



Phase 3: Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Upgrade controllers

NetApp
February 22, 2024

Inhalt

- Phase 3: Starten Sie Knoten 1 mit den Ersatz-Systemmodulen 1
 - Überblick 1
 - Starten Sie Knoten 1 mit den Ersatz-Systemmodulen 1
 - Überprüfen Sie die Installation node1 7
 - Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her 12
 - Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1 13

Phase 3: Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Überblick

In Phase 3 starten Sie node1 mit aktualisierten Systemmodulen und überprüfen die aktualisierte node1-Installation. Wenn Sie NetApp Volume Encryption (NVE) verwenden, stellen Sie die Konfiguration des Schlüsselmanagers wieder her. Außerdem werden node1 Aggregate und NAS-Daten-LIFs von node2 auf die aktualisierte Node1 verschoben und Sie überprüfen, ob die SAN-LIFs auf node1 vorhanden sind.

Schritte

1. "Starten Sie Knoten 1 mit den Ersatz-Systemmodulen"
2. "Überprüfen Sie die Installation node1"
3. "Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her"
4. "Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1"

Starten Sie Knoten 1 mit den Ersatz-Systemmodulen

Node1 mit den Ersatzmodulen ist nun startbereit. In diesem Abschnitt werden die Schritte beschrieben, die zum Starten von Knoten 1 mit den Ersatzmodulen für die folgenden Upgrade-Konfigurationen erforderlich sind:

Alter Knoten 1-Controller	Ersatz-Knoten 1-Systemmodule
AFF A220 als ASA konfiguriert	AFF A150-Controller-Modul ¹
AFF A220 AFF A200 AFF C 190	AFF A150-Controller-Modul ¹
FAS2620 FAS2720	FAS2820 Controller-Modul ¹
AFF A700 – als ASA konfiguriert	ASA A900-Controller und NVRAM-Module ²
AFF A700	AFF A900-Controller und NVRAM-Module ²
FAS9000	FAS9500 Controller- und NVRAM-Module ²

¹ beim Austausch von Controller-Modulen verschieben Sie alle Verbindungen vom alten zum Ersatz-Controller-Modul.

² beim Austauschen des Controllers und der NVRAM-Module verschieben Sie nur die Konsole und die Managementverbindungen.

Schritte

1. Wenn Sie NSE-Laufwerke (NetApp Storage Encryption) installiert haben, 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>



FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.

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](#)".

2. Starten Sie den Knoten im Startmenü:

```
boot_ontap menu
```

3. Weisen Sie die alten node1-Festplatten dem Ersatznode1 neu zu, indem Sie „22/7“ eingeben und die versteckte Option auswählen `boot_after_controller_replacement` Wenn der Node im Boot-Menü angehalten wird.

Nach einer kurzen Verzögerung werden Sie aufgefordert, den Namen des Node einzugeben, der ersetzt wird. Wenn gemeinsam genutzte Festplatten vorhanden sind (auch Advanced Disk Partitioning (ADP) oder partitionierte Festplatten), werden Sie aufgefordert, den Node-Namen des HA-Partners einzugeben.

Diese Eingabeaufforderungen sind möglicherweise in den Konsolenmeldungen verborgen. Wenn Sie keinen Node-Namen eingeben oder einen falschen Namen eingeben, werden Sie aufgefordert, den Namen erneut einzugeben.

Wenn `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive` Und oder
`[localhost:diskown.errorDuringIO:error]: error 3 (disk failed) on disk` Fehler auftreten, führen Sie die folgenden Schritte aus:



- a. Halten Sie den Node an der LOADER-Eingabeaufforderung an.
- b. Prüfen und setzen Sie die Storage Encryption Boot-Optionen zurück, die in erwähnt sind [Schritt 1](#).
- c. An der Loader-Eingabeaufforderung booten Sie:

```
boot_ontap
```

Das folgende Beispiel kann als Referenz verwendet werden:

