Clusterverwaltung mit der CLI

ONTAP 9

NetApp
October 01, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/system-admin/index.html on October 01, 2026. Always check docs.netapp.com for the latest.

Inhalt

Clusterverwaltung mit der CLI . . . 1
Informationen zur Clusterverwaltung mit der ONTAP CLI . . . 1
Cluster- und SVM-Administratoren . . . 1
Informationen zu den Administratorrollen für ONTAP Cluster und SVM . . . 1
Webbrowser-Zugriff auf ONTAP System Manager aktivieren oder deaktivieren . . . 1
Informationen zum ONTAP Cluster Management Server . . . 2
Arten von SVMs in einem ONTAP Cluster . . . 2
Zugriff auf den Cluster über die CLI (nur für Cluster-Administratoren) . . . 3
Zugriff auf ein ONTAP Cluster über den seriellen Port . . . 3
Auf einen ONTAP Cluster mit SSH-Anfragen zugreifen . . . 3
ONTAP SSH-Anmeldesicherheit . . . 6
Telnet- oder RSH-Zugriff auf ein ONTAP Cluster ermöglichen . . . 8
Zugriff auf einen ONTAP Cluster mit Telnet-Anfragen . . . 10
Auf einen ONTAP Cluster mit RSH-Anfragen zugreifen . . . 12
Die ONTAP Befehlszeilenschnittstelle verwenden . . . 14
Informationen zur ONTAP Befehlszeile . . . 14
Informationen zu den verschiedenen ONTAP Shells für CLI-Befehle . . . 14
Navigation durch die ONTAP CLI-Befehlsverzeichnisse . . . 16
Regeln zur Angabe von Werten in ONTAP CLI . . . 17
ONTAP Befehlsverlauf anzeigen und jeden Befehl aus dem Verlauf erneut ausführen . . . 18
ONTAP Tastenkombinationen zum Bearbeiten von CLI-Befehlen . . . 19
Die Berechtigungsstufen für ONTAP CLI-Befehle . . . 20
Die Berechtigungsstufe in der ONTAP CLI festlegen . . . 21
Anzeigeeinstellungen für die ONTAP CLI festlegen . . . 21
Abfrageoperatoren in der ONTAP CLI verwenden . . . 22
Erweiterte Abfragen mit den Befehlen modify und delete in der ONTAP CLI verwenden . . . 24
Die Ausgabe des ONTAP show-Befehls kann mit dem Parameter fields eingeschränkt werden. . . . 24
Die Positionsparameter der ONTAP CLI in der Befehlseingabe verwenden . . . 25
Zugriff auf die Manpages der ONTAP CLI . . . 27
Eine ONTAP CLI Sitzung aufzeichnen und die aufgezeichneten Sitzungen verwalten . . . 27
Eine CLI-Sitzung aufzeichnen . . . 28
Befehle zur Verwaltung von Protokollen von CLI-Sitzungen . . . 28
Befehle zur Verwaltung des automatischen Zeitüberschreitungszeitraums von CLI-Sitzungen . . . 29
Clusterverwaltung (nur für Clusteradministratoren) . . . 29
Details auf Knotenebene in einem ONTAP Cluster . . . 29
ONTAP Cluster-Details auf Clusterebene anzeigen . . . 30
ONTAP Clusterattribute ändern . . . 30
Den Replikationsstatus der ONTAP Clusterringe anzeigen . . . 31
ONTAP Cluster-Gesundheitsbewertungen mithilfe von Quorum und Epsilon . . . 32
Kapazitätsauslastung der Systemvolumes in einem ONTAP Cluster anzeigen . . . 33
Knoten verwalten . . . 33
Knoten zu einem ONTAP Cluster hinzufügen . . . 33
Knoten aus einem ONTAP Cluster entfernen . . . 36

ONTAP-Knotenprotokolle, Core-Dumps und MIB-Dateien können mit einem Webbrowser abgerufen werden . . . 40
Zugriff auf die Systemkonsole eines ONTAP Knotens . . . 41
ONTAP Node-Root-Volumes und Root-Aggregate verwalten . . . 43
Einen ONTAP Knoten für Wartungs- oder Fehlerbehebungszwecke starten oder stoppen . . . 46
Einen ONTAP-Knoten über das Bootmenü verwalten . . . 49
Die Attribute der Knoten in einem ONTAP Cluster anzeigen . . . 51
Attribute eines ONTAP Knotens ändern . . . 52
Umbenennen eines ONTAP Knotens . . . 53
Verwaltung eines ONTAP Clusters mit einem einzelnen Knoten . . . 53
Das SP/BMC-Netzwerk konfigurieren . . . 58
ONTAP Verwaltungsdatenverkehr im Netzwerk isolieren . . . 58
Informationen zur ONTAP SP/ BMC Netzwerkkonfiguration . . . 59
Automatische Netzwerkkonfiguration für ONTAP SP/BMC aktivieren . . . 60
Das ONTAP SP/BMC Netzwerk manuell konfigurieren . . . 61
Die ONTAP Service Processor API-Konfiguration anpassen . . . 63
Knoten aus der Ferne mit dem SP/BMC verwalten . . . 64
Einen ONTAP Knoten remote mit dem SP/BMC verwalten . . . 64
Remote-Knotenverwaltung mit dem ONTAP Service Processor . . . 64
Der ONTAP Baseboard Management Controller ermöglicht die Remoteverwaltung eines Knotens. . . . 66
ONTAP SP/BMC-Firmware-Updates verwalten . . . 67
ONTAP SP/BMC und Netzwerkschnittstelle für Firmware-Updates . . . 68
Zugriff auf den ONTAP Service Processor mit einem Cluster-Benutzerkonto . . . 69
Zugriff auf das ONTAP SP/BMC eines Knotens von einem Administrationshost . . . 70
Zugriff auf das ONTAP SP/BMC eines Knotens von der Systemkonsole . . . 71
Wie die ONTAP SP CLI, SP Konsole und Systemkonsolensitzungen zusammenhängen . . . 72
Die IP-Adresse des Administrationshosts wird hinzugefügt, um auf den ONTAP Service Processor zuzugreifen. . . . 73
Die Hilfeinformationen in der ONTAP SP/BMC CLI anzeigen . . . 74
ONTAP Befehle für die Remote-Knotenverwaltung . . . 76
ONTAP Knotenzustandsüberwachung anhand schwellenwertbasierter SP Sensormesswerte und Status . . . 84
ONTAP SP Sensorstatuswerte in der Systemsensor-Befehlsausgabe . . . 86
ONTAP Befehle für das Service Processor Management . . . 89
ONTAP Befehle für BMC Management . . . 92
Unterstützte CLI-Befehle für den ONTAP Baseboard Management Controller . . . 93
ONTAP Clusterzeit verwalten (nur für Clusteradministratoren) . . . 94
Befehle zur Verwaltung der Clusterzeit . . . 95
Banner und MOTD verwalten . . . 96
Informationen zum ONTAP Anmeldebanner und zum Text der Nachricht des Tages . . . 96
Ein ONTAP Anmeldebanner erstellen . . . 98
Der Bannertext, der auf ONTAP Cluster- und SVM-Ebene angezeigt wird, kann verwaltet werden. . . . 100
Nachrichtentext für ONTAP Benutzer für den Message-of-the-Day erstellen . . . 101
Die Verwaltung des Message-of-the-Day-Textes, der auf ONTAP Cluster- und SVM-Ebene angezeigt wird . . . 103

