



Cluster-Management mit der CLI

ONTAP 9

NetApp
April 24, 2024

Inhalt

Cluster-Management mit der CLI	1
Administrationsübersicht mit der CLI	1
Cluster- und SVM-Administratoren	1
Zugriff auf das Cluster über die CLI (nur Cluster-Administratoren)	3
Verwenden Sie die ONTAP Befehlszeilenschnittstelle	11
Verwalten von CLI-Sitzungen	27
Cluster-Management (nur Cluster-Administratoren)	28
Managen von Nodes	33
Konfigurieren Sie das SP/BMC-Netzwerk	57
Remote-Verwaltung von Knoten über den SP/BMC	64
Cluster-Zeit managen (nur Cluster-Administratoren)	95
Verwalten des Banners und der MOTD	98
Verwalten von Jobs und Zeitplanung	107
Backup und Restore von Cluster-Konfigurationen (nur Cluster-Administratoren)	110
Management von Core Dumps (nur Cluster-Administratoren)	120

Cluster-Management mit der CLI

Administrationsübersicht mit der CLI

Sie können ONTAP Systeme mit der Befehlszeilenschnittstelle (CLI) verwalten. Sie können die ONTAP Managementoberflächen verwenden, auf das Cluster zugreifen, Nodes managen und vieles mehr.

Sie sollten diese Verfahren unter den folgenden Umständen verwenden:

- Sie möchten mehr über den Umfang der ONTAP-Administratorfunktionen erfahren.
- Sie möchten die CLI verwenden, nicht System Manager oder ein automatisiertes Scripting Tool.

Verwandte Informationen

Weitere Informationen zur CLI-Syntax und -Verwendung finden Sie im <http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr/GUID-5CB10C70-AC11-41C0-8C16-B4D0DF916E9B.html> ["ONTAP 9 Manual Page Reference"] Dokumentation.

Cluster- und SVM-Administratoren

Cluster- und SVM-Administratoren

Cluster-Administratoren verwalten das gesamte Cluster und die Storage Virtual Machines (SVMs, früher Vserver genannt), die in dem Cluster enthalten sind. SVM-Administratoren managen nur ihre eigenen Daten-SVMs.

Cluster-Administratoren können den gesamten Cluster und seine Ressourcen verwalten. Zudem können sie Data SVMs einrichten und die SVM-Administration an SVM-Administratoren delegieren. Cluster-Administratoren verfügen über spezifische Funktionen, die von ihren Zugriffssteuerungsrollen abhängen. Standardmäßig verfügt ein Cluster-Administrator mit dem „admin“-Kontonamen oder Rollennamen über alle Funktionen, um das Cluster und SVMs zu verwalten.

SVM-Administratoren können nur ihren eigenen SVM-Storage und Netzwerkressourcen wie Volumes, Protokolle, LIFs und Services managen. Die spezifischen Funktionen, die SVM-Administratoren bieten, hängen von den Zugriffskontrollrollen ab, die von Cluster-Administratoren zugewiesen werden.



Die Befehlszeilenschnittstelle (CLI) von ONTAP verwendet in der Ausgabe weiterhin den Begriff „Vserver“ und `vserver`. Der Befehl- oder Parameternamen wurde nicht geändert.

Management des Zugriffs auf System Manager

Sie können den Zugriff eines Webbrowsers auf System Manager aktivieren oder deaktivieren. Sie können das System Manager-Protokoll auch anzeigen.

Sie können den Zugriff eines Webbrowsers auf System Manager mithilfe von `services web modify -name sysmgr -vserver cluster_name -enabled [true|false]`.

Die Protokollierung von System Manager wird im `/mroot/etc/log/mlog/sysmgr.log` Dateien des Node, der während des Zugriffs auf System Manager die Cluster-Management-LIF hostet. Sie

können die Protokolldateien über einen Browser anzeigen. Das Protokoll von System Manager ist auch in AutoSupport Meldungen enthalten.

Was ist der Cluster-Management-Server

Der Cluster-Management-Server, auch als *adminSVM* bezeichnet, ist eine spezialisierte Implementierung der Storage Virtual Machine (SVM), die den Cluster als eine einzelne, einfach zu verwaltende Einheit darstellt. Der Cluster-Management-Server dient nicht nur als grundlegende administrative Domäne, sondern ist auch Eigentümer von Ressourcen, die nicht logisch zu einer Daten-SVM gehören.

Der Cluster-Verwaltungsserver ist immer im Cluster verfügbar. Sie können über die Konsole oder Cluster-Management-LIF auf den Cluster-Managementserver zugreifen.

Bei Ausfall des Home-Netzwerk-Ports erfolgt automatisch ein Failover der Cluster-Management-LIF auf einen anderen Node im Cluster. Abhängig von den Konnektivitätsoptionen des verwendeten Managementprotokolls kann das Failover möglicherweise nicht bemerkt werden. Wenn Sie ein verbindungsloses Protokoll (z. B. SNMP) verwenden oder eine begrenzte Verbindung (z. B. HTTP) haben, werden Sie wahrscheinlich nicht bemerken, dass das Failover stattfindet. Wenn Sie jedoch eine langfristige Verbindung (z. B. SSH) verwenden, müssen Sie nach dem Failover eine Verbindung zum Cluster-Managementserver herstellen.

Wenn Sie ein Cluster erstellen, werden alle Merkmale der Cluster-Management-LIF konfiguriert, einschließlich seiner IP-Adresse, Netmask, des Gateway und des Ports.

Im Gegensatz zu einer Daten-SVM oder Node-SVM verfügt ein Cluster-Managementserver über keine Root-Volumes oder Host-Benutzer-Volumes (obwohl er System-Volumes hosten kann). Darüber hinaus kann ein Cluster-Management-Server nur LIFs des Cluster-Managementtyps nutzen.

Wenn Sie den ausführen `vserver show` Der Befehl wird in der Ausgabeliste für diesen Befehl der Cluster-Verwaltungsserver angezeigt.

SVMs

Ein Cluster besteht aus vier Arten von SVMs, die Sie beim Management des Clusters und seiner Ressourcen und Datenzugriff auf die Clients und Applikationen unterstützen.

Ein Cluster enthält die folgenden SVMs:

- Admin-SVM

Bei der Einrichtung des Clusters wird automatisch die Admin-SVM für den Cluster erstellt. Die Admin-SVM repräsentiert das Cluster.

- Node-SVM

Wenn der Node dem Cluster hinzugefügt wird, wird eine SVM erstellt, und der Node repräsentiert die einzelnen Nodes des Clusters.

- System-SVM (erweitert)

Für die Kommunikation auf Cluster-Ebene in einem IPspace wird automatisch eine System-SVM erstellt.

- Daten-SVM

Eine Daten-SVM stellt die Daten dar, die SVMs dienen. Nach der Cluster-Einrichtung muss ein Cluster-Administrator Daten-SVMs erstellen und diesen SVMs Volumes hinzufügen, um den Datenzugriff vom Cluster aus zu ermöglichen.

Ein Cluster muss mindestens eine Daten-SVM aufweisen, um seine Clients mit Daten versorgen zu können.



Sofern nichts anderes angegeben wird, bezieht sich der Begriff SVM auf eine Daten- (Datenservice-) SVM.

In der CLI werden SVMs als Vserver angezeigt.

Zugriff auf das Cluster über die CLI (nur Cluster-Administratoren)

Greifen Sie über den seriellen Port auf das Cluster zu

Sie können direkt über eine Konsole auf das Cluster zugreifen, die mit dem seriellen Port eines Node verbunden ist.

Schritte

1. Drücken Sie an der Konsole die Eingabetaste.

Das System antwortet mit der Eingabeaufforderung für die Anmeldung.

2. Führen Sie an der Anmeldeaufforderung einen der folgenden Schritte aus:

Zugriff auf das Cluster mit...	Geben Sie den folgenden Kontonamen ein...
Das Standard-Cluster-Konto	<code>admin</code>
Ein alternatives Administratorkonto	<code>username</code>

Das System antwortet mit der Passwort-Eingabeaufforderung.

3. Geben Sie das Kennwort für das Administratorkonto oder das Administratorbenutzerkonto ein, und drücken Sie dann die Eingabetaste.

Greifen Sie über SSH auf das Cluster zu

Sie können SSH-Anforderungen an das Cluster ausgeben, um administrative Aufgaben durchzuführen. SSH ist standardmäßig aktiviert.

Was Sie benötigen

- Sie müssen über ein Benutzerkonto verfügen, das für die Verwendung konfiguriert ist `ssh` Als Zugriffsmethode.

Der `-application` Parameter von `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Der `security login` ["Man-Pages"](#) Enthalten zusätzliche Informationen.

- Wenn Sie ein Active Directory (AD)-Domänenbenutzerkonto für den Zugriff auf das Cluster verwenden, muss ein Authentifizierungstunnel für das Cluster über eine CIFS-fähige Storage-VM eingerichtet worden sein, und Ihr AD-Domänenbenutzerkonto muss ebenfalls mit dem Cluster hinzugefügt worden sein `ssh` Als Zugriffsmethode und `domain` Als Authentifizierungsmethode.
- Wenn Sie IPv6-Verbindungen verwenden, muss IPv6 bereits auf dem Cluster konfiguriert und aktiviert sein. Firewallrichtlinien müssen bereits mit IPv6-Adressen konfiguriert sein.

Der `network options ipv6 show` Befehl zeigt an, ob IPv6 aktiviert ist. Der `system services firewall policy show` Befehl zeigt Firewallrichtlinien an.

Über diese Aufgabe

- Sie müssen einen OpenSSH 5.7 oder höher -Client verwenden.
- Nur das SSH v2-Protokoll wird unterstützt; SSH v1 wird nicht unterstützt.
- ONTAP unterstützt maximal 64 gleichzeitige SSH-Sitzungen pro Node.

Wenn sich die Cluster-Management-LIF auf dem Node befindet, wird dieses Limit zusammen mit der Node-Management-LIF verwendet.

Falls die Rate der eingehenden Verbindungen mehr als 10 pro Sekunde ist, wird der Dienst vorübergehend für 60 Sekunden deaktiviert.

- ONTAP unterstützt nur die Verschlüsselungsalgorithmen AES und 3DES für SSH (auch bekannt als *Chiffers*).

AES wird mit 128, 192 und 256 Bit in Schlüssellänge unterstützt. 3DES ist 56 Bit in Schlüssellänge wie im Original DES, wird aber dreimal wiederholt.

- Wenn der FIPS-Modus aktiviert ist, sollten SSH-Clients mit den öffentlichen Schlüssel-Algorithmen des Elliptic Curve Digital Signature Algorithm (ECDSA) verhandeln, damit die Verbindung erfolgreich hergestellt werden kann.
- Wenn Sie von einem Windows-Host aus auf die ONTAP-CLI zugreifen möchten, können Sie ein Dienstprogramm eines Drittanbieters wie z. B. PuTTY verwenden.
- Wenn Sie einen Windows AD-Benutzernamen verwenden, um sich bei ONTAP anzumelden, sollten Sie dieselben Groß- oder Kleinbuchstaben verwenden, die beim Erstellen des AD-Benutzernamens und des Domänennamens in ONTAP verwendet wurden.

Bei AD-Benutzernamen und -Domain-Namen wird die Groß-/Kleinschreibung nicht beachtet. Bei ONTAP-Benutzernamen muss die Groß-/Kleinschreibung beachtet werden. Eine Diskrepanz zwischen dem in ONTAP erstellten Benutzernamen und dem in AD erstellten Benutzernamen führt zu einem Anmeldefehler.

SSH-Authentifizierungsoptionen

- Ab ONTAP 9.3 ist dies möglich ["Aktivieren Sie SSH-Multi-Faktor-Authentifizierung"](#) Für lokale Administratorkonten.

Wenn die Multi-Faktor-Authentifizierung mittels SSH aktiviert ist, werden Benutzer mit einem öffentlichen Schlüssel und einem Passwort authentifiziert.

- Ab ONTAP 9.4 ist dies möglich ["Aktivieren Sie SSH-Multi-Faktor-Authentifizierung"](#) Für LDAP- und NIS-Remote-Benutzer.
- Ab ONTAP 9.13.1 können Sie optional der SSH-Authentifizierung eine Zertifikatsüberprüfung hinzufügen, um die Anmeldesicherheit zu erhöhen. Um dies zu tun, ["Verknüpfen Sie ein X.509-Zertifikat mit dem"](#)

öffentlichen Schlüssel" Die ein Konto verwendet. Wenn Sie sich mit SSH sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem X.509-Zertifikat anmelden, überprüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor Sie sich mit dem öffentlichen SSH-Schlüssel authentifizieren. Die SSH-Anmeldung wird abgelehnt, wenn das Zertifikat abgelaufen ist oder widerrufen wurde und der öffentliche SSH-Schlüssel automatisch deaktiviert wird.

- Ab ONTAP 9.14.1 können Sie optional die zwei-Faktor-Authentifizierung von Cisco Duo zur SSH-Authentifizierung hinzufügen, um die Anmeldesicherheit zu erhöhen. Nach der ersten Anmeldung, nachdem Sie die Cisco Duo-Authentifizierung aktiviert haben, müssen Benutzer ein Gerät registrieren, das als Authentifikator für SSH-Sitzungen dient. Siehe "[Konfigurieren Sie Cisco Duo 2FA für SSH-Anmeldungen](#)" Weitere Informationen zur Konfiguration der Cisco Duo SSH-Authentifizierung für ONTAP.

Schritte

1. Geben Sie von einem Administrationshost das ein `ssh` Befehl in einem der folgenden Formate:

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

Wenn Sie ein AD-Domänenbenutzerkonto verwenden, müssen Sie angeben *username* Im Format von *domainname\AD_accountname* (Mit doppelten umgekehrten Schrägstrichen nach dem Domain-Namen) oder "*domainname\AD_accountname*" (Eingeschlossen in doppelte Anführungszeichen und mit einem einzelnen umgekehrten Schrägstrich nach dem Domainnamen).

hostname_or_IP Ist der Host-Name oder die IP-Adresse der Cluster-Management-LIF oder eine Node-Management-LIF. Es wird empfohlen, die Cluster-Management-LIF zu verwenden. Sie können eine IPv4- oder IPv6-Adresse verwenden.

command Ist für SSH-interaktive Sessions nicht erforderlich.

Beispiele für SSH-Anforderungen

Die folgenden Beispiele zeigen, wie das Benutzerkonto mit dem Namen „joe“ eine SSH-Anforderung für den Zugriff auf ein Cluster ausgeben kann, dessen Cluster-Management-LIF 10.72.137.28 ist:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node           Health  Eligibility
-----
node1          true   true
node2          true   true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

Die folgenden Beispiele zeigen, wie das Benutzerkonto „john“ aus der Domäne „DOMAIN1“ eine SSH-Anforderung für den Zugriff auf einen Cluster ausgeben kann, dessen Cluster-Management-LIF 10.72.137.28 ist:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

Das folgende Beispiel zeigt, wie das Benutzerkonto mit dem Namen „joe“ eine SSH MFA-Anforderung für den Zugriff auf ein Cluster ausgeben kann, dessen Cluster-Management-LIF 10.72.137.32 ist:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```


SSH-Anmeldesicherheit

Ab ONTAP 9.5 können Sie Informationen zu früheren Anmeldungen, erfolglosen Anmeldeversuchen und Änderungen Ihrer Berechtigungen seit Ihrer letzten erfolgreichen Anmeldung anzeigen.

Sicherheitsbezogene Informationen werden angezeigt, wenn Sie sich erfolgreich als SSH-Admin-Benutzer einloggen. Sie werden über die folgenden Bedingungen benachrichtigt:

- Das letzte Mal, wenn Ihr Kontoname angemeldet wurde.
- Die Anzahl der fehlgeschlagenen Anmeldeversuche seit der letzten erfolgreichen Anmeldung.
- Gibt an, ob sich die Rolle seit der letzten Anmeldung geändert hat (z. B. wenn sich die Rolle des Administratorkontos von „admin“ in „Backup“ geändert hat)
- Gibt an, ob die Funktionen zum Hinzufügen, Ändern oder Löschen der Rolle seit der letzten Anmeldung geändert wurden.



Wenn eine der angezeigten Informationen verdächtig ist, sollten Sie sich sofort an Ihre Sicherheitsabteilung wenden.

Um diese Informationen bei der Anmeldung zu erhalten, müssen die folgenden Voraussetzungen erfüllt sein:

- Ihr SSH-Benutzerkonto muss in ONTAP bereitgestellt werden.
- Ihre SSH-Sicherheitsanmeldung muss erstellt werden.
- Ihr Anmeldeversuch muss erfolgreich sein.

Einschränkungen und andere Überlegungen bei der SSH-Anmeldesicherheit

Die folgenden Einschränkungen und Überlegungen gelten für die Sicherheitsinformationen für SSH-Anmeldungen:

- Die Informationen sind nur für SSH-basierte Anmeldungen verfügbar.
- Bei gruppenbasierten Administratorkonten wie LDAP/NIS- und AD-Konten können Benutzer die SSH-Anmeldeinformationen anzeigen, wenn die Gruppe, deren Mitglied sie sind, als Administratorkonto in ONTAP bereitgestellt wird.

Für diese Benutzer können jedoch keine Warnmeldungen über Änderungen an der Rolle des Benutzerkontos angezeigt werden. Außerdem können Benutzer, die zu einer AD-Gruppe gehören, die als Administratorkonto in ONTAP bereitgestellt wurde, nicht die Anzahl der fehlgeschlagenen Anmeldeversuche anzeigen, die seit der letzten Anmeldung aufgetreten sind.

- Die für einen Benutzer gespeicherten Informationen werden gelöscht, wenn das Benutzerkonto aus ONTAP gelöscht wird.
- Die Informationen werden nicht für andere Verbindungen als SSH angezeigt.

Beispiele für Sicherheitsdaten für SSH-Anmeldungen

Die folgenden Beispiele veranschaulichen die Art der Informationen, die nach der Anmeldung angezeigt

werden.

- Diese Meldung wird nach jeder erfolgreichen Anmeldung angezeigt:

```
Last Login : 7/19/2018 06:11:32
```

- Diese Meldungen werden angezeigt, wenn seit der letzten erfolgreichen Anmeldung erfolglos versucht wurde:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Diese Meldungen werden angezeigt, wenn Anmeldeversuche nicht erfolgreich waren und Ihre Berechtigungen seit der letzten erfolgreichen Anmeldung geändert wurden:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Aktivieren Sie Telnet- oder RSH-Zugriff auf den Cluster

Als Best Practice für Sicherheit sind Telnet und RSH in der vordefinierten Management-Firewall-Richtlinie deaktiviert (`mgmt`). Um es dem Cluster zu ermöglichen, Telnet- oder RSH-Anfragen zu akzeptieren, müssen Sie eine neue Management Firewall-Richtlinie erstellen, über die Telnet- oder RSH-Anfragen aktiviert sind, und die neue Richtlinie dann der Cluster-Management-LIF zuordnen.

