



## **Phase 3: Installieren und booten Sie node3**

### **Upgrade controllers**

NetApp  
July 05, 2024

# Inhalt

- Phase 3: Installieren und booten Sie node3 ..... 1
- Phase-3-Übersicht ..... 1
- Installieren und booten Sie node3 ..... 1
- Überprüfen Sie die Installation von node3 ..... 10
- Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3 ..... 17
- Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3 ..... 18

# Phase 3: Installieren und booten Sie node3

## Phase-3-Übersicht

In Phase 3 installieren und booten Sie node3, überprüfen, ob die Cluster- und Node-Management-Ports von node1 auf node3 online geschaltet sind, und überprüfen Sie die Installation von node3. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden die LIFs für NAS-Daten-LIFs und nicht-Root-Aggregate von node2 auf node3 verschoben und Sie überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

### Schritte

1. ["Installieren und booten Sie node3"](#)
2. ["Überprüfen Sie die Installation von node3"](#)
3. ["Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3"](#)
4. ["Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3"](#)

## Installieren und booten Sie node3

Sie installieren node3 im Rack, übertragen die Verbindungen von node1 zu node3, starten node3 und installieren ONTAP. Sie weisen dann alle Spare-Festplatten von node1, alle Festplatten, die zum Root-Volume gehören, und alle nicht-Root-Aggregate neu zu, die zu einem früheren Zeitpunkt nicht zu node2 verschoben wurden, wie in diesem Abschnitt beschrieben.

### Über diese Aufgabe

Der Umzugsvorgang wird zu Beginn dieser Phase angehalten. Dieser Prozess ist weitgehend automatisiert; der Vorgang hält an, damit Sie seinen Status überprüfen können. Sie müssen den Vorgang manuell fortsetzen. Außerdem müssen Sie überprüfen, ob die SAN LIFs erfolgreich online geschaltet wurden und den korrekten physischen FC-Ports in Knoten3 zugewiesen wurden.

Sie müssen als Netzboot node3 wechseln, wenn nicht die gleiche Version von ONTAP 9 installiert ist auf node1. Nachdem Sie node3 installiert haben, starten Sie es vom ONTAP 9-Image, das auf dem Webserver gespeichert ist. Anschließend können Sie die richtigen Dateien auf das Boot-Medium für nachfolgende Systemstarts herunterladen, indem Sie den Anweisungen in folgen ["Vorbereitungen für den Netzboot"](#).

### Schritte

1. stellen Sie sicher, dass Sie Platz im Rack für node3 haben.

Die Platz- und Höhenanforderungen der neuen Nodes können sich von den vorhandenen Nodes unterscheiden. Planen Sie den Platzbedarf für Ihr Upgrade-Szenario.

2. Installieren Sie node3 im Rack und befolgen Sie die Anweisungen *Installation und Setup* für Ihr Node-Modell.
3. Kabelnode3, Verschieben der Verbindungen von node1 nach node3.

Ab ONTAP 9.15.1 verfügen neue Controller-Modelle über nur einen „Schraubenschlüssel“ Port für den

Baseboard Management Controller (BMC) und Management-Verbindungen. Planen Sie die Verkabelungsänderungen entsprechend.

- Konsole (Remote-Management-Port)
- Cluster- und HA-Ports
- Datenports
- Cluster- und Node-Management-Ports
- Serial-Attached SCSI (SAS)- und Ethernet-Storage-Ports
- SAN-Konfigurationen: iSCSI-Ethernet-, FC- und NVMe/FC-Switch-Ports

Möglicherweise müssen Sie die Verbindungskabel zwischen den alten und den neuen Controllern ändern, um die Interoperabilität zwischen den verschiedenen Controller- und Kartenmodellen zu ermöglichen. Eine Verkabelungskarte der Ethernet-Storage-Shelfs für Ihre Systeme finden Sie im ["Verfahren zur Systeminstallation"](#).



Für ab ONTAP 9.15.1 eingeführte Controller verwenden Cluster und HA Interconnects die gleichen Ports. Bei Switch-verbundenen Konfigurationen müssen ähnliche Ports mit denselben Cluster-Switches verbunden werden. Wenn Sie beispielsweise von einem vorhandenen Controller auf einen AFF A1K aktualisieren, sollten Sie die e1a-Ports beider Nodes mit einem Switch und die e7a-Ports beider Nodes mit dem zweiten Switch verbinden.

4. Einschalten Sie den Netzstrom auf node3, und unterbrechen Sie dann den Bootvorgang, indem Sie an der Konsole Strg-C drücken, um auf die Eingabeaufforderung der Boot-Umgebung zuzugreifen.