ONTAP Jobs und Jobpläne verwalten . . . 106
Stellenkategorien . . . 106
Befehle zur Verwaltung von Jobs . . . 106
Befehle zur Verwaltung von Arbeitsplänen . . . 108
Sichern und Wiederherstellen von Cluster-Konfigurationen (nur für Clusteradministratoren) . . . 109
Informationen zu ONTAP Konfigurationssicherungsdateien . . . 109
Informationen zur Planung von Backups der ONTAP Cluster- und Knotenkonfigurationsdateien . . . 109
ONTAP Befehle zur Verwaltung von Konfigurationssicherungszeitplänen . . . 110
ONTAP Befehle zur Verwaltung von Sicherungsdateien für die Knotenkonfiguration . . . 110
Die ONTAP Knotenkonfigurationssicherungsdatei zum Wiederherstellen eines Knotens finden . . . 112
Einen Node mithilfe der ONTAP Node-Konfigurationssicherungsdatei wiederherstellen . . . 112
Die Sicherungsdatei der ONTAP Clusterkonfiguration zum Wiederherstellen eines Clusters finden . . . 114
Einen Cluster mithilfe der ONTAP Clusterkonfigurations-Sicherungsdatei wiederherstellen . . . 115
Einen Node mit dem ONTAP Cluster synchronisieren, damit das clusterweite Quorum gewährleistet ist. . . . 118
Knoten-Core-Dumps für einen ONTAP Cluster verwalten (nur für Cluster-Administratoren) . . . 118
Befehle zur Verwaltung von Core Dumps . . . 119

Clusterverwaltung mit der CLI

Informationen zur Clusterverwaltung mit der ONTAP CLI

ONTAP-Systeme lassen sich über die Befehlszeilenschnittstelle (CLI) verwalten. Die ONTAP Managementoberflächen können genutzt, auf den Cluster zugegriffen, Knoten verwaltet und vieles mehr durchgeführt werden.

Diese Vorgehensweise sollte unter folgenden Umständen angewendet werden:

- Der Funktionsumfang der ONTAP Administratorfähigkeiten soll nachvollzogen werden.
- Sie möchten die Befehlszeilenschnittstelle (CLI) verwenden, nicht System Manager oder ein automatisiertes Skripting-Tool.

Verwandte Informationen

Einzelheiten zur Syntax und Verwendung der Befehlszeilenschnittstelle sind in der "ONTAP-Befehlsreferenz" Dokumentation zu finden.

Cluster- und SVM-Administratoren

Informationen zu den Administratorrollen für ONTAP Cluster und SVM

Cluster-Administratoren verwalten den gesamten Cluster und die darin enthaltenen Storage Virtual Machines (SVMs, früher bekannt als Vserver). SVM-Administratoren verwalten nur ihre eigenen Daten-SVMs.

Clusteradministratoren können den gesamten Cluster und seine Ressourcen verwalten. Sie können auch Daten-SVMs einrichten und die SVM-Verwaltung an SVM-Administratoren delegieren. Die spezifischen Fähigkeiten, über die Clusteradministratoren verfügen, hängen von ihren Zugriffssteuerungsrollen ab. Standardmäßig verfügt ein Clusteradministrator mit dem Kontonamen oder Rollennamen „admin“ über alle Fähigkeiten zur Verwaltung des Clusters und der SVMs.

SVM-Administratoren können nur ihre eigenen SVM-Speicher und Netzwerkressourcen wie Volumes, Protokolle, LIFs und Dienste verwalten. Die spezifischen Berechtigungen, über die SVM-Administratoren verfügen, hängen von den Zugriffskontrollrollen ab, die von Cluster-Administratoren zugewiesen werden.

> Die ONTAP Befehlszeilenschnittstelle (CLI) verwendet weiterhin den Begriff *Vserver* in der Ausgabe, und `vserver` als Befehls- oder Parametername wurde nicht geändert.

