Überprüfungen nach dem Upgrade

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/upgrade/task_what_to_do_after_upgrade.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Überprüfungen nach dem Upgrade . . . 1
- ONTAP Verifizierungsworkflow nach dem Upgrade . . . 1
- Cluster nach einem ONTAP Upgrade überprüfen . . . 1
  - Clusterversion überprüfen . . . 1
  - Clusterzustand überprüfen . . . 2
  - Überprüfen, ob die automatische ungeplante Umschaltung aktiviert ist (MetroCluster FC-Konfigurationen nur) . . . 3
- LIFs nach einem ONTAP Upgrade wieder aktivieren und auf ihre Home-Ports zurücksetzen . . . 4
- Spezielle Konfigurationen . . . 5
  - Prüfungen nach dem Upgrade für spezifische ONTAP Konfigurationen . . . 5
  - Nach einem Upgrade sollte die ONTAP Netzwerkkonfiguration überprüft werden. . . . 6
  - Entfernen des EMS LIF Service aus den Netzwerkrichtlinien nach dem Upgrade von ONTAP . . . 9
  - Netzwerk- und Speicherstatus von MetroCluster nach einem ONTAP Upgrade überprüfen . . . 10
  - Die SAN-Konfiguration nach einem ONTAP Upgrade überprüfen . . . 13
  - KMIP-Server nach einem Upgrade von ONTAP 9.2 oder früher neu konfigurieren . . . 13
  - Verschobene Load-Sharing Mirror-Quell-Volumes nach einem ONTAP Upgrade neu zuordnen . . . 15
  - Wie ONTAP Upgrades die Benutzerkonten des Serviceprozessors ändern . . . 15
- Das Disk Qualification Package nach einem ONTAP Upgrade aktualisieren . . . 15

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

Stellen Sie sich die Frage …	Wenn Ihre Antwort ja lautet, ist Folgendes zu tun…
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.

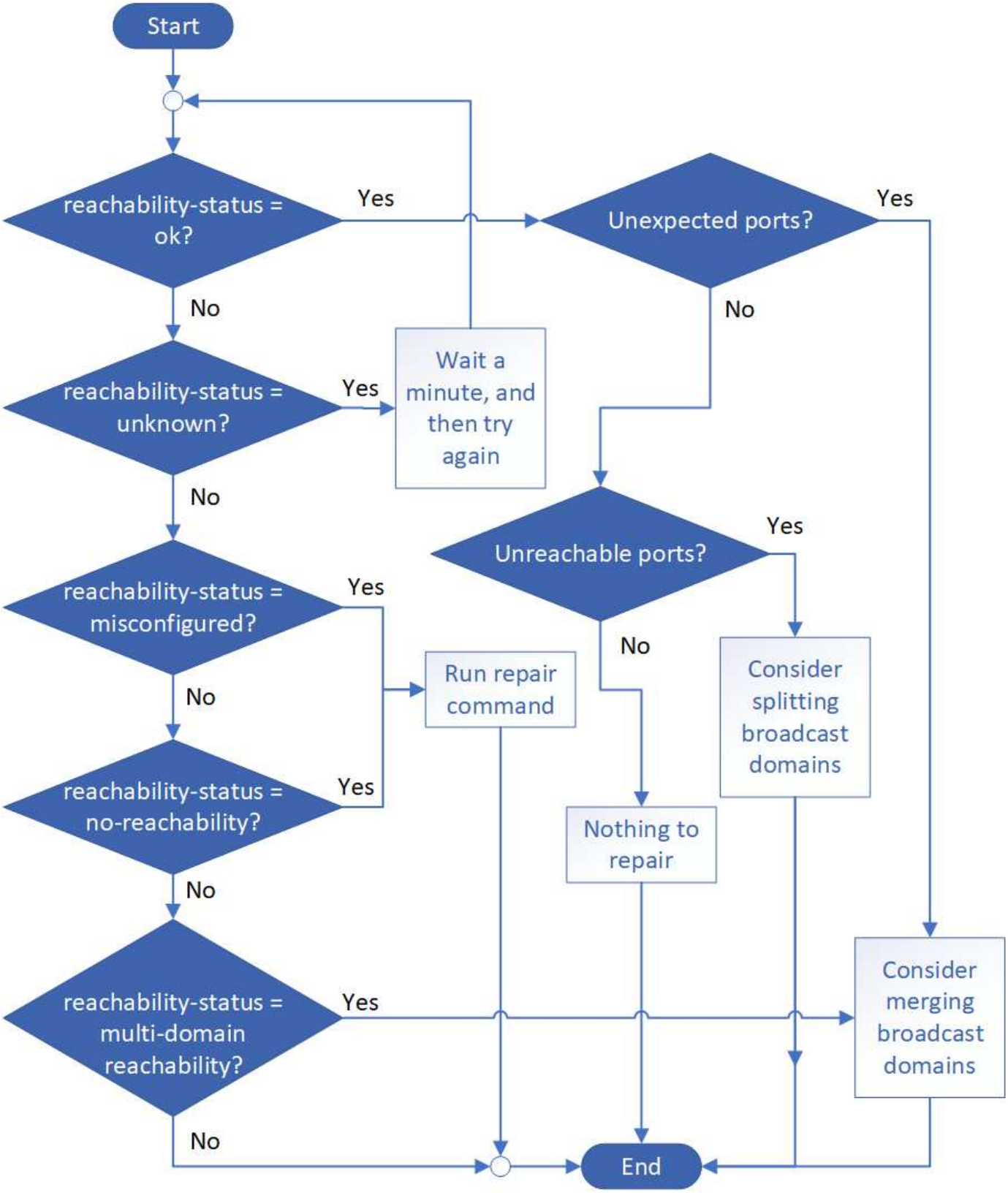
Schritt

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"

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.