Wenn Sie node3 booten, wird möglicherweise die folgende Warnmeldung angezeigt:

```
WARNING: The battery is unfit to retain data during a power outage. This is likely because the battery is discharged but could be due to other temporary conditions.
```

```
When the battery is ready, the boot process will complete and services will be engaged.
```

```
To override this delay, press 'c' followed by 'Enter'
```

5. Wenn die Warnmeldung in angezeigt wird [Schritt 4](#), Nehmen Sie die folgenden Aktionen:
  - a. Überprüfen Sie auf Meldungen der Konsole, die auf ein anderes Problem als eine schwache NVRAM-Batterie hinweisen und ergreifen Sie gegebenenfalls erforderliche Korrekturmaßnahmen.
  - b. Warten Sie, bis der Akku geladen ist und der Bootvorgang abgeschlossen ist.



**Achtung: Die Verzögerung nicht außer Kraft setzen; wenn der Akku nicht geladen werden darf, kann dies zu einem Datenverlust führen.**



Siehe ["Vorbereitungen für den Netzboot"](#).

6. Konfigurieren Sie die Netzboot-Verbindung, indem Sie eine der folgenden Aktionen auswählen.



Sie müssen den Management-Port und die IP als Netzboot-Verbindung verwenden. Verwenden Sie keine Daten-LIF-IP, oder es kann während des Upgrades ein Datenausfall auftreten.

Wenn DHCP (Dynamic Host Configuration Protocol) lautet...	Dann...
Wird Ausgeführt	Konfigurieren Sie die Verbindung automatisch mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: <code>ifconfig e0M -auto</code>
Nicht ausgeführt	Konfigurieren Sie die Verbindung manuell mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung: <code>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></code>  <i>filer_addr</i> Ist die IP-Adresse des Speichersystems (obligatorisch). <i>netmask</i> Ist die Netzwerkmaske des Storage-Systems (erforderlich). <i>gateway</i> Ist das Gateway für das Speichersystem (erforderlich). <i>dns_addr</i> Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk (optional). <i>dns_domain</i> Ist der Domain-Name (DNS) (optional).   Andere Parameter können für Ihre Schnittstelle erforderlich sein. Eingabe <code>help ifconfig</code> Details finden Sie in der Firmware-Eingabeaufforderung.

#### 7. Netzboot auf Node3 durchführen:

```
netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
```

Der <path\_to\_the\_web-accessible\_directory> Sollten Sie dazu führen, wo Sie das heruntergeladen haben <ontap\_version>\_image.tgz Im Abschnitt "[Vorbereitungen für den Netzboot](#)".



Unterbrechen Sie den Startvorgang nicht.

#### 8. im Startmenü Option wählen (7) Install new software first.

Mit dieser Menüoption wird das neue ONTAP-Image auf das Startgerät heruntergeladen und installiert.

Ignorieren Sie die folgende Meldung:

```
This procedure is not supported for Non-Disruptive Upgrade on an HA pair
```

Der Hinweis gilt für unterbrechungsfreie Upgrades der ONTAP und keine Upgrades von Controllern.



Aktualisieren Sie den neuen Node immer als Netzboot auf das gewünschte Image. Wenn Sie eine andere Methode zur Installation des Images auf dem neuen Controller verwenden, wird möglicherweise das falsche Image installiert. Dieses Problem gilt für alle ONTAP Versionen. Das Netzboot wird mit der Option kombiniert (7) `Install new software` Entfernt das Boot-Medium und platziert dieselbe ONTAP-Version auf beiden Image-Partitionen.

9. Wenn Sie aufgefordert werden, den Vorgang fortzusetzen, geben Sie ein `y`, Und wenn Sie zur Eingabe des Pakets aufgefordert werden, geben Sie die URL ein:

```
http://<web_server_ip/path_to_web-  
accessible_directory>/<ontap_version>_image.tgz
```

10. Vervollständigen Sie die folgenden Teilschritte, um das Controller-Modul neu zu starten:
  - a. Eingabe `n` So überspringen Sie die Backup-Recovery, wenn folgende Eingabeaufforderung angezeigt wird:

```
Do you want to restore the backup configuration now? {y|n}
```

- b. Eingabe `y` Um den Neustart zu starten, wenn die folgende Eingabeaufforderung angezeigt wird:

```
The node must be rebooted to start using the newly installed software. Do  
you want to reboot now? {y|n}
```

Das Controller-Modul wird neu gestartet, stoppt aber im Startmenü, da das Boot-Gerät neu formatiert wurde und die Konfigurationsdaten wiederhergestellt werden müssen.