Über diese Aufgabe

ONTAP verhindert das Ändern vordefinierter Firewall-Richtlinien, doch Sie können durch das Klonen vordefinierter Richtlinien eine neue Richtlinie erstellen `mgmt` Management-Firewall-Richtlinie und dann die Aktivierung von Telnet oder RSH unter der neuen Richtlinie. Allerdings sind Telnet und RSH keine sicheren Protokolle. Daher sollten Sie erwägen, SSH zum Zugriff auf den Cluster zu verwenden. SSH bietet eine sichere Remote Shell und interaktive Netzwerksitzung.

Führen Sie die folgenden Schritte durch, um Telnet- oder RSH-Zugriff auf die Cluster zu aktivieren:

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:
`set advanced`
2. Aktivieren eines Sicherheitsprotokolls (RSH oder Telnet):
`security protocol modify -application security_protocol -enabled true`
3. Erstellen Sie eine neue Management-Firewall-Richtlinie auf der Grundlage von `mgmt` Management-Firewallrichtlinie:
`system services firewall policy clone -policy mgmt -destination-policy policy-name`

4. Aktivieren Sie Telnet oder RSH unter der neuen Management Firewall-Richtlinie:
system services firewall policy create -policy policy-name -service security_protocol -action allow -ip-list ip_address/netmask Um alle IP-Adressen zuzulassen, sollten Sie angeben `-ip-list 0.0.0.0/0`
5. Zuordnen der neuen Richtlinie zu der Cluster-Management-LIF:
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt -firewall-policy policy-name

Greifen Sie über Telnet auf das Cluster zu

Sie können dem Cluster Telnet-Anfragen zur Ausführung von Administrationaufgaben ausgeben. Telnet ist standardmäßig deaktiviert.

Was Sie benötigen

Bevor Sie per Telnet auf das Cluster zugreifen können, müssen die folgenden Bedingungen erfüllt sein:

- Sie müssen über ein lokales Cluster-Benutzerkonto verfügen, das für die Verwendung von Telnet als Zugriffsmethode konfiguriert ist.

Der `-application` Parameter von `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Weitere Informationen finden Sie im `security login` Man-Pages.

- Telnet muss bereits in der Management-Firewall-Richtlinie aktiviert sein, die vom Cluster- oder Node-Management-LIFs verwendet wird, damit Telnet-Anfragen die Firewall durchlaufen können.

Standardmäßig ist Telnet deaktiviert. Der `system services firewall policy show` Befehl mit dem `-service telnet` Parameter zeigt an, ob Telnet in einer Firewallrichtlinie aktiviert wurde. Weitere Informationen finden Sie im `system services firewall policy` Man-Pages.

- Wenn Sie IPv6-Verbindungen verwenden, muss IPv6 bereits auf dem Cluster konfiguriert und aktiviert sein. Firewallrichtlinien müssen bereits mit IPv6-Adressen konfiguriert sein.

Der `network options ipv6 show` Befehl zeigt an, ob IPv6 aktiviert ist. Der `system services firewall policy show` Befehl zeigt Firewallrichtlinien an.

Über diese Aufgabe

- Telnet ist kein sicheres Protokoll.

Sie sollten SSH verwenden, um auf das Cluster zuzugreifen. SSH bietet eine sichere Remote Shell und interaktive Netzwerksitzung.

- ONTAP unterstützt maximal 50 gleichzeitige Telnet-Sitzungen pro Node.

Wenn sich die Cluster-Management-LIF auf dem Node befindet, wird dieses Limit zusammen mit der Node-Management-LIF verwendet.

Falls die Rate der kommenden Verbindungen mehr als 10 pro Sekunde ist, wird der Dienst vorübergehend für 60 Sekunden deaktiviert.

- Wenn Sie von einem Windows-Host aus auf die ONTAP-CLI zugreifen möchten, können Sie ein Dienstprogramm eines Drittanbieters wie z. B. PuTTY verwenden.

Schritte

1. Geben Sie an einem Administrationshost den folgenden Befehl ein:

```
telnet hostname_or_IP
```

hostname_or_IP ist der Host-Name oder die IP-Adresse der Cluster-Management-LIF oder eine Node-Management-LIF. Es wird empfohlen, die Cluster-Management-LIF zu verwenden. Sie können eine IPv4- oder IPv6-Adresse verwenden.

Beispiel für eine Telnet-Anforderung

Das folgende Beispiel zeigt, wie der Benutzer „joe“, der mit Telnet-Zugriff eingerichtet wurde, eine Telnet-Anforderung für den Zugriff auf einen Cluster ausgeben kann, dessen Cluster-Management-LIF 10.72.137.28 ist:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

Zugriff auf den Cluster über RSH

Sie können dem Cluster RSH-Anfragen zur Ausführung administrativer Aufgaben ausgeben. RSH ist kein sicheres Protokoll und ist standardmäßig deaktiviert.

Was Sie benötigen

Bevor Sie RSH verwenden können, müssen die folgenden Bedingungen erfüllt werden:

- Sie müssen über ein lokales Cluster-Benutzerkonto verfügen, das so konfiguriert ist, dass RSH als Zugriffsmethode verwendet wird.

Der `-application` Parameter von `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Weitere Informationen finden Sie im `security login` Man-Pages.

- RSH muss bereits in der Management-Firewall-Richtlinie aktiviert sein, die von den Cluster- oder Node-Management-LIFs verwendet wird, damit RSH-Anfragen die Firewall durchlaufen können.

RSH ist standardmäßig deaktiviert. Der `system services firewall policy show` Befehl mit dem `-service rsh` Parameter zeigt an, ob RSH in einer Firewallrichtlinie aktiviert wurde. Weitere Informationen finden Sie im `system services firewall policy` Man-Pages.

- Wenn Sie IPv6-Verbindungen verwenden, muss IPv6 bereits auf dem Cluster konfiguriert und aktiviert sein. Firewallrichtlinien müssen bereits mit IPv6-Adressen konfiguriert sein.

Der `network options ipv6 show` Befehl zeigt an, ob IPv6 aktiviert ist. Der `system services firewall policy show` Befehl zeigt Firewallrichtlinien an.

Über diese Aufgabe

- RSH ist kein sicheres Protokoll.

Sie sollten SSH verwenden, um auf das Cluster zuzugreifen. SSH bietet eine sichere Remote Shell und interaktive Netzwerksitzung.

- ONTAP unterstützt maximal 50 RSH-Sitzungen pro Node.

Wenn sich die Cluster-Management-LIF auf dem Node befindet, wird dieses Limit zusammen mit der Node-Management-LIF verwendet.

Falls die Rate der kommenden Verbindungen mehr als 10 pro Sekunde ist, wird der Dienst vorübergehend für 60 Sekunden deaktiviert.

Schritte

1. Geben Sie an einem Administrationshost den folgenden Befehl ein:

```
rsh hostname_or_IP -l username:passwordcommand
```

hostname_or_IP ist der Host-Name oder die IP-Adresse der Cluster-Management-LIF oder eine Node-Management-LIF. Es wird empfohlen, die Cluster-Management-LIF zu verwenden. Sie können eine IPv4- oder IPv6-Adresse verwenden.

command ist der Befehl, den Sie über RSH ausführen möchten.

Beispiel einer RSH-Anforderung

Das folgende Beispiel zeigt, wie der Benutzer namens „joe“, der mit RSH-Zugriff eingerichtet wurde, eine RSH-Anforderung zum Ausführen des ausgeben kann `cluster show` Befehl:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

2 entries were displayed.

```
admin_host$
```

Verwenden Sie die ONTAP Befehlszeilenschnittstelle

Über die ONTAP Befehlszeilenschnittstelle

Die Befehlszeilenschnittstelle (CLI) von ONTAP liefert eine befehlsbasierte Ansicht der Managementoberfläche. Sie geben an der Eingabeaufforderung des Storage-Systems Befehle ein, und die Befehlsergebnisse werden in Text angezeigt.

Die CLI-Eingabeaufforderung wird als dargestellt `cluster_name::>`.

Wenn Sie die Berechtigungsebene festlegen (d. h. die `-privilege` Parameter von `set` Befehl) zu `advanced` Die Eingabeaufforderung enthält ein Sternchen (*), z. B.:

```
cluster_name::*>
```

Übersicht über die verschiedenen Shells für CLI-Befehle (nur Cluster-Administratoren)

Der Cluster hat drei unterschiedliche Shells für CLI-Befehle, die *clustershell*, die *nodeshell* und die *systemshell*. Die Shells sind für unterschiedliche Zwecke, und sie haben jeweils einen anderen Befehlssatz.

- Die clustershell ist die native Shell, die automatisch gestartet wird, wenn Sie sich beim Cluster anmelden.

Er stellt alle Befehle bereit, die Sie für die Konfiguration und das Management des Clusters benötigen. Die clustershell CLI-Hilfe (wird von `?` ausgelöst ? An der clustershell Eingabeaufforderung) werden verfügbare clustershell-Befehle angezeigt. Der `man command_name` Mit dem Befehl in der clustershell wird die man-Page für den angegebenen clustershell-Befehl angezeigt.

- Die nodeshell ist eine spezielle Shell für Befehle, die nur auf Knotenebene wirksam werden.

Die Nodeshell ist durch die zugänglich `system node run` Befehl.

Die nodeshell CLI-Hilfe (ausgelöst von `?` Oder `help` Am nodeshell prompt) werden verfügbare nodeshell Befehle angezeigt. Der `man command_name` Mit dem Befehl in nodeshell wird die man-Page für den angegebenen nodeshell Befehl angezeigt.

Viele häufig verwendete Nodeshell Befehle und Optionen werden in der Clustershell alialisiert und können auch von der clustershell ausgeführt werden.

- Die Systemshell ist eine Low-Level-Shell, die nur zu Diagnose- und Fehlerbehebungszwecken verwendet wird.

Die Systemshell und das zugehörige „diag“-Konto sind für diagnostische Zwecke auf niedriger Ebene bestimmt. Für ihren Zugriff ist die Diagnose-Berechtigungsebene erforderlich und nur für den technischen Support reserviert, um Aufgaben zur Fehlerbehebung auszuführen.

Zugriff von nodeshell Befehlen und Optionen in der clustershell

Nodeshell Befehle und Optionen sind über die nodeshell zugänglich:

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

Viele häufig verwendete Nodeshell Befehle und Optionen werden in der Clustershell alialisiert und können auch von der clustershell ausgeführt werden.

Auf Nodeshell Optionen, die in der Clustershell unterstützt werden, kann über die zugegriffen werden `vserver options clustershell` Befehl. Um diese Optionen anzuzeigen, können Sie eine der folgenden Aktionen ausführen:

- Fragen Sie die clustershell-CLI mit `vserver options -vserver nodename_or_clustername -option-name ?`
- Auf das zugreifen `vserver options` Man-Page in der clustershell CLI mit `man vserver options`

Wenn Sie in der clustershell einen Befehl oder eine ältere Option eingeben und der Befehl oder die Option

einen entsprechenden clustershell-Befehl hat, informiert ONTAP Sie über den entsprechenden clustershell-Befehl.

Wenn Sie einen nodeshell- oder älteren Befehl oder eine Option eingeben, die in der Clustershell nicht unterstützt wird, informiert ONTAP Sie über den Status „nicht unterstützt“ für den Befehl oder die Option.

Zeigt die verfügbaren nodeshell-Befehle an

Sie können eine Liste der verfügbaren nodeshell Befehle erhalten, indem Sie die CLI-Hilfe aus der nodeshell.

Schritte

1. Um auf den nodeshell zuzugreifen, geben Sie den folgenden Befehl an der Systemaufforderung von clustershell ein:

```
system node run -node {nodename|local}
```

`local` Ist der Node, den Sie für den Zugriff auf das Cluster verwendet haben.



Der `system node run` Befehl hat einen Alias-Befehl, `run`.

2. Geben Sie den folgenden Befehl in die nodeshell ein, um die Liste der verfügbaren nodeshell Befehle anzuzeigen:

```
[commandname] help
```

``_commandname_`` Ist der Name des Befehls, dessen Verfügbarkeit Sie anzeigen möchten. Wenn Sie nicht einbeziehen ``_commandname_``, Die CLI zeigt alle verfügbaren nodeshell-Befehle an.

Ihre Eingabe `exit` Oder geben Sie Strg-D ein, um zur clustershell-CLI zurückzukehren.

Beispiel für die Anzeige von verfügbaren nodeshell Befehlen

Das folgende Beispiel greift auf die nodeshell eines Knotens namens `node2` zu und zeigt Informationen für den nodeshell Befehl `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

Methoden zur Navigation in CLI-Befehlsverzeichnissen

Befehle in der CLI sind in einer Hierarchie nach Befehlsverzeichnissen gegliedert. Sie können Befehle in der Hierarchie ausführen, indem Sie entweder den vollständigen Befehlspfad eingeben oder durch die Verzeichnisstruktur navigieren.

Bei Verwendung der CLI können Sie auf ein Befehlsverzeichnis zugreifen, indem Sie an der Eingabeaufforderung den Namen des Verzeichnisses eingeben und anschließend die Eingabetaste drücken. Der Verzeichnisname wird dann in den Text der Aufforderung enthalten, um anzugeben, dass Sie mit dem entsprechenden Befehlsverzeichnis interagieren. Um sich tiefer in die Befehlshierarchie zu bewegen, geben Sie den Namen eines Unterverzeichnisses für Befehle ein, gefolgt von der Eingabetaste. Der Unterverzeichnisname wird dann in den Text der Eingabeaufforderung aufgenommen und der Kontext wechselt in das Unterverzeichnis.

Sie können durch mehrere Befehlsverzeichnisse navigieren, indem Sie den gesamten Befehl eingeben. Beispielsweise können Sie Informationen über Festplattenlaufwerke anzeigen, indem Sie das eingeben `storage disk show` Befehl an der Eingabeaufforderung. Sie können den Befehl auch ausführen, indem Sie nacheinander durch ein Befehlsverzeichnis navigieren, wie im folgenden Beispiel gezeigt:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Sie können Befehle abkürzen, indem Sie nur die minimale Anzahl von Buchstaben in einen Befehl eingeben, der den Befehl für das aktuelle Verzeichnis eindeutig macht. Um beispielsweise den Befehl im vorherigen Beispiel zu kürzen, können Sie eingeben `st d sh`. Außerdem können Sie mit der Tabulatortaste die gekürzten Befehle erweitern und die Parameter eines Befehls, einschließlich der Standardparameter, anzeigen.

Sie können das verwenden `top` Befehl, um die oberste Ebene der Befehlshierarchie zu wechseln, und die `up` Befehl oder `..` Befehl, um in der Befehlshierarchie eine Stufe nach oben zu wechseln.



Befehle und Befehlsoptionen, denen ein Sternchen (*) in der CLI vorangestellt ist, können nur auf der erweiterten Berechtigungsebene oder höher ausgeführt werden.

Regeln zum Angeben von Werten in der CLI

Die meisten Befehle verfügen über einen oder mehrere erforderliche oder optionale Parameter. Für viele Parameter muss ein Wert angegeben werden. Es gibt einige Regeln zum Angeben von Werten in der CLI.

- Ein Wert kann eine Zahl, ein Boolescher Spezifikator, eine Auswahl aus einer Aufzählungsliste mit vordefinierten Werten oder eine Textzeichenfolge sein.

Einige Parameter akzeptieren eine kommasetrennte Liste mit zwei oder mehr Werten. Kommasetrennte Wertelisten müssen nicht in Anführungszeichen („“) stehen. Immer wenn Sie Text, ein Leerzeichen oder ein Abfragezeichen (wenn nicht als Abfrage beabsichtigt oder Text, der mit einem kleiner-als- oder größer-als-Symbol beginnt) angeben, müssen Sie diesen bzw. dieses mit Anführungszeichen umschließen.

- Die CLI interpretiert ein Fragezeichen („?“) Als Befehl werden Hiltinformationen für einen bestimmten

Befehl angezeigt.

- Einige Text, die Sie in die CLI eingeben, z. B. Befehlsnamen, Parameter und bestimmte Werte, ist nicht zwischen Groß- und Kleinschreibung zu beachten.

Wenn Sie beispielsweise Parameterwerte für das eingeben `vserver cifs` Befehle, Großschreibung wird ignoriert. Die meisten Parameterwerte, z. B. die Namen der Nodes, Storage Virtual Machines (SVMs), Aggregate, Volumes und logische Schnittstellen, werden jedoch von Groß-/Kleinschreibung berücksichtigt.

- Wenn Sie den Wert eines Parameters löschen möchten, der einen String oder eine Liste nimmt, geben Sie einen leeren Satz Anführungszeichen ("") oder einen Strich ("-") an.
- Das Hash-Zeichen („#“), auch als Rautzeichen bekannt, gibt einen Kommentar für eine Befehlszeileingabe an. Falls verwendet, sollte es nach dem letzten Parameter in einer Befehlszeile angezeigt werden.

Die CLI ignoriert den Text zwischen „#“ und dem Zeilenende.

Im folgenden Beispiel wird eine SVM mit einem Textkommentar erstellt. Die SVM wird dann geändert, um den Kommentar zu löschen:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

Im folgenden Beispiel zeigt ein Kommentar in der Befehlszeile, der das „#“-Zeichen verwendet, was der Befehl tut.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Methoden zur Anzeige des Befehlsverlaufs und der Neuausgabe von Befehlen

Jede CLI-Session führt den Verlauf aller Befehle durch, die in ihr ausgegeben wurden. Sie können den Befehlsverlauf der Sitzung anzeigen, in der Sie sich derzeit befinden. Sie können Befehle auch neu eingeben.

Zum Anzeigen des Befehlsverlaufs können Sie den verwenden `history` Befehl.

Zum Neugeben eines Befehls können Sie den verwenden `redo` Befehl mit einem der folgenden Argumente:

- Eine Zeichenfolge, die einem Teil eines vorherigen Befehls entspricht

Beispiel: Wenn der einzige `volume` Der Befehl, den Sie ausgeführt haben, ist `volume show`, Sie können die verwenden `redo volume` Befehl zum erneuten Ausführen des Befehls.

- Die numerische ID eines vorherigen Befehls, wie im aufgeführt `history` Befehl

Beispielsweise können Sie die verwenden `redo 4` Befehl zum Neugeben des vierten Befehls in der Verlaufsliste.

- Ein negativer Offset vom Ende der Verlaufsliste

Beispielsweise können Sie die verwenden `redo -2` Befehl zum Neugeben des Befehls, dass Sie vor zwei Befehlen ausgeführt haben.

Um beispielsweise den Befehl wieder auszuführen, der an dem Ende des Befehlsverlaufs liegt, geben Sie den folgenden Befehl ein:

```
cluster1::> redo -3
```

Tastenkombinationen zum Bearbeiten von CLI-Befehlen

Der Befehl an der aktuellen Eingabeaufforderung ist der aktive Befehl. Mit Tastenkombinationen können Sie den aktiven Befehl schnell bearbeiten. Diese Tastenkombinationen ähneln denen der UNIX `tcsh` Shell und des Emacs-Editors.