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 node1 disks.
Fetched 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:

```




Die im vorhergehenden Beispiel gezeigten System-IDs sind Beispiel-IDs. Die tatsächlichen System-IDs der Nodes, die Sie aktualisieren, unterscheiden sich.

Zwischen der Eingabe von Node-Namen an der Eingabeaufforderung und der Eingabeaufforderung für die Anmeldung wird der Node mehrmals neu gebootet, um die Umgebungsvariablen wiederherzustellen, die Firmware auf den im System verwendeten Karten zu aktualisieren und für andere ONTAP Updates zu sorgen.

Überprüfen Sie die Installation node1

Sie müssen die Installation von node1 mit den Ersatz-Systemmodulen überprüfen. Da keine Änderung an physischen Ports vorgenommen wird, sind Sie nicht verpflichtet, die physischen Ports von der alten Knoten1 auf den Ersatz-Knoten1 zuzuordnen.

Über diese Aufgabe

Nachdem Sie node1 mit dem Ersatz-Controller-Modul gestartet haben, überprüfen Sie, ob es richtig installiert ist. Sie müssen warten, bis node1 dem Quorum beitreten und dann den Controller-Ersatzvorgang fortsetzen.

An diesem Punkt in der Prozedur sollte der Upgrade-Vorgang des Controllers angehalten sein, da node1 versucht hat, Quorum automatisch beizutreten.

Schritte

1. Vergewissern Sie sich, dass node1 dem Quorum beigetreten ist:

```
cluster show -node node1 -fields health
```

Die Ausgabe des `health` Feld muss sein `true`.

2. Vergewissern Sie sich, dass node1 Teil desselben Clusters wie node2 ist und dass er sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

3. Wechseln 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 Controller-Ersatzvorgang hält für Eingriffe mit der folgenden Meldung an:

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

Node	Status	Error-Action
Node1	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 Abschnitt *Neuerstellen von VLANs, ifgrps und Broadcast-Domänen* unter node1_ umbenannt.

7. Wenn sich der Controller-Austausch im Status „Pause“ befindet, fahren Sie mit fort [Stellen Sie die Netzwerkkonfiguration auf node1 wieder her](#).

Stellen Sie die Netzwerkkonfiguration auf node1 wieder her

Nachdem Sie bestätigt haben, dass node1 sich im Quorum befindet und mit node2 kommunizieren kann, überprüfen Sie, dass node1 VLANs, Interface Groups und Broadcast-Domains auf node1 gesehen werden. Überprüfen Sie außerdem, ob alle node1-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](#)" Zum Verknüpfen mit dem Inhalt *Network Management*.

Schritte

1. Listen Sie alle physischen Ports auf, die auf Upgrade-Knoten1 stehen:

```
network port show -node node1
```

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 die Entscheidung zu erleichtern, welche Ports als Ports für Schnittstellengruppen, als VLAN-Basis-Ports oder als eigenständige physische Ports zum Hosten von LIFs verwendet werden sollten.

2. Liste der Broadcast-Domänen auf dem Cluster:

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

3. Die Erreichbarkeit des Netzwerkports aller Ports auf node1 auflisten:

```
network port reachability show -node node1
```

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster::> reachability show -node node1
(network port reachability show)
Node      Port      Expected Reachability      Reachability
Status
-----
Node1
a0a       Default:Default      ok
a0a-822   Default:822          ok
a0a-823   Default:823          ok
e0M       Default:Mgmt         ok
e11a      -                    no-reachability
e11b      -                    no-reachability
e11c      -                    no-reachability
e11d      -                    no-reachability
e3a       -                    no-reachability
e3b       -                    no-reachability
e4a       Cluster:Cluster      ok
e4e       Cluster:Cluster      ok
e5a       -                    no-reachability
e7a       -                    no-reachability
e9a       Default:Default      ok
e9a-822   Default:822          ok
e9a-823   Default:823          ok
e9b       Default:Default      ok
e9b-822   Default:822          ok
e9b-823   Default:823          ok
e9c       Default:Default      ok
e9d       Default:Default      ok
22 entries were displayed.
```

Im vorherigen Beispiel wurde node1 nach dem Austausch des Controllers gebootet. Einige Ports verfügen nicht über Reachability, da es keine physische Verbindung gibt. Sie müssen alle Ports mit einem anderen Status als für die Erreichbarkeit reparieren `ok`.



