



Boot-Medien – automatisierte Wiederherstellung

Install and maintain

NetApp
December 18, 2024

Inhalt

- Boot-Medien – automatisierte Wiederherstellung 1
 - Überblick über die automatische Boot-Medien Wiederherstellung - ASAA1K 1
 - Workflow für den Austausch von Startmedien – ASAA1K 1
 - Voraussetzungen für den Austausch von Startmedien – ASAA1K 1
 - Schalten Sie den außer Betrieb genommenen Controller - ASAA1K aus 2
 - Ersetzen Sie das Startmedium – ASAA1K 3
 - Automatische Startwiederherstellung - ASAA1K 4
 - Senden Sie das fehlerhafte Teil an NetApp - ASAA1K zurück 9

Boot-Medien – automatisierte Wiederherstellung

Überblick über die automatische Boot-Medien Wiederherstellung - ASA A1K

Sie können fehlerhafte Startmedien über die Option zum automatischen Ersetzen von Startmedien (BMR) ersetzen.

Beim automatischen Bootmedienaustausch wird das Boot-Image vom Partner-Node verwendet und automatisch die entsprechende Startmenüoption ausgeführt, um das Boot-Image auf den Ersatz-Boot-Medien zu installieren.

Workflow für den Austausch von Startmedien – ASA A1K

Führen Sie die folgenden Workflow-Schritte aus, um die Startmedien zu ersetzen.

1

"Überprüfen Sie die Anforderungen der Startmedien"

Um das Boot-Medium zu ersetzen, müssen Sie bestimmte Anforderungen erfüllen.

2

"Schalten Sie den beeinträchtigten Regler aus"

Fahren Sie den beeinträchtigten Controller herunter oder übernehmen Sie ihn, damit der funktionsunzuverlässige Controller weiterhin Daten aus dem Speicher für den beeinträchtigten Controller bereitstellen kann.

3

"Ersetzen Sie das Startmedium"

Entfernen Sie das fehlerhafte Startmedium aus dem System Management-Modul, und installieren Sie das Ersatz-Startmedium.

4

"Image auf dem Startmedium wiederherstellen (automatische Boot-Wiederherstellung)"

Stellen Sie das ONTAP-Image vom Partner-Controller wieder her.

5

"Senden Sie das fehlerhafte Teil an NetApp zurück"

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück.

Voraussetzungen für den Austausch von Startmedien – ASA A1K

Überprüfen Sie vor dem Austauschen des Startmediums die folgenden Anforderungen.

- Sie müssen die fehlerhafte Komponente durch eine vom Anbieter empfangene Ersatz-FRU-Komponente ersetzen.
- Es ist wichtig, dass Sie die Befehle in diesen Schritten auf dem richtigen Controller anwenden:
 - Der Controller *Impaired* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
 - Der *Healthy* Controller ist der HA-Partner des beeinträchtigten Controllers.
- Es dürfen keine fehlerhaften Cluster-Ports auf dem gestörten Controller vorhanden sein.

Schalten Sie den außer Betrieb genommenen Controller - ASA A1K aus

Sie müssen das Herunterfahren des außer Betrieb genommenen Controllers abschließen. Schalten Sie den außer Betrieb genommenen Controller aus oder übernehmen Sie ihn.

Um den beeinträchtigten Controller herunterzufahren, müssen Sie den Status des Controllers bestimmen und gegebenenfalls den Controller übernehmen, damit der gesunde Controller weiterhin Daten aus dem beeinträchtigten Reglerspeicher bereitstellen kann.

Über diese Aufgabe

- Wenn Sie über ein SAN-System verfügen, müssen Sie Event-Meldungen) für den beeinträchtigten Controller SCSI Blade überprüft haben `cluster kernel-service show`. Mit dem `cluster kernel-service show` Befehl (im erweiterten Modus von `priv`) werden der Knotenname, der Node, der Verfügbarkeitsstatus dieses Node und der Betriebsstatus dieses Node angezeigt "[Quorum-Status](#)".

Jeder Prozess des SCSI-Blades sollte sich im Quorum mit den anderen Nodes im Cluster befinden. Probleme müssen behoben werden, bevor Sie mit dem Austausch fortfahren.

- Wenn Sie über ein Cluster mit mehr als zwei Nodes verfügen, muss es sich im Quorum befinden. Wenn sich das Cluster nicht im Quorum befindet oder ein gesunder Controller FALSE anzeigt, um die Berechtigung und den Zustand zu erhalten, müssen Sie das Problem korrigieren, bevor Sie den beeinträchtigten Controller herunterfahren; siehe "[Synchronisieren eines Node mit dem Cluster](#)".