Webbrowser-Zugriff auf ONTAP System Manager aktivieren oder deaktivieren

Sie können den Zugriff eines Webbrowsers auf den System Manager aktivieren oder deaktivieren. Außerdem besteht die Möglichkeit, das System Manager Protokoll anzuzeigen.

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

Die System Manager Protokollierung wird in den `/mroot/etc/log/mlog/sysmgr.log` Dateien des Knotens aufgezeichnet, der zum Zeitpunkt des Zugriffs auf den System Manager die Cluster Management-LIF hostet. Die Protokolldateien können mit einem Browser angezeigt werden. Das System Manager Protokoll ist auch in AutoSupport Nachrichten enthalten.

Informationen zum ONTAP Cluster Management Server

Der Cluster-Management-Server, auch *admin*SVM genannt, ist eine spezialisierte Implementierung einer Storage Virtual Machine (SVM), die den Cluster als eine einzige verwaltbare Einheit darstellt. Zusätzlich zur Funktion als oberste administrative Domäne besitzt der Cluster-Management-Server Ressourcen, die logisch nicht zu einer Daten-SVM gehören.

Der Cluster-Management-Server ist im Cluster immer verfügbar. Der Cluster-Management-Server kann über die Konsole oder die Cluster-Management-LIF aufgerufen werden.

Bei Ausfall des Heimnetzwerkports schlägt die Cluster-Management-LIF automatisch auf einen anderen Node im Cluster um. Abhängig von den Konnektivitätseigenschaften des verwendeten Managementprotokolls kann der Failover wahrgenommen werden oder auch nicht. Bei Verwendung eines verbindungslosen Protokolls (zum Beispiel SNMP) oder einer eingeschränkten Verbindung (zum Beispiel HTTP) wird der Failover in der Regel nicht bemerkt. Bei einer langfristigen Verbindung (zum Beispiel SSH) ist nach dem Failover eine erneute Verbindung zum Cluster-Management-Server erforderlich.

Bei der Erstellung eines Clusters werden alle Eigenschaften der Cluster-Management-LIF konfiguriert, einschließlich ihrer IP-Adresse, Netzmaske, Gateway und Port.

Im Gegensatz zu einer Daten-SVM oder einer Knoten-SVM verfügt ein Cluster Management-Server nicht über ein Root-Volume oder hostet Benutzer-Volumes (obwohl er System-Volumes hosten kann). Außerdem kann ein Cluster Management-Server nur LIFs vom Typ Cluster Management haben.

Wenn Sie den `vserver show` Befehl ausführen, erscheint der Cluster Management-Server in der Ausgabeliste dieses Befehls.

Arten von SVMs in einem ONTAP Cluster

Ein Cluster besteht aus vier Arten von SVMs, die bei der Verwaltung des Clusters und seiner Ressourcen sowie beim Datenzugriff für Clients und Anwendungen helfen.

Ein Cluster enthält die folgenden SVM-Typen:

- Admin-SVM

  Der Cluster-Setup-Prozess erstellt automatisch die Admin-SVM für den Cluster. Die Admin-SVM repräsentiert den Cluster.

- Knoten-SVM

  Eine Node SVM wird erstellt, wenn der Knoten dem Cluster beitritt, und die Node SVM repräsentiert die einzelnen Knoten des Clusters.

- System SVM (erweitert)

  Eine System-SVM wird für die Kommunikation auf Clusterebene in einem IPspace automatisch erstellt.

- Data SVM

  Eine Daten-SVM repräsentiert die datenbereitstellenden SVMs. Nach der Cluster-Einrichtung muss ein Cluster-Administrator Daten-SVMs erstellen und diesen SVMs Volumes hinzufügen, um den Datenzugriff aus dem Cluster zu ermöglichen.

  Ein Cluster muss mindestens eine Daten-SVM besitzen, um Daten an seine Clients bereitzustellen.

  Sofern nicht anders angegeben, bezieht sich der Begriff SVM auf eine Data (datenservierende) SVM.

  In der CLI werden SVMs als Vservers angezeigt.

Zugriff auf den Cluster über die CLI (nur für Cluster-Administratoren)

Zugriff auf ein ONTAP Cluster über den seriellen Port

Der Cluster kann direkt über eine Konsole erreicht werden, die an den seriellen Port eines Node angeschlossen ist.

Schritte

1. An der Konsole die Eingabetaste drücken.

   Das System antwortet mit der Anmeldeaufforderung.

2. Am Anmelde-Prompt eine der folgenden Optionen auswählen:

Um auf den Cluster mit … zuzugreifen	Geben Sie den folgenden Kontonamen ein…
Das Standard-Clusterkonto	**`admin`**
Ein alternatives administratives Benutzerkonto	*`username`*

   Das System antwortet mit der Aufforderung zur Passworteingabe.

3. Das Passwort für das Admin- oder Administrationsbenutzerkonto eingeben und anschließend die Eingabetaste drücken.

Auf einen ONTAP Cluster mit SSH-Anfragen zugreifen

Sie können SSH-Anfragen an einen ONTAP Cluster senden, um administrative Aufgaben auszuführen. SSH ist standardmäßig aktiviert.

Bevor Sie beginnen

- Sie benötigen ein Benutzerkonto, das für die Verwendung von `ssh` als Zugriffsmethode konfiguriert ist.

  Der `-application` Parameter der `security login` Befehle gibt das Zugriffsverfahren für ein Benutzerkonto an. Weitere Informationen zu `security login` finden sich in der "ONTAP-Befehlsreferenz".

- Wenn Sie ein Active Directory (AD) Domänenbenutzerkonto für den Zugriff auf den Cluster verwenden, muss ein Authentifizierungstunnel für den Cluster über eine CIFS-fähige Storage-VM eingerichtet worden sein, und Ihr AD Domänenbenutzerkonto muss dem Cluster auch mit `ssh` als Zugriffsmethode und `domain` als Authentifizierungsverfahren hinzugefügt worden sein.