In der folgenden Tabelle werden die Tastenkombinationen zum Bearbeiten von CLI-Befehlen aufgeführt. „Strg-“ zeigt an, dass Sie die Strg-Taste gedrückt halten, während Sie das gewünschte Zeichen eingeben. „Esc-“ gibt an, dass Sie die Esc-Taste drücken und loslassen und dann das nach ihr angegebene Zeichen eingeben.

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination...
Bewegen Sie den Cursor um ein Zeichen zurück	Strg-B
Hinterpfeil	Bewegen Sie den Cursor um ein Zeichen nach vorne
Strg-F	Vorwärtspfeil
Bewegen Sie den Cursor um ein Wort zurück	ESC-B
Bewegen Sie den Cursor um ein Wort nach vorne	ESC-F
Bewegen Sie den Cursor an den Anfang der Zeile	Strg+A
Bewegen Sie den Cursor an das Ende der Zeile	Strg-E
Entfernen Sie den Inhalt der Befehlszeile vom Anfang der Zeile zum Cursor und speichern Sie ihn im Schnittpuffer. Der Cut-Puffer wirkt wie temporärer Speicher, ähnlich dem, was in einigen Programmen als <i>Clipboard</i> bezeichnet wird.	Strg-U

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination...
Entfernen Sie den Inhalt der Befehlszeile vom Cursor zum Zeilenende und speichern Sie ihn im Schnittpuffer	Strg-K
Entfernen Sie den Inhalt der Befehlszeile vom Cursor bis zum Ende des folgenden Wortes und speichern Sie ihn im Schnittpuffer	ESC-D
Entfernen Sie das Wort vor dem Cursor, und speichern Sie es im Schnittpuffer	Strg-W
Geben Sie den Inhalt des Schnittpuffers ein, und drücken Sie ihn in die Befehlszeile am Cursor	Strg-Y
Das Zeichen vor dem Cursor löschen	Strg-H
Rücktaste	Löschen Sie das Zeichen, in dem sich der Cursor befindet
Strg-D	Löschen Sie die Zeile
Strg-C	Deaktivieren Sie den Bildschirm
Strg-L	Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den vorherigen Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum vorherigen Eintrag.
Strg-P	ESC-P
Nach-oben-Pfeil	Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den nächsten Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum nächsten Eintrag.
Strg-N	ESC-N
Nach-unten-Pfeil	Erweitern Sie einen teilweise eingegebenen Befehl oder eine gültige Eingabe aus der aktuellen Bearbeitungsposition
Registerkarte	Strg-I
Kontextabhängige Hilfe anzeigen	?

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination...
Entfliehen Sie dem speziellen Mapping für das Fragezeichen ("?") character. For instance, to enter a question mark into a command's argument, press Esc and then the "`?" Zeichen.	Esc-?
TTY-Ausgabe starten	Strg-Q
TTY-Ausgang stoppen	Strg-S

Verwendung von administrativen Berechtigungsebenen

ONTAP-Befehle und -Parameter werden auf drei Berechtigungsebenen definiert: *Admin*, *Advanced* und *diagnostic*. Die Berechtigungsebenen zeigen die bei der Ausführung der Aufgaben erforderlichen Skill-Level an.

- *** Admin***

Die meisten Befehle und Parameter sind auf dieser Ebene verfügbar. Sie werden für allgemeine oder Routineaufgaben verwendet.

- *** Fortgeschrittene ***

Befehle und Parameter auf dieser Ebene werden nur selten verwendet, erfordern erweitertes Wissen und können bei Verwendung unangemessen zu Problemen führen.

Sie verwenden erweiterte Befehle oder Parameter nur mit Ratschlag von Support-Mitarbeitern.

- **Diagnose**

Diagnosebefehle und Parameter unterbrechen potenziell den Betrieb. Sie werden nur vom Support-Personal eingesetzt, um Probleme zu diagnostizieren und zu beheben.

Legen Sie die Berechtigungsebene in der CLI fest

Sie können die Berechtigungsebene in der CLI mit einstellen `set` Befehl. Änderungen an Berechtigungsebenen-Einstellungen gelten nur für die Sitzung, in der Sie sich befinden. Sie sind nicht persistent über Sitzungen.

Schritte

1. Verwenden Sie zum Festlegen der Berechtigungsebene in der CLI `set` Befehl mit dem `-privilege` Parameter.

Beispiel zum Festlegen der Berechtigungsebene

Im folgenden Beispiel wird die Berechtigungsebene auf „Advanced“ und dann auf „admin“ festgelegt:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

Legen Sie die Anzeigeeinstellungen in der CLI fest

Sie können die Anzeigeeinstellungen für eine CLI-Sitzung mithilfe der festlegen `set` Befehl und `rows` Befehl. Die festgelegten Einstellungen gelten nur für die Sitzung, in der Sie sich befinden. Sie sind nicht persistent über Sitzungen.

Über diese Aufgabe

Sie können die folgenden CLI-Anzeigeeinstellungen festlegen:

- Die Berechtigungsebene der Befehlssitzung
- Gibt an, ob Bestätigungen für möglicherweise zu störenden Befehle ausgegeben werden
- Ob `show` Befehle zeigen alle Felder an
- Das Zeichen oder Zeichen, das als Feldtrennzeichen verwendet werden soll
- Standardeinheit bei der Meldung von Datengrößen
- Die Anzahl der Zeilen, die in der aktuellen CLI-Sitzung angezeigt werden, bevor die Schnittstelle die Ausgabe unterbricht

Wenn die bevorzugte Anzahl von Zeilen nicht angegeben wird, wird sie automatisch auf der Grundlage der tatsächlichen Höhe des Terminals angepasst. Wenn die tatsächliche Höhe nicht definiert ist, ist die Standardanzahl der Zeilen 24.

- Die standardmäßige Storage Virtual Machine (SVM) oder Node
- Ob ein fortgesetzte Befehl beendet werden soll, wenn ein Fehler auftritt

Schritte

1. Verwenden Sie zum Festlegen von CLI-Anzeigeeinstellungen den `set` Befehl.

Um die Anzahl der Zeilen festzulegen, die in der aktuellen CLI-Sitzung angezeigt werden, können Sie auch die verwenden `rows` Befehl.

Weitere Informationen finden Sie auf den man-Pages für die `set` Befehl und `rows` Befehl.

Beispiel zum Festlegen von Anzeigeeinstellungen in der CLI

Im folgenden Beispiel wird ein Komma als Feldtrennzeichen festgelegt GB Als Standardeinheit für die Datengröße und setzt die Anzahl der Zeilen auf 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Methoden zur Verwendung von Abfrageoperatoren

Die Managementoberfläche unterstützt Abfragen und UNIX-Muster und Wildcards, damit Sie in Befehlszeilenparametern mehrere Werte abgleichen können.

In der folgenden Tabelle werden die unterstützten Abfrageoperatoren beschrieben:

Operator	Beschreibung
*	Platzhalter, der allen Einträgen entspricht. Beispiel: Der Befehl <code>volume show -volume *tmp*</code> Zeigt eine Liste aller Volumes an, deren Namen den String enthalten <code>tmp</code> .
!	KEIN Operator. Zeigt einen Wert an, der nicht zugeordnet werden soll, z. B. <code>!vs0</code> Zeigt an, dass der Wert nicht übereinstimmt <code>vs0</code> .
.	Oder Operator. Trennt zwei zu vergleichende Werte, z. B. <code>`*vs0</code>
<code>vs2*</code> Entspricht entweder <code>vs0</code> oder <code>vs2</code> . Sie können mehrere oder Anweisungen angeben, z. B. <code>`a</code>	<code>b*</code>
<code>*c*</code> Entspricht dem Eintrag <code>a</code> , Jeder Eintrag, der mit <code>b</code> beginnt, Und jeder Eintrag, der beinhaltet <code>c</code> .	<code>..</code>

Operator	Beschreibung
<p>Bereichsbediener.</p> <p>Beispiel: 5..10 Entspricht jedem Wert von 5 Bis 10, Inklusiv.</p>	<
<p>Kleiner als Operator.</p> <p>Beispiel: <20 Entspricht jedem Wert, der kleiner ist als 20.</p>	>
<p>Greater-than Operator.</p> <p>Beispiel: >5 Entspricht jedem Wert, der größer ist als 5.</p>	<=
<p>Kleiner als oder gleich dem Operator.</p> <p>Beispiel: ≤5 Entspricht jedem Wert, der kleiner oder gleich ist 5.</p>	>=

Operator	Beschreibung
Größer als oder gleich dem Operator. Beispiel: >=5 Entspricht jedem Wert, der größer oder gleich ist 5.	{query}

Wenn Sie Abfragezeichen als Literale analysieren möchten, müssen Sie die Zeichen in doppelte Anführungszeichen umschließen (z. B. "<10", "0..100", "*abc*", Oder "a|b") Für die korrekten Ergebnisse zurückgegeben werden.

Sie müssen RAW-Dateinamen in doppelte Anführungszeichen einfügen, um die Interpretation von Sonderzeichen zu verhindern. Dies gilt auch für Sonderzeichen, die von der Clustershell verwendet werden.

Sie können mehrere Abfrageoperatoren in einer Befehlszeile verwenden. Beispiel: Der Befehl `volume show -size >1GB -percent-used <50 -vserver !vs1` Zeigt alle Volumes an, die größer als 1 GB sind, weniger als 50 % Auslastung und nicht in der Storage Virtual Machine (SVM) mit dem Namen „vs1“.

Verwandte Informationen

["Tastenkombinationen zum Bearbeiten von CLI-Befehlen"](#)

Methoden zur Verwendung erweiterter Abfragen

Sie können erweiterte Abfragen verwenden, um für Objekte mit bestimmten Werten zu stimmen und Vorgänge durchzuführen.

Sie geben erweiterte Abfragen an, indem Sie sie in geschweiften Klammern ({}) schließen. Eine erweiterte Abfrage muss vor allen anderen Parametern als erstes Argument nach dem Befehlsnamen angegeben werden. So legen Sie z. B. alle Volumes offline fest, deren Namen den String enthalten `tmp`, Sie führen den Befehl im folgenden Beispiel aus:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Erweiterte Abfragen sind in der Regel nur mit `modify` Und `delete` Befehle. Sie haben keine Bedeutung in `create` Oder `show` Befehle.

Die Kombination von Abfragen und Änderungsvorgängen ist ein nützliches Werkzeug. Es kann jedoch zu Verwirrung und Fehlern führen, wenn es falsch umgesetzt wird. Beispiel: Verwenden der (erweiterten Berechtigung) `system node image modify` Befehl zum Festlegen des Standard-Software-Images eines

Node wird automatisch das andere Software-Image als nicht das Standard festgelegt. Der Befehl im folgenden Beispiel ist effektiv ein null Vorgang:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Mit diesem Befehl wird das aktuelle Standard-Image als nicht-Standard-Image festgelegt und dann das neue Standard-Image (das vorherige nicht-Standard-Image) auf das nicht-Standard-Image gesetzt. Dadurch werden die ursprünglichen Standardeinstellungen beibehalten. Sie können den Befehl wie im folgenden Beispiel angegeben verwenden, um den Vorgang ordnungsgemäß auszuführen:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Methoden zur Anpassung der Show-Befehlsausgabe mithilfe von Feldern

Wenn Sie das verwenden `-instance` Parameter mit A `show` Befehl zum Anzeigen von Details kann die Ausgabe langwierig sein und mehr Informationen enthalten, als Sie benötigen. Der `-fields` Parameter von A `show` Mit Befehl können Sie nur die von Ihnen angegebenen Informationen anzeigen.

Beispiel: Wird ausgeführt `volume show -instance` Wird wahrscheinlich in mehreren Bildschirmen von Informationen führen. Verwenden Sie können `volume show -fields fieldname[,fieldname...]` So passen Sie die Ausgabe so an, dass sie nur das angegebene Feld oder die angegebenen Felder enthält (zusätzlich zu den immer angezeigten Standardfeldern). Verwenden Sie können `-fields ?` Um gültige Felder für ein anzuzeigen `show` Befehl.

Das folgende Beispiel zeigt den Ausgabunterschied zwischen dem `-instance` Und das `-fields` Parameter:

```

cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume           true
cluster1-2 vol0    volume           true
vs1      root_vol
          volume           true
vs2      new_vol
          volume           true
vs2      root_vol
          volume           true
...
cluster1::>

```

Informationen zu Positionsparametern

Sie können die Positionsparameter-Funktionalität der ONTAP-CLI nutzen, um die Effizienz bei der Befehlseingabe zu steigern. Sie können einen Befehl abfragen, um Parameter zu identifizieren, die für den Befehl positioniert sind.

Was ist ein Positionsparameter

- Ein Positionsparameter ist ein Parameter, der nicht erfordert, dass Sie den Parameternamen angeben müssen, bevor Sie den Parameterwert angeben.
- Ein Positionsparameter kann in der Befehlseingabe mit nonpositionellen Parametern interspert werden,

solange er seine relative Sequenz mit anderen Positionsparametern im selben Befehl, wie im angegeben, beobachtet **`command_name`** ? Ausgabe:

- Ein Positionsparameter kann ein erforderlicher oder optionaler Parameter für einen Befehl sein.
- Ein Parameter kann für einen Befehl positioniert werden, jedoch nicht für einen anderen.



Die Verwendung der Positionsparameterfunktion in Skripten wird nicht empfohlen, insbesondere wenn die Positionsparameter für den Befehl optional sind oder optionale Parameter vor ihnen aufgeführt sind.

Einen Positionsparameter identifizieren

Sie können einen Positionsparameter in identifizieren **`command_name`** ? Befehlsausgabe. Ein Positionsparameter hat eckige Klammern um den Parameternamen in einem der folgenden Formate:

- `[-parameter_name] parameter_value` Zeigt einen erforderlichen Parameter, der sich positioniert.
- `[[[-parameter_name] parameter_value]` Zeigt einen optionalen Parameter, der positioniert ist.

Wenn beispielsweise in der als wie folgt angezeigt wird **`command_name`** ? Ausgabe, der Parameter ist Positional für den Befehl, der in angezeigt wird:

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]`

Wenn der Parameter jedoch als folgender angezeigt wird, ist er nicht positioniert für den Befehl, der in angezeigt wird:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Beispiele für die Verwendung von Positionsparametern

Im folgenden Beispiel wird der verwendet **`volume create`** ? Die Ausgabe zeigt, dass drei Parameter für den Befehl positioniert sind: `-volume`, `-aggregate`, und `-size`.

```

cluster1::> volume create ?
    -vserver <vserver name>           Vserver Name
    [-volume] <volume name>           Volume Name
    [-aggregate] <aggregate name>      Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]}] Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]               Volume Type (default: RW)
    [ -policy <text> ]                 Export Policy
    [ -user <user name> ]              User ID
    ...
    [ -space-guarantee|-s {none|volume} ] Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ] Space Reserved for Snapshot
Copies
    ...

```

Im folgenden Beispiel wird der verwendet `volume create` Befehl wird ohne Nutzung der Funktion des Positionsparameters angegeben:

```

cluster1::> volume create -vserver svml -volume voll -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

In den folgenden Beispielen wird die Positionsparameterfunktion verwendet, um die Effizienz der Befehlseingabe zu erhöhen. Die Positionsparameter werden im mit nonpositionellen Parametern interspert `volume create` Befehl, und die Positionsparameterwerte werden ohne die Parameternamen angegeben. Die Positionsparameter werden in der gleichen Reihenfolge angegeben, die vom angegeben wird **volume create ?** Ausgabe: Das ist der Wert für `-volume` Wird vor dem von angegeben `-aggregate`, Die wiederum vor der von angegeben ist `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

Methoden für den Zugriff auf ONTAP man-Pages

Seiten im ONTAP Handbuch (man) erläutern die Verwendung von ONTAP CLI Befehlen. Diese Seiten sind in der Befehlszeile verfügbar und werden auch in Release-specific *command references* veröffentlicht.

Verwenden Sie in der ONTAP-Befehlszeile den `man command_name` Befehl zum Anzeigen der manuellen Seite des angegebenen Befehls. Wenn Sie keinen Befehlsnamen angeben, wird der manuelle Seitenindex angezeigt. Sie können das verwenden `man man` Befehl zum Anzeigen von Informationen über das `man` Befehl selbst. Sie können eine man-Page verlassen, indem Sie eingeben `q`.

Siehe [Befehlsreferenz für Ihre Version von ONTAP 9](#) Um mehr über die in Ihrer Version verfügbaren ONTAP-Befehle für Administratoren und Fortgeschrittene zu erfahren.

Verwalten von CLI-Sitzungen

Sie können eine CLI-Sitzung in eine Datei mit einem festgelegten Namen und Größenlimit aufnehmen und anschließend die Datei auf ein FTP- oder HTTP-Ziel hochladen. Sie können auch Dateien anzeigen oder löschen, in denen Sie zuvor CLI-Sitzungen aufgezeichnet haben.

Notieren Sie eine CLI-Sitzung

Ein Datensatz einer CLI-Sitzung wird beendet, wenn Sie die Aufzeichnung beenden oder die CLI-Sitzung beenden oder wenn die Datei die angegebene Größenbeschränkung erreicht. Die standardmäßige Dateigröße beträgt 1 MB. Die maximale Dateigröße beträgt 2 GB.

Das Aufzeichnen einer CLI-Sitzung ist beispielsweise nützlich, wenn Sie ein Problem beheben und detaillierte Informationen speichern möchten oder wenn Sie eine permanente Aufzeichnung der Speichernutzung zu einem bestimmten Zeitpunkt erstellen möchten.

Schritte

1. Starten Sie die Aufzeichnung der aktuellen CLI-Sitzung in einer Datei:

```
system script start
```

Weitere Informationen zur Verwendung des `system script start` Befehl, siehe die man-Page.

ONTAP beginnt mit der Aufzeichnung Ihrer CLI-Sitzung in der angegebenen Datei.

2. Fahren Sie mit Ihrer CLI-Sitzung fort.
3. Wenn Sie fertig sind, beenden Sie die Aufzeichnung der Sitzung:

```
system script stop
```

Weitere Informationen zur Verwendung des `system script stop` Befehl, siehe die man-Page.

ONTAP beendet die Aufzeichnung Ihrer CLI-Sitzung.

Befehle zum Verwalten von Datensätzen von CLI-Sitzungen

Sie verwenden das `system script` Befehle zum Verwalten von Datensätzen von CLI-Sitzungen.

Ihr Ziel ist	Befehl
Starten Sie die Aufzeichnung der aktuellen CLI-Sitzung in in einer bestimmten Datei	<code>system script start</code>
Aufzeichnung der aktuellen CLI-Sitzung beenden	<code>system script stop</code>
Zeigt Informationen zu Datensätzen von CLI-Sitzungen an	<code>system script show</code>

Ihr Ziel ist	Befehl
Laden Sie einen Datensatz einer CLI-Sitzung auf ein FTP- oder HTTP-Ziel hoch	<code>system script upload</code>
Löschen eines Datensatzes einer CLI-Sitzung	<code>system script delete</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Befehle zum Verwalten der automatischen Zeitüberschreitung von CLI-Sitzungen

Der Wert für das Zeitlimit gibt an, wie lange eine CLI-Sitzung inaktiv bleibt, bevor sie automatisch beendet wird. Der Wert für die CLI-Zeitüberschreitung ist das gesamte Cluster. Das bedeutet, dass jeder Node in einem Cluster denselben CLI-Zeitüberschreitungswert verwendet.

Standardmäßig beträgt die automatische Zeitüberschreitung von CLI-Sitzungen 30 Minuten.

Sie verwenden das `system timeout` Befehle zum Verwalten der automatischen Zeitüberschreitung von CLI-Sitzungen.

Ihr Ziel ist	Befehl
Zeigt den automatischen Zeitüberschreitungszeitraum für CLI-Sessions an	<code>system timeout show</code>
Ändern Sie den automatischen Zeitüberschreitungszeitraum für CLI-Sitzungen	<code>system timeout modify</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Cluster-Management (nur Cluster-Administratoren)

Zeigt Informationen über die Nodes in einem Cluster an

Sie können Node-Namen anzeigen, unabhängig davon, ob die Nodes sich in einem ordnungsgemäßen Zustand befinden und ob sie zur Teilnahme am Cluster berechtigt sind. Auf der erweiterten Berechtigungsebene können Sie auch anzeigen, ob ein Node Epsilon hält.

Schritte

1. Um Informationen über die Nodes in einem Cluster anzuzeigen, verwenden Sie den `cluster show` Befehl.

Wenn Sie möchten, dass die Ausgabe zeigt, ob ein Node Epsilon enthält, führen Sie den Befehl auf der erweiterten Berechtigungsebene aus.

Beispiele zum Anzeigen der Nodes in einem Cluster

Im folgenden Beispiel werden Informationen über alle Nodes in einem Cluster mit vier Nodes angezeigt:

```
cluster1::> cluster show
Node           Health Eligibility
-----
node1          true   true
node2          true   true
node3          true   true
node4          true   true
```

Im folgenden Beispiel werden auf der erweiterten Berechtigungsebene ausführliche Informationen über den Node „node1“ angezeigt:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

      Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
  Epsilon: false
Eligibility: true
    Health: true
```

Zeigt Cluster-Attribute an

Sie können die eindeutige ID (UUID), den Namen, die Seriennummer, den Standort und die Kontaktinformationen eines Clusters anzeigen.