11. Wählen Sie den Wartungsmodus aus 5 Öffnen Sie das Startmenü, und geben Sie ein `y` Wenn Sie aufgefordert werden, den Startvorgang fortzusetzen.
12. ] Überprüfen Sie, ob Controller und Chassis als ha konfiguriert sind:

```
ha-config show
```

Das folgende Beispiel zeigt die Ausgabe von `ha-config show` Befehl:

```
Chassis HA configuration: ha  
Controller HA configuration: ha
```



Das System zeichnet in einem PROM auf, ob es sich um ein HA-Paar oder eine eigenständige Konfiguration handelt. Der Status muss auf allen Komponenten im Standalone-System oder im HA-Paar der gleiche sein.

13. Wenn der Controller und das Chassis nicht als ha konfiguriert sind, korrigieren Sie die Konfiguration mit den folgenden Befehlen:

```
ha-config modify controller ha
```

```
ha-config modify chassis ha
```

14. Vergewissern Sie sich, dass alle Ethernet-Ports, die zur Verbindung mit den Ethernet-Shelfs verwendet werden, als Speicher konfiguriert sind:

```
storage port show
```

Die angezeigte Ausgabe hängt von der Systemkonfiguration ab. Das folgende Ausgabebeispiel gilt für einen Knoten mit einer einzelnen Speicherkarte in Steckplatz 11. Die Ausgabe für Ihr System kann unterschiedlich sein:

```
*> storage port show
Port Type Mode      Speed (Gb/s) State      Status  VLAN ID
---- ---- -
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Ändern Sie die Ports, die nicht auf Speicher festgelegt sind:

```
storage port modify -p <port> -m storage
```

Alle mit Storage Shelves verbundenen Ethernet-Ports müssen als Storage konfiguriert werden, um den Zugriff auf Festplatten und Shelves zu ermöglichen.

16. Beenden des Wartungsmodus:

```
halt
```

Unterbrechen Sie den Autoboot, indem Sie auf drücken `Ctrl-C` An der Eingabeaufforderung für die Boot-Umgebung.

17. Überprüfen Sie in node2 das Systemdatum, die Uhrzeit und die Zeitzone:

```
date
```

18. Überprüfen Sie bei node3 das Datum mithilfe des folgenden Befehls an der Eingabeaufforderung der Boot-Umgebung:

```
show date
```

19. Stellen Sie bei Bedarf das Datum auf Knoten 3 ein:

```
set date <mm/dd/yyyy>
```

20. Überprüfen Sie bei node3 die Zeit mit dem folgenden Befehl an der Eingabeaufforderung der Boot-Umgebung:

```
show time
```

21. Stellen Sie bei Bedarf die Zeit auf node3 ein:

```
set time <hh:mm:ss>
```

22. Legen Sie im Boot-Loader die Partner-System-ID auf node3 fest:

```
setenv partner-sysid <node2_sysid>
```

Für Knoten 3, `partner-sysid` Muss der von node2 sein.

a. Einstellungen speichern:

```
saveenv
```

23. Überprüfen Sie den `partner-sysid` Für Knoten 3:

```
printenv partner-sysid
```

24. Wenn NetApp Storage Encryption (NSE) Laufwerke installiert sind, führen Sie die folgenden Schritte durch.



Falls Sie dies noch nicht bereits in der Prozedur getan haben, lesen Sie den Artikel in der Knowledge Base ["Wie erkennen Sie, ob ein Laufwerk FIPS-zertifiziert ist"](#) Ermitteln der Art der verwendeten Self-Encrypting Drives.

a. Einstellen `bootarg.storageencryption.support` Bis `true` Oder `false`:

Wenn die folgenden Laufwerke verwendet werden...	Dann...
NSE-Laufwerke, die den Self-Encryption-Anforderungen von FIPS 140-2 Level 2 entsprechen	<code>setenv bootarg.storageencryption.support true</code>
NetApp ohne FIPS SEDs	<code>setenv bootarg.storageencryption.support false</code>

b. Gehen Sie zum speziellen Startmenü und wählen Sie Option (10) Set Onboard Key Manager recovery secrets.

Geben Sie die Passphrase und die Backup-Informationen ein, die Sie zuvor aufgezeichnet haben. Siehe ["Management der Storage-Verschlüsselung mit dem Onboard Key Manager"](#).

25. Boot-Node im Startmenü:

```
boot_ontap menu
```

26. Gehen Sie auf node3 zum Boot-Menü und wählen Sie mit 22/7 die versteckte Option aus `boot_after_controller_replacement`. Geben Sie an der Eingabeaufforderung node1 ein, um die Festplatten von node1 node3 wie im folgenden Beispiel neu zuzuweisen.

## Erweitern Sie das Ausgabebeispiel der Konsole