Schritte

1. Wenn AutoSupport aktiviert ist, können Sie die automatische Case-Erstellung durch Aufrufen einer AutoSupport Meldung unterdrücken: `system node autosupport invoke -node * -type all -message MAINT=<# of hours>h`

Die folgende AutoSupport Meldung unterdrückt die automatische Erstellung von Cases für zwei Stunden: `cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Deaktivieren Sie das automatische Giveback von der Konsole des Controller mit dem ordnungsgemäßen Zustand: `storage failover modify -node local -auto-giveback false`



Wenn Sie sehen *Möchten Sie Auto-Giveback deaktivieren?*, geben Sie ein `y`.

3. Nehmen Sie den beeinträchtigten Controller zur LOADER-Eingabeaufforderung:

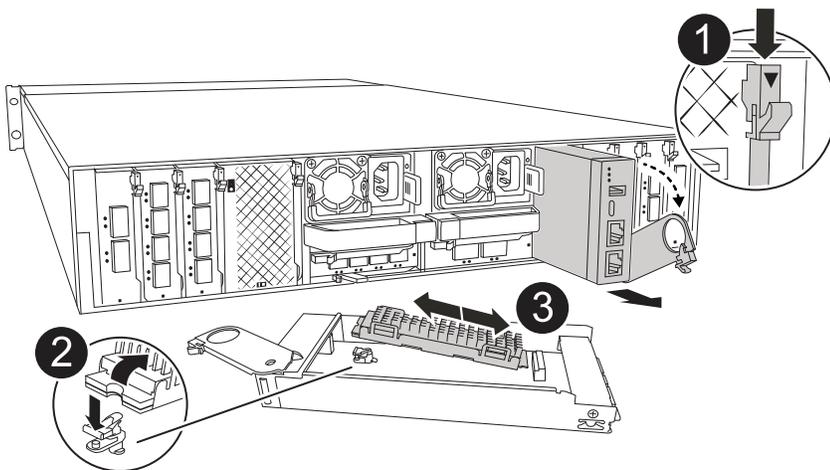
Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback...	Drücken Sie Strg-C, und antworten Sie dann <code>y</code> Wenn Sie dazu aufgefordert werden.
Eingabeaufforderung für das System oder Passwort	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: <code>storage failover takeover -ofnode impaired_node_name</code> Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

Ersetzen Sie das Startmedium – ASA A1K

Um das Startmedium zu ersetzen, müssen Sie das System Management-Modul von der Rückseite des Systems entfernen, das gestörte Startmedium entfernen und das Ersatz-Startmedium im System Management-Modul installieren.

Schritte

Das Startmedium befindet sich im System Management-Modul und kann durch Entfernen des Moduls aus dem System aufgerufen werden.



1	Nockenverriegelung des Systemmanagementmoduls
2	Verriegelungstaste für Startmedien
3	Boot-Medien

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Ziehen Sie die Netzteilkabel von den Netzteilen vom Controller ab.



Wenn Ihr Speichersystem über Gleichstromnetzteile verfügt, trennen Sie den Stromkabelblock von den Netzteilen.

- a. Entfernen Sie alle Kabel, die am System Management-Modul angeschlossen sind. Stellen Sie sicher, dass Sie den Ort kennzeichnen, an dem die Kabel angeschlossen wurden, damit Sie sie bei der Neuinstallation des Moduls an die richtigen Anschlüsse anschließen können.
 - b. Drehen Sie das Kabelführungs-Fach nach unten, indem Sie die Tasten an beiden Seiten an der Innenseite des Kabelführungs-Fachs ziehen und das Fach dann nach unten drehen.
 - c. Drücken Sie die CAM-Taste für die Systemverwaltung.
 - d. Drehen Sie die Nockenverriegelung so weit wie möglich nach unten.
 - e. Entfernen Sie das System-Management-Modul aus dem Gehäuse, indem Sie den Finger in die Öffnung des Nockenhebels stecken und das Modul aus dem Gehäuse ziehen.
 - f. Platzieren Sie das System-Management-Modul auf einer antistatischen Matte, damit das Startmedium zugänglich ist.
3. Entfernen Sie das Startmedium aus dem Verwaltungsmodul:
 - a. Drücken Sie die blaue Verriegelungstaste.
 - b. Drehen Sie das Startmedium nach oben, schieben Sie es aus dem Sockel und legen Sie es beiseite.
 4. Installieren Sie das Ersatz-Startmedium im System Management-Modul:
 - a. Richten Sie die Kanten der Startmedien am Buchsengehäuse aus, und schieben Sie sie vorsichtig in die Buchse.
 - b. Drehen Sie das Startmedium nach unten in Richtung Verriegelungstaste.
 - c. Drücken Sie die Verriegelungstaste, drehen Sie die Manschettenmedien ganz nach unten, und lassen Sie dann die Verriegelungstaste los.
 5. Installieren Sie das System Management-Modul neu.
 - a. Richten Sie das Modul an den Kanten der Öffnung des Gehäusesteckplatzes aus.
 - b. Schieben Sie das Modul vorsichtig in den Steckplatz bis zum Gehäuse, und drehen Sie dann die Nockenverriegelung ganz nach oben, um das Modul zu verriegeln.
 6. Drehen Sie das Kabelführungs-Fach bis in die geschlossene Position.
 - a. System-Management-Modul erneut verwenden.