Schritte

1. Verwenden Sie zum Anzeigen der Attribute eines Clusters das `cluster identity show` Befehl.

Beispiel zum Anzeigen von Cluster-Attributen

Im folgenden Beispiel werden der Name, die Seriennummer, der Standort und die Kontaktinformationen eines Clusters angezeigt.

```
cluster1::> cluster identity show
```

```
Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
Cluster Location: Sunnyvale
Cluster Contact: jsmith@example.com
```

Cluster-Attribute ändern

Sie können bei Bedarf die Attribute eines Clusters, z. B. den Cluster-Namen, den Standort und die Kontaktinformationen ändern.

Über diese Aufgabe

Sie können die UUID eines Clusters nicht ändern. Diese ist beim Erstellen des Clusters festgelegt.

Schritte

1. Verwenden Sie zum Ändern von Cluster-Attributen das `cluster identity modify` Befehl.

Der `-name` Parameter gibt den Namen des Clusters an. Der `cluster identity modify` Auf der man-Page werden die Regeln zur Angabe des Namens des Clusters beschrieben.

Der `-location` Parameter gibt den Speicherort für das Cluster an.

Der `-contact` Parameter gibt die Kontaktinformationen an, z. B. einen Namen oder eine E-Mail-Adresse.

Beispiel für die Umbenennung eines Clusters

Mit dem folgenden Befehl wird das aktuelle Cluster („cluster1“) in „cluster2“ umbenannt:

```
cluster1::> cluster identity modify -name cluster2
```

Zeigt den Status von Cluster-Replikationsringen an

Sie können den Status von Cluster-Replizierungsringen anzeigen, um Ihnen bei der Diagnose von Problemen im gesamten Cluster zu helfen. Wenn im Cluster Probleme auftreten, werden Sie möglicherweise von dem Support-Personal gebeten, diese Aufgabe auszuführen, um die Fehlerbehebung zu unterstützen.

Schritte

1. Verwenden Sie zum Anzeigen des Status von Cluster-Replikationsringen das `cluster ring show` Befehl auf der erweiterten Berechtigungsebene

Beispiel zum Anzeigen des Status von Cluster-Ring-Replizierung

Im folgenden Beispiel wird der Status des VLDB-Replikationsrings auf einem Knoten mit dem Namen node0 angezeigt:


```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1:*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
        Epoch: 5
Master Node: node0
  Local Node: node0
    DB Epoch: 5
DB Transaction: 56
  Number Online: 4
    RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

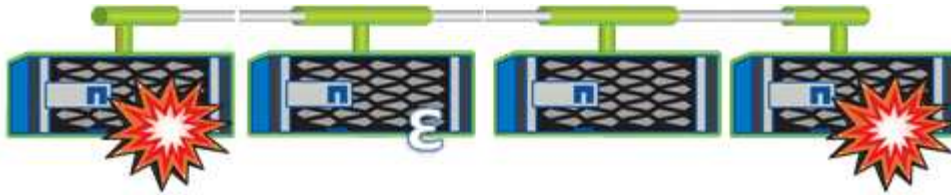
Über Quorum und Epsilon

Quorum und Epsilon sind wichtige Kennzahlen für den Clusterzustand und die Funktion, die gemeinsam zeigen, wie Cluster potenzielle Herausforderungen bei Kommunikation und Konnektivität bewältigen.

Quorum ist eine Voraussetzung für ein voll funktionsfähiges Cluster. Wenn ein Cluster Quorum aufweist, sind die meisten Knoten in einem ordnungsgemäßen Zustand und können miteinander kommunizieren. Wenn das Quorum verloren geht, verliert das Cluster die Möglichkeit, normale Cluster-Vorgänge zu erledigen. Es kann jederzeit nur eine Sammlung von Knoten Quorum enthalten, da alle Knoten gemeinsam eine Ansicht der Daten teilen. Wenn zwei nicht kommunizierende Knoten die Daten auf unterschiedliche Weise ändern dürfen, ist es daher nicht mehr möglich, die Daten in einer einzigen Datenansicht zu vergleichen.

Jeder Knoten im Cluster nimmt an einem Abstimmprotokoll teil, das einen Knoten *Master* wählt; jeder verbleibende Knoten ist ein *secondary*. Der Master-Node ist für die Synchronisierung von Informationen im gesamten Cluster verantwortlich. Wenn Quorum gebildet wird, wird es durch ständige Abstimmung beibehalten. Wenn der Hauptknoten offline geht und sich das Cluster noch im Quorum befindet, wird ein neuer Master von den Knoten ausgewählt, die online bleiben.

Da es die Möglichkeit einer Krawatte in einem Cluster mit einer geraden Anzahl von Knoten gibt, hat ein Knoten eine zusätzliche fraktionale Abstimmungsgewichtung namens *epsilon*. Wenn die Konnektivität zwischen zwei gleichen Teilen eines großen Clusters ausfällt, bleibt die Gruppe der Nodes mit epsilon ein Quorum, vorausgesetzt, dass alle Nodes ordnungsgemäß sind. Die folgende Abbildung zeigt beispielsweise ein Cluster mit vier Nodes, in dem zwei der Nodes ausgefallen sind. Da einer der verbliebenen Nodes jedoch Epsilon enthält, bleibt das Cluster im Quorum, auch wenn es nicht die einfache Mehrheit der gesunden Knoten gibt.



Epsilon wird beim Erstellen des Clusters automatisch dem ersten Knoten zugewiesen. Wenn der Node, auf dem Epsilon steht, ungesund wird, seinen Hochverfügbarkeits-Partner übernimmt oder vom Hochverfügbarkeitspartner übernommen wird, wird Epsilon automatisch einem gesunden Node in einem anderen HA-Paar neu zugewiesen.

Wenn ein Node offline geschaltet wird, kann sich dies darauf auswirken, dass das Cluster im Quorum bleibt. Daher gibt ONTAP eine Warnmeldung aus, wenn Sie versuchen, einen Vorgang durchzuführen, der entweder das Cluster aus dem Quorum entfernt, oder wenn es ein Ausfall von dem Verlust des Quorums entfernt wird. Sie können die Quorum-Warnmeldungen mit deaktivieren `cluster quorum-service options modify` Befehl auf der erweiterten Berechtigungsebene

Angenommen, die zuverlässige Konnektivität zwischen den Knoten des Clusters ist, ist ein größerer Cluster im Allgemeinen stabiler als ein kleinerer Cluster. Das Quorum, das die einfache Mehrheit der halben Nodes plus Epsilon erfordert, ist auf einem Cluster mit 24 Nodes einfacher zu warten als bei einem Cluster mit zwei Nodes.

Ein Cluster mit zwei Nodes stellt die Beibehaltung von Quorum vor besondere Herausforderungen. Cluster mit zwei Nodes verwenden *Cluster HA*, bei dem keines der Nodes Epsilon enthält. Stattdessen werden beide Nodes fortlaufend abgefragt, um sicherzustellen, dass bei einem Node ein voller Lese-/Schreibzugriff auf die Daten sowie Zugriff auf logische Schnittstellen und Managementfunktionen sichergestellt ist.

Welche System-Volumes sind

System-Volumes sind FlexVol-Volumes, die spezielle Metadaten enthalten, z. B. Metadaten für Audit-Protokolle für Fileservices. Diese Volumes sind im Cluster sichtbar, sodass Sie die Storage-Nutzung im Cluster umfassend berücksichtigen können.

System-Volumes sind Eigentum des Cluster-Management-Servers (auch als Admin-SVM bezeichnet) und werden automatisch erstellt, wenn die Prüfung von Fileservices aktiviert ist.

Sie können System-Volumes mithilfe von anzeigen `volume show` Befehl, die meisten anderen Volume-Vorgänge sind jedoch nicht zulässig. Beispielsweise können Sie kein System-Volume mit verwenden `volume modify` Befehl.

Das Beispiel zeigt vier System-Volumes auf der Administrator-SVM, die automatisch erstellt wurden, wenn das Auditing von Fileservices für eine Daten-SVM im Cluster aktiviert wurde:

```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

Managen von Nodes

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 hinzufügen, müssen alle vorhandenen Nodes im Cluster einen ordnungsgemäßen Zustand aufweisen (wird durch `cluster show` angezeigt).
- Wenn Sie einem 2-Node-Cluster ohne Switches Nodes hinzufügen, müssen Sie das 2-Node-Cluster ohne Switches mit einem von NetApp unterstützten Cluster Switch in ein Switch-Attached-Cluster konvertieren.

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

- Wenn Sie einem Single-Node-Cluster einen zweiten Node hinzufügen, muss der zweite Node installiert sein und das Cluster-Netzwerk konfiguriert sein.
- Wenn für das Cluster die automatische SP-Konfiguration aktiviert ist, muss das für den SP angegebene Subnetz über verfügbare Ressourcen verfügen, damit der beigetretene Node das angegebene Subnetz verwenden kann, um den SP automatisch zu konfigurieren.
- 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 [e0M]:
```

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://<node_mgmt_or_e0M_IP_address>`

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
```

Wenn die auf dem neuen Node ausgeführte ONTAP-Version von der auf dem vorhandenen Cluster ausgeführten Version abweicht, meldet das System eine `System checks Error: Cluster join operation cannot be performed at this time` Fehler. Dies ist das erwartete Verhalten. Führen Sie zum Fortfahren den `add-node -allow-mixed-version-join new_node_name` Befehl auf der erweiterten Berechtigungsebene von einem vorhandenen Node im Cluster aus.

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.

Verwandte Informationen

["ONTAP Cluster mit gemischten Versionen"](#)

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 nicht-Root-Volumes waren ["Verschoben"](#) Von Aggregaten, die dem Node gehören.
- Alle nicht-Root-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` Läuft 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`
- Wenn Sie die Verbindung zu 2 Nodes von einem 4-Node-Cluster aufheben, wird Cluster-HA auf den beiden verbleibenden Nodes automatisch aktiviert.



Alle System- und Benutzerdaten von allen Laufwerken, die mit dem Knoten verbunden sind, müssen für Benutzer unzugänglich 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. Überprüfen Sie, ob auf einem Node auf dem Cluster Epsilon gespeichert ist:

```
cluster show -epsilon true
```

3. Wenn auf einem Node im Cluster Epsilon gespeichert ist und der Node nicht verbunden wird, verschieben Sie Epsilon zu einem Node, dessen Verknüpfung nicht aufgehoben wird:

- a. Verschieben Sie Epsilon vom Node, der nicht verbunden werden soll

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

- b. Epsilon auf einen Node verschieben, der nicht verbunden werden soll:

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

4. Den aktuellen Master-Knoten identifizieren:

```
cluster ring show
```

Der Master-Node ist der Node mit Prozessen wie „mgmt“, „vldb“, „vifmgr“, „bcomd“ und „crs“.

5. Wenn der Knoten, den Sie entfernen möchten, der aktuelle Master-Knoten ist, aktivieren Sie den anderen Knoten im Cluster, der als Master-Knoten ausgewählt werden soll:

- a. Machen Sie den aktuellen Master-Node für die Teilnahme am Cluster unzulässig:

```
cluster modify - node <node_name> -eligibility false
```

Wenn der Master-Knoten nicht mehr berechtigt ist, wird einer der verbleibenden Nodes vom Cluster-Quorum als neuer Master ausgewählt.

- b. Machen Sie den vorherigen Master-Knoten wieder zur Teilnahme am Cluster berechtigt:

```
cluster modify - node <node_name> -eligibility true
```

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

Für diese ONTAP-Version...	Befehl
ONTAP 9.3	<pre>cluster unjoin</pre>
ONTAP 9.4 und höher	<pre>cluster remove-node*</pre>

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.

8. 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.

9. 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 Startmenüoption (4) Konfiguration bereinigen und initialisieren Sie alle Festplatten.

10. Zurück zur Administrator-Berechtigungsebene:

```
set -privilege admin
```

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

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 zuzugreifen. 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 `/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::>
```

Node-Root-Volumes und Root-Aggregate managen

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.

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.

- 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. Siehe [\[relocate-root\]](#).
- Das Root-Aggregat ist nur dem Root-Volumen des Knotens zugewiesen.

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

"NetApp Hardware Universe"

Geben Sie Speicherplatz im Root-Volume eines Node frei

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. Core Dump-Dateien des Node und ihre Namen anzeigen:

```
system node coredump show
```

2. Löschen Sie unerwünschte Core Dump-Dateien vom Node:

```
system node coredump delete
```

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 vol0:

```
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 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	<code>boot_ontap</code>
Das primäre ONTAP-Image vom Boot-Gerät	<code>boot_primary</code>
Das ONTAP Backup-Image vom Startgerät aus	<code>boot_backup</code>

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 heruntergefahrnde 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.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```



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 data-bbox="673 304 730 367">  </div> <p>Mit dieser Menüoption werden alle Daten auf den Festplatten des Knotens gelöscht und die Knotenkonfiguration auf die werkseitigen Standardeinstellungen zurückgesetzt.</p> <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 #ccc; 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>

