



Managen von Nodes

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

- Managen von Nodes 1
 - Zeigen Sie Node-Attribute an 1
 - Ändern von Node-Attributen 1
 - Benennen Sie einen Node um 2
 - Fügen Sie dem Cluster Nodes hinzu 2
 - Entfernen Sie die Nodes aus dem Cluster 5
 - Greifen Sie auf einen Knoten Protokoll, Core Dump, und MIB-Dateien mit einem Web-Browser 7
 - Greifen Sie auf die Systemkonsole eines Node zu 8
 - Regeln für Root-Volumes und Root-Aggregate der Nodes 10
 - Starten oder stoppen Sie einen Node 13
 - Verwalten Sie einen Knoten über das Startmenü 16
 - Verwalten Sie einen Node per Remote-Zugriff über den SP/BMC 19

Managen von Nodes

Zeigen Sie Node-Attribute an

Sie können die Attribute eines oder mehrerer Nodes im Cluster anzeigen, z. B. Name, Eigentümer, Standort Modellnummer, Seriennummer, Dauer des Node-Betriebs, Systemzustand und Teilnahmeberechtigung an einem Cluster.

Schritte

1. Um die Attribute eines angegebenen Node oder über alle Nodes in einem Cluster anzuzeigen, verwenden Sie den `system node show` Befehl.

Beispiel zum Anzeigen von Informationen über einen Node

Im folgenden Beispiel werden ausführliche Informationen über `node1` angezeigt:

```
cluster1::> system node show -node node1
      Node: node1
      Owner: Eng IT
      Location: Lab 5
      Model: model_number
      Serial Number: 12345678
      Asset Tag: -
      Uptime: 23 days 04:42
      NVRAM System ID: 118051205
      System ID: 0118051205
      Vendor: NetApp
      Health: true
      Eligibility: true
      Differentiated Services: false
      All-Flash Optimized: true
      Capacity Optimized: false
      QLC Optimized: false
      All-Flash Select Optimized: false
      SAS2/SAS3 Mixed Stack Support: none
```

Ändern von Node-Attributen

Sie können die Attribute eines Node nach Bedarf ändern. Zu den Attributen, die Sie ändern können, gehören die Besitzinformationen des Node, die Ortinformationen, das Asset-Tag und die Berechtigung, am Cluster teilzunehmen.

Über diese Aufgabe

Die Berechtigung eines Node, um am Cluster teilzunehmen, kann auf der erweiterten Berechtigungsebene mithilfe von geändert werden `-eligibility` Parameter von `system node modify` Oder `cluster modify` Befehl. Wenn Sie die Berechtigung eines Node auf festlegen `false`, Der Knoten wird im Cluster

inaktiv.



Sie können die Node-Berechtigung nicht lokal ändern. Er muss von einem anderen Node geändert werden. Auch bei einer Cluster-HA-Konfiguration kann die Node-eligibility nicht geändert werden.



Sie sollten vermeiden, die Berechtigung eines Node auf einzustellen `false`, Mit Ausnahme von Situationen wie Wiederherstellen der Node-Konfiguration oder verlängerte Node-Wartung. DER SAN- und NAS-Datenzugriff auf den Node kann davon betroffen sein, wenn der Node nicht verfügbar ist.

Schritte

1. Verwenden Sie die `system node modify` Befehl zum Ändern der Attribute eines Node.

Beispiel zum Ändern von Node-Attributen

Mit dem folgenden Befehl werden die Attribute des Node „node1“ geändert. Der Eigentümer des Knotens ist auf „Joe Smith“ eingestellt und die Asset-Tag-Nummer ist auf „js1234“ eingestellt:

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag js1234
```

Benennen Sie einen Node um

Sie können den Namen eines Node nach Bedarf ändern.

Schritte

1. Verwenden Sie zum Umbenennen eines Node die `system node rename` Befehl.

Der `-newname` Der Parameter gibt den neuen Namen für den Node an. Der `system node rename` Auf der man-Page werden die Regeln zur Angabe des Node-Namens beschrieben.

Wenn Sie mehrere Nodes im Cluster umbenennen möchten, müssen Sie den Befehl für jeden Node einzeln ausführen.



Der Node-Name kann nicht „all“ sein, da „all“ ein Systemname ist.

Beispiel für die Umbenennung eines Node

Mit dem folgenden Befehl wird der Node „node1“ in „node1a“ umbenannt:

```
cluster1::> system node rename -node node1 -newname node1a
```

Fügen Sie dem Cluster Nodes hinzu

Nach dem Erstellen eines Clusters können Sie die Erweiterung durch Hinzufügen von Nodes erweitern. Sie fügen jeweils nur einen Node hinzu.

Was Sie benötigen

- Wenn Sie einem Cluster mit mehreren Nodes Nodes hinzufügen, muss mehr als die Hälfte der im Cluster vorhandenen Nodes einen ordnungsgemäßen Zustand aufweisen (angegeben von) `cluster show`).
- Wenn Sie einem 2-Node-Cluster ohne Switches Nodes hinzufügen, müssen Sie die Cluster-Management- und Interconnect-Switches installiert und konfiguriert haben, bevor Sie zusätzliche Nodes hinzufügen.

Die Cluster-Funktion ohne Switches wird nur in einem Cluster mit zwei Nodes unterstützt.

Wenn ein Cluster mehr als zwei Nodes enthält oder vergrößert, ist keine Cluster-HA erforderlich und wird automatisch deaktiviert.

- Wenn Sie einem Single-Node-Cluster einen zweiten Node hinzufügen, muss der zweite Node installiert sein und das Cluster-Netzwerk konfiguriert sein.
- Wenn die automatische SP-Konfiguration auf dem Cluster aktiviert ist, muss das für den SP angegebene Subnetz über verfügbare Ressourcen für den Verbindungsknoten verfügen.

Ein Node, der dem Cluster hinzugefügt wird, verwendet das angegebene Subnetz, um die automatische Konfiguration für den SP durchzuführen.

- Sie müssen die folgenden Informationen für die Node-Management-LIF des neuen Node gesammelt haben:
 - Port
 - IP-Adresse
 - Netzmaske
 - Standard-Gateway

Über diese Aufgabe

Nodes müssen sich in geraden Zahlen befinden, damit sie zu HA-Paaren führen können. Nachdem Sie begonnen haben, dem Cluster einen Node hinzuzufügen, müssen Sie den Prozess abschließen. Der Node muss Teil des Clusters sein, bevor Sie mit dem Hinzufügen eines weiteren Node beginnen können.

Schritte

1. Schalten Sie den Node ein, den Sie dem Cluster hinzufügen möchten.

Der Node wird gebootet, und der Node Setup-Assistent wird auf der Konsole gestartet.

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0c]:
```

2. Beenden Sie den Knoten-Setup-Assistenten: `exit`

Der Knoten-Setup-Assistent wird beendet, und es wird eine Anmeldeaufforderung angezeigt. Sie werden gewarnt, dass Sie die Einrichtungsaufgaben nicht abgeschlossen haben.

3. Loggen Sie sich mit dem beim Administratorkonto ein `admin` Benutzername:

4. Starten Sie den Cluster Setup-Assistenten:

cluster setup

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
<https://10.63.11.29>

Otherwise, press Enter to complete cluster setup using the
command line interface:



Weitere Informationen zum Einrichten eines Clusters mit der Setup-GUI finden Sie im "[System Manager](#)" Online-Hilfe.

5. Drücken Sie die Eingabetaste, um die CLI zum Abschließen dieser Aufgabe zu verwenden. Wenn Sie dazu aufgefordert werden, ein neues Cluster zu erstellen oder einem vorhandenen Cluster beizutreten, geben Sie ein **join**.

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:  
join
```

6. Befolgen Sie die Anweisungen, um den Node einzurichten und mit dem Cluster zu verbinden:

- Um den Standardwert für eine Eingabeaufforderung zu akzeptieren, drücken Sie die Eingabetaste.
- Um Ihren eigenen Wert für eine Eingabeaufforderung einzugeben, geben Sie den Wert ein, und drücken Sie dann die Eingabetaste.

7. Wiederholen Sie die vorherigen Schritte für jeden weiteren Node, den Sie hinzufügen möchten.

Nachdem Sie fertig sind

Nachdem Sie dem Cluster Nodes hinzugefügt haben, sollten Sie für jedes HA-Paar ein Storage-Failover aktivieren.

Entfernen Sie die Nodes aus dem Cluster

Sie können nicht benötigte Nodes gleichzeitig von einem Cluster und einem Node entfernen. Nachdem Sie einen Node entfernt haben, müssen Sie auch seinen Failover-Partner entfernen. Wenn Sie einen Node entfernen, können seine Daten auf nicht mehr zugegriffen oder gelöscht werden.

Bevor Sie beginnen

Die folgenden Bedingungen müssen erfüllt sein, bevor die Nodes aus dem Cluster entfernt werden:

- Mehr als die Hälfte der Nodes im Cluster muss sich in einem ordnungsgemäßen Zustand befinden.
- Alle Daten auf dem Node, den Sie entfernen möchten, müssen evakuiert worden sein.
 - Dies kann auch sein ["Daten werden aus einem verschlüsselten Volume entfernt"](#).
- Alle Volumes waren ["Verschoben"](#) Oder ["Gelöscht"](#) Von Aggregaten, die dem Node gehören.
- Alle Aggregate wurden verwendet ["Gelöscht"](#) Vom Node.
- Wenn der Node Eigentümer von FIPS-Festplatten (Federal Information Processing Standards) oder Self-Encrypting Drives (SEDs) ist, ["Die Festplattenverschlüsselung wurde entfernt"](#) Indem die Festplatten in den ungeschützten Modus versetzt werden.
 - Dies könnte Sie auch interessieren ["FIPS-Laufwerke oder SEDs reinigen"](#).
- Daten-LIFs wurden ["Gelöscht"](#) Oder ["Umgezogen"](#) Vom Node.
- Die Cluster-Management-LIFs wurden ["Umgezogen"](#) Vom Node und den Home-Ports geändert.
- Alle Intercluster LIFs wurden ["Entfernt"](#).
 - Wenn Sie Intercluster LIFs entfernen, wird eine Warnung angezeigt, die ignoriert werden kann.
- Storage-Failover war ["Deaktiviert"](#) Für den Node.
- Alle LIF Failover-Regeln waren ["Geändert"](#) Um Ports auf dem Node zu entfernen.
- Alle VLANs auf dem Node waren ["Gelöscht"](#).
- Wenn auf dem Node LUNs entfernt werden sollen, sollten Sie dies tun ["Ändern Sie die Liste Selective LUN Map \(SLM\) Reporting-Nodes"](#) Bevor Sie den Node entfernen.

Wenn Sie den Node und dessen HA-Partner nicht aus der Liste der SLM-Reporting-Nodes entfernen, kann der Zugriff auf die LUNs, die sich zuvor auf dem Node befanden, verloren gehen, obwohl die Volumes, die die LUNs enthalten, auf einen anderen Node verschoben wurden.

Es wird empfohlen, eine AutoSupport Meldung zu senden, um den technischen Support von NetApp zu benachrichtigen, dass derzeit ein Entfernen von Nodes ausgeführt wird.

Hinweis: Sie dürfen keine Vorgänge wie durchführen `cluster remove-node`, `cluster unjoin`, und `node rename` Lläuft ein automatisiertes ONTAP Upgrade.

Über diese Aufgabe

Wenn Sie ein Cluster mit gemischten Versionen ausführen, können Sie den letzten Node niedriger Versionen

mithilfe eines der erweiterten Berechtigungsbefehle, beginnend mit ONTAP 9.3, entfernen:

- ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
- ONTAP 9.4 und höher: `cluster remove-node -skip-last-low-version-node-check`

Hinweis: Alle System- und Benutzerdaten von allen Festplatten, die mit dem Knoten verbunden sind, müssen Benutzern zugänglich gemacht werden, bevor ein Knoten aus dem Cluster entfernt wird. Wenn ein Node nicht ordnungsgemäß von einem Cluster entfernt wurde, wenden Sie sich an den NetApp Support, um Hilfe bei Optionen zur Recovery zu erhalten.

Schritte

1. Ändern Sie die Berechtigungsebene in erweitert:

```
set -privilege advanced
```

2. Wenn der Node, den Sie entfernen möchten, der aktuelle Master-Node ist, aktivieren Sie dann einen anderen Node im Cluster, der als Master-Node ausgewählt werden soll, indem Sie die Cluster-Berechtigung des Master-Node auf ändern `false`:

```
cluster modify -eligibility false
```

Der Master-Node ist der Node mit Prozessen wie „mgmt“, „vldb“, „vifmgr“, „bcomd“ und „crs“. Der `cluster ring show` Der erweiterte Befehl zeigt den aktuellen Master-Node an.