Automatische Startwiederherstellung - ASA A1K

Stellen Sie das ONTAP-Image vom Partnerknoten wieder her, wenn das Boot-Medium beschädigt ist.

Über diese Aufgabe

Wenn das Boot-Medium eines Node beschädigt ist, wird der Boot-Prozess an der Loader-Eingabeaufforderung angehalten und Boot-Fehlermeldungen angezeigt.

Wenn diese Boot-Fehlermeldungen angezeigt werden, müssen Sie das ONTAP-Image vom Partner-Node wiederherstellen.

Zeigt ein Beispiel für Boot-Fehlermeldungen an

```
Can't find primary boot device u0a.0
Can't find backup boot device u0a.1
ACPI RSDP Found at 0x777fe014

Starting AUTOBOOT press Ctrl-C to abort...
Could not load fat://boot0/X86_64/freebsd/image1/kernel: Device not
found

ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/Linux/image1/vmlinuz (boot0, fat)
ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/freebsd/image1/kernel (boot0, fat)

Autoboot of PRIMARY image failed. Device not found (-6)
LOADER-A>
```

Schritte

1. Geben Sie an der Loader-Eingabeaufforderung den Befehl ein:

```
boot_recovery -partner
```

Auf dem Bildschirm wird die folgende Meldung angezeigt:

```
Starting boot media recovery (BMR) process. Press Ctrl-C to abort...
```

2. Überwachen Sie den Recovery-Prozess für Startmedien, während Loader die lokalen Cluster-Ports konfiguriert und vom Partner-Node aus ausgeführt `netboot` wird.

Wenn Netzboot ausgeführt wird, wird die `Starting BMR` Meldung angezeigt.

3. Wählen Sie je nach Verschlüsselungsmethode die Option aus, die Ihrer Systemkonfiguration entspricht:

Keine Verschlüsselung

Wenn keine Verschlüsselung erkannt wird, wird der Wiederherstellungsvorgang des Startmediums ohne Schlüsselmanagement fortgesetzt.

- a. Überwachen Sie den Wiederherstellungsprozess weiter, während die Backup-Konfiguration, die env-Datei, mdb und rdb vom Partner-Node wiederhergestellt werden.
- b. Nach Abschluss der Wiederherstellung wird der Node neu gebootet. Die folgenden Meldungen weisen auf eine erfolgreiche Wiederherstellung hin:

```
varfs_backup_restore: update checksum for varfs.tgz
varfs_backup_restore: restore using
/cfcard/x86_64/freebsd/oldvarfs.tgz
varfs_backup_restore: Rebooting to load the new varfs
.
Terminated
varfs_backup_restore: bootarg.abandon_varfs is set! Skipping /var
backup.
```

- a. Wenn der Node neu gebootet wird, überprüfen Sie, ob die Boot-Medien erfolgreich wiederhergestellt wurden, indem Sie bestätigen, dass das System wieder online und funktionsfähig ist.
- b. Stellen Sie den funktionsbeeinträchtigten Controller wieder in den Normalbetrieb ein, indem Sie den Speicher zurückgeben:

```
storage failover giveback -ofnode impaired_node_name.
```

Onboard Key Manager (OKM)

Wenn Onboard Key Manager (OKM) erkannt wird, zeigt das System die folgende Eingabeaufforderung an.

```
key manager is configured.
Entering Bootmenu Option 10...

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

- a. Geben Sie in der Eingabeaufforderung Bootmenu die Option Bootmedia Recovery ein `Y`, um zu bestätigen, dass Sie die Bootmedia Recovery-Option verwenden möchten.
- b. Geben Sie die Passphrase für Onboard Key Manager ein, wenn Sie dazu aufgefordert werden, und geben Sie die Passphrase erneut ein, um sie zu bestätigen.

Beispiel für Passphrase-Eingabeaufforderungen anzeigen

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
Enter the backup data:
TmV0QXBwIEtleSBCbG9iAAECAAAEAAAAcAEAAAAAAAAA3yR6UAAAAACEAAAAAAAA
AA
QAAAAAAAAACJz1u2AAAAAPX84XY5AU0p4Jcb9t8wiwOZoqyJPJ4L6/j5FHJ9yj
/w
RVDO1sZB1E4HO79/zYc82nBwtiHaSPWCbkCrMWuQQDsiAAAAAAAAACgAAAAAAA
AA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAGAZJEIWvdeHr5RCavHGclo+wAAAAAAAA
AA
IgAAAAAAAAoAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAJAGr3tJA/LR
zU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAGAAAAAAAAABHVFpxAAAAAHUgdVq0EK
Np
.
.
.
.
```

- c. Überwachen Sie den Wiederherstellungsprozess weiter, während die Backup-Konfiguration, die env-Datei, mdb und rdb vom Partner-Node wiederhergestellt werden.