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` 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
```

Management von Single-Node-Clustern

Ein Single-Node Cluster ist eine spezielle Implementierung eines Clusters, das auf einem Standalone Node ausgeführt wird. Single-Node-Cluster sind nicht empfehlenswert, da sie keine Redundanz bieten. Bei einem Ausfall des Node geht der Datenzugriff verloren.



Für Fehlertoleranz und unterbrechungsfreien Betrieb wird dringend empfohlen, das Cluster mit zu konfigurieren "[Hochverfügbarkeit \(HA-Paare\)](#)".

Wenn Sie ein Single-Node-Cluster konfigurieren oder aktualisieren, sollten Sie die folgenden Punkte beachten:

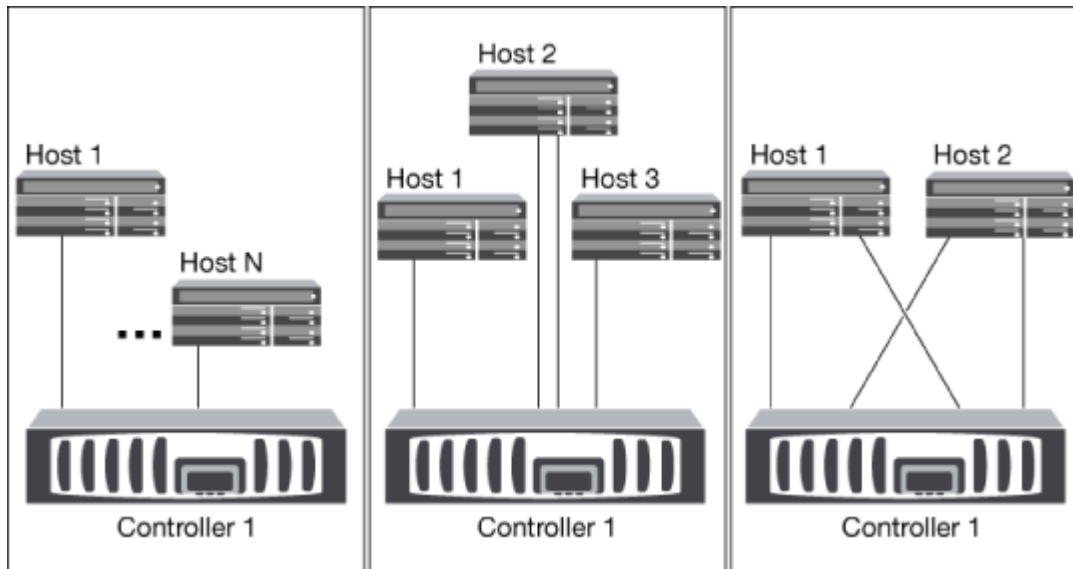
- Die Root-Volume-Verschlüsselung wird auf Single-Node-Clustern nicht unterstützt.
- Wenn Sie Nodes entfernen, um ein Single-Node-Cluster zu besitzen, sollten Sie die Cluster-Ports für den Datenverkehr ändern. Dazu ändern Sie die Cluster-Ports als Daten-Ports und erstellen anschließend Daten-LIFs an den Daten-Ports.
- Für Single-Node-Cluster können Sie das Konfigurations-Backup-Ziel während der Software-Einrichtung angeben. Nach dem Setup können diese Einstellungen mit ONTAP Befehlen geändert werden.
- Wenn mehrere Hosts mit dem Knoten verbunden sind, kann jeder Host mit einem anderen Betriebssystem wie Windows oder Linux konfiguriert werden. Wenn mehrere Pfade vom Host zum Controller vorhanden sind, muss ALUA auf dem Host aktiviert sein.

Möglichkeiten zur Konfiguration von iSCSI-SAN-Hosts mit einzelnen Nodes

Sie können iSCSI-SAN-Hosts so konfigurieren, dass sie eine direkte Verbindung zu einem einzelnen Knoten herstellen oder eine Verbindung über einen oder mehrere IP-Switches herstellen. Der Knoten kann mehrere iSCSI-Verbindungen zum Switch haben.

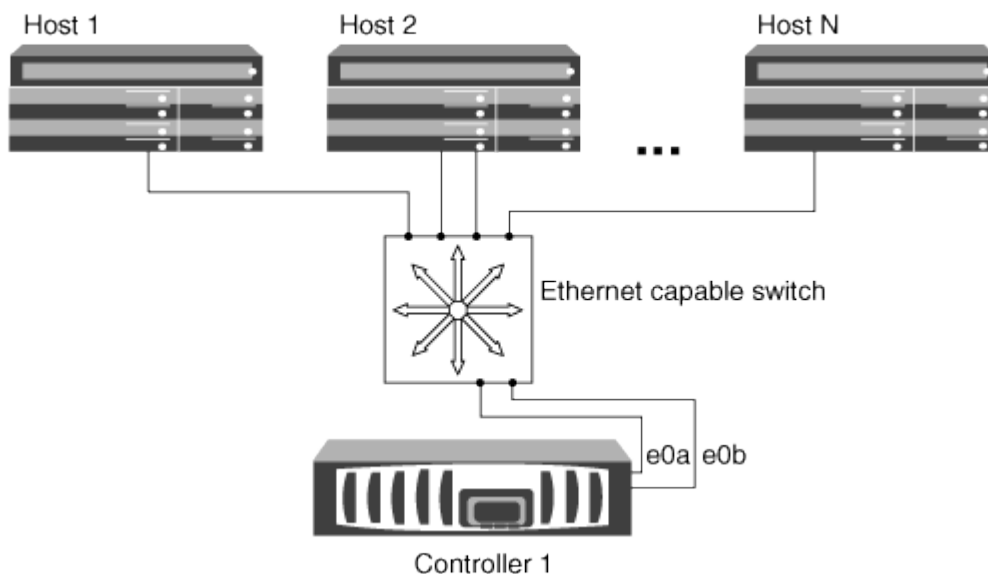
Direct-Attached Single Node-Konfigurationen

In Direct-Attached-Single-Node-Konfigurationen werden ein oder mehrere Hosts direkt mit dem Node verbunden.



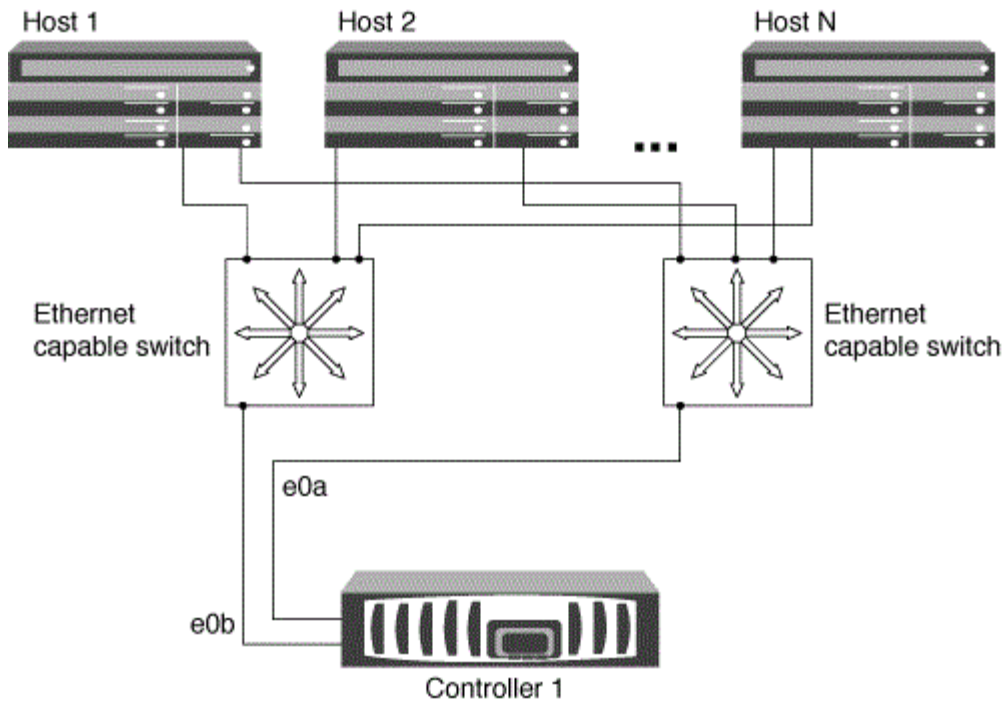
Single-Network-Konfiguration mit Single Node-Konfiguration

In Single-Network-Konfigurationen mit einem oder mehreren Hosts wird über einen Switch ein Node mit einem oder mehreren Hosts verbunden. Da es einen einzelnen Switch gibt, ist diese Konfiguration nicht vollständig redundant.



Single Node-Konfigurationen in mehreren Netzwerken

Bei Konfigurationen mit einem einzigen Netzwerk mit mehreren Nodes werden mindestens zwei Switches einen einzelnen Node mit einem oder mehreren Hosts verbunden. Da es mehrere Switches gibt, ist diese Konfiguration vollständig redundant.



Möglichkeiten zur Konfiguration von FC- und FC-NVMe-SAN-Hosts mit einzelnen Nodes

Sie können FC- und FC-NVMe-SAN-Hosts mit einzelnen Nodes über eine oder mehrere Fabrics konfigurieren. N-Port ID Virtualization (NPIV) ist erforderlich und muss auf allen FC Switches in der Fabric aktiviert sein. Sie können ohne Verwendung eines FC-Switch keine FC- oder FC-NVMe SAN-Hosts direkt an einzelne Nodes anschließen.

Single-Fabric-Single-Node-Konfigurationen

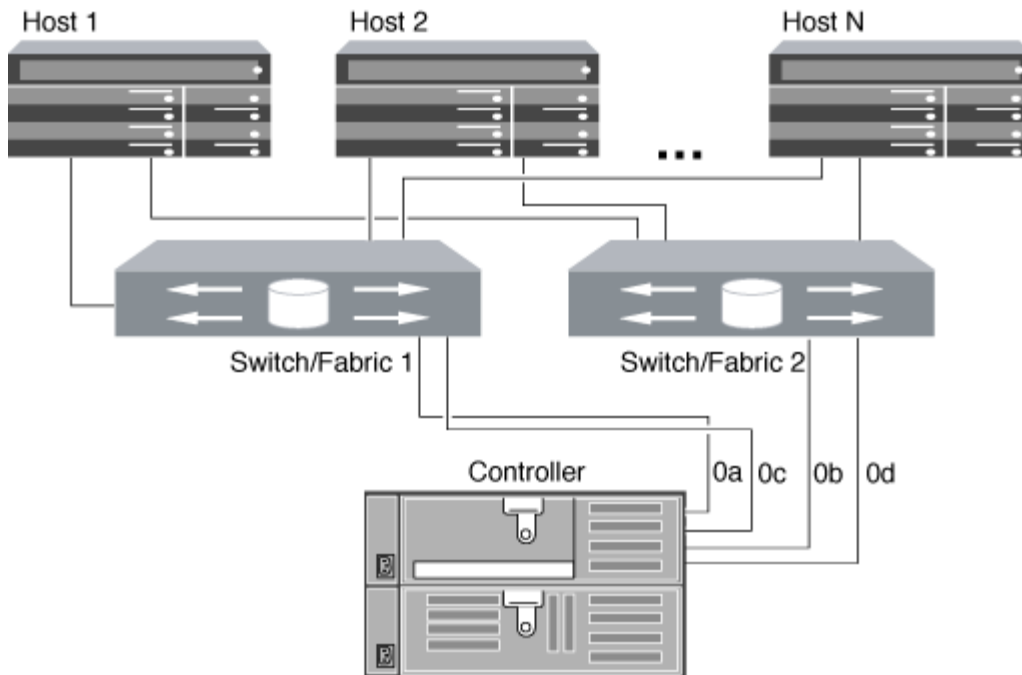
Bei Single-Fabric-Konfigurationen mit einem Node kann ein Switch einen einzelnen Node mit einem oder mehreren Hosts verbinden. Da es einen einzelnen Switch gibt, ist diese Konfiguration nicht vollständig redundant.

In Einzel-Fabric-Konfigurationen mit einem Node ist keine Multipathing-Software erforderlich, wenn Sie nur einen einzelnen Pfad vom Host zum Node haben.

Single Node-Konfigurationen in MultiFabric-Architektur

Bei Single-Node-Konfigurationen mit mehreren Fabrics müssen mindestens zwei Switches einen einzelnen Node mit einem oder mehreren Hosts verbinden. Die folgende Abbildung zeigt eine Single-Node-Konfiguration mit mehreren Fabrics und nur zwei Fabrics, wobei in jeder Konfiguration mit mehreren Fabric jedoch zwei oder mehr Fabrics möglich sind. In dieser Abbildung ist der Speicher-Controller im oberen Gehäuse montiert und das untere Gehäuse kann leer sein oder ein IOMX-Modul besitzen, wie in diesem Beispiel.

Die FC-Ziel-Ports (0a, 0c, 0b, 0d) in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern variieren je nach Modell des Storage-Node und ob Sie Erweiterungsadapter verwenden.



Verwandte Informationen

["Technischer Bericht 4684 von NetApp: Implementing and Configuring Modern SANs with NVMe-of"](#)

ONTAP Upgrade für Single-Node-Cluster

Ab ONTAP 9.2 können Sie die ONTAP CLI verwenden, um eine automatische Aktualisierung eines Single-Node-Clusters durchzuführen. Da Single-Node-Cluster keine Redundanz aufweisen, sind Updates immer mit Unterbrechungen verbunden. Mit System Manager können nicht störende Upgrades durchgeführt werden.

Bevor Sie beginnen

Sie müssen das Upgrade abschließen ["Vorbereitung"](#) Schritte.

Schritte

1. Löschen Sie das frühere ONTAP-Softwarepaket:

```
cluster image package delete -version previous_package_version
```

2. Laden Sie das ONTAP-Zielsoftwarepaket herunter:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```

3. Vergewissern Sie sich, dass das Softwarepaket im Repository für Cluster-Pakete verfügbar ist:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.7              M/DD/YYYY 10:32:15
```

4. Vergewissern Sie sich, dass das Cluster bereit für ein Upgrade ist:

```
cluster image validate -version package_version_number
```

```
cluster1::> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Überwachen Sie den Fortschritt der Validierung:

```
cluster image show-update-progress
```

6. Führen Sie alle erforderlichen Aktionen durch, die durch die Validierung identifiziert wurden.

7. Optional können Sie eine Schätzung für das Software-Upgrade erstellen:

```
cluster image update -version package_version_number -estimate-only
```

Die Schätzung für das Software-Upgrade zeigt Details zu jeder zu aktualisierenden Komponente sowie die geschätzte Dauer des Upgrades an.

8. Durchführen des Software-Upgrades:

```
cluster image update -version package_version_number
```



Wenn ein Problem auftritt, wird das Update angehalten und Sie werden aufgefordert, Korrekturmaßnahmen zu ergreifen. Mit dem Befehl „Cluster image show-Update-progress“ können Sie Details zu Problemen und den Fortschritt des Updates anzeigen. Nach der Behebung des Problems können Sie das Update mithilfe des Befehls „Resume-Update“ für das Cluster Image fortsetzen.

9. Zeigt den Status des Cluster-Updates an:

```
cluster image show-update-progress
```

Der Node wird im Rahmen des Updates neu gebootet und kann nicht beim Neubooten aufgerufen werden.

10. Auslösen einer Benachrichtigung:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

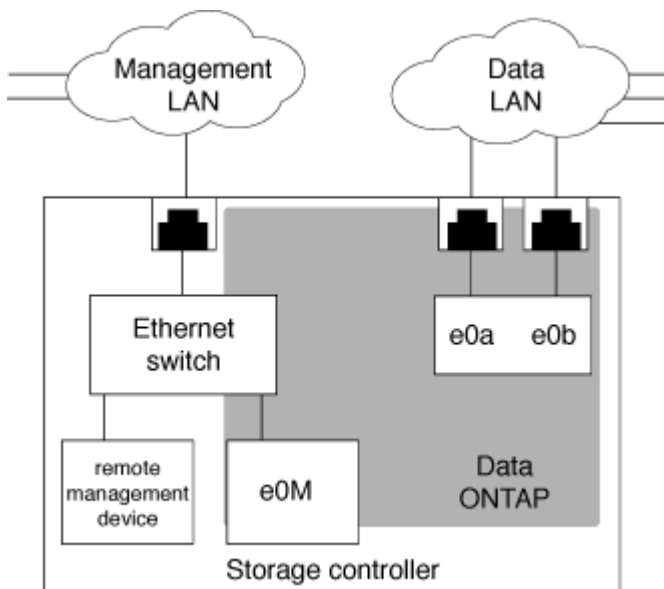
Wenn Ihr Cluster nicht für das Senden von Meldungen konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

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-Netzwerkconfiguration

Sie können die automatische Netzwerkconfiguration auf Cluster-Ebene für den SP aktivieren (empfohlen). Sie können die automatische SP-Netzwerkconfiguration auch deaktiviert (die Standardeinstellung) lassen und die SP-Netzwerkconfiguration 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 `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 Netzwerkconfiguration 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-Netzwerkconfiguration 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 Netzwerkconfiguration 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-Netzwerkconfiguration 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 netzwerkbasierende Firmware-Updates oder die netzwerkbasierende 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
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.

Remote-Verwaltung von Knoten 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.

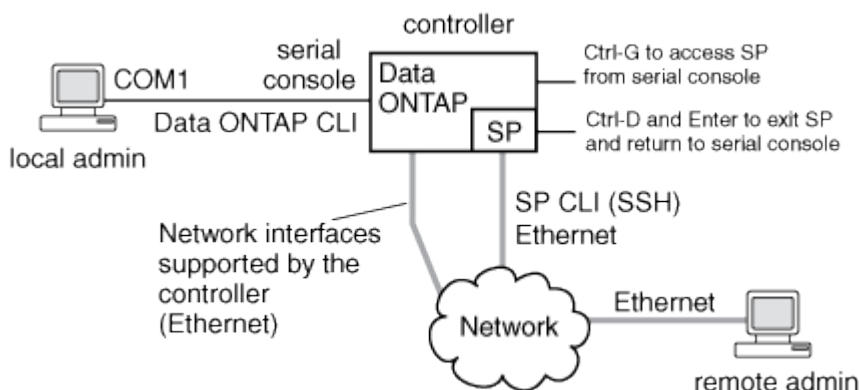
Wenn Meldungen an die Konsole gesendet werden, speichert der SP sie im Konsole-Protokoll. Das Konsole-Protokoll bleibt gespeichert, solange der SP von einem der Netzteile des Node mit Strom versorgt wird. Da der SP mit Standby-Strom betrieben wird, bleibt er auch dann verfügbar, wenn der Node aus- und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

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 compatible Version aktualisiert, die von der ONTAP-Version unterstützt wird, auf die Sie zurückgesetzt oder heruntergestuft 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"](#)

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 `joe`, 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 `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 Hilfinformationen 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>
```

2. Um Hilfinformationen 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 -v Mit der Option werden SP-Statistiken in ausführlicher Form angezeigt. Der -d Option fügt das SP-Debug-Protokoll zur Anzeige hinzu.	<code>bmc status [-v . -d]</code> Der -v Mit der Option werden SP-Statistiken in ausführlicher Form angezeigt. Der -d 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 Controllern 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	<code>system forensics</code> <code>[show.log dump.log clear]</code>		
Melden Sie sich bei der Systemkonsole an	<code>system console</code>		<code>system node run-console</code>
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).	<code>system power on</code>	
<code>system node power on</code> (Erweiterte Berechtigungsebene)	<code>system power off</code>		

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Oder dieser ONTAP Befehl ...
system power cycle			<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>  <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</p> <p>Mit dem -firmware {primary.backup.current} Parameter(erweiterte Berechtigungsebene)</p> <p>system node reset</p>	<div data-bbox="505 327 561 384"></div> <p>Dieser Vorgang bewirkt ein nicht ordnungsgemäßes Herunterfahren des Node.</p> <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	<code>exit</code>

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:

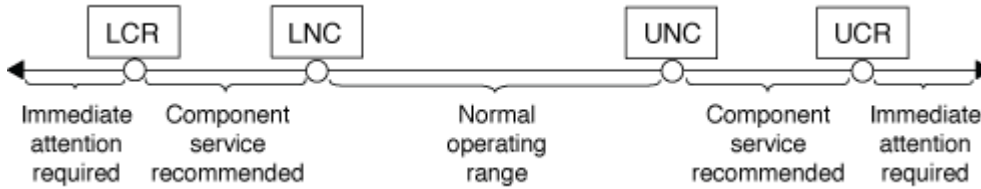
- Unterer kritischer Schwellenwert (LCR)
- Unterer nicht kritischer Schwellenwert (LNC)
- Oberer nicht kritischer Schwellenwert (UNC)
- Oberer kritischer Schwellenwert (UCR)

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 node1> 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 angezeigt `Current` (Spalte in der SP-CLI) `system sensors` Befehlsausgabe ausführen, 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-Netzwerkconfiguration, SP-Firmware-Image, SSH-Zugriff auf den SP und allgemeine SP-Administration.

Befehle zum Verwalten der SP-Netzwerkconfiguration


Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Aktivieren Sie die automatische SP-Netzwerkconfiguration 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-Netzwerkconfiguration 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-Netzwerkconfiguration 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 	<p><code>system service-processor network modify</code></p>
<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 	<p><code>system service-processor network show</code></p> <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 	<p><code>system service-processor api-service modify</code></p> <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: <pre>system service-processor api-service renew-internal-certificates</pre> Für ONTAP 9.4 oder früher: <pre>system service-processor api-service renew-certificates</pre> <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>  <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 y 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>
Zeigt den Status für das aktuelle, von ONTAP ausgelöste Firmware-Update an, einschließlich der folgenden Informationen: <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	system service-processor image show/modify
Aktualisieren der BMC-Firmware	system service-processor image update
Zeigt den Status der neuesten BMC-Firmware-Aktualisierung an	system service-processor image update-progress show
Aktivieren Sie die automatische Netzwerkkonfiguration für den BMC, um eine IPv4- oder IPv6-Adresse im angegebenen Subnetz zu verwenden	system service-processor network auto-configuration enable
Deaktivieren Sie die automatische Netzwerkkonfiguration für eine IPv4- oder IPv6-Adresse im für den BMC angegebenen Subnetz	system service-processor network auto-configuration disable
Anzeigen der automatischen BMC-Netzwerkkonfiguration	system service-processor network auto-configuration show

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.

Cluster-Zeit managen (nur Cluster-Administratoren)

Wenn die Cluster-Zeit nicht stimmt, können Probleme auftreten. ONTAP ermöglicht Ihnen das manuelle Einstellen der Zeitzone, des Datums und der Uhrzeit auf dem Cluster, sollten Sie NTP-Server (Network Time Protocol) so konfigurieren, dass die Cluster-Zeit synchronisiert wird.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung konfigurieren.