```
cluster::*> cluster modify -node node1 -eligibility false
```

3. Melden Sie sich bei der Remote-Node-Management-LIF oder der Cluster-Management-LIF auf einem anderen Node an als dem, der entfernt wird.
4. Entfernen des Node aus dem Cluster:

Für diese ONTAP-Version...	Befehl
ONTAP 9.3	cluster unjoin
ONTAP 9.4 und höher	cluster remove-node

Wenn Sie über ein Cluster mit gemischter Version verfügen und den Node mit der letzten niedrigeren Version entfernen, verwenden Sie das `-skip-last-low-version-node-check` Parameter mit diesen Befehlen.

Das System informiert Sie über Folgendes:

- Außerdem müssen Sie den Failover-Partner des Node aus dem Cluster entfernen.
- Nachdem der Node entfernt wurde und bevor er einem Cluster erneut beitreten kann, müssen Sie die Startmenü-Option (4) Clean Configuration verwenden und alle Festplatten oder Optionen (9) Configure Advanced Drive Partitioning initialisieren, um die Konfiguration des Node zu löschen und alle Festplatten zu initialisieren.

Wenn die Bedingungen angegeben sind, die Sie vor dem Entfernen des Node berücksichtigen

müssen, wird eine Fehlermeldung generiert. Beispielsweise könnte die Meldung angeben, dass der Node über gemeinsam genutzte Ressourcen verfügt, die Sie entfernen müssen, oder dass sich der Node in einer Cluster HA-Konfiguration oder in einer Storage-Failover-Konfiguration befindet, die Sie deaktivieren müssen.

Wenn der Knoten der Quorum-Master ist, verliert der Cluster kurz und kehrt dann zum Quorum zurück. Dieser Quorum-Verlust ist temporär und hat keine Auswirkungen auf Datenoperationen.

5. Wenn eine Fehlermeldung Fehlerbedingungen anzeigt, beheben Sie diese Bedingungen und führen Sie den erneut aus `cluster remove-node` Oder `cluster unjoin` Befehl.

Der Node wird automatisch neu gebootet, wenn er erfolgreich aus dem Cluster entfernt wurde.

6. Löschen Sie bei einer Neuordnung des Node die Node-Konfiguration und initialisieren Sie alle Festplatten:
 - a. Drücken Sie während des Bootens Strg-C, um das Boot-Menü anzuzeigen, wenn Sie dazu aufgefordert werden.
 - b. Wählen Sie die Startmenü-Option **(4) Konfiguration reinigen und initialisieren Sie alle Festplatten**.
7. Zurück zur Administrator-Berechtigungsebene:

```
set -privilege admin
```

8. Wiederholen Sie die vorherigen Schritte, um den Failover-Partner aus dem Cluster zu entfernen.

Nachdem Sie fertig sind

Wenn Sie Nodes entfernt haben, um ein Single-Node-Cluster zu haben, sollten Sie die Cluster-Ports ändern, um Datenverkehr bereitzustellen, indem Sie die Cluster-Ports als Daten-Ports ändern und dann Daten-LIFs für die Daten-Ports erstellen.

Greifen Sie auf einen Knoten Protokoll, Core Dump, und MIB-Dateien mit einem Web-Browser

Die Service Processor Infrastruktur (`spi`) Web-Service ist standardmäßig aktiviert, um einen Webbrowser zu aktivieren, um auf die Log-, Core Dump- und MIB-Dateien eines Knotens im Cluster zugreifen. Der Zugriff auf die Dateien bleibt auch dann möglich, wenn der Node ausfällt, wenn der Node vom Partner übernommen wird.

Was Sie benötigen

- Die Cluster-Management-LIF muss aktiv sein.

Sie können die Management-LIF des Clusters oder einen Node verwenden, um auf die zuzugreifen `spi` Webservice: Allerdings wird die Verwendung der Cluster-Management-LIF empfohlen.

Der `network interface show` Befehl zeigt den Status aller LIFs im Cluster an.

- Sie müssen ein lokales Benutzerkonto verwenden, um auf das zugreifen zu können `spi` Webservice, Domänenbenutzerkonten werden nicht unterstützt.
- Wenn Ihr Benutzerkonto nicht über die Rolle „admin“ verfügt (die Zugriff auf das hat `spi` Webservice standardmäßig), muss Ihre Zugriffskontrollrolle Zugriff auf die gewährt werden `spi` Webservice:

Der `vserver services web access show` Befehl zeigt an, welche Rollen Zugriff auf welche Webservices erhalten.

- Wenn Sie das „admin“-Benutzerkonto nicht verwenden (das umfasst das `http` Zugriffsmethode standardmäßig) muss Ihr Benutzerkonto mit dem eingerichtet werden `http` Zugriffsmethode.

Der `security login show` Mit dem Befehl werden die Zugriffs- und Anmeldemethoden für Benutzerkonten und ihre Zugriffssteuerungsrollen angezeigt.

- Wenn Sie HTTPS für sicheren Webzugriff verwenden möchten, muss SSL aktiviert und ein digitales Zertifikat installiert werden.

Der `system services web show` Befehl zeigt die Konfiguration der Web Protocol Engine auf Cluster-Ebene an.

Über diese Aufgabe

Der `spi` Der Webdienst ist standardmäßig aktiviert, und der Dienst kann manuell deaktiviert werden (`vserver services web modify -vserver * -name spi -enabled false`).

Die Rolle „admin“ erhält Zugriff auf das `spi` Der Webdienst ist standardmäßig aktiviert, und der Zugriff kann manuell deaktiviert werden (`services web access delete -vserver cluster_name -name spi -role admin`).

Schritte

1. Rufen Sie den im Webbrowser auf `spi` Webservice-URL in einem der folgenden Formate:

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` Ist die IP-Adresse der Cluster-Management-LIF.

2. Wenn Sie vom Browser dazu aufgefordert werden, geben Sie Ihr Benutzerkonto und Ihr Passwort ein.

Nach der Authentifizierung Ihres Kontos zeigt der Browser Links zum an `/mroot/etc/log/`, `/mroot/etc/crash/`, und `/mroot/etc/mib/` Verzeichnisse jedes Node im Cluster.

Greifen Sie auf die Systemkonsole eines Node zu

Wenn ein Node im Boot-Menü oder an der Eingabeaufforderung für die Boot-Umgebung hängt, können Sie ihn nur über die Systemkonsole aufrufen (auch „*Serial Console*“). Sie können von einer SSH-Verbindung zum SP des Node oder zum Cluster auf die Systemkonsole eines Node zugreifen.

Über diese Aufgabe

Sowohl der SP als auch die ONTAP bieten Befehle, mit denen Sie auf die Systemkonsole zugreifen können. Über den SP können Sie jedoch nur auf die Systemkonsole seines eigenen Node zugreifen. Über das Cluster können Sie auf die Systemkonsole jedes Node im Cluster zugreifen.

Schritte

1. Zugriff auf die Systemkonsole eines Node:

Wenn Sie im...	Diesen Befehl eingeben...
SP-CLI des Node	<code>system console</code>
CLI VON ONTAP	<code>system node run-console</code>

2. Melden Sie sich bei der Systemkonsole an, wenn Sie dazu aufgefordert werden.
3. Um die Systemkonsole zu verlassen, drücken Sie Strg-D

Beispiele für den Zugriff auf die Systemkonsole

Das folgende Beispiel zeigt das Ergebnis der Eingabe des `system console` Befehl an der Eingabeaufforderung „SP node2“. Die Systemkonsole zeigt an, dass node2 an der Eingabeaufforderung für die Boot-Umgebung hängt. Der `boot_ontap` Der Befehl wird an der Konsole eingegeben, um den Node für ONTAP zu booten. Strg-D wird dann gedrückt, um die Konsole zu verlassen und zum SP zurückzukehren.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
...
```

(Strg-D gedrückt wird, um die Systemkonsole zu verlassen.)

```
Connection to 123.12.123.12 closed.
SP node2>
```

Das folgende Beispiel zeigt das Ergebnis der Eingabe des `system node run-console` Befehl von ONTAP zum Zugriff auf die Systemkonsole von node2, die an der Eingabeaufforderung der Boot-Umgebung hängt. Der `boot_ontap` Befehl wird an der Konsole eingegeben, um node2 to ONTAP zu booten. Strg-D wird dann gedrückt, um die Konsole zu verlassen und zur ONTAP zurückzukehren.

```

cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
...

```

(Strg-D gedrückt wird, um die Systemkonsole zu verlassen.)

```

Connection to 123.12.123.12 closed.
cluster1::>

```

Regeln für Root-Volumes und Root-Aggregate der Nodes

Regeln für Root-Volumes und Root-Aggregate der Nodes – Übersicht

Das Root-Volume eines Node enthält spezielle Verzeichnisse und Dateien für diesen Node. Das Root-Aggregat enthält das Root-Volume. Einige Regeln regeln das Root-Volume und das Root-Aggregat eines Nodes.

Das Root-Volume eines Node ist ein FlexVol-Volume, das werkseitig oder über die Setup-Software installiert wird. Er ist für Systemdateien, Log-Dateien und Core-Dateien reserviert. Der Verzeichnisname lautet `/mroot`, Die nur über die Systemshell durch technischen Support zugänglich ist. Die Mindestgröße für das Root-Volume eines Node hängt vom Plattformmodell ab.

- Die folgenden Regeln regeln das Root-Volume des Nodes:
 - Sofern Sie vom technischen Support nicht dazu aufgefordert werden, ändern Sie die Konfiguration oder den Inhalt des Root-Volumes nicht.
 - Speichern Sie keine Benutzerdaten im Root-Volume.

Das Speichern von Benutzerdaten im Root-Volume erhöht die Storage-Giveback zwischen Nodes in einem HA-Paar.

- Sie können das Root-Volume zu einem anderen Aggregat verschieben.

[Verschieben von Root-Volumes in neue Aggregate](#)

- Das Root-Aggregat ist nur dem Root-Volumen des Knotens zugewiesen.

ONTAP verhindert, dass Sie andere Volumes im Root-Aggregat erstellen.

["NetApp Hardware Universe"](#)

Freier Speicherplatz auf dem Root-Volume eines Knotens

Eine Warnmeldung wird angezeigt, wenn das Root-Volume eines Node voll oder fast voll ist. Der Knoten kann nicht ordnungsgemäß ausgeführt werden, wenn sein Root-Volume voll ist. Sie können Speicherplatz auf dem Root-Volume eines Node freigeben, indem Sie Core Dump-Dateien, Paket-Trace-Dateien und Snapshot Kopien des Root-Volumes löschen.

Schritte

1. Zeigen Sie die Core Dump-Dateien und deren Namen des Node mithilfe von `an system node coredump show` Befehl.
2. Löschen Sie unerwünschte Core Dump-Dateien vom Node mithilfe von `system node coredump delete` Befehl.
3. Zugriff auf die Hölle:

```
system node run -node nodename
```

nodename Ist der Name des Node, dessen Root-Volume-Platz Sie freigeben möchten.

4. Wechseln Sie zur nodeshell erweiterten Privilege-Ebene aus der nodeshell:

```
priv set advanced
```

5. Die Paketverfolgungsdateien des Knotens über die nodeshell anzeigen und löschen:

- a. Alle Dateien im Root-Volume des Nodes anzeigen:

```
ls /etc
```

- b. Wenn Paketverfolgungsdateien vorhanden sind (`*.trc`) Befinden sich im Root-Volume des Knotens, löschen Sie sie einzeln:

```
rm /etc/log/packet_traces/file_name.trc
```

6. Root-Volume-Snapshot-Kopien des Node über den Knotenpunkt ermitteln und löschen:

- a. Geben Sie den Namen des Root-Volumes an:

```
vol status
```

Das Root-Volume wird durch das Wort „root“ in der Spalte „Optionen“ des angezeigt `vol status` Befehlsausgabe.

Im folgenden Beispiel lautet das Root-Volume `vol10`:

```
node1*> vol status
```

Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

a. Anzeige von Root-Volume Snapshot Kopien:

```
snap list root_vol_name
```

b. Löschen unerwünschter Root-Volume Snapshot Kopien:

```
snap delete root_vol_namesnapshot_name
```

7. Verlassen Sie die nodeshell und kehren Sie zur Clustershell zurück:

```
exit
```

Verschieben von Root-Volumes in neue Aggregate

Beim Root-Austauschverfahren wird das aktuelle Root-Aggregat ohne Unterbrechung zu einem anderen Festplattensatz migriert.

Über diese Aufgabe

Storage-Failover muss aktiviert sein, um Root-Volumes zu verschieben. Sie können das verwenden `storage failover modify -node nodename -enable true` Befehl zum Aktivieren des Failovers.

Sie können den Speicherort des Root-Volumes in ein neues Aggregat in den folgenden Szenarien ändern:

- Wenn sich die Wurzelaggregate nicht auf der Festplatte befinden, die Sie bevorzugen
- Wenn Sie die mit dem Node verbundenen Festplatten neu anordnen möchten
- Wenn Sie einen Shelf-Austausch der EOS Platten-Shelves durchführen

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set privilege advanced
```

2. Verschieben des Root-Aggregats:

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-Node**

Gibt den Knoten an, der das Root-Aggregat besitzt, das Sie migrieren möchten.

- **-disklist**

Gibt die Liste der Festplatten an, auf denen das neue Root-Aggregat erstellt wird. Alle Festplatten müssen Ersatzteile und Eigentum des gleichen Knotens sein. Die Mindestanzahl der benötigten Festplatten hängt vom RAID-Typ ab.

- **-RAID-Typ**

Gibt den RAID-Typ des Root-Aggregats an. Der Standardwert ist `raid-dp`.

3. Überwachen des Fortschritts des Jobs:

```
job show -id jobid -instance
```

Ergebnisse

Wenn alle Vorprüfungen erfolgreich sind, startet der Befehl einen Ersatzauftrag für das Root-Volume und wird beendet. Erwarten Sie, dass der Node neu gestartet wird.

Starten oder stoppen Sie einen Node

Starten oder Stoppen einer Knotenübersicht

Möglicherweise müssen Sie einen Node aus Wartungs- oder Fehlerbehebungsgründen starten oder stoppen. Dies können Sie über die ONTAP CLI, die Eingabeaufforderung der Boot-Umgebung oder die SP-CLI ausführen.

Verwenden des SP-CLI-Befehls `system power off` Oder `system power cycle` Zum aus- und Wiedereinschalten eines Knotens kann es zu einem unsachgemäßen Herunterfahren des Knotens (auch als „*dirty Shutdown*“ bezeichnet) führen und nicht als Ersatz für ein graziertes Herunterfahren über die ONTAP dienen `system node halt` Befehl.

Booten Sie einen Node an der Eingabeaufforderung des Systems neu

Sie können einen Node im normalen Modus von der Eingabeaufforderung des Systems neu booten. Ein Node wird für das Booten über das Boot-Gerät, z. B. eine PC CompactFlash Card, konfiguriert.

Schritte

1. Wenn das Cluster vier oder mehr Nodes enthält, vergewissern Sie sich, dass der neu zu bootende Node das Epsilon nicht hält:

- a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

- b. Bestimmen Sie, auf welchem Node das Epsilon enthalten ist:

```
cluster show
```

Das folgende Beispiel zeigt, dass „node1“ Epsilon enthält:

```
cluster1::*> cluster show
Node           Health  Eligibility  Epsilon
-----
node1          true    true         true
node2          true    true         false
node3          true    true         false
node4          true    true         false
4 entries were displayed.
```

- a. Wenn der zu bootende Node das Epsilon hält, entfernen Sie das Epsilon vom Knoten:

```
cluster modify -node node_name -epsilon false
```

- b. Weisen Sie Epsilon einem anderen Knoten zu, der weiter oben bleibt:

```
cluster modify -node node_name -epsilon true
```

- c. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Verwenden Sie die `system node reboot` Befehl zum Neubooten des Node.

Wenn Sie den nicht angeben `-skip-lif-migration` Parameter, der Befehl versucht, vor dem Neubooten Daten und Cluster-Management-LIFs synchron auf einen anderen Node zu migrieren. Wenn die LIF-Migration fehlschlägt oder zeitausgeführt wird, wird der Neustart abgebrochen und ONTAP zeigt einen Fehler an, der den Fehler bei der LIF-Migration angibt.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

Der Node startet den Neubootvorgang. Die Eingabeaufforderung für die Anmeldung bei ONTAP wird angezeigt und gibt an, dass der Neustart abgeschlossen ist.

Starten Sie ONTAP an der Eingabeaufforderung der Boot-Umgebung

Sie können die aktuelle Version oder das Backup-Release von ONTAP booten, wenn Sie sich an der Eingabeaufforderung eines Node in der Boot-Umgebung befinden.

Schritte

1. Rufen Sie die Eingabeaufforderung der Boot-Umgebung über die Eingabeaufforderung des Speichersystems mit auf `system node halt` Befehl.

Auf der Konsole des Storage-Systems wird die Eingabeaufforderung der Boot-Umgebung angezeigt.

2. Geben Sie an der Eingabeaufforderung der Boot-Umgebung einen der folgenden Befehle ein:

Zum Booten...	Eingeben...
Der aktuellen Version von ONTAP	boot_ontap
Das primäre ONTAP-Image vom Boot-Gerät	boot_primary
Das ONTAP Backup-Image vom Startgerät aus	boot_backup

Wenn Sie sich nicht sicher sind, welches Bild verwendet werden soll, sollten Sie dies verwenden boot_ontap Im ersten Fall.

Fahren Sie einen Node herunter

Sie können einen Node herunterfahren, wenn er nicht mehr reagiert, oder wenn das Support-Personal sie als Teil der Fehlerbehebung aufgibt.

Schritte

1. Wenn das Cluster vier oder mehr Nodes enthält, vergewissern Sie sich, dass der zu heruntergefahren zu gefahrende Node das Epsilon nicht hält:

- a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

- b. Bestimmen Sie, auf welchem Node das Epsilon enthalten ist:

```
cluster show
```

Das folgende Beispiel zeigt, dass „node1“ Epsilon enthält:

```
cluster1::*> cluster show
Node           Health  Eligibility  Epsilon
-----
node1          true    true         true
node2          true    true         false
node3          true    true         false
node4          true    true         false
4 entries were displayed.
```

- a. Wenn der zu heruntergefahren Knoten das Epsilon hält, entfernen Sie das Epsilon vom Knoten:

```
cluster modify -node node_name -epsilon false
```

- b. Weisen Sie Epsilon einem anderen Knoten zu, der weiter oben bleibt:

```
cluster modify -node node_name -epsilon true
```

c. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Verwenden Sie die `system node halt` Befehl zum Herunterfahren des Node.

Wenn Sie den nicht angeben `-skip-lif-migration` Parameter, der Befehl versucht, vor dem Herunterfahren Daten- und Cluster-Management-LIFs synchron auf einen anderen Node zu migrieren. Wenn die LIF-Migration fehlschlägt oder eine Zeitüberschreitung ausfällt, wird der Shutdown-Prozess abgebrochen und ONTAP zeigt einen Fehler an, der den Fehler bei der LIF-Migration angibt.

Sie können einen Core Dump beim Herunterfahren manuell auslösen, indem Sie beide verwenden `-dump` Parameter.

Im folgenden Beispiel wird der Node mit dem Namen „node1“ für die Hardware-Wartung heruntergefahren:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

Verwalten Sie einen Knoten über das Startmenü

Sie können über das Startmenü Konfigurationsprobleme auf einem Node beheben, das Admin-Passwort zurücksetzen, Festplatten initialisieren, die Node-Konfiguration zurücksetzen und die Node-Konfigurationsinformationen zurück auf das Boot-Gerät wiederherstellen.



Wenn ein HA-Paar nutzt "[Verschlüsselung von SAS- oder NVMe-Laufwerken \(SED, NSE, FIPS\)](#)", Sie müssen die Anweisungen im Thema folgen "[Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren](#)". Für alle Laufwerke innerhalb des HA-Paars vor der Initialisierung des Systems (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Schritte

1. Starten Sie den Node neu, um mit dem auf das Boot-Menü zuzugreifen `system node reboot` Befehl an der Eingabeaufforderung des Systems.

Der Node startet den Neubootvorgang.

2. Drücken Sie während des Neubootens Strg-C, um das Boot-Menü anzuzeigen, wenn Sie dazu aufgefordert werden.

Auf dem Node werden die folgenden Optionen für das Startmenü angezeigt:


```
(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
Selection (1-9)?
```



Boot Menu Option (2) Boot ohne /etc/rc ist veraltet und hat keine Auswirkung auf das System.

3. Wählen Sie eine der folgenden Optionen aus, indem Sie die entsprechende Nummer eingeben:

An...	Auswählen...
Fahren Sie mit dem Booten des Node im normalen Modus fort	1) Normaler Start
Ändern Sie das Passwort des Node. Dies ist auch das Passwort für das `admin`	3) Passwort Ändern

An...	Auswählen...
<p>Initialisieren Sie die Festplatten des Node und erstellen Sie ein Root-Volume für den Node</p>	<p>4) Reinigen Sie die Konfiguration und initialisieren Sie alle Festplatten</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;">  <p>Mit dieser Menüoption werden alle Daten auf den Festplatten des Knotens gelöscht und die Knotenkonfiguration auf die werkseitigen Standardeinstellungen zurückgesetzt.</p> </div> <p>Wählen Sie dieses Menüelement nur aus, nachdem der Knoten aus einem Cluster entfernt wurde (nicht verbunden) und nicht mit einem anderen Cluster verbunden ist.</p> <p>Bei einem Node mit internen oder externen Festplatten-Shelfs wird das Root-Volume auf den internen Festplatten initialisiert. Wenn keine internen Festplatten-Shelfs vorhanden sind, wird das Root-Volume auf den externen Festplatten initialisiert.</p> <p>Bei einem System, auf dem die FlexArray-Virtualisierung mit internen oder externen Festplatten-Shelfs ausgeführt wird, werden die Array-LUNS nicht initialisiert. Alle nativen Festplatten auf internen oder externen Shelfs werden initialisiert.</p> <p>Für ein System, auf dem die FlexArray-Virtualisierung mit nur Array-LUNS ausgeführt wird und keine internen oder externen Festplatten-Shelfs, wird das Root-Volume im Speicher-Array-LUNS initialisiert. Siehe "FlexArray wird installiert".</p> <p>Wenn der Knoten, den Sie initialisieren möchten, über Festplatten verfügt, die für die Root-Daten-Partitionierung partitioniert wurden, müssen die Festplatten unpartitioniert werden, bevor der Knoten initialisiert werden kann, siehe 9) Erweiterte Laufwerkpartitionierung konfigurieren und "Festplatten- und Aggregatmanagement".</p>
<p>Führen Sie Wartungsvorgänge für Aggregate und Festplatten durch und erhalten Sie detaillierte Aggregat- und Festplatteninformationen.</p>	<p>5) Bootvorgang im Wartungsmodus</p> <p>Sie beenden den Wartungsmodus mit <code>halt</code> Befehl.</p>
<p>Stellen Sie die Konfigurationsinformationen vom Root-Volume des Node auf das Boot-Gerät, z. B. eine PC CompactFlash Card, wieder her</p>	<p>6) Flash aus Backup-Konfiguration aktualisieren</p> <p>ONTAP speichert einige Node-Konfigurationsinformationen auf dem Boot-Gerät. Beim Neubooten des Node werden die Informationen zum Boot-Gerät automatisch auf dem Root-Volume des Node gesichert. Wenn das Startgerät beschädigt wird oder ersetzt werden muss, müssen Sie diese Menüoption verwenden, um die Konfigurationsinformationen aus dem Stammvolumen des Knotens wieder auf das Startgerät wiederherzustellen.</p>

An...	Auswählen...
Installieren Sie auf dem Node neue Software	<p>7) Neue Software zuerst installieren</p> <p>Wenn die ONTAP-Software auf dem Boot-Gerät keine Unterstützung für das Speicher-Array bietet, das Sie für das Root-Volume verwenden möchten, können Sie mit dieser Menüoption eine Version der Software erhalten, die Ihr Speicher-Array unterstützt und auf dem Knoten installieren.</p> <p>Diese Menüoption dient nur zur Installation einer neueren Version der ONTAP-Software auf einem Knoten, auf dem kein Root-Volume installiert ist. Do_Not_ Verwenden Sie diese Menüoption, um ONTAP zu aktualisieren.</p>
Booten Sie den Node neu	8) Node neu booten
Heben Sie die Partitionierung aller Festplatten auf, entfernen Sie deren Besitzinformationen oder reinigen Sie die Konfiguration und initialisieren Sie das System mit ganzen oder partitionierten Festplatten	<p>9) Konfigurieren Der Erweiterten Laufwerkpartitionierung</p> <p>Ab ONTAP 9.2 bietet die Option „Advanced Drive Partitioning“ zusätzliche Managementfunktionen für Festplatten, die für Root-Daten oder Root-Daten-Partitionierung konfiguriert sind. Die folgenden Optionen sind über die Boot-Option 9 verfügbar:</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div>

Verwalten Sie einen Node per Remote-Zugriff über den SP/BMC

Remote-Management eines Node über die Übersicht zum SP/BMC

Sie können einen Node Remote über einen integrierten Controller verwalten, der als Service-Prozessor (SP) oder Baseboard Management Controller (BMC) bezeichnet wird. Dieser Remote Management Controller ist in allen aktuellen Plattformmodellen enthalten. Der Controller bleibt unabhängig vom Betriebsstatus des Node betriebsbereit.

Die folgenden Plattformen unterstützen BMC anstelle des SP:

- FAS 8700

- FAS 8300
- FAS27x0
- AFF A800
- AFF A700s
- AFF A400
- AFF A320
- AFF A220
- AFF C 190

Allgemeines zum SP

Der Service-Prozessor (SP) ist ein Remote-Managementgerät, mit dem Sie Remote auf einen Node zugreifen, diesen überwachen und Probleme beheben können.

Zu den wichtigsten Funktionen des SP gehören:

- Über den SP können Sie Remote auf einen Node zugreifen, um unabhängig vom Status des Node Controller Diagnose, Herunterfahren, ein- und Ausschalten oder ein Neubooten des Node zu ermöglichen.

Der SP wird mit Standby-Spannung betrieben, die verfügbar ist, solange der Node von mindestens einem seiner Netzteile mit Strom versorgt wird.

Sie können sich von einem Administrationshost aus mithilfe einer Secure-Shell-Client-Applikation beim SP anmelden. Anschließend können Sie die SP-CLI für die Remote-Überwachung und die Fehlerbehebung für den Node verwenden. Darüber hinaus können Sie mit dem SP auf die serielle Konsole zugreifen und ONTAP Befehle Remote ausführen.

Sie können von der seriellen Konsole aus auf den SP zugreifen oder vom SP aus auf die serielle Konsole zugreifen. Der SP ermöglicht Ihnen das gleichzeitige Öffnen einer SP-CLI-Sitzung und einer separaten Konsolensitzung.

Wenn beispielsweise von einem Temperatursensor ein kritisch hoher oder niedriger Wert wird, löst ONTAP den SP aus, um das Motherboard ordnungsgemäß herunterzufahren. Wenn die serielle Konsole nicht mehr reagiert, können Sie jedoch weiterhin Strg-G auf der Konsole drücken, um auf die SP-CLI zuzugreifen. Anschließend können Sie die verwenden `system power on` Oder `system power cycle` Befehl vom SP zum ein- und Ausschalten des Node sowie aus- und Wiedereinschalten des Node.

- Der SP überwacht Umgebungssensoren und protokolliert Ereignisse, sodass Sie rechtzeitig und effektiv Serviceaktionen vornehmen können.

Der SP überwacht Umgebungssensoren, z. B. Temperaturen des Node, Spannungen, Ströme und Lüftergeschwindigkeiten. Wenn ein Umgebungssensor einen anormalen Zustand aufweist, protokolliert der SP die anormalen Messwerte, benachrichtigt den ONTAP über das Problem und sendet Warnmeldungen und „deigene System“-Benachrichtigungen je nach Bedarf über eine AutoSupport-Meldung, unabhängig davon, ob der Node AutoSupport Meldungen senden kann.

Der SP protokolliert zudem Ereignisse, z. B. Boot-Status, Änderungen an der Field Replaceable Unit (FRU), von ONTAP generierte Ereignisse und den SP-Befehlshistorie. Sie können eine AutoSupport Meldung manuell aufrufen, um die SP-Protokolldateien einzubeziehen, die von einem angegebenen Node erfasst werden.

Abgesehen vom Generieren dieser Meldungen im Auftrag eines Node, der nicht verfügbar ist und dem Anschließen zusätzlicher Diagnoseinformationen an AutoSupport Meldungen anhängen, hat der SP keine Auswirkungen auf die AutoSupport Funktion. Die AutoSupport-Konfigurationseinstellungen und das Verhalten bei Nachrichteninhalten werden von ONTAP übernommen.



Der SP muss sich nicht auf das verlassen `-transport` Parametereinstellung des `system node autosupport modify` Befehl zum Senden von Benachrichtigungen. Der SP verwendet nur das Simple Mail Transport Protocol (SMTP) und erfordert die AutoSupport-Konfiguration des Hosts, um Mail-Host-Informationen einzubeziehen.

Wenn SNMP aktiviert ist, generiert der SP SNMP-Traps an konfigurierte Trap-Hosts für alle „deigenen System“ Ereignisse.

- Der SP hat einen nichtflüchtigen Arbeitsspeicherpuffer, in dem bis zu 4,000 Ereignisse in einem Systemereignisprotokoll (SEL) gespeichert werden können. Anhand dieses Protokolls können Sie Probleme diagnostizieren.

Das SEL speichert jeden Eintrag des Prüfprotokolls als Audit-Ereignis. Sie wird im integrierten Flash-Speicher auf dem SP gespeichert. Die Ereignisliste aus dem SEL wird automatisch vom SP über eine AutoSupport Meldung an die angegebenen Empfänger gesendet.

Das SEL enthält die folgenden Informationen:

- Vom SP erkannte Hardware-Events, beispielsweise Sensorstatus zu Netzteilen, Spannung oder anderen Komponenten
 - Vom SP erkannte Fehler, beispielsweise ein Kommunikationsfehler, ein Ausfall des Lüfters oder ein Arbeitsspeicher- oder CPU-Fehler
 - Kritische Softwareereignisse, die vom Node an den SP gesendet werden, beispielsweise Panic, ein Fehlschlag bei der Kommunikation, ein Fehlschlag beim Booten oder ein vom Benutzer verursachter „deigenes System“ als Folge der Ausgabe des SP `system reset` Oder `system power cycle` Befehl
- Der SP überwacht die serielle Konsole unabhängig davon, ob Administratoren angemeldet oder mit der Konsole verbunden sind.

Wenn Meldungen an die Konsole gesendet werden, speichert der SP sie im Konsole-Protokoll. Das Konsole-Protokoll bleibt gespeichert, solange der SP von einem der Netzteile des Node mit Strom versorgt wird. Da der SP mit Standby-Strom betrieben wird, bleibt er auch dann verfügbar, wenn der Node aus- und wieder eingeschaltet oder ganz ausgeschaltet wird.

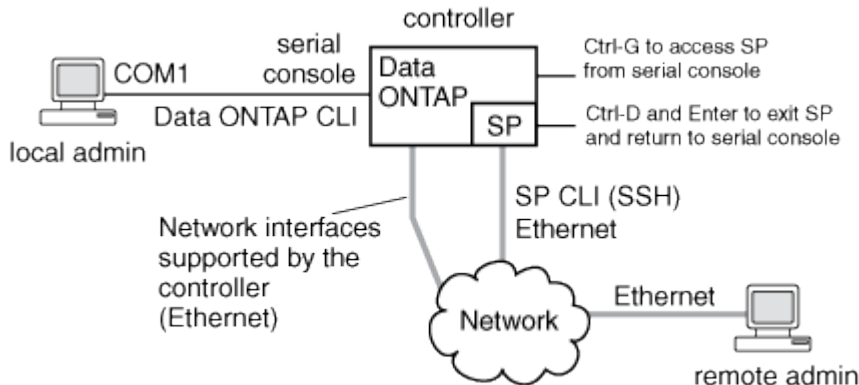
- Die Hardware-gestützte Übernahme ist verfügbar, wenn der SP konfiguriert ist.
- Der SP-API-Service ermöglicht die Kommunikation zwischen ONTAP und dem SP über das Netzwerk.

Der Service verbessert das ONTAP Management des SP durch die Unterstützung netzwerkbasierter Funktionen, wie z. B. das Verwenden der Netzwerkschnittstelle für das SP-Firmware-Update, sodass ein Node auf die SP-Funktionalität oder die Systemkonsole eines anderen Node zugreifen kann und das SP-Protokoll von einem anderen Node hochgeladen wird.

Sie können die Konfiguration des SP-API-Dienstes ändern, indem Sie den Port des Dienstes ändern, die SSL- und SSH-Zertifikate erneuern, die vom Dienst für die interne Kommunikation verwendet werden, oder den Service komplett deaktivieren.

Das folgende Diagramm zeigt den Zugriff auf ONTAP und den SP eines Node. Auf die SP-Schnittstelle ist über

den Ethernet-Port zugegriffen (wird durch ein Schraubenschlüsselsymbol auf der Rückseite des Chassis angezeigt):



Was der Baseboard Management Controller tut

Ab ONTAP 9.1 wird die Software auf bestimmten Hardware-Plattformen auf die Unterstützung eines neuen integrierten Controllers unter dem Namen Baseboard Management Controller (BMC) zugeschnitten. Der BMC verfügt über CLI-Befehle (Command Line Interface), mit denen Sie das Gerät Remote managen können.

Der BMC arbeitet ähnlich wie der Service-Prozessor (SP) und verwendet viele der gleichen Befehle. Mit dem BMC können Sie Folgendes tun:

- Konfigurieren Sie die BMC-Netzwerkeinstellungen.
- Greifen Sie per Remote-Zugriff auf einen Node zu und führen Sie Node-Managementaufgaben durch, z. B. Diagnose, Herunterfahren, aus- und Wiedereinschalten oder Neubooten des Node.

Es gibt einige Unterschiede zwischen SP und BMC:

- Der BMC überwacht die Umgebungsbedingungen von Netzteilenelementen, Kühlelementen, Temperatursensoren, Spannungssensoren und Stromsensoren. Der BMC meldet Sensorinformationen über IPMI an ONTAP.
- Einige Befehle für Hochverfügbarkeit (HA) und Storage unterscheiden sich.
- Der BMC sendet keine AutoSupport-Nachrichten.

Automatische Firmware-Updates sind auch verfügbar, wenn ONTAP 9.2 GA oder höher mit den folgenden Anforderungen ausgeführt wird:

- BMC-Firmware-Version 1.15 oder höher muss installiert sein.



Zur Aktualisierung der BMC-Firmware von 1.12 auf 1.15 oder höher ist ein manuelles Update erforderlich.

- BMC startet automatisch neu, nachdem ein Firmware-Update abgeschlossen wurde.



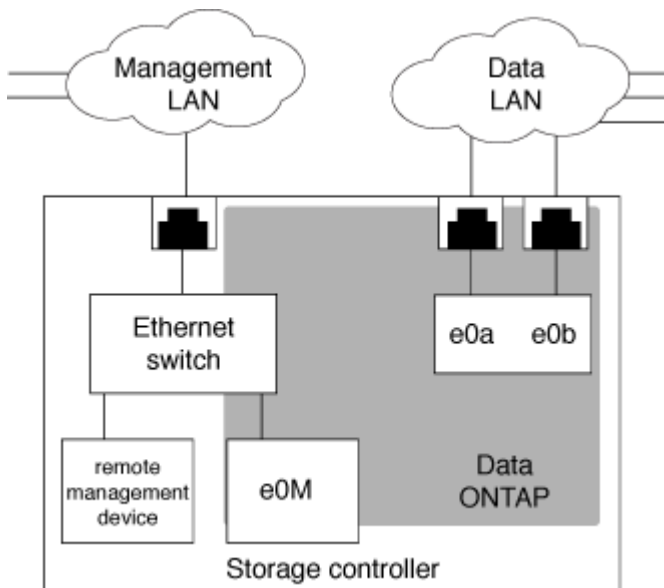
Node-Vorgänge werden bei einem BMC-Neustart nicht beeinträchtigt.

Konfigurieren Sie das SP/BMC-Netzwerk

Isolierung des Managementnetzwerk-Traffic

Es handelt sich um eine Best Practice, um SP/BMC und die E0M Management-Schnittstelle in einem für Management-Datenverkehr dedizierten Subnetz zu konfigurieren. Ein laufender Datenverkehr über das Managementnetzwerk kann zu Performance-Einbußen und Routing-Problemen führen.

Der Management-Ethernet-Port an den meisten Storage Controllern (angezeigt durch ein Schraubenschlüsselsymbol auf der Rückseite des Chassis) ist mit einem internen Ethernet-Switch verbunden. Der interne Switch bietet Konnektivität zum SP/BMC sowie zur E0M Managementoberfläche, über die Sie mittels TCP/IP-Protokollen wie Telnet, SSH und SNMP auf das Storage-System zugreifen können.



Wenn Sie das Remote-Management-Gerät und E0M verwenden möchten, müssen Sie diese in demselben IP-Subnetz konfigurieren. Da es sich hierbei um Schnittstellen mit niedriger Bandbreite handelt, empfiehlt es sich, SP/BMC und E0M in einem für den Management-Datenverkehr dedizierten Subnetz zu konfigurieren.

Wenn Sie den Verwaltungsdatenverkehr nicht isolieren können oder wenn Ihr dediziertes Managementnetzwerk ungewöhnlich groß ist, sollten Sie versuchen, das Volumen des Netzwerkdatenverkehrs so gering wie möglich zu halten. Übermäßiger Ingress-Broadcast- oder Multicast-Datenverkehr kann die SP/BMC-Leistung beeinträchtigen.



Einige Storage Controller, z. B. die AFF A800, verfügen über zwei externe Ports: Einen für BMC und die andere für E0M. Für diese Controller müssen BMC und E0M in demselben IP-Subnetz nicht konfiguriert werden.

Überlegungen zur SP/BMC-Netzwerkkonfiguration

Sie können die automatische Netzwerkkonfiguration auf Cluster-Ebene für den SP aktivieren (empfohlen). Sie können die automatische SP-Netzwerkkonfiguration auch deaktiviert (die Standardeinstellung) lassen und die SP-Netzwerkkonfiguration manuell auf Node-Ebene verwalten. Für jeden Fall sind einige Überlegungen zu beachten.



Dieses Thema gilt sowohl für den SP als auch für den BMC.

Die automatische SP-Netzwerkconfiguration ermöglicht dem SP, Adress-Ressourcen (einschließlich IP-Adresse, Subnetzmaske und Gateway-Adresse) aus dem angegebenen Subnetz zu verwenden, um das Netzwerk automatisch einzurichten. Bei der automatischen SP-Netzwerkconfiguration müssen Sie für den SP jedes Node keine IP-Adressen manuell zuweisen. Standardmäßig ist die automatische SP-Netzwerkconfiguration deaktiviert. Dies liegt daran, dass bei Aktivierung der Configuration zunächst das für die Configuration zu verwendende Subnetz im Cluster definiert werden muss.

Wenn Sie die automatische Netzwerkconfiguration des SP aktivieren, gelten die folgenden Szenarien und Überlegungen:

- Wenn der SP noch nie konfiguriert wurde, wird das SP-Netzwerk automatisch basierend auf dem für die automatische SP-Netzwerkconfiguration angegebenen Subnetz konfiguriert.
- Wenn der SP zuvor manuell konfiguriert wurde oder wenn die bestehende SP-Netzwerkconfiguration auf einem anderen Subnetz basiert, wird das SP-Netzwerk aller Nodes im Cluster basierend auf dem Subnetz neu konfiguriert, das Sie in der automatischen SP-Netzwerkconfiguration angeben.

Die Neukonfiguration kann dazu führen, dass dem SP eine andere Adresse zugewiesen wird. Dies hat möglicherweise Auswirkungen auf die DNS-Konfiguration und ihre Fähigkeit zur Behebung von SP-Hostnamen. Aus diesem Grund müssen Sie möglicherweise Ihre DNS-Konfiguration aktualisieren.

- Ein Node, der dem Cluster hinzugefügt wird, verwendet das angegebene Subnetz, um sein SP-Netzwerk automatisch zu konfigurieren.
- Der `system service-processor network modify` Mit dem Befehl können Sie die SP-IP-Adresse nicht ändern.

Wenn die automatische SP-Netzwerkconfiguration aktiviert ist, können Sie mit dem Befehl nur die SP-Netzwerkschnittstelle aktivieren oder deaktivieren.

- Wenn zuvor die automatische SP-Netzwerkconfiguration aktiviert war, führt das Deaktivieren der SP-Netzwerkschnittstelle dazu, dass die zugewiesene Adressressource freigegeben wird und zum Subnetz zurückgegeben wird.
- Wenn Sie die SP-Netzwerkschnittstelle deaktivieren und dann erneut aktivieren, wird möglicherweise der SP mit einer anderen Adresse neu konfiguriert.

Wenn die automatische SP-Netzwerkconfiguration deaktiviert ist (standardmäßig), gelten die folgenden Szenarien und Überlegungen:

- Wenn der SP noch nie konfiguriert wurde, wird die SP-IPv4-Netzwerkconfiguration standardmäßig mit IPv4 DHCP verwendet und IPv6 ist deaktiviert.

Ein Node, der dem Cluster hinzugefügt wird, verwendet standardmäßig auch IPv4 DHCP für seine SP-Netzwerkconfiguration.

- Der `system service-processor network modify` Mit dem Befehl können Sie die SP-IP-Adresse eines Node konfigurieren.

Wenn Sie versuchen, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind, wird eine Warnmeldung angezeigt. Wenn Sie die Warnung ignorieren und mit der manuellen Adresszuweisung fortfahren, kann dies zu einem Szenario mit doppelten Adressen führen.

Wenn die automatische SP-Netzwerkconfiguration nach erfolgter Aktivierung deaktiviert ist, gelten die

folgenden Szenarien und Überlegungen:

- Wenn bei der automatischen SP-Netzwerkconfiguration die IPv4-Adressfamilie deaktiviert ist, verwendet das SP-IPv4-Netzwerk standardmäßig DHCP, und das `system service-processor network modify` Mit dem Befehl können Sie die SP-IPv4-Konfiguration für einzelne Nodes ändern.
- Wenn bei der automatischen SP-Netzwerkconfiguration die IPv6-Adressfamilie deaktiviert ist, ist das SP-IPv6-Netzwerk ebenfalls deaktiviert, und die `system service-processor network modify` Mit dem Befehl können Sie die SP-IPv6-Konfiguration für einzelne Nodes aktivieren und ändern.

Aktivieren Sie die automatische Netzwerkconfiguration für den SP/BMC

Wenn der SP zur Verwendung der automatischen Netzwerkconfiguration aktiviert ist, wird ein manuelles Konfigurieren des SP-Netzwerks bevorzugt. Da die automatische SP-Netzwerkconfiguration die Cluster-weit aufweist, müssen Sie das SP-Netzwerk für einzelne Nodes nicht manuell verwalten.



Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

- Das Subnetz, das Sie für die automatische SP-Netzwerkconfiguration verwenden möchten, muss bereits im Cluster definiert sein und darf keine Ressourcenkonflikte mit der SP-Netzwerkschnittstelle aufweisen.

Der `network subnet show` Mit dem Befehl werden Subnetzinformationen für das Cluster angezeigt.

Der Parameter, der die Subnetzzuordnung erzwingt (das `-force-update-lif-associations` Parameter von `network subnet` Befehle) wird nur auf Netzwerk-LIFs unterstützt, nicht auf der SP-Netzwerkschnittstelle.

- Wenn Sie IPv6-Verbindungen für den SP verwenden möchten, muss IPv6 bereits für ONTAP konfiguriert und aktiviert sein.

Der `network options ipv6 show` Befehl zeigt den aktuellen Status von IPv6-Einstellungen für ONTAP an.

Schritte

1. Geben Sie die IPv4- oder IPv6-Adressenfamilie und den Namen des Subnetzes an, den der SP mit dem verwenden soll `system service-processor network auto-configuration enable` Befehl.
2. Zeigt die automatische SP-Netzwerkconfiguration mithilfe der an `system service-processor network auto-configuration show` Befehl.
3. Wenn Sie die SP-IPv4- und -IPv6-Netzwerkschnittstelle anschließend für alle Nodes im Quorum deaktivieren bzw. erneut aktivieren möchten, verwenden Sie das `system service-processor network modify` Befehl mit dem `-address-family [IPv4|IPv6]` Und `-enable [true|false]` Parameter.

Wenn die automatische SP-Netzwerkconfiguration aktiviert ist, können Sie die SP-IP-Adresse für einen Node im Quorum nicht ändern. Sie können nur die SP-IPv4- und -IPv6-Netzwerkschnittstelle aktivieren bzw. deaktivieren.

Wenn ein Node nicht über Quorum verfügt, können Sie die SP-Netzwerkconfiguration des Node, einschließlich der SP-IP-Adresse, durch Ausführen ändern `system service-processor network modify` Bestätigen Sie auf dem Node, dass Sie die automatische SP-Netzwerkconfiguration für den Node außer Kraft setzen möchten. Wenn der Node jedoch dem Quorum Beitritt, erfolgt die automatische SP-

Neukonfiguration für den Node auf Grundlage des angegebenen Subnetzes.

Konfigurieren Sie das SP/BMC-Netzwerk manuell

Wenn keine automatische Netzwerkkonfiguration für den SP eingerichtet ist, müssen Sie das SP-Netzwerk eines Node manuell konfigurieren, damit der Zugriff auf den SP über eine IP-Adresse möglich ist.

Was Sie benötigen

Wenn Sie IPv6-Verbindungen für den SP verwenden möchten, muss IPv6 bereits für ONTAP konfiguriert und aktiviert sein. Der `network options ipv6` Befehle verwalten IPv6-Einstellungen für ONTAP.



Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Sie können den SP für die Verwendung einer IPv4, einer IPv6 oder beides konfigurieren. Die SP-IPv4-Konfiguration unterstützt statische und DHCP-Adressen, und die SP-IPv6-Konfiguration unterstützt nur statische Adressen.

Wenn die automatische SP-Netzwerkkonfiguration eingerichtet wurde, müssen Sie das SP-Netzwerk für einzelne Nodes und den nicht manuell konfigurieren `system service-processor network modify` Mit dem Befehl können Sie nur die SP-Netzwerkschnittstelle aktivieren oder deaktivieren.

Schritte

1. Konfigurieren Sie mit dem das SP-Netzwerk für einen Node `system service-processor network modify` Befehl.
 - Der `-address-family` Der Parameter gibt an, ob die IPv4- oder IPv6-Konfiguration des SP geändert werden soll.
 - Der `-enable` Parameter aktiviert die Netzwerkschnittstelle der angegebenen IP-Adressfamilie.
 - Der `-dhcp` Der Parameter gibt an, ob die Netzwerkkonfiguration vom DHCP-Server oder der von Ihnen angegebenen Netzwerkadresse verwendet werden soll.

Sie können DHCP aktivieren (durch Einstellung `-dhcp` Bis `v4`) Nur, wenn Sie IPv4 verwenden. Sie können DHCP für IPv6-Konfigurationen nicht aktivieren.

- Der `-ip-address` Der Parameter gibt die öffentliche IP-Adresse für den SP an.

Wenn Sie versuchen, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind, wird eine Warnmeldung angezeigt. Wenn Sie die Warnung ignorieren und mit der manuellen Adresszuweisung fortfahren, kann dies zu einer doppelten Adresszuweisung führen.

- Der `-netmask` Der Parameter gibt die Netmask für den SP an (wenn IPv4 verwendet wird).
 - Der `-prefix-length` Parameter gibt die Netzwerkpräfixlänge der Subnetzmaske für den SP an (bei Verwendung von IPv6).
 - Der `-gateway` Der Parameter gibt die Gateway-IP-Adresse für den SP an.
2. Konfigurieren Sie das SP-Netzwerk für die im Cluster verbliebenen Nodes, indem Sie den Schritt 1 wiederholen.
 3. Zeigt die SP-Netzwerkkonfiguration an und überprüfen Sie den SP-Setup-Status mithilfe von `system service-processor network show` Befehl mit dem `-instance` Oder `-field setup-status`

Parameter.

Für einen Node kann der SP-Setup-Status eines der folgenden Werte angezeigt werden:

- not-setup — nicht konfiguriert
- succeeded — Konfiguration erfolgreich
- in-progress — Konfiguration wird ausgeführt
- failed — Konfiguration fehlgeschlagen

Beispiel für das Konfigurieren des SP-Netzwerks

Im folgenden Beispiel wird der SP eines Node zur Verwendung von IPv4 konfiguriert, der SP aktiviert und die SP-Netzwerkconfiguration angezeigt, um die Einstellungen zu überprüfen:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                Node: node1
            Address Type: IPv4
    Interface Enabled: true
        Type of Device: SP
                Status: online
            Link Status: up
            DHCP Status: none
            IP Address: 192.168.123.98
            MAC Address: ab:cd:ef:fe:ed:02
            Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
  Router Assigned IP Address: -
    Link Local IP Address: -
      Gateway IP Address: 192.168.123.1
        Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
          Subnet Name: -
Enable IPv6 Router Assigned Address: -
      SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

Ändern der Konfiguration des SP-API-Service

Die SP-API ist eine sichere Netzwerk-API, über die ONTAP über das Netzwerk mit dem SP kommunizieren kann. Sie können den vom SP-API-Service verwendeten Port ändern, die Zertifikate verlängern, die der Service für die interne Kommunikation verwendet, oder den Service vollständig deaktivieren. Sie müssen die Konfiguration nur in seltenen Situationen ändern.

Über diese Aufgabe

- Der SP-API-Service verwendet den Port 50000 Standardmäßig.

Sie können den Portwert ändern, wenn sich beispielsweise der Port in einer Netzwerkeinstellung befindet 50000 Wird für die Kommunikation durch eine andere Netzwerkanwendung verwendet, oder Sie möchten zwischen Datenverkehr von anderen Anwendungen und Datenverkehr unterscheiden, der vom SP-API-Dienst erzeugt wird.

- Die vom SP-API-Service verwendeten SSL- und SSH-Zertifikate sind intern zum Cluster und nicht extern verteilt.

In dem unwahrscheinlichen Fall, dass die Zertifikate kompromittiert werden, können Sie sie erneuern.

- Der SP-API-Service ist standardmäßig aktiviert.

Der SP-API-Service muss nur in seltenen Fällen deaktiviert werden, z. B. in einem privaten LAN, in dem der SP nicht konfiguriert oder verwendet wird, und Sie den Service deaktivieren möchten.

Wenn der SP-API-Service deaktiviert ist, akzeptiert die API keine eingehenden Verbindungen. Zudem sind Funktionen wie netzwerkbasierte Firmware-Updates oder die netzwerkbasierte Protokollerfassung für SP „deigenes System“ nicht mehr verfügbar. Das System wechselt zu über die serielle Schnittstelle.

Schritte

1. Wechseln Sie mit der zur erweiterten Berechtigungsebene `set -privilege advanced` Befehl.
2. Ändern der SP-API-Service-Konfiguration:

Ihr Ziel ist	Verwenden Sie den folgenden Befehl...
Ändern Sie den Port, der vom SP-API-Service verwendet wird	<code>system service-processor api-service modify</code> Mit dem <code>-port {49152..65535}</code> -Parameter

Ihr Ziel ist	Verwenden Sie den folgenden Befehl...
Erneuern der vom SP-API-Service verwendeten SSL- und SSH-Zertifikate für die interne Kommunikation	<ul style="list-style-type: none"> • Für die Verwendung mit ONTAP 9.5 oder höher <code>system service-processor api-service renew-internal-certificate</code> • Für ONTAP 9.4 und frühere Verwendung <code>system service-processor api-service renew-certificates</code> <p>Wenn kein Parameter angegeben wird, werden nur die Host-Zertifikate (einschließlich der Client- und Server-Zertifikate) erneuert.</p> <p>Wenn der <code>-renew-all true</code> Parameter wird angegeben, sowohl die Host-Zertifikate als auch das Root-CA-Zertifikat werden erneuert.</p>
komm	
Deaktiviert bzw. reaktiviert den SP-API-Service	<code>system service-processor api-service modify</code> Mit dem <code>-is-enabled {true</code>

3. Zeigt die SP-API-Service-Konfiguration mit dem an `system service-processor api-service show` Befehl.

Methoden zum Verwalten von SP/BMC-Firmware-Updates

Die ONTAP enthält ein SP-Firmware-Image, das als *Baseline Image* bezeichnet wird. Falls nachfolgend eine neue Version der SP-Firmware verfügbar wird, können Sie die SP-Firmware herunterladen und auf die heruntergeladene Version aktualisieren, ohne die ONTAP-Version aktualisieren zu müssen.



Dieses Thema gilt sowohl für den SP als auch für den BMC.

ONTAP bietet folgende Methoden zum Verwalten von SP-Firmware-Updates:

- Die Funktion für die automatische Aktualisierung des SP ist standardmäßig aktiviert, sodass die SP-Firmware in folgenden Szenarien automatisch aktualisiert werden kann:
 - Wenn Sie ein Upgrade auf eine neue Version von ONTAP durchführen

Das ONTAP-Upgrade umfasst automatisch das Update der SP-Firmware, vorausgesetzt, dass die in ONTAP enthaltene SP-Firmware-Version höher ist als die auf dem Node ausgeführte SP-Version.



ONTAP erkennt ein automatisches Update auf dem SP und löst eine Korrekturmaßnahme aus, um die automatische SP-Aktualisierung bis zu dreimal zu wiederholen. Wenn alle drei Wiederholungen fehlschlagen, lesen Sie den Link zum Knowledge Base-Artikel: [Health SPAutoUpgrade überwachen Fehler MajorWarnung SP-Upgrade schlägt fehl - AutoSupport-Meldung](#).

- Wenn Sie eine Version der SP-Firmware von der NetApp Support Site herunterladen und die heruntergeladene Version ist neuer als die Version, auf der der SP derzeit ausgeführt wird
- Wenn Sie ein Downgrade oder ein Wechsel zu einer früheren Version von ONTAP durchführen

Die SP-Firmware wird automatisch auf die neueste kompatible Version aktualisiert, die von der ONTAP-Version unterstützt wird, auf die Sie zurückgesetzt oder herabgestuft wurden. Ein manuelles Update der SP-Firmware ist nicht erforderlich.

Sie haben die Möglichkeit, die automatische Update-Funktion des SP mit zu deaktivieren `system service-processor image modify` Befehl. Es wird jedoch empfohlen, die Funktion aktiviert zu lassen. Die Deaktivierung der Funktionalität kann zu suboptimalen oder nicht qualifizierten Kombinationen zwischen dem ONTAP-Image und dem SP-Firmware-Image führen.

- Mit ONTAP können Sie ein SP-Update manuell auslösen und angeben, wie das Update mithilfe der erfolgen soll `system service-processor image update` Befehl.

Sie können die folgenden Optionen angeben:

- Das zu verwendende SP-Firmware-Paket (`-package`)

Sie können die SP-Firmware auf ein heruntergeladenes Paket aktualisieren, indem Sie den Namen der Paketdatei angeben. Im Vormarsch `system image package show` Mit dem Befehl werden alle Paketdateien (einschließlich der Dateien für das SP-Firmware-Paket) angezeigt, die auf einem Node verfügbar sind.

- Gibt an, ob das Baseline-SP-Firmware-Paket für das SP-Update verwendet wird (`-baseline`)

Sie können die SP-Firmware auf die Baseline-Version aktualisieren, die mit der derzeit ausgeführten ONTAP-Version gebündelt wird.



Wenn Sie einige der erweiterten Update-Optionen oder -Parameter verwenden, werden die Konfigurationseinstellungen des BMC möglicherweise vorübergehend gelöscht. Nach dem Neustart kann es bis zu 10 Minuten dauern, bis ONTAP die BMC-Konfiguration wiederherstellen kann.

- ONTAP ermöglicht Ihnen, den Status des aktuellen SP-Firmware-Updates anzuzeigen, der von ONTAP ausgelöst wird, mithilfe der `system service-processor image update-progress show` Befehl.

Jede vorhandene Verbindung zum SP wird beendet, wenn die SP-Firmware aktualisiert wird. In diesem Fall wird das Update der SP-Firmware automatisch oder manuell ausgelöst.

Verwandte Informationen

["NetApp Downloads: System-Firmware und -Diagnose"](#)

Wenn der SP/BMC die Netzwerkschnittstelle für Firmware-Updates verwendet

Ein Update der SP-Firmware, das von ONTAP mit dem SP, der Version 1.5, 2.5, 3.1 oder höher ausgeführt wird, unterstützt den Einsatz eines IP-basierten Dateiübertragungsmechanismus über die SP Netzwerkschnittstelle.



Dieses Thema gilt sowohl für den SP als auch für den BMC.

Ein Update der SP-Firmware über die Netzwerkschnittstelle ist schneller als ein Update über die serielle Schnittstelle. Es verringert das Wartungsfenster, während das die SP-Firmware aktualisiert wird und auch den ONTAP Betrieb nicht unterbrechungsfrei. Die SP-Versionen, die diese Funktion unterstützen, sind in ONTAP enthalten. Sie sind außerdem auf der NetApp Support-Website verfügbar und können auf Controllern installiert werden, auf denen eine kompatible Version von ONTAP ausgeführt wird.

Wenn Sie SP-Version 1.5, 2.5, 3.1 oder höher verwenden, gelten die folgenden Firmware-Aktualisierungsmethoden:

- Ein durch ONTAP ausgelöstes SP-Firmware-Update wird standardmäßig das Netzwerkinterface für das Update verwendet. Wenn jedoch eine der folgenden Bedingungen eintritt, schaltet das automatische SP-Update auf die serielle Schnittstelle für das Firmware-Update um:
 - Die SP-Netzwerkschnittstelle ist nicht konfiguriert oder nicht verfügbar.
 - Die IP-basierte Dateiübertragung schlägt fehl.
 - Der SP-API-Service ist deaktiviert.

Unabhängig von der ausgeführten SP-Version verwendet ein Update der SP-Firmware, das von der SP-CLI ausgelöst wird, immer die SP-Netzwerkschnittstelle für das Update.

Verwandte Informationen

["NetApp Downloads: System-Firmware und -Diagnose"](#)

Zugriff auf den SP/BMC

Konten, die auf den SP zugreifen können

Wenn Sie versuchen, auf den SP zuzugreifen, werden Sie nach Berechtigungen gefragt. Cluster-Benutzerkonten, die mit dem erstellt werden `service-processor` Applikationstyp hat Zugriff auf die SP-CLI auf jedem Node des Clusters. SP-Benutzerkonten werden über ONTAP verwaltet und per Passwort authentifiziert. Ab ONTAP 9.9 müssen die SP-Benutzerkonten über den verfügen `admin` Rolle:

Benutzerkonten für den Zugriff auf den SP werden über ONTAP statt über die SP-CLI verwaltet. Ein Cluster-Benutzerkonto kann auf den SP zugreifen, wenn es mit dem erstellt wird `-application` Parameter von `security login create` Befehl ist auf festgelegt `service-processor` Und das `-authmethod` Parameter auf gesetzt `password`. Der SP unterstützt nur die Passwort-Authentifizierung.

Sie müssen das angeben `-role` Parameter beim Erstellen eines SP-Benutzerkontos.

- In ONTAP 9.9.1 und höheren Versionen müssen Sie angeben `admin` Für das `-role` Parameter und alle Änderungen an einem Konto erfordern das `admin` Rolle: Andere Rollen sind aus Sicherheitsgründen nicht mehr zulässig.
 - Wenn Sie ein Upgrade auf ONTAP 9.9.1 oder neuere Versionen durchführen, lesen Sie ["Ändern von Benutzerkonten, die auf den Service Processor zugreifen können"](#).
 - Beim Wechsel zurück zu ONTAP 9.8 oder älteren Versionen finden Sie Informationen unter ["Überprüfen Sie, ob Benutzerkonten, die auf den Service Processor zugreifen können"](#).
- In ONTAP 9.8 und älteren Versionen kann jede Rolle jedoch auf den SP zugreifen `admin` Wird empfohlen.

Standardmäßig enthält das Cluster-Benutzerkonto mit dem Namen „admin“ das `service-processor` Applikationstyp und hat Zugriff auf den SP.

ONTAP verhindert, dass Sie Benutzerkonten mit Namen erstellen, die für das System reserviert sind (z. B. „root“ und „naroot“). Sie können keinen systemreservierten Namen für den Zugriff auf das Cluster oder den SP verwenden.

Sie können aktuelle SP-Benutzerkonten mithilfe der anzeigen `-application service-processor` Parameter von `security login show` Befehl.

Greifen Sie von einem Administrationshost aus auf den SP/BMC zu

Sie können sich über einen Administrationshost beim SP eines Node einloggen, um Node-Managementaufgaben Remote auszuführen.

Was Sie benötigen

Folgende Bedingungen müssen erfüllt sein:

- Der Administrationshost, den Sie für den Zugriff auf den SP verwenden, muss SSHv2 unterstützen.
- Ihr Benutzerkonto muss bereits für den Zugriff auf den SP eingerichtet sein.

Für den Zugriff auf den SP muss Ihr Benutzerkonto mit dem erstellt worden sein `-application` Parameter von `security login create` Befehl ist auf festgelegt `service-processor` Und das `-authmethod` Parameter auf gesetzt `password`.



Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Wenn der SP so konfiguriert ist, dass er eine IPv4- oder IPv6-Adresse verwendet, und wenn fünf SSH-Anmeldeversuche von einem Host innerhalb von 10 Minuten nacheinander fehlschlagen, weist der SP SSH-Anmeldeanfragen zurück und setzt die Kommunikation mit der IP-Adresse des Hosts 15 Minuten lang aus. Die Kommunikation wird nach 15 Minuten fortgesetzt, und Sie können versuchen, sich erneut beim SP anzumelden.

Mit ONTAP können Sie keine systemreservierten Namen (z. B. „root“ und „naroot“) für den Zugriff auf das Cluster oder den SP erstellen oder verwenden.

Schritte

1. Melden Sie sich vom Administrations-Host beim SP an:

```
ssh username@SP_IP_address
```

2. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für ein `username`.

Die SP-Eingabeaufforderung wird angezeigt. Hier wird angegeben, dass Sie auf die SP-CLI zugreifen können.

Beispiele für SP-Zugriff von einem Administrationshost aus

Im folgenden Beispiel wird gezeigt, wie Sie sich mit einem Benutzerkonto beim SP einloggen `joel`, Die für den Zugriff auf den SP eingerichtet wurde.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

In den folgenden Beispielen wird veranschaulicht, wie Sie sich bei einem Node, auf dem SSH für IPv6 eingerichtet ist, mit der globalen IPv6-Adresse oder über den IPv6-Router angekündigte Adresse beim SP einloggen.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Greifen Sie über die Systemkonsole auf den SP/BMC zu

Sie können über die Systemkonsole (auch „*serial Console*“) auf den SP zugreifen, um Überwachungs- oder Fehlerbehebungsaufgaben durchzuführen.

Über diese Aufgabe

Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Schritte

1. Greifen Sie von der Systemkonsole auf die SP-CLI zu, indem Sie an der Eingabeaufforderung Strg-G drücken.
2. Melden Sie sich bei der SP-CLI an, wenn Sie dazu aufgefordert werden.

Die SP-Eingabeaufforderung wird angezeigt. Hier wird angegeben, dass Sie auf die SP-CLI zugreifen können.

3. Beenden Sie die SP-CLI und kehren Sie zur Systemkonsole zurück, indem Sie Strg-D drücken und dann die Eingabetaste drücken.

Beispiel für den Zugriff auf die SP-CLI von der Systemkonsole

Im folgenden Beispiel werden die Ergebnisse beim Drücken von Strg-G von der Systemkonsole angezeigt, um auf die SP-CLI zuzugreifen. Der `help system power` Befehl wird an der SP-Eingabeaufforderung eingegeben, gefolgt von Strg-D und anschließend mit der Eingabetaste zur Systemkonsole.

