="#">"Broadcast-Domänen zusammenführen"</a> Oder <a href="#">"Port-Erreichbarkeit reparieren"</a>.</p>
Unbekannt	<p>Wenn der Status „unbekannt“ lautet, warten Sie einige Minuten, und versuchen Sie den Befehl erneut.</p>

Nachdem Sie einen Port repariert haben, müssen Sie die vertriebenen LIFs und VLANs überprüfen und

beheben. Wenn der Port Teil einer Schnittstellengruppe war, müssen Sie auch verstehen, was mit dieser Schnittstellengruppe passiert ist. Weitere Informationen finden Sie unter ["Port-Erreichbarkeit reparieren"](#).

## Entfernen Sie den LIF-Dienst aus den Netzwerkdienstrichtlinien

Wenn Sie EMS-Nachrichten (Event Management System) eingerichtet haben, bevor Sie ein Upgrade von ONTAP 9.7 oder früher auf ONTAP 9.8 oder höher nach dem Upgrade durchführen, werden Ihre EMS-Nachrichten möglicherweise nicht zugestellt.

Während des Upgrades wird Management-ems, der EMS-LIF-Dienst, zu allen bestehenden Service-Richtlinien hinzugefügt. Dadurch können EMS-Nachrichten von einem der LIFs gesendet werden, die mit einer der Service-Richtlinien verknüpft sind. Wenn das ausgewählte LIF nicht auf das Ziel der Ereignisbenachrichtigung zugreifen kann, wird die Meldung nicht ausgegeben.

Um dies zu verhindern, sollten Sie nach dem Upgrade den EMS-LIF-Dienst aus den Netzwerkdienstpolicies entfernen, die keine Erreichbarkeit des Ziels bieten.

### Schritte

1. Identifizieren Sie die LIFs und zugehörigen Netzwerk-Service-Richtlinien, über die EMS-Meldungen gesendet werden können:

```
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. Überprüfen Sie jede LIF auf Verbindung zum EMS-Ziel:

```
network ping -lif lif_name -vserver svm_name -destination  
destination_address
```

Führen Sie dies auf jedem Knoten aus.

## Beispiele

```
cluster-1::> network ping -lif nodel-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. Geben Sie die erweiterte Berechtigungsebene ein:

```
set advanced
```

4. Entfernen Sie für die LIFs, die nicht über diese verfügen, den Management-ems LIF-Service aus den entsprechenden Service-Richtlinien:

```
network interface service-policy remove-service -vserver svm_name
-policy service_policy_name -service management-ems
```

5. Überprüfen Sie, dass die Management-ems LIF jetzt nur mit den LIFs verknüpft ist, die die Erreichbarkeit des EMS-Ziels bieten:

```
network interface show -fields service-policy -services management-ems
```

## Verwandte Links

["LIFs und Service-Richtlinien in ONTAP 9.6 und höher"](#)

## Nach einem ONTAP Upgrade überprüfen Sie den Netzwerk- und Storage-Status für MetroCluster Konfigurationen

Nachdem Sie ein ONTAP Cluster in einer MetroCluster Konfiguration aktualisiert haben, sollten Sie den Status der LIFs, Aggregate und Volumes für jedes Cluster überprüfen.

1. Überprüfen Sie den LIF-Status:

```
network interface show
```

Im normalen Betrieb müssen LIFs für Quell-SVMs einen Administratorstatus von „up“ aufweisen und sich auf ihren Home-Nodes befinden. LIFs für Ziel-SVMs müssen nicht auf ihren Home-Nodes up-to-located sein. Durch die Umschaltung verfügen alle LIFs über einen Administratorstatus von oben, müssen sich aber nicht auf ihren Home-Nodes befinden.

```

cluster1::> network interface show

```

Current Is	Logical	Status	Network	Current	
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. Überprüfen Sie den Status der Aggregate:

```
storage aggregate show -state !online
```

Mit diesem Befehl werden alle Aggregate angezeigt, die *Not* online sind. Im normalen Betrieb müssen alle Aggregate am lokalen Standort online sein. Wenn die MetroCluster-Konfiguration jedoch um den Switch geht, können Root-Aggregate am Disaster-Recovery-Standort offline sein.

Dieses Beispiel zeigt ein Cluster im normalen Betrieb:

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

Dieses Beispiel zeigt ein Cluster in 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. Überprüfen Sie den Status der Volumes:

```
volume show -state !online
```

Dieser Befehl zeigt alle Volumes an, die *Not* online sind.

Wenn die MetroCluster-Konfiguration sich im normalen Betrieb befindet (sie befindet sich nicht im Switchover-Status), sollte die Ausgabe alle Volumes anzeigen, die zu den sekundären SVMs des Clusters gehören (diejenigen mit dem SVM-Namen, angehängt mit „-mc“).

Diese Volumes sind nur bei einem Switchover online verfügbar.