```
LOADER-A> boot_ontap menu
.
<output truncated>
.
All rights reserved.
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
.
<output truncated>
.
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7
(22/7) Print this secret List
(25/6) Force boot with multiple filesystem disks missing.
(25/7) Boot w/ disk labels forced to clean.
(29/7) Bypass media errors.
(44/4a) Zero disks if needed and create new flexible root volume.
(44/7) Assign all disks, Initialize all disks as SPARE, write DDR
labels
.
<output truncated>
.
(wipeconfig) Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition) Boot after MCC transition
(9a) Unpartition all disks and remove
their ownership information.
(9b) Clean configuration and
initialize node with partitioned disks.
```

```
(9c) Clean configuration and
initialize node with whole disks.
(9d) Reboot the node.
(9e) Return to main boot menu.
```

The boot device has changed. System configuration information could be lost. Use option (6) to restore the system configuration, or option (4) to initialize all disks and setup a new system.

Normal Boot is prohibited.

Please choose one of the following:

- (1) Normal Boot.
- (2) Boot without /etc/rc.
- (3) Change password.
- (4) Clean configuration and initialize all disks.
- (5) Maintenance mode boot.
- (6) Update flash from backup config.
- (7) Install new software first.
- (8) Reboot node.
- (9) Configure Advanced Drive Partitioning.
- (10) Set Onboard Key Manager recovery secrets.
- (11) Configure node for external key management.

Selection (1-11)? boot\_after\_controller\_replacement

This will replace all flash-based configuration with the last backup to disks. Are you sure you want to continue?: yes

.

<output truncated>

.

Controller Replacement: Provide name of the node you would like to replace:<nodename of the node being replaced>

Changing sysid of node nodel disks.

Fetches sanown old\_owner\_sysid = 536940063 and calculated old sys id = 536940063

Partner sysid = 4294967295, owner sysid = 536940063

.

<output truncated>

.

varfs\_backup\_restore: restore using /mroot/etc/varfs.tgz

varfs\_backup\_restore: attempting to restore /var/kmip to the boot device

varfs\_backup\_restore: failed to restore /var/kmip to the boot device

varfs\_backup\_restore: attempting to restore env file to the boot device

varfs\_backup\_restore: successfully restored env file to the boot device wrote key file "/tmp/rndc.key"

varfs\_backup\_restore: timeout waiting for login

varfs\_backup\_restore: Rebooting to load the new varfs

Terminated

```

<node reboots>
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
<output truncated>
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
Login:

```



Im obigen Beispiel der Konsolenausgabe werden Sie von ONTAP aufgefordert, den Namen des Partner-Node anzugeben, wenn das System ADP-Festplatten (Advanced Disk Partitioning) verwendet.

27. Wenn das System in eine Reboot-Schleife mit der Meldung geht `no disks found`, zeigt dies an, dass ein Problem mit der Neuzuweisung der Festplatte aufgetreten ist. Informationen zur Behebung des Problems finden Sie unter "[Fehlerbehebung](#)".

28. Drücken Sie `Ctrl-C` während des Autoboots, um den Knoten an der Eingabeaufforderung anzuhalten `LOADER>`.

29. Wechseln Sie an der `LOADER`-Eingabeaufforderung in den Wartungsmodus:

```
boot_ontap maint
```

30. Überprüfen Sie die Festplattenkonnektivität, den Controller-Modell-String, die HA-Konfiguration und andere Details zur Hardware-Konnektivität.

31. Beenden des Wartungsmodus:

```
halt
```

32. Starten Sie an der `LOADER`-Eingabeaufforderung:

```
boot_ontap menu
```

Beim Booten erkennt der Node jetzt alle Festplatten, die zuvor ihm zugewiesen waren, und kann wie erwartet gebootet werden.

Wenn die Clusterknoten, die Sie ersetzen, die Root-Volume-Verschlüsselung verwenden, kann ONTAP die Volume-Informationen von den Festplatten nicht lesen. Stellen Sie die Schlüssel für das Root-Volume wieder her.



Dies gilt nur, wenn das Root-Volume NetApp-Volume-Verschlüsselung verwendet.

a. Zurück zum speziellen Startmenü:

```
LOADER> boot_ontap menu
```

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.

Selection (1-11)? 10
```

b. Wählen Sie **(10) Set Onboard Key Manager Recovery Secrets**

c. Eingabe `y` An der folgenden Eingabeaufforderung:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

d. Geben Sie an der Eingabeaufforderung die Passphrase für das Schlüsselmanagement ein.

e. Geben Sie bei Aufforderung die Backup-Daten ein.