Über diese Aufgabe

- Ein OpenSSH-Client ab Version 5.7 muss verwendet werden.
- Es wird ausschließlich das SSH v2 Protokoll unterstützt; SSH v1 wird nicht unterstützt.
- ONTAP unterstützt maximal 64 gleichzeitige SSH-Sitzungen pro Knoten.

  Befindet sich die Cluster-Management-LIF auf dem Node, teilt sie sich dieses Limit mit der Node-Management-LIF.

  Wenn die Anzahl der eingehenden Verbindungen mehr als 10 pro Sekunde beträgt, wird der Dienst vorübergehend für 60 Sekunden deaktiviert.

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

  AES unterstützt Schlüssellängen von 128, 192 und 256 Bit. 3DES verwendet wie das ursprüngliche DES eine Schlüssellänge von 56 Bit, die jedoch dreimal wiederholt wird.

- Wenn der FIPS-Modus aktiviert ist, sollten SSH-Clients mit den öffentlichen Schlüsselalgorithmen des Elliptic Curve Digital Signature Algorithm (ECDSA) verhandeln, damit die Verbindung erfolgreich ist.
- Wenn von einem Windows-Host aus auf die ONTAP-CLI zugegriffen werden soll, kann ein Drittanbieter-Tool wie PuTTY verwendet werden.
- Wenn Sie sich mit einem Windows AD-Benutzernamen bei ONTAP anmelden, sollten Sie die gleichen Groß- und Kleinbuchstaben verwenden, die bei der Erstellung des AD-Benutzernamens und des Domänennamens in ONTAP verwendet wurden.

  AD-Benutzernamen und Domänennamen sind nicht case-sensitiv. ONTAP-Benutzernamen sind jedoch case-sensitiv. Eine Abweichung in der Groß- und Kleinschreibung zwischen dem in ONTAP erstellten Benutzernamen und dem in AD erstellten Benutzernamen führt zu einem Anmeldefehler.

SSH Authentifizierungsoptionen

- Ab ONTAP 9.3 ist es möglich, "SSH-Multifaktor-Authentifizierung aktivieren" für lokale Administratorkonten zu verwenden.

  Wenn die SSH-Multifaktor Authentifizierung aktiviert ist, erfolgt die Authentifizierung der Benutzer mithilfe eines öffentlichen Schlüssels und eines Passworts.

- Ab ONTAP 9.4 kann "SSH-Multifaktor-Authentifizierung aktivieren" für LDAP- und NIS-Remote-Benutzer verwendet werden.
- Ab ONTAP 9.13.1 können Sie optional die Zertifikatsvalidierung zum SSH-Authentifizierungsprozess hinzufügen, um die Anmeldesicherheit zu erhöhen. Dazu "Ein X.509-Zertifikat mit dem öffentlichen Schlüssel verknüpfen" das ein Konto verwendet, überprüfen. Wenn Sie sich per SSH mit sowohl einem öffentlichen SSH-Schlüssel als auch einem X.509-Zertifikat anmelden, prüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor mit dem öffentlichen SSH-Schlüssel authentifiziert wird. Die SSH-Anmeldung wird verweigert, wenn dieses Zertifikat abgelaufen oder widerrufen ist, und der öffentliche SSH-Schlüssel wird automatisch deaktiviert.
- Ab ONTAP 9.14.1 können ONTAP-Administratoren "Cisco Duo Zwei-Faktor-Authentifizierung zum SSH-Authentifizierungsprozess hinzufügen" die Anmeldesicherheit erhöhen. Nach der Aktivierung der Cisco

Duo Authentifizierung müssen Benutzer beim ersten Anmelden ein Gerät als Authentifikator für SSH-Sitzungen registrieren.

- Ab ONTAP 9.15.1 können Administratoren "Dynamische Autorisierung konfigurieren" zusätzliche adaptive Authentifizierung für SSH-Benutzer basierend auf dem Vertrauenswert des Benutzers bereitstellen.
- Ab ONTAP 9.19.1 können Administratoren den "security ssh publickey show -vserver -host-key-algorithm command" verwenden, um den Fingerabdruck des ONTAP-Hostschlüssels anzuzeigen. Dies ermöglicht Administratoren zu überprüfen, ob dieser Fingerabdruck mit dem in ONTAP gespeicherten übereinstimmt.

Schritte

1. Von einem Host mit Zugriff auf das Netzwerk des ONTAP-Clusters den `ssh` Befehl in einem der folgenden Formate eingeben:
   - **ssh *username@hostname_or_IP* [*command*]**
   - **ssh -l *username hostname_or_IP* [*command*]**

Wenn Sie ein AD-Domänenbenutzerkonto verwenden, muss *username* im Format *domainname**AD_accountname* (mit doppelten Backslashes nach dem Domänennamen) oder "*domainname**AD_accountname*" (in doppelten Anführungszeichen und mit einem einfachen Backslash nach dem Domänennamen) angegeben werden.

hostname_or_IP ist der Hostname oder die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF. Die Verwendung des Cluster-Management-LIF wird empfohlen. Es kann eine IPv4- oder IPv6-Adresse verwendet werden.

command ist für SSH-interaktive Sitzungen nicht erforderlich.