```
cluster1::>
```

(Drücken Sie Strg-G, um auf die SP-CLI zuzugreifen.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Drücken Sie Strg-D und anschließend die Eingabetaste, um zur Systemkonsole zurückzukehren.)

```
cluster1::>
```

Beziehung zwischen der SP-CLI, der SP-Konsole und den Systemkonsolensitzungen

Sie können eine SP-CLI-Session öffnen, um einen Node Remote zu verwalten, und eine separate SP-Konsolensitzung öffnen, um auf die Konsole des Node zuzugreifen. Die SP-Konsolensitzung spiegelt die Ausgabe, die in einer gleichzeitigen Systemkonsolensitzung angezeigt wird. Der SP und die Systemkonsole verfügen über unabhängige Shell-Umgebungen mit unabhängiger Anmeldeauthentifizierung.

Wenn Sie Allgemeines zur SP-CLI, zur SP-Konsole und zu Systemkonsolensitzungen tun, können Sie einen Node Remote verwalten. Im Folgenden wird die Beziehung zwischen den Sitzungen beschrieben:

- Nur ein Administrator kann sich gleichzeitig bei der SP-CLI-Sitzung anmelden. Mit dem SP können Sie jedoch sowohl eine SP-CLI-Sitzung als auch eine separate SP-Konsolensitzung öffnen.

Die SP-CLI wird mit der SP-Eingabeaufforderung angezeigt (`SP>`). In einer SP-CLI-Session können Sie den SP verwenden `system console` Befehl zum Starten einer SP-Konsolensitzung. Gleichzeitig können Sie eine separate SP-CLI-Sitzung über SSH starten. Wenn Sie Strg-D drücken, um die SP-Konsolensitzung zu beenden, kehren Sie automatisch zur SP-CLI-Session zurück. Wenn eine SP-CLI-Session bereits vorhanden ist, werden Sie mit einer Meldung gefragt, ob Sie die vorhandene SP-CLI-Session beenden möchten. Wenn Sie „y“ eingeben, wird die vorhandene SP-CLI-Sitzung beendet und Sie können von der SP-Konsole zur SP-CLI zurückkehren. Diese Aktion wird im SP-Ereignisprotokoll aufgezeichnet.

In einer ONTAP-CLI-Session, die über SSH verbunden ist, können Sie zur Systemkonsole eines Node wechseln, indem Sie die ONTAP ausführen `system node run-console` Befehl von einem anderen Node.

- Aus Sicherheitsgründen besitzen die SP-CLI-Session und die Systemkonsolensitzung eine unabhängige Anmeldeauthentifizierung.

Wenn Sie eine SP-Konsolensitzung über die SP-CLI initiieren (über den SP) `system console` Befehl). Sie werden aufgefordert, die Anmeldeinformationen für die Systemkonsole einzugeben. Wenn Sie über eine Systemkonsolensession auf die SP-CLI zugreifen (durch Drücken von Strg-G), werden Sie nach den

SP-CLI-Berechtigungen gefragt.

- Die SP-Konsolensitzung und die Systemkonsolensitzung verfügen über unabhängige Shell-Umgebungen.

Die SP-Konsolensitzung spiegelt die Ausgabe, die in einer gleichzeitigen Systemkonsolensitzung angezeigt wird. Jedoch spiegelt die gleichzeitige Systemkonsolensitzung nicht die SP-Konsolensitzung.

Die SP-Konsolensitzung spiegelt die Ausgabe gleichzeitiger SSH-Sessions nicht.

Verwalten Sie die IP-Adressen, die auf den SP zugreifen können

Standardmäßig akzeptiert der SP SSH-Verbindungsanfragen von Administrations-Hosts beliebiger IP-Adressen. Sie können den SP so konfigurieren, dass nur SSH-Verbindungsanforderungen von den Administrations-Hosts akzeptiert werden, die die angegebenen IP-Adressen haben. Die Änderungen, die Sie vornehmen, beziehen sich auf SSH-Zugriff auf den SP aller Nodes im Cluster.

Schritte

1. Gewähren Sie SP-Zugriff nur auf die IP-Adressen, die Sie mit angeben `system service-processor ssh add-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter.

- Der Wert des `-allowed-addresses` Der Parameter muss im Format von angegeben werden `address/netmask`, Und mehrfach `address/netmask` Paare müssen z. B. durch Kommas getrennt werden. `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Einstellen des `-allowed-addresses` Parameter an `0.0.0.0/0, ::/0` Aktiviert alle IP-Adressen für den Zugriff auf den SP (Standard).

- Wenn Sie die Standardeinstellung ändern, indem Sie den SP-Zugriff auf nur die von Ihnen angegebenen IP-Adressen beschränken, werden Sie von ONTAP aufgefordert, zu bestätigen, dass die angegebenen IP-Adressen die Standardeinstellung „allow all“ ersetzen sollen (`0.0.0.0/0, ::/0`).
- Der `system service-processor ssh show` Mit dem Befehl werden die IP-Adressen angezeigt, die auf den SP zugreifen können.

2. Wenn Sie eine angegebene IP-Adresse vom Zugriff auf den SP blockieren möchten, verwenden Sie die `system service-processor ssh remove-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter.

Wenn Sie alle IP-Adressen beim Zugriff auf den SP blockieren, kann auf den SP kein Administrations-Host mehr zugegriffen werden.

Beispiele für das Verwalten der IP-Adressen, die auf den SP zugreifen können

In den folgenden Beispielen wird die Standardeinstellung für SSH-Zugriff auf den SP angezeigt, die Standardeinstellung wird geändert, indem nur der SP-Zugriff auf die angegebenen IP-Adressen beschränkt wird, die angegebenen IP-Adressen aus der Zugriffsliste entfernt und dann der SP-Zugriff für alle IP-Adressen wiederhergestellt wird:

```

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
      with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
      addresses will be denied access. To restore the "allow all"
default,
      use the "system service-processor ssh add-allowed-addresses
      -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
      {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

```

Verwenden Sie die Online-Hilfe von SP/BMC CLI

In der Online-Hilfe werden die SP/BMC CLI-Befehle und -Optionen angezeigt.

Über diese Aufgabe

Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Schritte

1. Geben Sie zum Anzeigen von Hiltinformationen für die SP/BMC-Befehle Folgendes ein:

Um auf die SP-Hilfe zuzugreifen...	Um auf die BMC-Hilfe zuzugreifen...
Typ <code>help</code> An der SP-Eingabeaufforderung.	Typ <code>system</code> An der BMC-Eingabeaufforderung.

Im folgenden Beispiel wird die Online-Hilfe der SP-CLI angezeigt.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

Das folgende Beispiel zeigt die BMC CLI Online-Hilfe.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

- Um Hiltinformationen für die Option eines SP/BMC-Befehls anzuzeigen, geben Sie ein `help` Vor oder nach dem SP/BMC-Befehl.

Im folgenden Beispiel wird die Online-Hilfe der SP-CLI für den SP angezeigt `events` Befehl.

```

SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events

```

Das folgende Beispiel zeigt die Online-Hilfe von BMC CLI für den BMC `system power` Befehl.