Sie müssen die Passphrase und Sicherungsdaten im erhalten haben "[Bereiten Sie die Knoten für ein Upgrade vor](#)" Abschnitt dieses Verfahrens.

f. Nachdem das System wieder zum speziellen Startmenü gestartet wurde, führen Sie die Option **(1) Normal Boot** aus



In dieser Phase ist möglicherweise ein Fehler aufgetreten. Wenn ein Fehler auftritt, wiederholen Sie die Teilschritte in [Schritt 32](#) , bis das System ordnungsgemäß gebootet wird.

## Überprüfen Sie die Installation von node3

Sie müssen überprüfen, ob die physischen Ports von node1 den physischen Ports auf node3 korrekt zugeordnet sind. Dadurch kann node3 nach dem Upgrade mit anderen Knoten im Cluster und mit dem Netzwerk kommunizieren.

**Über diese Aufgabe**

Siehe "[Quellen](#)" Verknüpfen mit *Hardware Universe*, um Informationen über die Ports auf den neuen Nodes zu erfassen. Die Informationen werden später in diesem Abschnitt verwendet.

Abhängig vom Modell der Nodes kann das physische Port-Layout variieren. Wenn der neue Node gestartet wird, versucht ONTAP, zu ermitteln, welche Ports die Cluster LIFs hosten sollten, damit es automatisch zu Quorum kommt.

Wenn die physischen Ports auf node1 nicht direkt den physischen Ports auf node3 zugeordnet werden, wird der folgende Abschnitt angezeigt [Stellen Sie die Netzwerkkonfiguration auf node3 wieder her](#) Muss zur Reparatur der Netzwerkverbindung verwendet werden.

Nach der Installation und dem Booten von node3 müssen Sie überprüfen, ob die Installation korrekt ist. Sie müssen warten, bis Knoten 3 dem Quorum beitreten und dann den Umzugsvorgang fortsetzen.

An diesem Punkt des Verfahrens wird der Vorgang angehalten, da node3 dem Quorum beitrifft.

### Schritte

1. Vergewissern Sie sich, dass node3 dem Quorum beigetreten ist:

```
cluster show -node node3 -fields health
```

Die Ausgabe des health Feld muss sein true.

2. Vergewissern Sie sich, dass node3 Teil desselben Clusters wie node2 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

3. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set advanced
```

4. Überprüfen Sie den Status des Controller-Austauschvorgangs und vergewissern Sie sich, dass er sich in einem Pause-Zustand befindet und sich im gleichen Zustand wie zuvor in node1 befand, um die physischen Aufgaben beim Installieren neuer Controller und Verschieben von Kabeln auszuführen:

```
system controller replace show
```

```
system controller replace show-details
```

5. Setzen Sie den Austausch des Controllers wieder ein:

```
system controller replace resume
```

6. Der Austausch des Controllers wird anhand der folgenden Meldung unterbrochen:

```
Cluster::*> system controller replace show
```

Node	Status	Error-Action
-----		
-----		
Node1(now node3)	Paused-for-intervention	Follow the instructions given in
Node2	None	Step Details

Step Details:

-----

To complete the Network Reachability task, the ONTAP network configuration must be manually adjusted to match the new physical network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For detailed commands and instructions, refer to the "Re-creating VLANs, ifgrps, and broadcast domains" section of the upgrade controller hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-replacement network displaced-vlans restore" to restore the VLAN on the desired port.

2 entries were displayed.



In diesem Verfahren wurde der Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node3\_ umbenannt.

7. Wenn der Controller-Austausch im Status „Pause“ steht, fahren Sie mit dem nächsten Abschnitt dieses Dokuments fort, um die Netzwerkkonfiguration auf dem Node wiederherzustellen.

## Stellen Sie die Netzwerkkonfiguration auf node3 wieder her

Nachdem Sie bestätigt haben, dass node3 sich im Quorum befindet und mit node2 kommunizieren kann, überprüfen Sie, ob node1 VLANs, Interface Groups und Broadcast-Domains auf node3 zu sehen sind. Überprüfen Sie außerdem, ob alle node3-Netzwerk-Ports in ihren richtigen Broadcast-Domänen konfiguriert sind.

### Über diese Aufgabe

Weitere Informationen zum Erstellen und Neuerstellen von VLANs, Schnittstellengruppen und Broadcast-Domänen finden Sie unter "[Quellen](#)" Verknüpfen mit *Network Management*.

### Schritte

1. Listen Sie alle physischen Ports auf, die auf dem aktualisierten Knoten 1 (als Knoten 3 bezeichnet) sind:

```
network port show -node node3
```

Alle physischen Netzwerk-Ports, VLAN-Ports und Schnittstellen-Gruppen-Ports auf dem Node werden angezeigt. In dieser Ausgabe sehen Sie alle physischen Ports, die in verschoben wurden Cluster Broadcast-Domäne von ONTAP Sie können diese Ausgabe verwenden, um zu entscheiden, welche Ports als Ports für Schnittstellengruppen, VLAN-Basis-Ports oder eigenständige physische Ports zum Hosten von LIFs verwendet werden müssen.

2. Liste der Broadcast-Domänen auf dem Cluster:

```
network port broadcast-domain show
```

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node3 auflisten:

```
network port reachability show
```

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
          e0M      Default:Mgmt                ok
          e10a     Default:Default             ok
          e10b     -                            no-reachability
          e10c     Default:Default             ok
          e10d     -                            no-reachability
          e1a      Cluster:Cluster              ok
          e1b     -                            no-reachability
          e7a      Cluster:Cluster              ok
          e7b     -                            no-reachability
node2_node4
          e0M      Default:Mgmt                ok
          e4a     Default:Default             ok
          e4b     -                            no-reachability
          e4c     Default:Default             ok
          e4d     -                            no-reachability
          e3a     Cluster:Cluster              ok
          e3b     Cluster:Cluster              ok
18 entries were displayed.
```

Im vorherigen Beispiel wird node1\_node3 kurz nach dem Austausch des Controllers gestartet. Einige Ports verfügen nicht über die Fähigkeit, ihre zu erwartenden Broadcast-Domänen zu erreichen und müssen repariert werden.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node3 mit einem anderen Status als der Erreichbarkeit ok. Führen Sie den folgenden Befehl aus, zuerst auf beliebigen physischen Ports, dann auf

beliebigen VLAN-Ports, nacheinander:

```
network port reachability repair -node <node_name> -port <port_name>
```

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node nodel_node3 -port e4a
```

```
Warning: Repairing port "nodel_node3: e4a" may cause it to move into a  
different broadcast domain, which can cause LIFs to be re-homed away  
from the port. Are you sure you want to continue? {y|n}:
```

Wie oben dargestellt, wird eine Warnmeldung für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Wiederachbarkeit der Broadcast-Domain unterscheiden können, wo sie sich derzeit befindet. Überprüfen Sie die Verbindung des Ports und die Antwort *y* Oder *n* Je nach Bedarf.

Überprüfen Sie, ob alle physischen Ports die erwartete Erreichbarkeit haben:

```
network port reachability show
```

Während die Reparatur der Erreichbarkeit durchgeführt wird, versucht ONTAP, die Ports in die richtigen Broadcast-Domänen zu platzieren. Wenn jedoch die Erreichbarkeit eines Ports nicht ermittelt werden kann und keiner der bestehenden Broadcast-Domänen angehört, wird ONTAP neue Broadcast-Domains für diese Ports erstellen.

5. Wenn die Konfiguration der Schnittstellengruppe nicht mit dem physischen Portlayout des neuen Controllers übereinstimmt, ändern Sie diese mit den folgenden Schritten.

- a. Sie müssen zunächst physische Ports entfernen, die als Ports für Schnittstellengruppen von ihrer Broadcast-Domain-Mitgliedschaft verwendet werden sollen. Dazu verwenden Sie den folgenden Befehl:

```
network port broadcast-domain remove-ports -broadcast-domain <broadcast-  
domain_name> -ports <node_name:port_name>
```

- b. Hinzufügen eines Mitgliedports zu einer Schnittstellengruppe:

```
network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port  
<port_name>
```

- c. Die Schnittstellengruppe wird der Broadcast-Domäne automatisch ca. eine Minute nach dem Hinzufügen des ersten Mitgliedports hinzugefügt.
- d. Vergewissern Sie sich, dass die Schnittstellengruppe der entsprechenden Broadcast-Domäne hinzugefügt wurde:

```
network port reachability show -node <node_name> -port <ifgrp>
```

Wenn der Status der Erreichbarkeit der Schnittstellengruppe nicht lautet *ok*, Weisen Sie es der entsprechenden Broadcast-Domain zu:

```
network port broadcast-domain add-ports -broadcast-domain
<broadcast_domain_name> -ports <node:port>
```

6. Weisen Sie der Broadcast-Domäne geeignete physische Ports zu Cluster , indem Sie die folgenden Schritte ausführen:

- a. Ermitteln Sie, welche Ports eine Reachability zum haben Cluster Broadcast-Domäne:

```
network port reachability show -reachable-broadcast-domains Cluster:Cluster
```

- b. Reparieren Sie jeden Port mit Erreichbarkeit zum Cluster Broadcast-Domäne, wenn ihr Status der Erreichbarkeit nicht lautet ok:

```
network port reachability repair -node <node_name> -port <port_name>
```

7. Verschieben Sie die verbleibenden physischen Ports in ihre richtigen Broadcast-Domänen mithilfe eines der folgenden Befehle:

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
network port broadcast-domain add-port
```

Vergewissern Sie sich, dass keine unerreichbaren oder unerwarteten Ports vorhanden sind. Überprüfen Sie den Status der Erreichbarkeit aller physischen Ports mithilfe des folgenden Befehls und überprüfen Sie die Ausgabe, um sicherzustellen, dass der Status lautet ok:

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

8. Stellen Sie alle VLANs wieder her, die möglicherweise verschoben wurden, indem Sie die folgenden Schritte ausführen:

- a. Versetzte VLANs auflisten:

```
cluster controller-replacement network displaced-vlans show
```

Die Ausgabe sollte wie folgt angezeigt werden:

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node   Base Port   VLANs
-----
Node1  a0a         822, 823
       e4a         822, 823
2 entries were displayed.
```

- b. Stellen Sie VLANs wieder her, die von ihren früheren Basis-Ports verdrängt wurden:

```
cluster controller-replacement network displaced-vlans restore
```

Das folgende Beispiel zeigt die Wiederherstellung von VLANs, die aus der Schnittstellengruppe „a0a“ wieder in dieselbe Schnittstellengruppe verschoben wurden:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

Das folgende Beispiel zeigt die Wiederherstellung von verlagerten VLANs am Port „e9a“ an' e9d:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

Wenn eine VLAN-Wiederherstellung erfolgreich ist, werden die verschobenen VLANs auf dem angegebenen Zielport erstellt. Die VLAN-Wiederherstellung schlägt fehl, wenn der Zielport Mitglied einer Schnittstellengruppe ist oder der Zielport nicht verfügbar ist.

Warten Sie etwa eine Minute, bis neu wiederhergestellte VLANs in ihren entsprechenden Broadcast-Domänen platziert werden.

- a. Erstellen Sie bei Bedarf neue VLAN-Ports für VLAN-Ports, die nicht im enthalten sind `cluster controller-replacement network displaced-vlans show` Ausgabe sollte aber auf anderen physischen Ports konfiguriert werden.

9. Löschen Sie alle leeren Broadcast-Domänen, nachdem alle Port-Reparaturen abgeschlossen wurden:

```
network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. Überprüfung der Anschlussfähigkeit:

```
network port reachability show
```

Wenn alle Ports korrekt konfiguriert und den richtigen Broadcast-Domänen hinzugefügt wurden, wird das angezeigt `network port reachability show` Der Befehl sollte den Status der Erreichbarkeit als `ok` Für alle verbundenen Ports und den Status als `no-reachability` Für Ports ohne physische Konnektivität. Wenn ein Port einen anderen Status als diese beiden meldet, führen Sie die Reparatur der Nachweisbarkeit durch und fügen Sie Ports aus ihren Broadcast-Domänen hinzu oder entfernen Sie sie gemäß Anweisungen in [Schritt 4](#).

11. Vergewissern Sie sich, dass alle Ports in Broadcast-Domänen platziert wurden:

```
network port show
```

12. Vergewissern Sie sich, dass alle Ports in den Broadcast-Domänen die richtige MTU (Maximum Transmission Unit) konfiguriert haben:

```
network port broadcast-domain show
```

13. Stellen Sie die LIF-Start-Ports wieder her und geben Sie ggf. den Vserver(s) und die Home Ports von LIFs an, die über folgende Schritte wiederhergestellt werden müssen:

- a. Führen Sie alle vertriebenen LIFs auf:

```
displaced-interface show
```

- b. LIF-Home-Knoten und Home-Ports wiederherstellen:

```
cluster controller-replacement network displaced-interface restore-home-node  
-node <node_name> -vserver <vserver_name> -lif-name <LIF_name>
```

14. Überprüfen Sie, ob alle LIFs einen Home Port haben und administrativ höher sind:

```
network interface show -fields home-port, status-admin
```

## Wiederherstellung der Key-Manager-Konfiguration auf Knoten 3

Wenn Sie mithilfe von NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) Volumes auf dem System verschlüsseln, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht synchronisieren, können beim Verschieben der Node1-Aggregate mit ARL von node2 auf node3 Ausfälle auftreten, da node3 nicht über die erforderlichen Schlüssel zum Online-Zugriff verschlüsselter Volumes und Aggregate verfügt.