Nach Abschluss der Wiederherstellung wird der Node neu gebootet. Die folgenden Meldungen weisen auf eine erfolgreiche Wiederherstellung hin:

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.
```

- d. Wenn der Node neu gebootet wird, überprüfen Sie, ob die Boot-Medien erfolgreich wiederhergestellt wurden, indem Sie bestätigen, dass das System wieder online und funktionsfähig ist.
- e. Stellen Sie den funktionsbeeinträchtigten Controller wieder in den Normalbetrieb ein, indem Sie den Speicher zurückgeben:

```
storage failover giveback -ofnode impaired_node_name.
```

- f. Führen Sie nach dem Booten nur mit dem CFO-Aggregat den folgenden Befehl aus.

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

Externer Schlüsselmanager (EKM)

Wenn EKM konfiguriert ist, zeigt das System die folgende Eingabeaufforderung an.

```
Error when fetching key manager config from partner <IP>:  
  
Has key manager been configured on this system? {y|n}
```

- a. Geben Sie ein `y`, wenn EKM konfiguriert wurde.

```
key manager is configured.  
Entering Bootmenu Option 11...
```

Sie werden aufgefordert, die EKM-Einstellungen einzugeben, die beim Einrichten verwendet wurden.

- b. Geben Sie jede EKM-Konfigurationseinstellung ein, wenn Sie dazu aufgefordert werden.
c. Überprüfen Sie, ob die Attribute für die Cluster-UUID und die Keystore-UUID korrekt sind.

- Rufen Sie auf dem Partner-Node die Cluster-UUID mit dem folgenden Befehl ab.

```
cluster identity show
```

- Rufen Sie auf dem Partner-Node die Keystore-UUID mit den folgenden Befehlen ab.

```
vserver show -type admin -fields uuid
```

```
key-manager keystore show -vserver <nodename>
```

- Wenn der Partner-Node nicht verfügbar ist, verwenden Sie den Mroot-AK-Schlüssel, um die UUID abzurufen:

- Geben Sie für die Cluster-UUID den folgenden Befehl ein:

```
x-NETAPP-ClusterName: <cluster name>
```

- Geben Sie für die Keystore-UUID den folgenden Befehl ein:

```
x-NETAPP-KeyUsage: MROOT-AK
```

- d. Geben Sie bei der entsprechenden Aufforderung die Werte für Keystore-UUID und Cluster-UUID ein.
- e. Je nachdem, ob der Schlüssel erfolgreich wiederhergestellt wurde, führen Sie eine der folgenden Aktionen durch:
- Wenn der Schlüssel erfolgreich wiederhergestellt wurde, wird der Wiederherstellungsprozess fortgesetzt und der Knoten neu gestartet. Fahren Sie mit Schritt 4 fort.
 - Wenn der Schlüssel nicht erfolgreich wiederhergestellt wurde, hält das System an und zeigt

Fehler- und Warnmeldungen an. Führen Sie den Wiederherstellungsprozess erneut aus.

Zeigt ein Beispiel für Fehler und Warnmeldungen bei der Schlüsselwiederherstellung an

```
ERROR: kmip_init: halting this system with encrypted
mroot...

WARNING: kmip_init: authentication keys might not be
available.

System cannot connect to key managers.

ERROR: kmip_init: halting this system with encrypted
mroot...

Terminated

Uptime: 11m32s

System halting...

LOADER-B>
```

- f. Wenn der Node neu gebootet wird, überprüfen Sie, ob die Boot-Medien erfolgreich wiederhergestellt wurden, indem Sie bestätigen, dass das System wieder online und funktionsfähig ist.
- g. Stellen Sie den funktionsbeeinträchtigten Controller wieder in den Normalbetrieb ein, indem Sie den Speicher zurückgeben:

```
storage failover giveback -ofnode impaired_node_name.
```

4. Wenn die automatische Rückübertragung deaktiviert wurde, aktivieren Sie sie erneut:

```
storage failover modify -node local -auto-giveback true.
```

5. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fehlerstellung wieder her:

```
system node autosupport invoke -node * -type all -message MAINT=END.
```

Senden Sie das fehlerhafte Teil an NetApp - ASA A1K zurück

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück. ["Rückgabe und Austausch von Teilen"](#) Weitere Informationen finden Sie auf der Seite.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.