Was nach einer ONTAP Rücksetzung zu tun ist

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/revert/task_verify_health.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Was nach einer ONTAP Rücksetzung zu tun ist . . . 1
- Cluster- und Speicherzustand nach einer ONTAP Rücksetzung überprüfen . . . 1
  - Clusterzustand überprüfen . . . 1
  - Speicherzustand überprüfen . . . 3
  - Clientzugriff (SMB und NFS) überprüfen . . . 4
- Aktivierung der automatischen Umschaltung nach einer ONTAP MetroCluster Rücksetzung . . . 4
- LIFs nach einer ONTAP Umstellung auf die Home-Ports aktivieren und zurücksetzen . . . 5
- Snapshot-Richtlinien nach einem ONTAP Revert aktivieren . . . 7
- IPv6-Firewall-Einträge nach einer ONTAP Rücksetzung überprüfen . . . 7
- Überprüfung der Benutzerkonten des Serviceprozessors nach der Rückkehr zu ONTAP 9.8 . . . 8

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.