Dieses Beispiel zeigt einen Cluster im normalen Betrieb, 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    voll1            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. Vergewissern Sie sich, dass es keine inkonsistenten Volumes gibt:

```
volume show -is-inconsistent true
```

Weitere Informationen finden Sie im Knowledge Base-Artikel ["Volume zeigt WAFL inkonsistent an"](#) Die Vorgehensweise für inkonsistente Volumes

## Überprüfen Sie die SAN-Konfiguration nach einem Upgrade

Nach einem ONTAP Upgrade sollten Sie in einer SAN-Umgebung überprüfen, ob jeder Initiator, der mit einer LIF verbunden war, vor dem Upgrade erfolgreich mit der LIF verbunden wurde.

1. Vergewissern Sie sich, dass jeder Initiator mit dem richtigen LIF verbunden ist.

Sie sollten die Liste der Initiatoren mit der Liste vergleichen, die Sie während der Upgrade-Vorbereitung erstellt haben.

Für...	Eingeben...
ISCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>

Für...	Eingeben...
FC	<pre>fcv initiator show -fields igroup,wwpn,lif</pre>

## Nach einem Upgrade von ONTAP 9.2 oder einer älteren Version werden KMIP-Serververbindungen neu konfiguriert

Nach dem Upgrade von ONTAP 9.2 oder einer älteren Version auf ONTAP 9.3 oder höher müssen Sie alle externen KMIP-Serververbindungen (Key Management) neu konfigurieren.

### Schritte

1. Konfiguration der Schlüsselmanager-Konnektivität:

```
security key-manager setup
```

2. Fügen Sie Ihre KMIP-Server hinzu:

```
security key-manager add -address key_management_server_ip_address
```

3. Vergewissern Sie sich, dass KMIP-Server verbunden sind:

```
security key-manager show -status
```

4. Abfrage der Schlüsselsever:

```
security key-manager query
```

5. Neuen Authentifizierungsschlüssel und neue Passphrase erstellen:

```
security key-manager create-key -prompt-for-key true
```

Die Passphrase muss mindestens 32 Zeichen lang sein.

6. Abfrage des neuen Authentifizierungsschlüssels:

```
security key-manager query
```



7. Weisen Sie Ihren Self-Encrypting Disks (SEDs) den neuen Authentifizierungsschlüssel zu:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```



Stellen Sie sicher, dass Sie den neuen Authentifizierungsschlüssel aus Ihrer Abfrage verwenden.

8. Weisen Sie den SEDs bei Bedarf einen FIPS-Schlüssel zu:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

## Verschieben Sie verschobene Load-Sharing-Spiegelungs-Quell-Volumes nach einem ONTAP Upgrade

Nach dem Upgrade von ONTAP müssen Quell-Volumes mit Load-Sharing-Spiegelung wieder an ihre Standorte vor dem Upgrade verschoben werden.

### Schritte

1. Ermitteln Sie den Speicherort, an den Sie das Load-Sharing-Mirror-Quellvolume verschieben, indem Sie den Datensatz verwenden, den Sie erstellt haben, bevor Sie das Load-Sharing-Spiegelquellvolume verschieben.
2. Verschieben Sie das Quell-Volume der Load-Sharing-Spiegelung zurück an den ursprünglichen Speicherort:

```
volume move start
```

## Ändern von Benutzerkonten, die auf den Service Processor zugreifen können

Wenn Sie Benutzerkonten in ONTAP 9.8 oder einer älteren Version erstellt haben, die mit einer nicht-Administratorrolle auf den Service-Prozessor (SP) zugreifen können und ein Upgrade auf ONTAP 9.9.1 oder höher durchführen, enthält der alle nicht-Administratorwerte in `-role` Parameter wurde in geändert `admin`.

Weitere Informationen finden Sie unter ["Konten, die auf den SP zugreifen können"](#).

## Aktualisieren Sie das Disk Qualification Package

Nach dem Upgrade der ONTAP-Software sollten Sie das ONTAP-DQP-Paket (Disk

Qualification Package) herunterladen und installieren. Das DQP wird im Rahmen eines ONTAP-Upgrades nicht aktualisiert.

Der DQP enthält die richtigen Parameter für die ONTAP-Interaktion mit allen neu qualifizierten Laufwerken. Wenn Ihre DQP-Version keine Informationen für ein neu qualifiziertes Laufwerk enthält, verfügt ONTAP nicht über die Informationen zur ordnungsgemäßen Konfiguration des Laufwerks.

Es empfiehlt sich, den DQP vierteljährlich zu aktualisieren. Sie sollten den DQP auch aus den folgenden Gründen aktualisieren:

- Immer, wenn Sie einem Node im Cluster einen neuen Laufwerkstyp oder eine neue Laufwerksgröße hinzufügen

Wenn Sie beispielsweise bereits über 1-TB-Laufwerke verfügen und 2-TB-Laufwerke hinzufügen, müssen Sie nach dem aktuellen DQP-Update suchen.

- Jedes Mal, wenn Sie die Festplatten-Firmware aktualisieren
- Immer wenn neuere Festplatten-Firmware oder DQP-Dateien verfügbar sind

#### **Verwandte Informationen**

- ["NetApp Downloads: Disk Qualification Package"](#)
- ["NetApp Downloads: Festplatten-Firmware"](#)

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.