### Über diese Aufgabe

Die Verschlüsselungskonfiguration mit den neuen Nodes synchronisieren, indem Sie die folgenden Schritte durchführen:

### Schritte

1. Führen Sie den folgenden Befehl von node3 aus:

```
security key-manager onboard sync
```

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node3 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

```
::> security key-manager key query -node node3 -fields restored -key  
-type SVM-KEK
```

## Beispiel

```
::> security key-manager key query -node node3 -fields restored -key
-type SVM-KEK

node      vserver    key-server  key-id
restored
-----
node3     svm1       ""          00000000000000000000200000000000a008a81976
true                                           2190178f9350e071fbb90f00000000000000000
```

## Verschieben Sie Aggregate ohne Root-Root-Fehler und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, von node2 auf node3

Nachdem Sie die Netzwerkkonfiguration auf node3 und bevor Sie Aggregate von node2 auf node3 verschoben haben, müssen Sie überprüfen, ob die NAS-Daten-LIFs, die zu node1 gehören und sich derzeit auf node2 befinden, von node2 in node3 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN-LIFs auf node3 vorhanden sind.

### Über diese Aufgabe

Remote-LIFs verarbeiten den Datenverkehr zu SAN-LUNs während des Upgrades. Das Verschieben von SAN-LIFs ist für den Zustand des Clusters oder des Service während des Upgrades nicht erforderlich. SAN LIFs werden nicht verschoben, es sei denn, sie müssen neuen Ports zugeordnet werden. Sie überprüfen, ob die LIFs sich in einem ordnungsgemäßen Zustand befinden und sich auf den entsprechenden Ports befinden, nachdem Sie node3 in den Online-Modus versetzt haben.

### Schritte

1. Die iSCSI LIFs finden automatisch die richtigen Home Ports mithilfe der Erreichbarkeit. Die FC- und NVMe/FC-SAN-LIFs werden nicht automatisch verschoben. Sie zeigen weiterhin den Home-Port an, an dem sie vor dem Upgrade waren.

Prüfen Sie die SAN LIFs auf Knoten3:

- a. Ändern Sie alle iSCSI SAN LIFs, die über einen „down“-Status für die neuen Daten-Ports verfügen:

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. Ändern Sie alle FC- und NVMe/FC-SAN-LIFs, die den neuen Controller Zuhause haben, und melden Sie den Betriebsstatus der FCP-Ports am neuen Controller an:

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

## 2. Wiederaufnahme des Betriebs der Versetzung:

```
system controller replace resume
```

Das System führt die folgenden Aufgaben aus:

- Cluster-Quorum-Prüfung
- System-ID-Prüfung
- Prüfung der Bildversion
- Überprüfung der Zielplattform
- Prüfung der Netzwerkanachhabilität

Der Vorgang unterbricht in dieser Phase in der Überprüfung der Netzwerknachprüfbarkeit.

## 3. Wiederaufnahme des Betriebs der Versetzung:

```
system controller replace resume
```

Das System führt folgende Prüfungen durch:

- Cluster-Zustandsprüfung
- LIF-Statusüberprüfung für Cluster

Nach Durchführung dieser Prüfungen verschiebt das System die nicht-Root-Aggregate und NAS-Daten-LIFs, die sich im Besitz von node1 befinden, auf den neuen Controller, node3. Der Controller-Ersatzvorgang hält nach Abschluss der Ressourcenverschiebung die Pause ein.

## 4. Überprüfen Sie den Status der Aggregatverschiebung und der LIF-Verschiebung von NAS-Daten:

```
system controller replace show-details
```

Wenn der Austausch des Controllers unterbrochen wird, prüfen und korrigieren Sie den Fehler, falls zutreffend, und führen Sie das Problem anschließend aus `resume` Um den Vorgang fortzusetzen.

## 5. Falls erforderlich, stellen Sie alle vertriebenen LIFs wieder her. Liste aller vertriebenen LIFs:

```
cluster controller-replacement network displaced-interface show
```

Wenn LIFs verschoben werden, stellen Sie den Home-Node wieder in Knoten 3 wieder her:

```
cluster controller-replacement network displaced-interface restore-home-node
```

## 6. Setzen Sie den Vorgang fort, um das System zur Durchführung der erforderlichen Nachprüfungen zu auffordern:

```
system controller replace resume
```

Das System führt die folgenden Nachprüfungen durch:

- Cluster-Quorum-Prüfung
- Cluster-Zustandsprüfung
- Aggregatrekonstruktion
- Aggregatstatus-Prüfung
- Überprüfung des Festplattenstatus
- LIF-Statusüberprüfung für Cluster
- Lautstärkerprüfung

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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, BEISPIELHAFT 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.