Beispiele für SSH-Anfragen

Die folgenden Beispiele zeigen, wie das Benutzerkonto mit dem Namen “joe” eine SSH-Anfrage an einen Cluster stellen 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 mit dem Namen “john” aus der Domäne mit dem Namen “DOMAIN1” eine SSH-Anfrage an einen Cluster stellen 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-Anfrage stellen kann, um auf einen Cluster zuzugreifen, 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.
```

Verwandte Informationen

"Administratorauthentifizierung und RBAC"

ONTAP SSH-Anmeldesicherheit

Ab ONTAP 9.5 sind Informationen über frühere Anmeldungen, erfolglose Anmeldeversuche und Änderungen Ihrer Berechtigungen seit Ihrer letzten erfolgreichen Anmeldung verfügbar.

Sicherheitsrelevante Informationen werden angezeigt, wenn Sie sich erfolgreich als SSH-Administrator

anmelden. Es erfolgt eine Benachrichtigung über die folgenden Bedingungen:

- Das letzte Mal, als Ihr Kontoname angemeldet war.
- Die Anzahl der erfolglosen Anmeldeversuche seit der letzten erfolgreichen Anmeldung.
- Ob sich die Rolle seit dem letzten Login geändert hat (zum Beispiel, wenn sich die Rolle des Administratorkontos von "admin" zu "backup" geändert hat)
- Ob die Berechtigungen zum Hinzufügen, Ändern oder Löschen der Rolle seit der letzten Anmeldung geändert wurden.

> Wenn einige der angezeigten Informationen verdächtig erscheinen, sollte umgehend die Sicherheitsabteilung kontaktiert werden.

Um diese Informationen beim Anmelden zu erhalten, müssen folgende Voraussetzungen erfüllt sein:

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

Einschränkungen und weitere Überlegungen zur Sicherheit bei der SSH-Anmeldung

Für die Sicherheitsinformationen zur SSH-Anmeldung gelten die folgenden Einschränkungen und Überlegungen:

- 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, der sie angehören, als Administratorkonto in ONTAP bereitgestellt ist.

  Warnmeldungen über Änderungen an der Rolle des Benutzerkontos können diesen Benutzern jedoch nicht angezeigt werden. Außerdem können Benutzer, die einer Active Directory Gruppe angehören, die als Administratorkonto in ONTAP bereitgestellt wurde, die Anzahl der fehlgeschlagenen Anmeldeversuche seit ihrer letzten Anmeldung nicht einsehen.

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

Beispiele für SSH-Anmeldesicherheitsinformationen

Die folgenden Beispiele veranschaulichen die Art von Informationen, die nach dem Login angezeigt werden.

- Diese Meldung wird nach jedem erfolgreichen Login angezeigt:

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

- Diese Meldungen werden angezeigt, wenn seit der letzten erfolgreichen Anmeldung erfolglose Anmeldeversuche stattgefunden haben:

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

- Diese Meldungen werden angezeigt, wenn es fehlgeschlagene Anmeldeversuche gab 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
```

Telnet- oder RSH-Zugriff auf ein ONTAP Cluster ermöglichen

Als Sicherheitsbest Practice sind Telnet und RSH standardmäßig deaktiviert. Damit der Cluster Telnet- oder RSH-Anfragen akzeptiert, muss der Dienst in der Standardrichtlinie für Verwaltungsdienste aktiviert werden.

Telnet und RSH sind keine sicheren Protokolle, die Verwendung von SSH für den Zugriff auf den Cluster wird empfohlen. SSH bietet eine sichere Remote-Shell und eine interaktive Netzwerksitzung. Weitere Informationen finden sich unter "Zugriff auf den Cluster über SSH".

Über diese Aufgabe

- ONTAP unterstützt maximal 50 gleichzeitige Telnet- oder RSH-Sitzungen pro Knoten.

  Befindet sich die Cluster-Management-LIF auf dem Node, teilt sie sich dieses Limit mit der Node-Management-LIF.

  Wenn die Anzahl der eingehenden Verbindungen mehr als 10 pro Sekunde beträgt, wird der Dienst vorübergehend für 60 Sekunden deaktiviert.

- Für RSH Befehle sind erweiterte Berechtigungen erforderlich.

ONTAP 9.10.1 oder höher

Schritte

1. Bestätigen Sie, dass das RSH- oder Telnet-Sicherheitsprotokoll aktiviert ist:

   ```
   security protocol show
   ```

   a. Wenn das Sicherheitsprotokoll RSH oder Telnet aktiviert ist, erfolgt der nächste Schritt.

   b. Falls das Sicherheitsprotokoll RSH oder Telnet nicht aktiviert ist, kann es mit dem folgenden Befehl aktiviert werden:

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

   Weitere Informationen zu `security protocol show` und `security protocol modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Bestätigen Sie, dass der `management-rsh-server` oder `management-telnet-server` Dienst

auf den Management-LIFs vorhanden ist:

```
network interface show -services management-rsh-server
```

oder

```
network interface show -services management-telnet-server
```

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

a. Falls der `management-rsh-server` oder `management-telnet-server` Dienst existiert, zum nächsten Schritt übergehen.

b. Falls der `management-rsh-server` oder `management-telnet-server` Dienst nicht existiert, kann der folgende Befehl zum Hinzufügen verwendet werden:

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-rsh-server

network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-telnet-server
```

Weitere Informationen zu `network interface service-policy add-service` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP 9.9 oder früher

Über diese Aufgabe

ONTAP verhindert, dass vordefinierte Firewall-Richtlinien geändert werden können, aber es besteht die Möglichkeit, eine neue Richtlinie zu erstellen, indem die vordefinierte `mgmt` Management-Firewall-Richtlinie geklont und anschließend Telnet oder RSH in der neuen Richtlinie aktiviert wird.

Schritte

1. In den erweiterten Berechtigungsmodus wechseln:

```
set advanced
```

2. Ein Sicherheitsprotokoll (RSH oder Telnet) aktivieren:

```
security protocol modify -application security_protocol -enabled true
```

3. Eine neue Management-Firewall-Richtlinie wird auf Basis der `mgmt`Management-Firewall-Richtlinie erstellt:

```
system services firewall policy clone -policy mgmt -destination-policy
policy-name
```

4. Telnet oder RSH in der neuen Management-Firewall-Richtlinie aktivieren:

```
system services firewall policy create -policy policy-name -service
security_protocol -action allow -ip-list ip_address/netmask
```

Um alle IP-Adressen zuzulassen, sollte Folgendes angegeben werden: `-ip-list 0.0.0.0/0`

5. Die neue Richtlinie wird mit der Cluster-Management-LIF verknüpft:

```
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
-firewall-policy policy-name
```

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

Zugriff auf einen ONTAP Cluster mit Telnet-Anfragen

Sie können Telnet-Anfragen an den Cluster senden, um administrative Aufgaben auszuführen. Telnet ist standardmäßig deaktiviert.

Telnet und RSH sind keine sicheren Protokolle, die Verwendung von SSH für den Zugriff auf den Cluster wird empfohlen. SSH bietet eine sichere Remote-Shell und eine interaktive Netzwerksitzung. Weitere Informationen finden sich unter "Zugriff auf den Cluster über SSH".

Bevor Sie beginnen

Folgende Bedingungen müssen erfüllt sein, bevor Sie mit Telnet auf den Cluster zugreifen können:

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

  Der `-application` Parameter der `security login` Befehle gibt das Zugriffsverfahren für ein Benutzerkonto an. Weitere Informationen zu `security login` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

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

  Befindet sich die Cluster-Management-LIF auf dem Node, teilt sie sich dieses Limit mit der Node-Management-LIF.

  Wenn die Anzahl der eingehenden Verbindungen 10 pro Sekunde übersteigt, wird der Service für 60 Sekunden vorübergehend deaktiviert.

- Wenn von einem Windows-Host aus auf die ONTAP-CLI zugegriffen werden soll, kann ein Drittanbieter-Tool wie PuTTY verwendet werden.
- Für RSH Befehle sind erweiterte Berechtigungen erforderlich.

ONTAP 9.10.1 oder höher

Schritte

1. Bestätigen Sie, dass das Telnet Sicherheitsprotokoll aktiviert ist:

   ```
   security protocol show
   ```

   a. Wenn das Telnet-Sicherheitsprotokoll aktiviert ist, erfolgt der nächste Schritt.

   b. Falls das Telnet-Sicherheitsprotokoll nicht aktiviert ist, kann es mit dem folgenden Befehl aktiviert werden:

   ```
   security protocol modify -application telnet -enabled true
   ```

Weitere Informationen zu `security protocol show` und `security protocol modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Bestätigen Sie, dass der `management-telnet-server` Dienst auf den Management-LIFs vorhanden ist:

   ```
   network interface show -services management-telnet-server
   ```

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

   a. Falls der `management-telnet-server` Dienst existiert, wird mit dem nächsten Schritt fortgefahren.

   b. Falls der `management-telnet-server` Dienst nicht existiert, kann der folgende Befehl zum Hinzufügen verwendet werden:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   Weitere Informationen zu `network interface service-policy add-service` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP 9.9 oder früher

Bevor Sie beginnen

Folgende Bedingungen müssen erfüllt sein, bevor Sie mit Telnet auf den Cluster zugreifen können:

- Telnet muss bereits in der Management-Firewall-Richtlinie aktiviert sein, die von den Cluster- oder Knotenmanagement-LIFs verwendet wird, damit Telnet-Anfragen die Firewall passieren können.

  Telnet ist standardmäßig deaktiviert. Der `system services firewall policy show` Befehl mit dem `-service telnet` Parameter zeigt an, ob Telnet in einer Firewall-Richtlinie aktiviert ist. Weitere Informationen zu `system services firewall policy` finden sich in der "ONTAP-Befehlsreferenz".

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

  Der `network options ipv6 show`Befehl zeigt an, ob IPv6 aktiviert ist. Weitere Informationen zu `network options ipv6 show` finden sich in der "ONTAP-Befehlsreferenz". Der `system services firewall policy show`Befehl zeigt Firewall-Richtlinien an.

Schritte

1. Auf einem Administrationsrechner ist folgender Befehl einzugeben:

   ```
   telnet hostname_or_IP
   ```

   `hostname_or_IP` ist der Hostname oder die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF. Die Verwendung des Cluster-Management-LIF wird empfohlen. Es kann eine IPv4- oder IPv6-Adresse verwendet werden.

Beispiel einer Telnet-Anfrage

Das folgende Beispiel zeigt, wie der Benutzer mit dem Namen „joe“, der mit Telnet-Zugriff eingerichtet wurde, eine Telnet-Anfrage stellen kann, um auf einen Cluster zuzugreifen, dessen Cluster-Management-LIF

10.72.137.28 ist:

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Auf einen ONTAP Cluster mit RSH-Anfragen zugreifen

Sie können RSH-Anfragen an den Cluster senden, um administrative Aufgaben auszuführen. RSH ist kein sicheres Protokoll und ist standardmäßig deaktiviert.

Telnet und RSH sind keine sicheren Protokolle, die Verwendung von SSH für den Zugriff auf den Cluster wird empfohlen. SSH bietet eine sichere Remote-Shell und eine interaktive Netzwerksitzung. Weitere Informationen finden sich unter "Zugriff auf den Cluster über SSH".

Bevor Sie beginnen

Folgende Bedingungen müssen erfüllt sein, bevor Sie RSH zum Zugriff auf den Cluster verwenden können:

- Sie benötigen ein lokales Cluster-Benutzerkonto, das für die Verwendung von RSH als Zugriffsmethode konfiguriert ist.

  Der `-application` Parameter der `security login` Befehle gibt das Zugriffsverfahren für ein Benutzerkonto an. Weitere Informationen zu `security login` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

- ONTAP unterstützt maximal 50 gleichzeitige RSH-Sitzungen pro Knoten.

  Befindet sich die Cluster-Management-LIF auf dem Node, teilt sie sich dieses Limit mit der Node-Management-LIF.

  Wenn die Anzahl der eingehenden Verbindungen mehr als 10 pro Sekunde beträgt, wird der Dienst vorübergehend für 60 Sekunden deaktiviert.

- Für RSH Befehle sind erweiterte Berechtigungen erforderlich.

ONTAP 9.10.1 oder höher

Schritte

1. Bestätigen Sie, dass das RSH Sicherheitsprotokoll aktiviert ist:

   ```
   security protocol show
   ```

   a. Wenn das RSH Sicherheitsprotokoll aktiviert ist, erfolgt der nächste Schritt.

   b. Falls das RSH-Sicherheitsprotokoll nicht aktiviert ist, kann es mit dem folgenden Befehl aktiviert werden:

```
security protocol modify -application rsh -enabled true
```

Weitere Informationen zu `security protocol show` und `security protocol modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Bestätigen Sie, dass der `management-rsh-server` Dienst auf den Management-LIFs vorhanden ist:

```
network interface show -services management-rsh-server
```

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

   a. Falls der `management-rsh-server` Dienst existiert, wird mit dem nächsten Schritt fortgefahren.

   b. Falls der `management-rsh-server` Dienst nicht existiert, kann der folgende Befehl zum Hinzufügen verwendet werden:

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-rsh-server
```

Weitere Informationen zu `network interface service-policy add-service` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP 9.9 oder früher

Bevor Sie beginnen

Folgende Bedingungen müssen erfüllt sein, bevor Sie RSH zum Zugriff auf den Cluster verwenden können:

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

  Standardmäßig ist RSH deaktiviert. Der Befehl system services firewall policy show mit dem `-service rsh` Parameter zeigt an, ob RSH in einer Firewall-Richtlinie aktiviert ist. Weitere Informationen zu `system services firewall policy` finden sich in der "ONTAP-Befehlsreferenz".

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

  Der `network options ipv6 show`Befehl zeigt an, ob IPv6 aktiviert ist. Weitere Informationen zu `network options ipv6 show` finden sich in der "ONTAP-Befehlsreferenz". Der `system services firewall policy show`Befehl zeigt Firewall-Richtlinien an.

Schritte

1. Auf einem Administrationsrechner ist folgender Befehl einzugeben:

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

`hostname_or_IP` ist der Hostname oder die IP-Adresse des Cluster-Management-LIF oder eines Node-Management-LIF. Die Verwendung des Cluster-Management-LIF wird empfohlen. Es kann eine IPv4- oder IPv6-Adresse verwendet werden.

`command` ist der Befehl, der über RSH ausgeführt werden soll.

Beispiel einer RSH-Anfrage

Das folgende Beispiel zeigt, wie der Benutzer mit dem Namen “joe”, der mit RSH-Zugriff eingerichtet wurde, eine RSH-Anfrage stellen kann, um den `cluster show` Befehl auszuführen:

```
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$
```

Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".

Die ONTAP Befehlszeilenschnittstelle verwenden

Informationen zur ONTAP Befehlszeile

Die ONTAP Befehlszeilenschnittstelle (CLI) bietet eine befehlsbasierte Ansicht der Managementoberfläche. Befehle werden an der Eingabeaufforderung des Speichersystems eingegeben, und die Befehlsergebnisse erscheinen als Text.

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

Wenn die Berechtigungsstufe (d. h. der `-privilege`Parameter des `set`Befehls) auf `advanced` gesetzt ist, enthält die Eingabeaufforderung ein Sternchen (*), zum Beispiel:

```
cluster_name::*>
```

Weitere Informationen zu `set` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zu den verschiedenen ONTAP Shells für CLI-Befehle

Der Cluster verfügt über drei verschiedene Shells für CLI-Befehle, die *clustershell*, die *nodeshell* und die *systemshell*. Die Shells dienen unterschiedlichen Zwecken und verfügen jeweils über einen anderen Befehlssatz.

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

  Es stellt alle Befehle bereit, die Sie zum Konfigurieren und Verwalten des Clusters benötigen. Die Clustershell CLI-Hilfe (aufgerufen durch `?` an der Clustershell-Eingabeaufforderung) zeigt die verfügbaren Clustershell-Befehle an. Der `man`-Befehl in der Clustershell zeigt die Manpage für den angegebenen Clustershell-Befehl an (`man <command_name>`. Weitere Informationen zu `man` finden sich in der "ONTAP-Befehlsreferenz".

- Die Nodeshell ist eine spezielle Shell für Befehle, die nur auf Knotenebene wirksam sind.

Die nodeshell ist über den `system node run` Befehl zugänglich. Weitere Informationen zu `system node run` finden sich in der "ONTAP-Befehlsreferenz".

Die nodeshell CLI-Hilfe (aufgerufen durch `?` oder `help` an der nodeshell-Eingabeaufforderung) zeigt die verfügbaren nodeshell-Befehle an. Der `man`-Befehl in der nodeshell zeigt die Manpage für den angegebenen nodeshell-Befehl an.

Viele häufig verwendete Nodeshell-Befehle und Optionen werden in die Clustershell getunnelt oder als Aliase bereitgestellt und können auch von der Clustershell aus ausgeführt werden.

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

  Die systemshell und das zugehörige `diag` Konto sind für Low-Level-Diagnosezwecke vorgesehen. Für den Zugriff ist die Berechtigungsstufe „Diagnose“ erforderlich und er ist ausschließlich dem technischen Support zur Durchführung von Fehlerbehebungsaufgaben vorbehalten.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Zugriff auf Nodeshell-Befehle 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 die Clustershell getunnelt oder als Aliase bereitgestellt und können auch von der Clustershell aus ausgeführt werden.