Während des Upgrades sollten sich die Netzwerkports und ihre Konnektivität nicht ändern. Alle Ports sollten sich in den richtigen Broadcast-Domänen befinden, und die Erreichbarkeit des Netzwerkports sollte sich nicht ändern. Bevor Sie jedoch LIFs von node2 zurück auf node1 verschieben, müssen Sie die Erreichbarkeit und den Integritätsstatus der Netzwerk-Ports überprüfen.

4. Reparieren Sie die Erreichbarkeit für jeden Port auf node1 mit einem anderen Status als der Erreichbarkeit `ok` Mit dem folgenden Befehl in der folgenden Reihenfolge:

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

- a. Physische Ports
- b. VLAN-Ports

Die Ausgabe sollte wie im folgenden Beispiel angezeigt werden:

```
Cluster ::> reachability repair -node node1 -port e11b
```

```
Warning: Repairing port "node1:e11b" 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}:
```

Eine Warnmeldung, wie im vorhergehenden Beispiel dargestellt, wird für Ports mit einem Wiederanmeldungs-Status erwartet, die sich vom Status der Erreichbarkeit der Broadcast-Domäne unterscheiden können, in der 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. Überprüfen der Port-Erreichbarkeit:

```
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](#).

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

```
network port show
```

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

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

8. Stellen Sie die LIF-Home-Ports wieder her und geben Sie ggf. den Vserver und die LIF-Home-Ports an, die Sie mit folgenden Schritten wiederherstellen müssen:

- a. Führen Sie alle vertriebenen LIFs auf:

```
displaced-interface show
```

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

```
displaced-interface restore-home-node -node node_name -vserver vserver_name  
-lif-name LIF_name
```

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

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

Stellen Sie die Key-Manager-Konfiguration auf dem aktualisierten Node1 wieder her

Wenn Sie NetApp Aggregate Encryption (NAE) oder NetApp Volume Encryption (NVE) zur Verschlüsselung von Volumes auf dem System verwenden, das Sie aktualisieren, muss die Verschlüsselungskonfiguration mit den neuen Nodes synchronisiert werden. Wenn Sie den Schlüsselmanager nicht neu synchronisieren, wenn Sie die node1-Aggregate mithilfe von ARL von node2 zur aktualisierten node1 verschieben, können Ausfälle auftreten, da node1 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 aus node1:

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

2. Überprüfen Sie, ob der SVM-KEK-Schlüssel auf „true“ in node1 wiederhergestellt wird, bevor Sie die Datenaggregate verschieben:

```
::> security key-manager key query -node node1 -fields restored -key  
-type SVM-KEK
```

Beispiel

```
::> security key-manager key query -node node1 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node1	svml	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f0000000000000000

Verschieben Sie Aggregate und NAS-Daten-LIFs, die sich im Besitz von Knoten1 befinden, von Knoten 2 auf die aktualisierte Knoten 1

Nachdem Sie die Netzwerkkonfiguration auf Knoten 1 überprüft und bevor Sie Aggregate von Knoten 2 zu Knoten 1 verschieben, überprüfen Sie, ob die NAS-Daten-LIFs, die zu Knoten 1 gehören, die sich derzeit auf Knoten 2 befinden, von Knoten 2 zu Knoten 1 verschoben werden. Sie müssen außerdem überprüfen, ob die SAN LIFs auf Knoten1 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. Nachdem Sie node1 in den Online-Modus versetzt haben, müssen Sie überprüfen, ob sich die LIFs in einem ordnungsgemäßen Zustand und auf den entsprechenden Ports befinden.

Schritte

1. 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.

2. Durchführen einer Prüfung der Netzwerkfähigkeit:

```
network port reachability show -node node1
```

Vergewissern Sie sich, dass alle verbundenen Ports, einschließlich der Schnittstellengruppe und VLAN-Ports, ihren Status als anzeigen OK.

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, in die neue Knoten1.

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 node1 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 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.