NTP ist immer aktiviert. Es ist jedoch nach wie vor eine Konfiguration erforderlich, damit der Cluster mit einer externen Datenquelle synchronisiert werden kann. ONTAP ermöglicht es Ihnen, die NTP-Konfiguration des Clusters wie folgt zu verwalten:

- Sie können dem Cluster maximal 10 externe NTP-Server zuweisen (`cluster time-service ntp server create`).
 - Um Redundanz und Qualität des Zeitdienstes zu gewährleisten, sollten Sie mindestens drei externe NTP-Server mit dem Cluster verbinden.
 - Sie können einen NTP-Server mit seiner IPv4- oder IPv6-Adresse oder dem vollqualifizierten Host-Namen angeben.
 - Sie können die zu verwendende NTP-Version (v3 oder v4) manuell angeben.

Standardmäßig wählt ONTAP automatisch die NTP-Version aus, die für einen bestimmten externen NTP-Server unterstützt wird.

Wenn die angegebene NTP-Version für den NTP-Server nicht unterstützt wird, kann kein Zeitaustausch stattfinden.

- Auf der erweiterten Berechtigungsebene können Sie einen externen NTP-Server angeben, der mit dem Cluster verbunden ist und als primäre Datenquelle für die Korrektur und Anpassung der Cluster-Zeit dient.
- Sie können die NTP-Server anzeigen, die mit dem Cluster verbunden sind (`cluster time-service ntp server show`).
- Sie können die NTP-Konfiguration des Clusters ändern (`cluster time-service ntp server modify`).

- Sie können die Verbindung des Clusters von einem externen NTP-Server beenden (`cluster time-service ntp server delete`).
- Sie können die Konfiguration auf der erweiterten Berechtigungsebene zurücksetzen, indem Sie die Zuordnung aller externen NTP-Server zum Cluster löschen (`cluster time-service ntp server reset`).

Ein Knoten, der einem Cluster Beitreitt, nimmt automatisch die NTP-Konfiguration des Clusters an.

Über die Verwendung von NTP hinaus können Sie mit ONTAP auch die Cluster-Zeit manuell verwalten. Diese Funktion ist hilfreich, wenn Sie eine falsche Uhrzeit korrigieren müssen (beispielsweise ist die Zeit eines Node nach einem Neubooten deutlich falsch). In diesem Fall können Sie eine ungefähre Zeit für das Cluster angeben, bis NTP mit einem externen Zeitserver synchronisieren kann. Die manuell eingestellte Zeit wirkt sich auf alle Nodes im Cluster aus.

Sie haben folgende Möglichkeiten, die Cluster-Zeit manuell zu verwalten:

- Sie können für das Cluster die Zeitzone, das Datum und die Uhrzeit einstellen oder ändern (`cluster date modify`).
- Sie können die aktuellen Zeitzone-, Datums- und Zeiteinstellungen des Clusters anzeigen (`cluster date show`).



Job-Zeitpläne passen nicht auf manuelle Cluster-Datums- und -Zeitänderungen an. Diese Jobs werden planmäßig ausgeführt, basierend auf der aktuellen Cluster-Zeit, zu der der Job erstellt wurde oder zum Zeitpunkt der letzten Ausführung des Jobs. Wenn Sie deshalb das Cluster-Datum oder die -Zeit manuell ändern, müssen Sie das verwenden `job show` Und `job history show` Befehle zur Überprüfung, ob alle geplanten Jobs entsprechend Ihren Anforderungen in eine Warteschlange verschoben und abgeschlossen werden.

Befehle zum Verwalten der Cluster-Zeit

Sie verwenden das `cluster time-service ntp server` Befehle zum Verwalten der NTP-Server für das Cluster. Sie verwenden das `cluster date` Befehle zum manuellen Verwalten der Cluster-Zeit.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung konfigurieren.

Mit den folgenden Befehlen können Sie die NTP-Server für das Cluster verwalten:

Ihr Ziel ist	Befehl
Verbinden Sie das Cluster ohne symmetrische Authentifizierung mit einem externen NTP-Server	<code>cluster time-service ntp server create -server server_name</code>
Verbinden Sie den Cluster mit einem externen NTP-Server mit symmetrischer Authentifizierung Verfügbar in ONTAP 9.5 oder höher	<div> <code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code> </div> <div> <p>Der <code>key_id</code> Beziehen Sie sich auf einen vorhandenen gemeinsamen Schlüssel, der mit 'Cluster Time-Service ntp key' konfiguriert ist.</p> </div>

Ihr Ziel ist	Befehl
Symmetrische Authentifizierung für einen vorhandenen NTP-Server aktivieren ein vorhandener NTP-Server kann angepasst werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen Verfügbar in ONTAP 9.5 oder höher	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Deaktivieren Sie die symmetrische Authentifizierung	<pre>cluster time-service ntp server modify -server server_name -is-authentication-enabled false</pre>
Konfigurieren Sie einen freigegebenen NTP-Schlüssel	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Freigegebene Schlüssel werden durch eine ID bezeichnet. Die ID, der Typ und der Wert müssen auf dem Node und dem NTP-Server identisch sein</p> </div>
Zeigt Informationen zu den NTP-Servern an, die mit dem Cluster verbunden sind	<pre>cluster time-service ntp server show</pre>
Ändern Sie die Konfiguration eines externen NTP-Servers, der mit dem Cluster verbunden ist	<pre>cluster time-service ntp server modify</pre>
Distanzieren Sie einen NTP-Server vom Cluster	<pre>cluster time-service ntp server delete</pre>
Setzen Sie die Konfiguration zurück, indem Sie alle externen NTP-Server-Verknüpfungen mit dem Cluster löschen	<pre>cluster time-service ntp server reset</pre> <div>  <p>Dieser Befehl erfordert die erweiterte Berechtigungsebene.</p> </div>

Mit den folgenden Befehlen können Sie die Cluster-Zeit manuell verwalten:

Ihr Ziel ist	Befehl
Zeitzone, Datum und Uhrzeit einstellen oder ändern	<pre>cluster date modify</pre>
Zeigt die Zeitzone, das Datum und die Zeiteinstellungen für das Cluster an	<pre>cluster date show</pre>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Verwalten des Banners und der MOTD

Verwalten Sie die Übersicht über Banner und MOTD

Mit ONTAP können Sie ein Anmeldebanner oder eine Nachricht des Tages (MOTD) konfigurieren, um administrative Informationen an CLI-Benutzer des Clusters oder der Storage Virtual Machine (SVM) zu kommunizieren.

Ein Banner wird in einer Konsolensitzung (nur für Cluster-Zugriff) oder in einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, bevor ein Benutzer zur Authentifizierung wie beispielsweise einem Passwort aufgefordert wird. Beispielsweise können Sie mit dem Banner eine Warnmeldung wie die folgende an eine Person anzeigen, die versucht, sich beim System anzumelden:

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

Eine MOTD wird in einer Konsolensitzung (nur für Cluster-Zugriff) oder einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, nachdem ein Benutzer authentifiziert wurde, jedoch bevor die Clustershell-Eingabeaufforderung angezeigt wird. Sie können z. B. die MOTD verwenden, um eine Willkommens- oder Informationsnachricht anzuzeigen, z. B. die folgende, die nur authentifizierte Benutzer sehen:

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

Sie können den Inhalt des Banners oder der MOTD mit dem erstellen oder ändern `security login banner modify` Oder `security login motd modify` Befehle können mit folgenden Methoden ausgeführt werden:

- Sie können die CLI interaktiv oder nicht interaktiv verwenden, um den Text anzugeben, der für das Banner oder MOTD verwendet werden soll.

Der interaktive Modus wird gestartet, wenn der Befehl ohne den verwendet wird `-message` Oder `-uri` Parameter, ermöglicht die Verwendung von Newlines (auch als Zeilenende bezeichnet) in der Meldung.

Der nicht-interaktive Modus, in dem der verwendet wird `-message` Parameter, der die Meldungszeichenfolge angeben soll, unterstützt keine Zeilenumbruch.

- Sie können Inhalte von einem FTP- oder HTTP-Speicherort für das Banner oder MOTD hochladen.
- Sie können die MOTD so konfigurieren, dass dynamischer Inhalt angezeigt wird.

Beispiele für das, was Sie die MOTD für die dynamische Anzeige konfigurieren können, sind:

- Cluster-Name, Node-Name oder SVM-Name
- Cluster-Datum und -Uhrzeit
- Name des Benutzers, der sich anmeldet
- Letzte Anmeldung für den Benutzer auf einem beliebigen Node im Cluster
- Anmeldename oder IP-Adresse
- Der Name des Betriebssystems
- Softwareversion
- Effektive Cluster-Version `String security login motd modify` Auf der Hauptseite werden die Escape-Sequenzen beschrieben, mit denen Sie MOTD aktivieren können, um dynamisch generierten Inhalt anzuzeigen.

Das Banner unterstützt keine dynamischen Inhalte.

Sie können Banner und MOTD auf Cluster- oder SVM-Ebene managen:

- Folgende Fakten gelten für das Banner:
 - Das für den Cluster konfigurierte Banner wird auch für alle SVMs verwendet, die keine Bannernachricht definiert haben.
 - Ein Banner auf SVM-Ebene kann für jede SVM konfiguriert werden.

Wenn ein Banner auf Cluster-Ebene konfiguriert wurde, wird es durch das Banner auf SVM-Ebene für die angegebene SVM überschrieben.

- Folgende Fakten gelten für die MOTD:
 - Standardmäßig ist das für den Cluster konfigurierte MOTD auch für alle SVMs aktiviert.
 - Außerdem kann für jede SVM ein MOTD auf SVM-Ebene konfiguriert werden.

Wenn sich Benutzer bei der SVM anmelden, werden in diesem Fall zwei MOTDs angezeigt, eine auf Cluster-Ebene definiert und die andere auf SVM-Ebene.

- Die MOTD auf Cluster-Ebene kann vom Cluster-Administrator pro SVM aktiviert oder deaktiviert werden.

Wenn der Cluster-Administrator die MOTD auf Cluster-Ebene für eine SVM deaktiviert, wird der bei der SVM anmeldet Benutzer die MOTD auf Cluster-Ebene nicht angezeigt.

Erstellen Sie ein Banner

Sie können ein Banner erstellen, um eine Meldung an jemanden anzuzeigen, der versucht, auf das Cluster oder die SVM zuzugreifen. Das Banner wird in einer Konsolensitzung (nur für Cluster-Zugriff) oder in einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, bevor ein Benutzer zur Authentifizierung aufgefordert wird.

Schritte

1. Verwenden Sie die `security login banner modify` Befehl zum Erstellen eines Banners für das Cluster oder SVM:

Ihr Ziel ist	Dann...
Geben Sie eine Nachricht an, die eine einzelne Zeile ist	Verwenden Sie die <code>-message „text“</code> Parameter, um den Text anzugeben.
Fügen Sie neue Zeilen (auch als Zeilenende bezeichnet) in die Nachricht ein	Verwenden Sie den Befehl ohne das <code>-message</code> Oder <code>-uri</code> Parameter zum Starten des interaktiven Modus zum Bearbeiten des Banners.
Laden Sie Inhalte von einem Speicherort hoch, um für das Banner zu verwenden	Verwenden Sie die <code>-uri</code> Parameter zum Festlegen des FTP- oder HTTP-Speicherorts des Inhalts.

Die maximale Größe eines Banners beträgt 2,048 Byte, einschließlich Newlines.

Ein Banner, das mit dem erstellt wurde `-uri` Parameter ist statisch. Es wird nicht automatisch aktualisiert, um nachfolgende Änderungen des Quellinhalts wiederzugeben.

Das für das Cluster erstellte Banner wird auch für alle SVMs angezeigt, die über kein vorhandenes Banner verfügen. Jedes nachträglich erstellte Banner für eine SVM überschreibt das Banner auf Cluster-Ebene für diese SVM. Angeben des `-message` Parameter mit einem Bindestrich innerhalb doppelter Anführungszeichen ("`-`") Bei der SVM wird die SVM zurückgesetzt, um den Banner auf Cluster-Ebene zu verwenden.

- Überprüfen Sie, ob das Banner erstellt wurde, indem Sie es mit dem anzeigen `security login banner show` Befehl.

Angeben des `-message` Parameter mit leerem String ("") Zeigt Banner an, die keinen Inhalt haben.

Angeben des `-message` Parameter mit "`-`" Zeigt alle (Admin oder Daten) SVMs an, die nicht über ein Banner konfiguriert sind.

Beispiele für die Erstellung von Bannern

Im folgenden Beispiel wird der nicht interaktive Modus verwendet, um ein Banner für den Cluster „cluster1“ zu erstellen:

```
cluster1::> security login banner modify -message "Authorized users only!"
cluster1::>
```

Im folgenden Beispiel wird mithilfe des interaktiven Modus ein Banner für die SVM „svm1“ erstellt:

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0          1          2          3          4          5          6          7
8
1234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!

cluster1::>
```

Im folgenden Beispiel werden die Banner angezeigt, die erstellt wurden:

```
cluster1::> security login banner show
Vserver: cluster1
Message
-----
---
Authorized users only!

Vserver: svm1
Message
-----
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

Verwandte Informationen

[Verwalten des Banners](#)

Verwalten des Banners

Sie können das Banner auf Cluster- oder SVM-Ebene managen. Das für den Cluster konfigurierte Banner wird auch für alle SVMs verwendet, die keine Bannernachricht definiert haben. Ein nachträglich erstelltes Banner für eine SVM überschreibt das Cluster-Banner für diese SVM.

Wahlmöglichkeiten

- Managen Sie das Banner auf Cluster-Ebene:

Ihr Ziel ist	Dann...
Erstellen Sie ein Banner zur Anzeige aller CLI-Login-Sessions	Setzen Sie ein Banner auf Cluster-Ebene: `*security login banner modify -vserver <i>cluster_name</i> { [-message "text"]
<i>[-uri ftp_or_http_addr] }</i> *`	Entfernen Sie das Banner für alle Anmeldungen (Cluster und SVM)
Setzen Sie das Banner auf einen leeren String (""): security login banner modify -vserver * -message ""	Überschreiben eines Banners, das von einem SVM-Administrator erstellt wurde
Ändern der SVM-Banner-Meldung: `*security login banner modify -vserver <i>svm_name</i> { [-message "text"]	<i>[-uri ftp_or_http_addr] }</i> *`

- Banner auf SVM-Ebene managen:

Angaben `-vserver svm_name` ist im SVM-Kontext nicht erforderlich.

Ihr Ziel ist	Dann...
Setzen Sie das vom Cluster-Administrator bereitgestellte Banner mit einem anderen Banner für die SVM außer Kraft	Banner für SVM erstellen: `*security login banner modify -vserver <i>svm_name</i> { [-message "text"]
<i>[-uri ftp_or_http_addr] }</i> *`	Unterdrücken Sie das vom Cluster-Administrator bereitgestellte Banner, sodass für die SVM kein Banner angezeigt wird
Setzen Sie das SVM-Banner auf einen leeren String für die SVM: security login banner modify -vserver <i>svm_name</i> -message ""	Verwenden Sie das Banner auf Cluster-Ebene, wenn die SVM derzeit ein Banner auf SVM-Ebene verwendet

Erstellen Sie eine MOTD

Sie können eine Tagesnachricht (MOTD) erstellen, um Informationen an authentifizierte CLI-Benutzer zu kommunizieren. Die MOTD wird in einer Konsolensitzung (nur für Cluster-Zugriff) oder einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, nachdem ein Benutzer authentifiziert wurde, jedoch vor der Anzeige der clustershell-

Eingabeaufforderung.

Schritte

1. Verwenden Sie die `security login motd modify` Befehl zum Erstellen einer MOTD für das Cluster oder die SVM:

Ihr Ziel ist	Dann...
Geben Sie eine Nachricht an, die eine einzelne Zeile ist	Verwenden Sie die <code>-message „text“</code> Parameter, um den Text anzugeben.
Zeilenende einschließen (auch als Zeilenende bekannt)	Verwenden Sie den Befehl ohne das <code>-message</code> Oder <code>-uri</code> Parameter zum Starten des interaktiven Modus zur Bearbeitung der MOTD.
Laden Sie Inhalte von einem Speicherort für die MOTD-Nutzung hoch	Verwenden Sie die <code>-uri</code> Parameter zum Festlegen des FTP- oder HTTP-Speicherorts des Inhalts.

Die maximale Größe für einen MOTD beträgt 2,048 Byte, einschließlich Neuzeilen.

Der `security login motd modify` Auf der Hauptseite werden die Escape-Sequenzen beschrieben, mit denen Sie MOTD aktivieren können, um dynamisch generierten Inhalt anzuzeigen.

Eine MOTD, die mithilfe von erstellt wird `-uri` Parameter ist statisch. Es wird nicht automatisch aktualisiert, um nachfolgende Änderungen des Quellinhalts wiederzugeben.

Standardmäßig wird auch für alle SVM-Anmeldungen ein für das Cluster erstellter MOTD angezeigt sowie eine MOTD auf SVM-Ebene, die Sie separat für eine bestimmte SVM erstellen können. Einstellen des `-is-cluster-message-enabled` Parameter an `false` Bei einer SVM wird verhindert, dass die MOTD auf Cluster-Ebene für diese SVM angezeigt wird.

2. Überprüfen Sie, ob die MOTD erstellt wurde, indem Sie sie mit dem anzeigen `security login motd show` Befehl.

Angaben des `-message` Parameter mit leerem String ("") Zeigt MOTDs an, die nicht konfiguriert sind oder keinen Inhalt haben.

Siehe "[Sicherheitsanmeldung motd modify](#)" Befehlsmanpage für eine Liste von Parametern, die verwendet werden soll, um die MOTD zu aktivieren, um dynamisch generierte Inhalte anzuzeigen. Prüfen Sie unbedingt die auf Ihre ONTAP-Version spezifische man Page.

Beispiele für die Erstellung von MOTDs

Im folgenden Beispiel wird der nicht interaktive Modus verwendet, um eine MOTD für den Cluster „cluster1“ zu erstellen:

```
cluster1::> security login motd modify -message "Greetings!"
```

Das folgende Beispiel verwendet den interaktiven Modus, um eine MOTD für die SVM „svm1“ zu erstellen, die Escape-Sequenzen zur Anzeige dynamisch generierter Inhalte verwendet:

```
cluster1::> security login motd modify -vserver svm1
```

Enter the message of the day for Vserver "svm1".

Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to abort.

0 1 2 3 4 5 6 7
8

1234567890123456789012345678901234567890123456789012345678901234
567890

Welcome to the \n SVM. Your user ID is '\N'. Your last successful login
was \L.

Im folgenden Beispiel werden die erstellten MOTDs angezeigt:

```
cluster1::> security login motd show
```

Vserver: cluster1

Is the Cluster MOTD Displayed?: true

Message

Greetings!

Vserver: svm1

Is the Cluster MOTD Displayed?: true

Message

Welcome to the \n SVM. Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.