```

BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>

```

Befehle zum Remote-Management eines Node

Sie können einen Node Remote verwalten, indem Sie auf seinen SP zugreifen und SP-CLI-Befehle ausführen, um Node-Management-Aufgaben auszuführen. Für verschiedene häufig ausgeführte Remote Node-Managementaufgaben können Sie zudem ONTAP-Befehle von einem anderen Node im Cluster verwenden. Einige SP-Befehle sind plattformspezifisch und sind möglicherweise nicht auf Ihrer Plattform verfügbar.

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
Zeigt verfügbare SP-Befehle oder Unterbefehle eines angegebenen SP-Befehls an	<code>help [command]</code>		
Zeigt die aktuelle Berechtigungsebene für die SP-CLI an	<code>priv show</code>		
Legen Sie die Berechtigungsebene fest, um auf den angegebenen Modus für die SP-CLI zuzugreifen	<code>priv set {admin. advanced.diag}</code>		
Zeigt Datum und Uhrzeit des Systems an	<code>date</code>		<code>date</code>


Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
Zeigt Ereignisse an, die vom SP protokolliert werden	<code>events {all . info . newest number . oldest number . search keyword}</code>		
Zeigt den SP-Status und Informationen zur Netzwerkkonfiguration an	<code>sp status [-v . -d]</code> Der <code>-v</code> Mit der Option werden SP-Statistiken in ausführlicher Form angezeigt. Der <code>-d</code> Option fügt das SP-Debug-Protokoll zur Anzeige hinzu.	<code>bmc status [-v . -d]</code> Der <code>-v</code> Mit der Option werden SP-Statistiken in ausführlicher Form angezeigt. Der <code>-d</code> Option fügt das SP-Debug-Protokoll zur Anzeige hinzu.	<code>system service-processor show</code>
Zeigt die Länge der Laufzeit des SP und die durchschnittliche Anzahl der Jobs in der Warteschlange der letzten 1, 5 und 15 Minuten an	<code>sp uptime</code>	<code>bmc uptime</code>	
Zeigt Protokolle der Systemkonsole an	<code>system log</code>		
Zeigt die SP-Protokollarchive oder die Dateien in einem Archiv an	<code>sp log history show [-archive {latest .{all . archive-name}}] [-dump {all . file-name}]</code>	<code>bmc log history show [-archive {latest .{all . archive-name}}] [-dump {all . file-name}]</code>	
Zeigt den Stromstatus des Controllers eines Node an	<code>system power status</code>		<code>system node power show</code>
Zeigt Informationen zur Batterie an	<code>system battery show</code>		
Zeigen Sie ACP-Informationen oder den Status von Expander-Sensoren an	<code>system acp [show . sensors show]</code>		
Listen Sie alle System-FRUs und ihre IDs auf	<code>system fru list</code>		

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
Zeigt Produktinformationen für die angegebene FRU an	<code>system fru show fru_id</code>		
Zeigt das FRU-Datenhistorie-Protokoll an	<code>system fru log show</code> (Erweiterte Berechtigungsebene)		
Zeigt den Status der Umgebungssensoren an, einschließlich ihrer Status und aktuellen Werte	<code>system sensors</code> Oder <code>system sensors show</code>		<code>system node environment sensors show</code>
Status und Details für den angegebenen Sensor anzeigen	<code>system sensors get sensor_name</code> Sie erhalten können <code>sensor_name</code> Durch Verwendung des <code>system sensors</code> Oder im <code>system sensors show</code> Befehl.		
Zeigt die Versionsinformationen der SP-Firmware an	<code>version</code>		<code>system service-processor image show</code>
Zeigt den SP-Befehlshistorie an	<code>sp log audit</code> (Erweiterte Berechtigungsebene)	<code>bmc log audit</code>	
Zeigt die SP-Debug-Informationen an	<code>sp log debug</code> (Erweiterte Berechtigungsebene)	<code>bmc log debug</code> (Erweiterte Berechtigungsebene)	
Zeigt die SP-Meldungsdatei an	<code>sp log messages</code> (Erweiterte Berechtigungsebene)	<code>bmc log messages</code> (Erweiterte Berechtigungsebene)	

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
Anzeigen der Einstellungen für das Sammeln der Systemforensik bei einem Watchdog-Reset-Ereignis, Anzeigen der Systemforensik-Informationen, die während eines Watchdog-Reset-Ereignisses gesammelt wurden, oder Löschen der gesammelten Informationen zur Systemforensik	system forensics [show.log dump.log clear]		
Melden Sie sich bei der Systemkonsole an	system console		system node run-console
Drücken Sie Strg-D, um die Systemkonsolensitzung zu beenden.	Schalten Sie den Knoten ein oder aus, oder führen Sie ein aus- und wieder ein (aus- und wieder einschalten).	system power on	
system node power on (Erweiterte Berechtigungsebene)	system power off		

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
<p>system power cycle</p>			<p>Die Standby-Stromversorgung bleibt eingeschaltet, damit der SP unterbrechungsfrei betrieben wird. Während des Einschaltzyklus erfolgt eine kurze Pause, bevor der Strom wieder eingeschaltet wird.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Wenn der Node mit diesen Befehlen aus- und wieder eingeschaltet wird, kann dies zu einem fehlerhaften Herunterfahren des Nodes führen (auch als „dirty shutdown“ bezeichnet) und kein Ersatz für ein ordnungsgemäßes Herunterfahren mithilfe der ONTAP system node halt Befehl.</p> </div>

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
Erstellen Sie einen Core Dump, und setzen Sie den Node zurück	<pre>system core [-f]</pre> <p>Der <code>-f</code> Option erzwingt die Erstellung eines Core Dump und das Zurücksetzen des Node.</p>		<pre>system node coredump trigger</pre> <p>(Erweiterte Berechtigungsebene)</p>
<p>Diese Befehle haben den gleichen Effekt wie das Drücken der NMI-Taste (Non-Maskable Interrupt) auf einem Knoten, was zu einem nicht ordnungsgemäßen Herunterfahren des Knotens und einem Dump der Kerndateien beim Beenden des Knotens führt. Diese Befehle sind hilfreich, wenn ONTAP auf dem Node aufgehängt ist oder nicht auf Befehle wie reagiert <code>system node shutdown</code>. Die generierten Core Dump-Dateien werden in der Ausgabe des angezeigt <code>system node coredump show</code> Befehl. Der SP bleibt betriebsbereit, solange die Input-Stromversorgung des Node nicht unterbrochen wird.</p>	<p>Booten Sie den Node mit einem optional angegebenen BIOS-Firmware-Image (primäres, Backup oder aktuell) neu, um Probleme wie ein beschädigtes Image des Boot-Geräts des Node wiederherzustellen</p>	<pre>system reset {primary.backup.current}</pre>	

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
<p>system node reset Mit dem -firmware {primary.backup.current} Parameter(erweiterte Berechtigungsebene)</p> <p>system node reset</p>	<div style="border: 1px solid black; padding: 5px; width: fit-content; margin-bottom: 10px;">  <p>Dieser Vorgang bewirkt ein nicht ordnungsgemäßes Herunterfahren des Node.</p> </div> <p>Wenn kein BIOS-Firmware-Image angegeben wird, wird das aktuelle Image für das Neubooten verwendet. Der SP bleibt betriebsbereit, solange die Input-Stromversorgung des Node nicht unterbrochen wird.</p>	<p>Zeigt den Status eines automatischen Updates der Akku-Firmware an oder aktiviert bzw. deaktiviert das automatische Update der Akku-Firmware beim nächsten Booten des SP</p>	<p>system battery auto_update [status.enable.disable]</p> <p>(Erweiterte Berechtigungsebene)</p>
		<p>Vergleicht das aktuelle Akku-Firmware-Image mit einem angegebenen Firmware-Image</p>	<p>system battery verify [image_URL]</p> <p>(Erweiterte Berechtigungsebene)</p> <p>Wenn image_URL ist nicht angegeben, wird das Standard-Akku-Firmware-Image zum Vergleich verwendet.</p>
		<p>Aktualisieren Sie die Akku-Firmware vom Image am angegebenen Speicherort</p>	<p>system battery flash image_URL</p> <p>(Erweiterte Berechtigungsebene)</p> <p>Sie verwenden diesen Befehl, wenn das automatische Update der Akku-Firmware aus einem bestimmten Grund fehlgeschlagen ist.</p>

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
		Aktualisieren Sie die SP-Firmware mithilfe des Images am angegebenen Speicherort	<code>sp update image_URL image_URL</code> Darf 200 Zeichen nicht überschreiten.
<code>bmc update image_URL image_URL</code> Darf 200 Zeichen nicht überschreiten.	<code>system service-processor image update</code>	Bootet den SP neu	<code>sp reboot</code>
	<code>system service-processor reboot-sp</code>		Löscht den NVRAM-Flash-Inhalt
<code>system nvram flash clear</code> (Erweiterte Berechtigungsebene) Dieser Befehl kann nicht gestartet werden, wenn die Stromversorgung des Controllers ausgeschaltet ist (<code>system power off</code>).			Beenden Sie die SP-CLI

Informationen zu den schwellenwertbasierten SP-Sensormesswerten und Statuswerten der Befehlsausgabe des Befehls „System Sensors“

Schwellenwertbasierte Sensoren messen regelmäßig verschiedene Systemkomponenten. Der SP vergleicht den Messwert eines schwellenwertbasierten Sensors mit dessen voreingestellten Grenzwerten, die die gültigen Betriebsbedingungen einer Komponente definieren.

Auf der Grundlage des Sensormesswerts zeigt der SP den Sensorstatus an, der Ihnen beim Monitoring des Zustands der Komponente helfen soll.

Beispiele schwellenwertbasierter Sensoren sind Sensoren für Systemtemperaturen, Spannungen, Ströme und Lüftergeschwindigkeiten. Die spezifische Liste schwellenwertbasierter Sensoren hängt von der Plattform ab.

Schwellenwertbasierte Sensoren verfügen über die folgenden Schwellenwerte, die in der Ausgabe des SP angezeigt werden `system sensors` Befehl:

- Unterer kritischer Schwellenwert (LCR)
- Unterer nicht kritischer Schwellenwert (LNC)
- Oberer nicht kritischer Schwellenwert (UNC)
- Oberer kritischer Schwellenwert (UCR)

Ein Sensormesswert zwischen LNC und LCR bzw. zwischen UNC und UCR bedeutet, dass die Komponente Anzeichen eines Problems aufweist und möglicherweise ein Systemausfall nicht ausgeschlossen werden kann. Daher sollten Sie eine baldige Komponentenwartung einplanen.

Ein Sensormesswert unter LCR oder über UCR bedeutet, dass die Komponente eine Fehlfunktion aufweist und ein Systemausfall droht. Daher erfordert eine sofortige Aktion.

Im folgenden Diagramm sind die Schweregrade dargestellt, die durch die Schwellenwerte angegeben werden:



Unter finden Sie den Messwert eines schwellenwertbasierten Sensors `Current` (Spalte `im`) `system sensors` Befehlsausgabe. Der `system sensors get sensor_name` Der Befehl zeigt zusätzliche Details für den angegebenen Sensor an. Wenn der Messwert eines schwellenwertbasierten Sensors den nicht kritischen und kritischen Schwellenwert überschreitet, meldet der Sensor ein Problem mit dem größer werdenden Schweregrad. Wenn der Messwert einen Grenzwert überschreitet, befindet sich der Status des Sensors in `system sensors` Befehlsausgabe ändert sich von `ok` Bis `nc` (Nicht kritisch) oder `cr` (Kritisch) abhängig vom überschrittenen Schwellenwert und eine Ereignismeldung wird im SEL-Ereignisprotokoll protokolliert.

Manche schwellenwertbasierten Sensoren weisen nicht alle vier Schwellenwertstufen auf. Für diese Sensoren werden die fehlenden Schwellenwerte angezeigt `na` Als ihre Grenzen im `system sensors` Befehlsausgabe, die angibt, dass der bestimmte Sensor keinen Grenzwert für den angegebenen Schwellenwert hat und der SP diesen Schwellenwert für den entsprechenden Sensor nicht überwacht.

Beispiel der Befehlsausgabe des Befehls „System Sensors“

Im folgenden Beispiel werden einige der von angezeigten Informationen angezeigt `system sensors` Befehl in der SP-CLI:


```
SP nodel> system sensors
```

Sensor Name	Current	Unit	Status	LCR	LNC
UNC	UCR				
CPU0_Temp_Margin	-55.000	degrees C	ok	na	na
-5.000	0.000				
CPU1_Temp_Margin	-56.000	degrees C	ok	na	na
-5.000	0.000				
In_Flow_Temp	32.000	degrees C	ok	0.000	10.000
42.000	52.000				
Out_Flow_Temp	38.000	degrees C	ok	0.000	10.000
59.000	68.000				
CPU1_Error	0x0	discrete	0x0180	na	na
na	na				
CPU1_Therm_Trip	0x0	discrete	0x0180	na	na
na	na				
CPU1_Hot	0x0	discrete	0x0180	na	na
na	na				
IO_Mid1_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
IO_Mid2_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
CPU_VTT	1.106	Volts	ok	1.028	1.048
1.154	1.174				
CPU0_VCC	1.154	Volts	ok	0.834	0.844
1.348	1.368				
3.3V	3.323	Volts	ok	3.053	3.116
3.466	3.546				
5V	5.002	Volts	ok	4.368	4.465
5.490	5.636				
STBY_1.8V	1.794	Volts	ok	1.678	1.707
1.892	1.911				
...					

Beispiel der Befehlsausgabe des Befehls „System Sensors“ für einen schwellenwertbasierten Sensor

Das folgende Beispiel zeigt das Ergebnis der Eingabe `system sensors get sensor_name` in der SP-CLI für den schwellenwertbasierten Sensor 5V:

```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID           : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading      : 5.002 (+/- 0) Volts
Status              : ok
Lower Non-Recoverable : na
Lower Critical       : 4.246
Lower Non-Critical   : 4.490
Upper Non-Critical   : 5.490
Upper Critical       : 5.758
Upper Non-Recoverable : na
Assertion Events     :
Assertions Enabled    : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+

```

Allgemeines zu den diskreten SP-Sensor-Statuswerten der Befehlsausgabe des Befehls „System Sensors“

Diskrete Sensoren verfügen über keine Schwellenwerte. Die Messwerte werden unter `Current` (Spalte in der SP-CLI) `system sensors` Befehlsausgabe ausgeführt, keine tatsächlichen Bedeutungen haben und werden daher vom SP ignoriert. Der `Status` (Spalte im) `system sensors` Mit der Befehlsausgabe werden die Statuswerte diskreter Sensoren im hexadezimalen Format angezeigt.

Beispiele diskreter Sensoren sind Sensoren für den Lüfter sowie für Netzteil- und Systemfehler. Die spezifische Liste der diskreten Sensoren hängt von der Plattform ab.

Sie können die SP-CLI verwenden `system sensors get sensor_name` Befehl für die Interpretation der Statuswerte für die meisten diskreten Sensoren. Die folgenden Beispiele zeigen die Ergebnisse der Eingabe `system sensors get sensor_name` Für die diskreten Sensoren `CPU0_Error` und `IO_Slot1_Present`:

```

SP node1> system sensors get CPU0_Error

Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID           : 7.97
Sensor Type (Discrete) : Temperature
States Asserted      : Digital State
                     : [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID          : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted    : Availability State
                   [Device Present]

```

Obwohl der `system sensors get sensor_name` Der Befehl zeigt die Statusinformationen für die meisten diskreten Sensoren an. Er bietet keine Statusinformationen für die diskreten Sensoren „System_FW_Status“, „System_Watchdog“, „PSU1_Input_Type“ und „PSU2_Input_Type“. Sie können die folgenden Informationen nutzen, um die Statuswerte dieser Sensoren zu interpretieren.

„System_FW_Status“

Der Zustand des Sensors „System_FW_Status“ wird in Form von angezeigt `0xAABB`. Sie können die Informationen von kombinieren `AA` Und `BB` Um den Zustand des Sensors zu ermitteln.

`AA` Kann einen der folgenden Werte aufweisen:

Werte	Zustand des Sensors
01	Fehler der System-Firmware
02	Die System-Firmware hängt
04	Fortschritt der System-Firmware

`BB` Kann einen der folgenden Werte aufweisen:

Werte	Zustand des Sensors
00	Die System-Software wurde ordnungsgemäß heruntergefahren
01	Arbeitsspeicher wird initialisiert
02	NVMEM-Initialisierungsvorgang läuft (wenn NVMEM vorhanden ist)
04	Wiederherstellen der Werte des Arbeitsspeicher-Controller-Hubs (MCH) (sofern NVMEM vorhanden ist)
05	Der Benutzer hat Setup aufgerufen

Werte	Zustand des Sensors
13	Booten des Betriebssystems oder LOADER
1F	BIOS wird gestartet
20	LOADER wird ausgeführt
21	LOADER programmiert die primäre BIOS-Firmware. Sie dürfen das System nicht herunterfahren.
22	LOADER programmiert die alternative BIOS-Firmware. Sie dürfen das System nicht herunterfahren.
2F	ONTAP wird ausgeführt
60	SP hat das System heruntergefahren
61	SP hat das System hochgefahren
62	SP hat das System zurückgesetzt
63	SP Watchdog aus- und wieder einschalten
64	SP Watchdog-Kaltstart

Beispiel: Der Status „0x042F“ des Sensors „System_FW_Status“ bedeutet „Fortschritt der System-Firmware (04), ONTAP läuft (2F)“.

„System_Watchdog“

Der Sensor „System_Watchdog“ kann einen der folgenden Zustände aufweisen:

- **0x0080**

Der Zustand dieses Sensors hat sich nicht geändert

Werte	Zustand des Sensors
0x0081	Timer-Interrupt
0x0180	Timer abgelaufen
0x0280	Hard Reset
0x0480	Schalten Sie aus

Werte	Zustand des Sensors
0x0880	Aus- und wieder einschalten

Beispiel: Der Status „0x0880“ des Sensors „System_Watchdog“ bedeutet, dass eine Watchdog-Zeitüberschreitung eingetreten ist, die ein aus- und Wiedereinschalten des Systems verursacht.

PSU1_Input_Type und PSU2_Input_Type

Die Sensoren „PSU1_Input_Type“ und „PSU2_Input_Type“ gelten nicht für Gleichstrom-Netzteile (DC). Bei Wechselstromnetzteilen (AC) kann der Status der Sensoren einen der folgenden Werte aufweisen:

Werte	Zustand des Sensors
0x01 xx	220V-Netzteil
0x02 xx	110-V-Netzteil

Beispiel: Der Status „0x0280“ des Sensors „PSU1_Input_Type“ gibt an, dass es sich bei dem Netzteil um ein 110V-Netzteil handelt.

Befehle zum Verwalten des SP über ONTAP

ONTAP bietet Befehle zum Verwalten des SP, einschließlich der SP-Netzwerkkonfiguration, SP-Firmware-Image, SSH-Zugriff auf den SP und allgemeine SP-Administration.

Befehle zum Verwalten der SP-Netzwerkkonfiguration


Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Aktivieren Sie die automatische SP-Netzwerkkonfiguration für den SP, um die IPv4- oder IPv6-Adressfamilie des angegebenen Subnetzes zu verwenden	<code>system service-processor network auto-configuration enable</code>
Deaktivieren Sie die automatische SP-Netzwerkkonfiguration für die IPv4- oder IPv6-Adressfamilie des für den SP angegebenen Subnetzes	<code>system service-processor network auto-configuration disable</code>
Zeigt die automatische SP-Netzwerkkonfiguration an	<code>system service-processor network auto-configuration show</code>

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
<p>Konfigurieren Sie das SP-Netzwerk für einen Node manuell, einschließlich folgender:</p> <ul style="list-style-type: none"> • Die IP-Adressfamilie (IPv4 oder IPv6) • Gibt an, ob die Netzwerkschnittstelle der angegebenen IP-Adressenfamilie aktiviert werden soll • Wenn Sie IPv4 verwenden, geben Sie an, ob Sie die Netzwerkkonfiguration vom DHCP-Server oder von der angegebenen Netzwerkadresse verwenden möchten • Die öffentliche IP-Adresse für den SP • Die Netmask für den SP (bei Verwendung von IPv4) • Die Netzwerk-Präfixlänge der Subnetzmaske für den SP (bei Verwendung von IPv6) • Die Gateway-IP-Adresse für den SP 	<pre>system service-processor network modify</pre>
<p>Zeigen Sie die SP-Netzwerkkonfiguration an, einschließlich der folgenden:</p> <ul style="list-style-type: none"> • Die konfigurierte Adressfamilie (IPv4 oder IPv6) und ob sie aktiviert ist • Der Typ des Remote-Management-Geräts • Der aktuelle SP-Status und der Link-Status • Netzwerkkonfiguration, wie IP-Adresse, MAC-Adresse, Netmask, Subnetz-Präfixlänge, Router-zugewiesene IP-Adresse, Link lokale IP-Adresse und Gateway-IP-Adresse • Die Zeit, zu der der SP zuletzt aktualisiert wurde • Der Name des Subnetzes, das für die automatische SP-Konfiguration verwendet wird • Gibt an, ob die vom IPv6-Router zugewiesene IP-Adresse aktiviert ist • Status der SP-Netzwerk-Einrichtung • Grund für den Fehler bei der Einrichtung des SP-Netzwerks 	<pre>system service-processor network show</pre> <p>Zum Anzeigen vollständiger SP-Netzwerkdetails ist der erforderlich <code>-instance</code> Parameter.</p>
<p>Ändern Sie die SP-API-Service-Konfiguration, einschließlich folgender Komponenten:</p> <ul style="list-style-type: none"> • Ändern des Ports, der vom SP-API-Service verwendet wird • Aktivieren oder Deaktivieren des SP-API-Service 	<pre>system service-processor api-service modify</pre> <p>(Erweiterte Berechtigungsebene)</p>

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Zeigt die SP-API-Servicekonfiguration an	<pre>system service-processor api-service show</pre> <p>(Erweiterte Berechtigungsebene)</p>
Erneuern der vom SP-API-Service verwendeten SSL- und SSH-Zertifikate für die interne Kommunikation	<ul style="list-style-type: none"> • Für ONTAP 9.5 oder höher: <code>system service-processor api-service renew-internal-certificates</code> • Für ONTAP 9.4 oder früher: <code>system service-processor api-service renew-certificates</code> <p>(Erweiterte Berechtigungsebene)</p>

Befehle zum Verwalten des SP-Firmware-Images

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Zeigen Sie Details zum derzeit installierten SP-Firmware-Image an, einschließlich: <ul style="list-style-type: none"> • Der Typ des Remote-Management-Geräts • Das Image (primär oder Backup), aus dem der SP gebootet wird, seinen Status und die Firmware-Version • Gibt an, ob das automatische Update der Firmware aktiviert ist und ob der letzte Aktualisierungsstatus angezeigt wird 	<pre>system service-processor image show</pre> <p>Der <code>-is-current</code> Parameter gibt das Image (primär oder Backup) an, von dem der SP derzeit gebootet wird, nicht wenn die installierte Firmware-Version auf dem aktuellen Stand ist.</p>
Aktiviert bzw. deaktiviert das automatische Firmware-Update des SP	<pre>system service-processor image modify</pre> <p>Standardmäßig wird die SP-Firmware automatisch mit dem Update der ONTAP aktualisiert oder wenn eine neue Version der SP-Firmware manuell heruntergeladen wird. Es wird nicht empfohlen, das automatische Update zu deaktivieren, da dies zu suboptimalen oder nicht qualifizierten Kombinationen zwischen dem ONTAP Image und dem SP-Firmware-Image führen kann.</p>

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Laden Sie manuell ein SP-Firmware-Image auf einem Node herunter	<pre>system node image get</pre> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>Bevor Sie den ausführen <code>system node image</code> Befehle. Sie müssen die Berechtigungsebene auf „erweitert“ setzen (<code>set -privilege advanced</code>) Geben Sie <code>y</code> ein, wenn Sie dazu aufgefordert werden, fortzufahren.</p> </div> <p>Das SP-Firmware-Image ist mit ONTAP verpackt. Sie müssen die SP-Firmware nur manuell herunterladen, es sei denn, Sie möchten eine SP-Firmware-Version verwenden, die sich von der des ONTAP-Paketens unterscheidet.</p>
<p>Zeigt den Status für das aktuelle, von ONTAP ausgelöste Firmware-Update an, einschließlich der folgenden Informationen:</p> <ul style="list-style-type: none"> • Die Start- und Endzeit für das aktuelle SP-Firmware-Update • Ob ein Update ausgeführt wird und der Prozentsatz, der abgeschlossen ist 	<pre>system service-processor image update-progress show</pre>

Befehle zum Verwalten von SSH-Zugriff auf den SP

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Gewähren Sie nur SP-Zugriff auf die angegebenen IP-Adressen	<pre>system service-processor ssh add-allowed-addresses</pre>
Blockieren Sie die angegebenen IP-Adressen vom Zugriff auf den SP	<pre>system service-processor ssh remove-allowed-addresses</pre>
Zeigt die IP-Adressen an, die auf den SP zugreifen können	<pre>system service-processor ssh show</pre>

Befehle für die allgemeine SP-Administration

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Zeigt allgemeine SP-Informationen an, einschließlich folgender: <ul style="list-style-type: none"> • Der Typ des Remote-Management-Geräts • Der aktuelle SP-Status • Gibt an, ob das SP-Netzwerk konfiguriert ist • Netzwerkinformationen, z. B. die öffentliche IP-Adresse und die MAC-Adresse • Die Version der SP-Firmware und die Version der Intelligent Platform Management Interface (IPMI) • Gibt an, ob das automatische Update der SP-Firmware aktiviert ist 	<code>system service-processor show</code> Zum Anzeigen vollständiger SP-Informationen muss das <code>-instance</code> Parameter.
Bootet den SP auf einem Node neu	<code>system service-processor reboot-sp</code>
Generieren und senden Sie eine AutoSupport Meldung, die die SP-Protokolldateien, die von einem angegebenen Node erfasst wurden, enthält	<code>system node autosupport invoke-splog</code>
Zeigt die Zuordnungszuordnung der gesammelten SP-Protokolldateien im Cluster an, einschließlich der Sequenznummern für die SP-Protokolldateien, die sich in jedem Sammlungs-Node befinden	<code>system service-processor log show-allocations</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

ONTAP-Befehle für BMC Management

Diese ONTAP-Befehle werden vom Baseboard Management Controller (BMC) unterstützt.

BMC verwendet einige der gleichen Befehle wie der Service-Prozessor (SP). Die folgenden SP-Befehle werden von BMC unterstützt.

Ihr Ziel ist	Verwenden Sie diesen Befehl
Rufen Sie die BMC-Informationen an	<code>system service-processor show</code>
BMC-Netzwerkkonfiguration anzeigen/ändern	<code>system service-processor network show/modify</code>
Setzen Sie den BMC zurück	<code>system service-processor reboot-sp</code>

Ihr Ziel ist	Verwenden Sie diesen Befehl
Anzeigen/Ändern der Details des derzeit installierten BMC-Firmware-Images	<code>system service-processor image show/modify</code>
Aktualisieren der BMC-Firmware	<code>system service-processor image update</code>
Zeigt den Status der neuesten BMC-Firmware-Aktualisierung an	<code>system service-processor image update-progress show</code>
Aktivieren Sie die automatische Netzwerkkonfiguration für den BMC, um eine IPv4- oder IPv6-Adresse im angegebenen Subnetz zu verwenden	<code>system service-processor network auto-configuration enable</code>
Deaktivieren Sie die automatische Netzwerkkonfiguration für eine IPv4- oder IPv6-Adresse im für den BMC angegebenen Subnetz	<code>system service-processor network auto-configuration disable</code>
Anzeigen der automatischen BMC-Netzwerkkonfiguration	<code>system service-processor network auto-configuration show</code>

Bei Befehlen, die von der BMC-Firmware nicht unterstützt werden, wird die folgende Fehlermeldung zurückgegeben.

```
::> Error: Command not supported on this platform.
```

BMC-CLI-Befehle

Sie können sich am BMC über SSH anmelden. Die folgenden Befehle werden von der BMC-Befehlszeile unterstützt.

Befehl	Funktion
System	Zeigt eine Liste aller Befehle an.
Systemkonsole	Stellt eine Verbindung mit der Konsole des Systems her. Nutzung <code>Ctrl+D</code> Um die Sitzung zu beenden.
Systemkern	Gibt einen Dump des Systemkerns aus und setzt ihn zurück.
Aus- und Wiedereinschalten des Systems	Schaltet das System aus und wieder ein.
Das System wird ausgeschaltet	Schaltet das System aus.

Befehl	Funktion
Das System wird eingeschaltet	Schaltet das System ein.
Der Status der Stromversorgung des Systems	Zeigt den Status der Netzspannung des Systems an.
System zurücksetzen	Setzen Sie das System zurück.
Systemprotokoll	Zeigt die Protokolle der Systemkonsole an
System-fru zeigt [id] an.	Zeigt alle/ausgewählte FRU-Informationen (Field Replaceable Unit) an.

Copyright-Informationen

Copyright © 2023 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.