Verwalten der MOTD

Sie können die Meldung des Tages (MOTD) auf Cluster- oder SVM-Ebene managen. Standardmäßig ist das für den Cluster konfigurierte MOTD auch für alle SVMs aktiviert. Außerdem kann für jede SVM ein MOTD auf SVM-Ebene konfiguriert werden. Die MOTD auf Cluster-Ebene kann für jede SVM durch den Cluster-Administrator aktiviert oder deaktiviert werden.

Eine Liste der Escape-Sequenzen, mit denen dynamisch Inhalte für die MOTD generiert werden können, finden Sie im ["Befehlsreferenz"](#).

Wahlmöglichkeiten

- Verwalten Sie die MOTD auf Clusterebene:

Ihr Ziel ist	Dann...
Erstellen Sie eine MOTD für alle Anmeldungen, wenn keine MOTD vorhanden ist	Legen Sie eine MOTD auf Cluster-Ebene fest: `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "]
[-uri <i>ftp_or_http_addr</i>] }*	Ändern Sie das MOTD für alle Anmeldungen, wenn keine MOTDs auf SVM-Ebene konfiguriert sind
Ändern Sie die MOTD auf Cluster-Ebene: `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "] }	[-uri <i>ftp_or_http_addr</i>] }*
Entfernen Sie das MOTD für alle Anmeldungen, wenn keine MOTDs auf SVM-Ebene konfiguriert sind	Legen Sie die MOTD auf Cluster-Ebene auf einen leeren String fest (""): security login motd modify -vserver <i>cluster_name</i> -message ""
Verwenden Sie für jede SVM eine MOTD auf Cluster-Ebene statt die SVM-Ebene	Legen Sie eine MOTD auf Cluster-Ebene fest und setzen Sie dann alle MOTDs auf eine leere Zeichenfolge mit aktivierter MOTD auf Cluster-Ebene: a. `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "]
[-uri <i>ftp_or_http_addr</i>] }* .. security login motd modify { -vserver !"cluster_name" } -message "" -is -cluster-message-enabled true	Wird ein MOTD nur für ausgewählte SVMs angezeigt, und es wird kein MOTD auf Cluster-Ebene verwendet
Legen Sie die MOTD auf Cluster-Ebene auf einen leeren String fest und legen Sie dann MOTDs auf SVM-Ebene für ausgewählte SVMs fest: a. security login motd modify -vserver <i>cluster_name</i> -message "" b. `*security login motd modify -vserver <i>svm_name</i> { [-message " <i>text</i> "]	[-uri <i>ftp_or_http_addr</i>] }* + Sie können diesen Schritt bei Bedarf für jede SVM wiederholen.
Verwenden Sie für alle SVMs (Daten und Admin) dasselbe MOTD auf SVM-Ebene	Legen Sie den Cluster und alle SVMs so fest, dass er dasselbe MOTD verwenden soll: `*security login motd modify -vserver * { [-message " <i>text</i> "]

Ihr Ziel ist	Dann...
<pre>[-uri <i>ftp_or_http_addr</i>] }*</pre> <p>[NOTE]</p> <p>====</p> <p>Wenn Sie den interaktiven Modus verwenden, werden Sie von der CLI aufgefordert, die MOTD einzeln für das Cluster und jede SVM einzugeben. Sie können dieselbe MOTD in jede Instanz einfügen, wenn Sie dazu aufgefordert werden.</p> <p>====</p>	<p>Ein MOTD auf Cluster-Ebene steht optional allen SVMs zur Verfügung, soll aber nicht, dass der MOTD für Cluster-Anmeldungen angezeigt wird</p>
<p>Legen Sie eine MOTD auf Cluster-Ebene fest, deaktivieren Sie jedoch die Anzeige für das Cluster:</p> <pre>*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</pre>	<pre>[-uri <i>ftp_or_http_addr</i>] } -is-cluster-message-enabled false*</pre>
<p>Entfernen Sie alle MOTDs auf Cluster- und SVM-Ebene, wenn nur einige SVMs über MOTDs auf Cluster-Ebene und SVM-Ebene verfügen</p>	<p>Legen Sie den Cluster und alle SVMs so fest, dass für die MOTD ein leerer String verwendet wird:</p> <pre>security login motd modify -vserver * -message ""</pre>
<p>Ändern Sie die MOTD nur für die SVMs mit einer nicht leeren Zeichenfolge, wenn andere SVMs einen leeren String verwenden und wenn auf Clusterebene ein anderes MOTD verwendet wird</p>	<p>Verwenden Sie erweiterte Abfragen, um die MOTD selektiv zu ändern:</p> <pre>*security login motd modify { -vserver !"cluster_name" -message !"" } { [-message "<i>text</i>"]</pre>
<pre>[-uri <i>ftp_or_http_addr</i>] }*</pre>	<p>Alle MOTDs, die spezifischen Text enthalten (z. B. „Januar“ gefolgt von „2015“), können überall in einer einzelnen oder mehrzeiligen Nachricht angezeigt werden, auch wenn der Text über verschiedene Zeilen aufgeteilt wird</p>
<p>Verwenden Sie eine Abfrage, um MOTDs anzuzeigen:</p> <pre>security login motd show -message *<i>January</i>*<i>2015</i>*</pre>	<p>Erstellen Sie interaktiv ein MOTD, das mehrere und aufeinanderfolgende Zeilen enthält (auch als Zeilenende oder EOLs bezeichnet).</p>

- Management von MOTD auf SVM-Ebene:

Angaben `-vserver svm_name` ist im SVM-Kontext nicht erforderlich.

Ihr Ziel ist	Dann...
Verwenden Sie ein anderes MOTD auf SVM-Ebene, wenn für die SVM bereits eine MOTD auf SVM-Ebene vorhanden ist	Ändern Sie die MOTD auf SVM-Ebene: `*security login motd modify -vserver <i>svm_name</i> { [-message " <i>text</i> "]
<code>[-uri <i>ftp_or_http_addr</i>] }*</code>	Verwenden Sie nur das MOTD auf Cluster-Ebene für die SVM, wenn die SVM bereits über eine MOTD auf SVM-Ebene verfügt
Legen Sie die MOTD auf SVM-Ebene auf einen leeren String fest, und lassen Sie den Clusteradministrator die MOTD auf Clusterebene für die SVM aktivieren: a. <code>security login motd modify -vserver <i>svm_name</i> -message ""</code> b. (Für den Cluster-Administrator) <code>security login motd modify -vserver <i>svm_name</i> -is-cluster-message-enabled true</code>	Die SVM zeigt keine MOTD an, wenn derzeit sowohl die MOTDs auf Cluster- als auch die SVM-Ebene für die SVM angezeigt werden

Verwalten von Jobs und Zeitplanung

Jobs werden in eine Jobwarteschlange platziert und im Hintergrund ausgeführt, wenn Ressourcen verfügbar sind. Wenn ein Job zu viele Cluster-Ressourcen benötigt, können Sie ihn anhalten oder anhalten, bis die Nachfrage auf dem Cluster geringer ist. Sie können auch Jobs überwachen und neu starten.

Jobkategorien

Es gibt drei Kategorien von Jobs, die Sie verwalten können: Server-verbundene, Cluster-verbundene und private.

Ein Job kann in einer der folgenden Kategorien sein:

- **Server-verbundene Jobs**

Diese Jobs werden vom Management-Framework in die Warteschlange für einen bestimmten Knoten gestellt, der ausgeführt werden soll.

- **Cluster-verbundene Jobs**

Diese Jobs werden vom Management-Framework in die Warteschlange für jeden Node im auszulauenden Cluster verschoben.

- **Privatjobs**

Diese Jobs sind für einen Knoten spezifisch und verwenden nicht die replizierte Datenbank (RDB) oder einen anderen Cluster-Mechanismus. Für Befehle, die private Jobs verwalten, ist die erweiterte Berechtigungsebene oder höher erforderlich.

Befehle zum Verwalten von Jobs

Wenn Sie einen Befehl eingeben, der einen Job aufruft, werden Sie in der Regel über den Befehl informiert, dass der Job in die Warteschlange verschoben wurde und anschließend zur CLI-Eingabeaufforderung zurückkehrt. Einige Befehle berichten stattdessen den Job-Fortschritt und kehren erst dann zur CLI-Eingabeaufforderung zurück, wenn der Job abgeschlossen ist. In diesen Fällen können Sie Strg-C drücken, um den Job in den Hintergrund zu verschieben.

Ihr Ziel ist	Befehl
Informationen zu allen Jobs anzeigen	<code>job show</code>
Informationen zu Jobs auf Node-Basis anzeigen	<code>job show bynode</code>
Zeigt Informationen zu Cluster-verbundenen Jobs an	<code>job show-cluster</code>
Zeigt Informationen zu abgeschlossenen Jobs an	<code>job show-completed</code>
Zeigt Informationen zum Jobverlauf an	<code>job history show</code> Für jeden Knoten im Cluster werden bis zu 25,000 Job-Datensätze gespeichert. Daher kann der Versuch, den gesamten Jobverlauf anzuzeigen, sehr viel Zeit in Anspruch nehmen. Um möglicherweise lange Wartezeiten zu vermeiden, sollten Sie Jobs nach Node, Storage Virtual Machine (SVM) oder Datensatz-ID anzeigen.
Zeigen Sie die Liste der privaten Jobs an	<code>job private show</code> (Erweiterte Berechtigungsebene)
Informationen zu abgeschlossenen privaten Jobs anzeigen	<code>job private show-completed</code> (Erweiterte Berechtigungsebene)
Zeigt Informationen zum Initialisierungsstatus für Job Manager an	<code>job initstate show</code> (Erweiterte Berechtigungsebene)
Überwachen des Fortschritts eines Jobs	<code>job watch-progress</code>
Überwachen Sie den Fortschritt eines privaten Jobs	<code>job private watch-progress</code> (Erweiterte Berechtigungsebene)
Unterbrechen Sie einen Job	<code>job pause</code>
Unterbrechen Sie einen privaten Job	<code>job private pause</code> (Erweiterte Berechtigungsebene)

Ihr Ziel ist	Befehl
Einen angehaltenen Job fortsetzen	<code>job resume</code>
Setzen Sie einen angehaltenen privaten Job fort	<code>job private resume</code> (Erweiterte Berechtigungsebene)
Stoppen Sie einen Job	<code>job stop</code>
Beenden Sie einen privaten Job	<code>job private stop</code> (Erweiterte Berechtigungsebene)
Löschen Sie einen Job	<code>job delete</code>
Löschen Sie einen privaten Job	<code>job private delete</code> (Erweiterte Berechtigungsebene)
Beenden Sie die Zuordnung eines Jobs mit Cluster-Verbindung zu einem nicht verfügbaren Node, dem er gehört, sodass ein anderer Node die Verantwortung für diesen Job übernehmen kann	<code>job unclaim</code> (Erweiterte Berechtigungsebene)



Sie können das `event log show` Befehl zur Ermittlung des Ergebnisses eines abgeschlossenen Jobs.

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Befehle zum Verwalten von Job-Zeitplänen

Viele Aufgaben – beispielsweise Volume Snapshot Kopien – können für die Ausführung auf bestimmten Zeitplänen konfiguriert werden. Zeitpläne, die zu bestimmten Zeiten ausgeführt werden, werden als *cron* Zeitpläne bezeichnet (ähnlich wie bei UNIX *cron* Zeitpläne). Zeitpläne, die in Intervallen ausgeführt werden, werden als „*interval*“-Zeitpläne bezeichnet. Sie verwenden das `job schedule` Befehle zum Verwalten von Job-Zeitplänen.

Job-Zeitpläne passen nicht auf manuelle Änderungen am Cluster-Datum und -Uhrzeit an. Diese Jobs werden planmäßig ausgeführt, basierend auf der aktuellen Cluster-Zeit, zu der der Job erstellt wurde oder zum Zeitpunkt der letzten Ausführung des Jobs. Wenn Sie daher das Cluster-Datum oder die -Zeit manuell ändern, sollten Sie das verwenden `job show` Und `job history show` Befehle zur Überprüfung, ob alle geplanten Jobs entsprechend Ihren Anforderungen in eine Warteschlange verschoben und abgeschlossen werden.

Wenn das Cluster Teil einer MetroCluster-Konfiguration ist, müssen die Job-Zeitpläne auf beiden Clustern identisch sein. Wenn Sie einen Job-Zeitplan erstellen, ändern oder löschen, müssen Sie diesen Vorgang auf dem Remote-Cluster ausführen.

Ihr Ziel ist	Befehl
Informationen zu allen Zeitplänen anzeigen	<code>job schedule show</code>
Zeigt die Liste der Jobs nach Zeitplan an	<code>job schedule show-jobs</code>
Informationen zu cron-Zeitplänen anzeigen	<code>job schedule cron show</code>
Zeigt Informationen zu Intervallzeitplänen an	<code>job schedule interval show</code>
Erstellen Sie einen cron-Zeitplan	<code>job schedule cron create</code> Ab ONTAP 9.10.1 können Sie die SVM für Ihren Jobzeitplan hinzufügen.
Erstellen eines Intervallplans	<code>job schedule interval create</code> Sie müssen mindestens einen der folgenden Parameter angeben: <code>-days</code> , <code>-hours</code> , <code>-minutes</code> , Oder <code>-seconds</code> .
Ändern Sie einen Cron-Zeitplan	<code>job schedule cron modify</code>
Ändern eines Intervallplans	<code>job schedule interval modify</code>
Löschen Sie einen Zeitplan	<code>job schedule delete</code>
Löschen Sie einen Cron-Zeitplan	<code>job schedule cron delete</code>
Einen Intervallzeitplan löschen	<code>job schedule interval delete</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Backup und Restore von Cluster-Konfigurationen (nur Cluster-Administratoren)

Welche Backup-Dateien sind für die Konfiguration

Bei den Backup-Dateien der Konfiguration handelt es sich um Archivdateien (.7z), die Informationen über alle konfigurierbaren Optionen enthalten, die für den ordnungsgemäßen Betrieb des Clusters und der darin enthaltenen Knoten benötigt werden.

Diese Dateien speichern die lokale Konfiguration jedes Nodes sowie die clusterweite replizierte Konfiguration.

Sie verwenden Konfigurations-Backup-Dateien, um ein Backup der Cluster-Konfiguration durchzuführen und wiederherzustellen.

Es gibt zwei Arten von Konfigurations-Backup-Dateien:

- **Knoten Konfiguration Backup-Datei**

Jeder gesunde Node im Cluster umfasst eine Backup-Datei für die Node-Konfiguration, die alle Konfigurationsinformationen und Metadaten enthält, die für den ordnungsgemäßen Betrieb des Node im Cluster erforderlich sind.

- **Sicherungsdatei der Clusterkonfiguration**

Zu diesen Dateien gehören ein Archiv aller Backup-Dateien der Node-Konfiguration im Cluster sowie die replizierten Clusterkonfigurationsinformationen (die replizierte Datenbank oder RDB-Datei). Backup-Dateien der Cluster-Konfiguration ermöglichen es Ihnen, die Konfiguration des gesamten Clusters oder eines beliebigen Nodes im Cluster wiederherzustellen. Die Backup-Zeitpläne für die Cluster-Konfiguration erstellen diese Dateien automatisch und speichern sie auf mehreren Knoten im Cluster.



Konfigurations-Backup-Dateien enthalten nur Konfigurationsinformationen. Dabei werden keine Benutzerdaten berücksichtigt. Informationen zum Wiederherstellen von Benutzerdaten finden Sie unter "[Datensicherung](#)".

Automatisierte Backups der Node- und Cluster-Konfigurationen

Drei separate Zeitpläne erstellen automatisch Backup-Dateien für die Cluster- und Node-Konfiguration und replizieren sie auf den Nodes im Cluster.

Die Backup-Dateien der Konfiguration werden automatisch gemäß den folgenden Zeitplänen erstellt:

- Alle 8 Stunden
- Täglich
- Wöchentlich

Zu jeder dieser Zeiten wird auf jedem gesunden Node im Cluster eine Backup-Datei für die Node-Konfiguration erstellt. Alle Backup-Dateien der Node-Konfiguration werden dann in einer Backup-Datei mit einer einzelnen Cluster-Konfiguration zusammen mit der replizierten Cluster-Konfiguration erfasst und auf einem oder mehreren Nodes im Cluster gespeichert.

Befehle zum Management von Backup-Zeitplänen der Konfiguration

Sie können das verwenden `system configuration backup settings` Befehle zum Managen von Backup-Zeitplänen für die Konfiguration.

Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.



Ihr Ziel ist	Befehl
<p>Ändern Sie die Einstellungen für einen Konfigurations-Backup-Zeitplan:</p> <ul style="list-style-type: none"> Geben Sie eine Remote-URL an (HTTP, HTTPS, FTP, FTPS oder TFTP), bei der die Konfigurations-Backup-Dateien zusätzlich zu den Standardstandorten im Cluster hochgeladen werden Geben Sie einen Benutzernamen an, der zur Anmeldung an der Remote-URL verwendet werden soll Legen Sie die Anzahl der Backups fest, die für jeden Backup-Zeitplan der Konfiguration beibehalten werden sollen 	<pre>system configuration backup settings modify</pre> <p>Wenn Sie HTTPS in der Remote-URL verwenden, verwenden Sie das <code>-validate-certification</code> Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatvalidierung. Die Zertifikatvalidierung ist standardmäßig deaktiviert.</p> <div>  <p>Der Webserver, auf den Sie die Backup-Konfigurationsdatei hochladen, muss die für HTTP- und POST-Vorgänge aktivierten Vorgänge für HTTPS aktiviert haben. Weitere Informationen finden Sie in der Dokumentation Ihres Webserver.</p> </div>
Legen Sie das Kennwort fest, mit dem Sie sich bei der Remote-URL anmelden können	<pre>system configuration backup settings set-password</pre>
Zeigen Sie die Einstellungen für den Konfigurations-Backup-Zeitplan an	<pre>system configuration backup settings show</pre> <div>  <p>Sie stellen die ein <code>-instance</code> Parameter zum Anzeigen des Benutzernamens und der Anzahl der Backups, die für jeden Zeitplan beibehalten werden sollen.</p> </div>

Befehle zum Management von Backup-Dateien der Konfiguration

Sie verwenden das `system configuration backup` Befehle zum Management von Backup-Dateien für die Cluster- und Node-Konfiguration.

Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

Ihr Ziel ist	Befehl
Erstellen einer neuen Backup-Datei für Nodes oder Cluster-Konfigurationen	<pre>system configuration backup create</pre>
Kopieren einer Backup-Konfigurationsdatei von einem Node auf einen anderen Node im Cluster	<pre>system configuration backup copy</pre>

Ihr Ziel ist	Befehl
<p>Hochladen einer Konfigurations-Backup-Datei von einem Knoten im Cluster auf eine Remote-URL (FTP, HTTP, HTTPS, TFTP oder FTPS)</p>	<p><code>system configuration backup upload</code></p> <p>Wenn Sie HTTPS in der Remote-URL verwenden, verwenden Sie das <code>-validate-certification</code> Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatvalidierung. Die Zertifikatvalidierung ist standardmäßig deaktiviert.</p> <div data-bbox="850 653 902 709">  </div> <p>Der Webserver, auf den Sie die Backup-Konfigurationsdatei hochladen, muss die für HTTP- und POST-Vorgänge aktivierten Vorgänge für HTTPS aktiviert haben. Einige Webserver erfordern möglicherweise die Installation eines zusätzlichen Moduls. Weitere Informationen finden Sie in der Dokumentation Ihres Webserver. Die unterstützten URL-Formate variieren je nach ONTAP-Version. Informationen zu Ihrer ONTAP Version finden Sie in der Hilfe zur Befehlszeile.</p>
<p>Laden Sie eine Sicherungsdatei der Konfiguration von einer Remote-URL auf einen Node im Cluster herunter, und validieren Sie, falls angegeben, das digitale Zertifikat</p>	<p><code>system configuration backup download</code></p> <p>Wenn Sie HTTPS in der Remote-URL verwenden, verwenden Sie das <code>-validate-certification</code> Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatvalidierung. Die Zertifikatvalidierung ist standardmäßig deaktiviert.</p>
<p>Benennen Sie eine Sicherungsdatei für die Konfiguration auf einem Node im Cluster um</p>	<p><code>system configuration backup rename</code></p>
<p>Zeigen Sie die Backup-Dateien für einen oder mehrere Nodes im Cluster an, die für eine oder mehrere Nodes konfiguriert sind</p>	<p><code>system configuration backup show</code></p>
<p>Löschen einer Backup-Konfigurationsdatei auf einem Knoten</p>	<p><code>system configuration backup delete</code></p> <div data-bbox="850 1713 902 1770">  </div> <p>Mit diesem Befehl wird nur die Backup-Datei der Konfiguration auf dem angegebenen Node gelöscht. Wenn auch die Backup-Datei der Konfiguration auf anderen Knoten im Cluster vorhanden ist, bleibt sie auf diesen Knoten.</p>

Suchen Sie eine Backup-Konfigurationsdatei, die für die Wiederherstellung eines Knotens verwendet werden soll

Zum Wiederherstellen einer Node-Konfiguration verwenden Sie eine Konfigurations-Backup-Datei auf einer Remote-URL oder auf einem Node im Cluster.

Über diese Aufgabe

Sie können die Backup-Datei einer Node-Konfiguration entweder als Cluster oder als Node verwenden.

Schritt

1. Stellen Sie die Sicherungsdatei für die Konfiguration dem Knoten zur Verfügung, für den Sie die Konfiguration wiederherstellen müssen.

Wenn sich die Backup-Datei der Konfiguration befindet...	Dann...
Unter einer Remote-URL	Verwenden Sie die <code>system configuration backup download</code> Mit dem Befehl auf der erweiterten Berechtigungsebene können Sie ihn auf den wiederherzuenden Node herunterladen.
Auf einem Node im Cluster	<ol style="list-style-type: none">a. Verwenden Sie die <code>system configuration backup show</code> Befehl auf der erweiterten Berechtigungsebene, um die Liste der Backup-Konfigurationsdateien anzuzeigen, die im Cluster verfügbar sind, die die Konfiguration des wiederherzuenden Node enthält.b. Wenn die von Ihnen identifizierte Konfigurations-Backup-Datei nicht auf dem wiederherzuenden Knoten vorhanden ist, verwenden Sie den <code>system configuration backup copy</code> Befehl zum Kopieren auf den Node zum Wiederherstellen.

Wenn Sie zuvor den Cluster neu erstellt haben, sollten Sie eine Konfigurations-Backup-Datei wählen, die nach der Cluster-Erholung erstellt wurde. Wenn Sie eine Backup-Datei der Konfiguration verwenden müssen, die vor der Cluster-Erholung erstellt wurde, dann müssen Sie nach der Wiederherstellung des Knotens den Cluster erneut erstellen.

Stellen Sie die Node-Konfiguration mithilfe einer Backup-Konfigurationsdatei wieder her

Sie stellen die Node-Konfiguration mithilfe der Backup-Datei der Konfiguration wieder her, die Sie für den Wiederherstellungsknoten identifiziert und bereitgestellt haben.

Über diese Aufgabe

Sie sollten diese Aufgabe nur durchführen, um nach einem Notfall, der zum Verlust der lokalen Konfigurationsdateien des Knotens führte, wiederherzustellen.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Wenn der Node sich in einem ordnungsgemäßen Zustand befindet, verwenden Sie auf der erweiterten Berechtigungsebene eines anderen Node die `cluster modify` Befehl mit dem `-node` Und `-eligibility` Parameter, die nicht unterstützt werden sollen, und um sie vom Cluster zu isolieren.

Wenn der Knoten nicht ordnungsgemäß ist, sollten Sie diesen Schritt überspringen.

In diesem Beispiel wird `node2` so geändert, dass er nicht zur Teilnahme am Cluster berechtigt ist, damit seine Konfiguration wiederhergestellt werden kann:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Verwenden Sie die `system configuration recovery node restore` Befehl auf der erweiterten Berechtigungsebene zum Wiederherstellen der Node-Konfiguration aus einer Backup-Konfigurationsdatei.

Wenn der Knoten seine Identität verloren hat, einschließlich seines Namens, sollten Sie den verwenden `-nodename-in-backup` Parameter zum Angeben des Node-Namens in der Backup-Datei der Konfiguration.

In diesem Beispiel wird die Konfiguration des Node mithilfe einer der auf dem Node gespeicherten Backup-Konfigurationsdateien wiederhergestellt:

```
cluster1::*> system configuration recovery node restore -backup  
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with  
files contained in the specified backup file. Use this  
command only to recover from a disaster that resulted  
in the loss of the local configuration files.  
The node will reboot after restoring the local configuration.  
Do you want to continue? {y|n}: y
```

Die Konfiguration wird wiederhergestellt und der Node wird neu gebootet.

4. Wenn Sie den nicht zugelassenen Knoten markiert haben, verwenden Sie den `system configuration recovery cluster sync` Befehl, um den Node als berechtigt zu markieren und mit dem Cluster zu synchronisieren.
5. Wenn Sie in einer SAN-Umgebung arbeiten, verwenden Sie das `system node reboot` Befehl zum Neustart des Knotens und Wiederherstellung des SAN Quorum.

Nachdem Sie fertig sind

Wenn Sie das Cluster zuvor neu erstellt haben und wenn Sie die Node-Konfiguration mithilfe einer Backup-Konfigurationsdatei wiederherstellen, die vor der erneuten Erstellung dieses Clusters erstellt wurde, müssen Sie das Cluster erneut erstellen.

Suchen Sie eine Konfiguration zum Wiederherstellen eines Clusters

Zur Wiederherstellung eines Clusters verwenden Sie die Konfiguration entweder für einen Node im Cluster oder für eine Backup-Datei einer Cluster-Konfiguration.

Schritte

1. Wählen Sie eine Art von Konfiguration, um das Cluster wiederherzustellen.

- Ein Node im Cluster

Wenn das Cluster mehr als einen Node enthält und einer der Nodes über eine Cluster-Konfiguration verfügt, als sich das Cluster in der gewünschten Konfiguration befand, können Sie das Cluster mithilfe der auf diesem Node gespeicherten Konfiguration wiederherstellen.

In den meisten Fällen ist der Knoten, der den Replikationsring mit der letzten Transaktions-ID enthält, der für das Wiederherstellen der Cluster-Konfiguration am besten verwendet werden kann. Der `cluster ring show` Mit dem Befehl auf der erweiterten Berechtigungsebene können Sie eine Liste der replizierten Ringe anzeigen, die auf jedem Node im Cluster verfügbar sind.

- Eine Backup-Datei für die Cluster-Konfiguration

Wenn Sie keinen Node mit der korrekten Cluster-Konfiguration identifizieren können oder wenn das Cluster aus einem einzelnen Node besteht, können Sie eine Backup-Datei für die Cluster-Konfiguration verwenden, um das Cluster wiederherzustellen.

Wenn Sie das Cluster von einer Backup-Datei der Konfiguration wiederherstellen, gehen alle seit dem Backup vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Backup-Datei der Konfiguration und der vorhandenen Konfiguration behoben werden. Siehe Knowledge Base-Artikel ["ONTAP Configurations-Backup Resolution Guide"](#) Zur Anleitung zur Fehlerbehebung.

2. Wenn Sie sich für eine Backup-Datei der Cluster-Konfiguration entscheiden, stellen Sie die Datei dem Knoten zur Verfügung, den Sie verwenden möchten, um das Cluster wiederherzustellen.

Wenn sich die Backup-Datei der Konfiguration befindet...	Dann...
Unter einer Remote-URL	Verwenden Sie die <code>system configuration backup download</code> Mit dem Befehl auf der erweiterten Berechtigungsebene können Sie ihn auf den wiederherzuenden Node herunterladen.

Wenn sich die Backup-Datei der Konfiguration befindet...	Dann...
Auf einem Node im Cluster	<p>a. Verwenden Sie die <code>system configuration backup show</code> Befehl auf der erweiterten Berechtigungsebene zum Suchen einer Backup-Datei für die Cluster-Konfiguration, die erstellt wurde, als das Cluster in der gewünschten Konfiguration ausgeführt wurde.</p> <p>b. Wenn sich die Backup-Datei für die Cluster-Konfiguration nicht auf dem Node befindet, den Sie zur Wiederherstellung des Clusters verwenden möchten, verwenden Sie den <code>system configuration backup copy</code> Befehl zum Kopieren auf den Node zum Wiederherstellen.</p>

Wiederherstellen einer Cluster-Konfiguration aus einer vorhandenen Konfiguration

Zum Wiederherstellen einer Cluster-Konfiguration aus einer vorhandenen Konfiguration nach einem Cluster-Ausfall erstellen Sie das Cluster erneut mit der von Ihnen gewählten Cluster-Konfiguration, die dem Wiederherstellungsknoten zur Verfügung gestellt wurde, und fügen Sie dann jeden zusätzlichen Node wieder zum neuen Cluster hinzu.

Über diese Aufgabe

Sie sollten diese Aufgabe nur ausführen, um nach einem Ausfall die Konfiguration des Clusters zu verlieren.



Wenn Sie das Cluster erneut aus einer Sicherungsdatei der Konfiguration erstellen, müssen Sie sich an den technischen Support wenden, um alle Abweichungen zwischen der Backup-Datei der Konfiguration und der im Cluster vorhandenen Konfiguration zu beheben.

Wenn Sie das Cluster von einer Backup-Datei der Konfiguration wiederherstellen, gehen alle seit dem Backup vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Backup-Datei der Konfiguration und der vorhandenen Konfiguration behoben werden. Weitere Informationen finden Sie im Knowledge Base-Artikel ["ONTAP Leitfaden zur Lösung der Konfigurationssicherung enthält Hinweise zur Fehlerbehebung"](#).

Schritte

1. Deaktivieren Sie Storage-Failover für jedes HA-Paar:

```
storage failover modify -node node_name -enabled false
```

Sie müssen den Storage-Failover nur einmal für jedes HA-Paar deaktivieren. Wenn Sie den Storage-Failover für einen Node deaktivieren, ist auch das Storage-Failover beim Partner des Nodes deaktiviert.

2. Anhalten jedes Knotens mit Ausnahme des wiederherenden Knotens:

```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

4. Verwenden Sie auf dem Recovery-Node den **system configuration recovery cluster recreate** Befehl zum erneuten Erstellen des Clusters.

In diesem Beispiel wird das Cluster mithilfe der Konfigurationsinformationen, die auf dem wiederherzuenden Node gespeichert sind, neu erstellt:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

Auf dem wiederherstellenden Node wird ein neues Cluster erstellt.

5. Wenn Sie das Cluster aus einer Sicherungsdatei der Konfiguration neu erstellen, überprüfen Sie, ob die Cluster-Recovery noch läuft:

```
system configuration recovery cluster show
```

Sie müssen den Cluster-Recovery-Status nicht überprüfen, wenn Sie das Cluster von einem ordnungsgemäßen Node neu erstellen.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Booten aller Nodes, die neu mit dem neu erstellten Cluster verbunden werden müssen

Sie müssen die Nodes nacheinander neu booten.

7. Gehen Sie für jeden Node, der mit dem neu erstellten Cluster verbunden werden muss, wie folgt vor:

- a. Fügen Sie auf dem neu erstellten Cluster von einem gesunden Node erneut dem Ziel-Node bei:

```
system configuration recovery cluster rejoin -node node_name
```


In diesem Beispiel wird der Zielknoten „node2“ wieder dem neu erstellten Cluster hinzugefügt:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Der Ziel-Node wird neu gebootet und Beitritt zum Cluster.

- b. Vergewissern Sie sich, dass der Ziel-Node ordnungsgemäß ist und das Quorum mit den übrigen Nodes im Cluster gebildet wurde:

```
cluster show -eligibility true
```

Der Ziel-Node muss dem neu erstellten Cluster erneut beitreten, bevor Sie einem anderen Node erneut beitreten können.

```
cluster1::*> cluster show -eligibility true
Node                Health  Eligibility  Epsilon
-----
node0                true    true         false
node1                true    true         false
2 entries were displayed.
```

8. Wenn Sie das Cluster aus einer Backup-Konfigurationsdatei neu erstellen, setzen Sie den Recovery-Status auf abgeschlossen:

```
system configuration recovery cluster modify -recovery-status complete
```

9. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

10. Wenn der Cluster nur aus zwei Nodes besteht, verwenden Sie den **cluster ha modify** Befehl zum Reaktivieren der Cluster HA
11. Verwenden Sie die **storage failover modify** Befehl zum Reaktivieren von Storage Failover für jedes HA-Paar.

Nachdem Sie fertig sind

Wenn der Cluster über SnapMirror Peer-Beziehungen verfügt, müssen Sie diese Beziehungen auch neu erstellen. Weitere Informationen finden Sie unter "[Datensicherung](#)".

Synchronisieren eines Node mit dem Cluster

Wenn ein oder mehrere Knoten nicht mit dem Cluster synchronisiert sind, müssen Sie den Knoten synchronisieren, um die replizierte Datenbank (RDB) auf dem Knoten wiederherzustellen und in das Quorum zu bringen.

Schritt

1. Verwenden Sie von einem gesunden Knoten die `system configuration recovery cluster sync` Befehl auf der erweiterten Berechtigungsebene zum Synchronisieren des Node, der nicht mit der Cluster-Konfiguration synchronisiert ist.

Dieses Beispiel synchronisiert einen Knoten (*node2*) mit dem Rest des Clusters:

```
cluster1::*> system configuration recovery cluster sync -node node2
```

```
Warning: This command will synchronize node "node2" with the cluster
configuration, potentially overwriting critical cluster
configuration files on the node. This feature should only be
used to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress. This
command will cause all the cluster applications on node
"node2" to restart, interrupting administrative CLI and Web
interface on that node.
```

```
Do you want to continue? {y|n}: y
```

```
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

Ergebnis

Die RDB wird zum Node repliziert, und der Node kann am Cluster teilnehmen.

Management von Core Dumps (nur Cluster-Administratoren)

Wenn eine Panik eines Node auftritt, wird ein Core Dump angezeigt, und das System erstellt eine Core Dump-Datei, die vom technischen Support zum Beheben des Problems verwendet werden kann. Sie können Core Dump-Attribute konfigurieren oder anzeigen. Sie können auch eine Core Dump-Datei speichern, anzeigen, segmentieren, hochladen oder löschen.

Sie haben folgende Möglichkeiten, Core Dumps zu verwalten:

- Konfigurieren von Core Dumps und Anzeigen der Konfigurationseinstellungen
- Anzeigen von Basisinformationen, dem Status und den Attributen von Core Dumps

Core Dump-Dateien und -Berichte werden in gespeichert `/mroot/etc/crash/` Verzeichnis eines Knotens. Sie können den Verzeichnisinhalte mithilfe der anzeigen `system node coredump` Befehle oder

einen Webbrowser.



- Speichern des Core Dump-Inhalts und Hochladen der gespeicherten Datei an einen bestimmten Speicherort oder technischen Support


ONTAP verhindert, dass Sie das Speichern einer Core Dump-Datei während eines Takeover, einer Aggregatverschiebung oder einer Rückgabe initiieren.

- Löschen von Core Dump-Dateien, die nicht mehr benötigt werden

Befehle zum Verwalten von Core Dumps

Sie verwenden das `system node coredump config` Befehle zum Verwalten der Konfiguration von Core Dumps, die `system node coredump` Befehle zum Verwalten der Core Dump-Dateien und des `system node coredump reports` Befehle zum Managen von Kernberichten für Anwendungen.

Ihr Ziel ist	Befehl
Konfigurieren von Core Dumps	<code>system node coredump config modify</code>
Zeigt die Konfigurationseinstellungen für Core Dumps an	<code>system node coredump config show</code>
Zeigt grundlegende Informationen zu Core Dumps an	<code>system node coredump show</code>
Lösen Sie manuell einen Core Dump aus, wenn Sie einen Node neu booten	<code>system node reboot</code> Mit beiden <code>-dump</code> Und <code>-skip-lif-migration-before-reboot</code> Parameter  Der Link: https://docs.netapp.com/us-en/ontap-cli-9141/system-node-reboot.html#parameters Der Parameter <code>skip-lif-migration-before-reboot</code> gibt an, dass die LIF-Migration vor dem Neustart übersprungen wird.
Lösen Sie beim Herunterfahren eines Node manuell einen Core Dump aus	<code>system node halt</code> Mit beiden <code>-dump</code> Und <code>-skip-lif-migration-before-shutdown</code> Parameter  Der Link: https://docs.netapp.com/us-en/ontap-cli-9141/system-node-halt.html#parameters Der Parameter <code>skip-lif-migration-before-shutdown</code> gibt an, dass die LIF-Migration vor dem Herunterfahren übersprungen wird.
Speichern eines angegebenen Core Dump	<code>system node coredump save</code>

Ihr Ziel ist	Befehl
Speichern Sie alle nicht gespeicherten Core Dumps auf einem angegebenen Node	<code>system node coredump save-all</code>
Generieren und senden Sie eine AutoSupport-Nachricht mithilfe einer Core Dump-Datei, die Sie angeben	<code>system node autosupport invoke-core-upload</code> <div>  <p>Der <code>-uri</code> Der optionale Parameter gibt ein alternatives Ziel für die AutoSupport Meldung an.</p> </div>
Zeigt Statusinformationen zu Core Dumps an	<code>system node coredump status</code>
Löschen eines angegebenen Core Dump	<code>system node coredump delete</code>
Löschen Sie alle nicht gespeicherten Core Dumps oder alle gespeicherten Core-Dateien auf einem Node	<code>system node coredump delete-all</code>
Zeigt die Berichte zum Anwendungs-Core-Dump an	<code>system node coredump reports show</code>
Löschen eines Core Dump-Berichts der Anwendung	<code>system node coredump reports delete</code>

Verwandte Informationen

["ONTAP 9-Befehle"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.