Die in der Clustershell unterstützten Nodeshell-Optionen können über den `vserver options clustershell` Befehl aufgerufen werden. Diese Optionen lassen sich durch eine Abfrage der Clustershell-CLI mit `vserver options -vserver` *`nodename_or_clustername`* `-option-name ?` anzeigen.

Wenn in der Clustershell ein Nodeshell- oder Legacy-Befehl oder eine entsprechende Option eingegeben wird und dieser Befehl oder diese Option einen entsprechenden Clustershell-Befehl hat, informiert ONTAP über den zu verwendenden Clustershell-Befehl.

Wenn ein Node-Shell- oder Legacy-Befehl oder eine Option eingegeben wird, die in der Cluster-Shell nicht unterstützt wird, informiert ONTAP über den Status „`nicht unterstützt`“ für den Befehl oder die Option.

Verfügbare Nodeshell-Befehle

Eine Liste der verfügbaren nodeshell Befehle ist über die CLI-Hilfe der nodeshell abrufbar.

Schritte

1. Um auf die Nodeshell zuzugreifen, den folgenden Befehl an der Systemeingabeaufforderung der Clustershell eingeben:

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

   `local` ist der Knoten, den Sie für den Zugriff auf den Cluster verwendet haben.

   Der `system node run`Befehl hat einen Aliasbefehl, `run`.

2. Im Nodeshell kann mit dem folgenden Befehl die Liste der verfügbaren Nodeshell-Befehle angezeigt werden:

   [*commandname*] help

   ```
   `_commandname_` ist der Name des Befehls, dessen Verfügbarkeit Sie
   anzeigen möchten. Wenn  `_commandname_` nicht angegeben wird, zeigt die
   CLI alle verfügbaren nodeshell Befehle an.
   ```

   Sie drücken die Eingabetaste `exit` oder geben Strg+d ein, um zur Clustershell CLI zurückzukehren.

   Weitere Informationen zu `exit` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel für die Anzeige der verfügbaren Nodeshell-Befehle

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

```
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]]
```

Navigation durch die ONTAP CLI-Befehlsverzeichnisse

Die Befehle in der Befehlszeilenschnittstelle (CLI) sind in einer Hierarchie durch Befehlsverzeichnisse organisiert. Befehle in der Hierarchie können entweder durch Eingabe des vollständigen Befehlspfads oder durch Navigation durch die Verzeichnisstruktur ausgeführt werden.

Bei Verwendung der Befehlszeilenschnittstelle (CLI) kann auf ein Befehlsverzeichnis zugegriffen werden, indem der Name des Verzeichnisses an der Eingabeaufforderung eingegeben und anschließend die Eingabetaste gedrückt wird. Der Verzeichnisname erscheint dann in der Eingabeaufforderung, um anzuzeigen, dass mit dem entsprechenden Befehlsverzeichnis interagiert wird. Um tiefer in die Befehlshierarchie zu gelangen, wird der Name eines Befehlsunterverzeichnisses eingegeben und anschließend die Eingabetaste gedrückt. Der Name des Unterverzeichnisses erscheint dann in der Eingabeaufforderung, und der Kontext wechselt zu diesem Unterverzeichnis.

Sie können durch mehrere Befehlsverzeichnisse navigieren, indem Sie den gesamten Befehl eingeben. Beispielsweise können Sie Informationen über Festplattenlaufwerke anzeigen, indem Sie den `storage disk show` Befehl an der Eingabeaufforderung eingeben. Der Befehl kann auch ausgeführt werden, indem jeweils

durch ein Befehlsverzeichnis navigiert wird, wie im folgenden Beispiel dargestellt:

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

Weitere Informationen zu `storage disk show` finden sich in der "ONTAP-Befehlsreferenz".

Sie können Befehle abkürzen, indem Sie nur die Mindestanzahl an Buchstaben eingeben, die den Befehl im aktuellen Verzeichnis eindeutig macht. Beispielsweise kann zur Abkürzung des Befehls im vorherigen Beispiel `st d sh` eingegeben werden. Die Tabulatortaste kann auch verwendet werden, um abgekürzte Befehle zu vervollständigen und die Parameter eines Befehls, einschließlich der Standardparameterwerte, anzuzeigen.

Mit dem `top` Befehl wird zur obersten Ebene der Befehlshierarchie gewechselt, und mit dem `up` Befehl oder `..` Befehl wird eine Ebene höher in der Befehlshierarchie gewechselt.

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

Verwandte Informationen

- "Spitze"
- "hoch"

Regeln zur Angabe von Werten in ONTAP CLI

Die meisten Befehle enthalten einen oder mehrere erforderliche oder optionale Parameter. Für viele Parameter muss ein Wert angegeben werden. Es gibt einige Regeln für die Angabe von Werten in der Befehlszeile.

- Ein Wert kann eine Zahl, ein boolescher Wert, eine Auswahl aus einer Liste vordefinierter Werte oder ein Text-String sein.

  Einige Parameter akzeptieren eine durch Kommas getrennte Liste mit zwei oder mehr Werten. Durch Kommas getrennte Listen von Werten müssen nicht in Anführungszeichen (" ") stehen. Wann immer Text, ein Leerzeichen oder ein Abfragezeichen angegeben wird (sofern es sich nicht um eine Abfrage oder um Text handelt, der mit einem Kleiner-als- oder Größer-als-Zeichen beginnt), muss die Entität in Anführungszeichen gesetzt werden.

- Die CLI interpretiert ein Fragezeichen (`?`) als Befehl zum Anzeigen von Hilfeinformationen für einen bestimmten Befehl.
- Bei einigen Texten, die Sie in der CLI eingeben, wie Befehlsnamen, Parameter und bestimmte Werte, wird nicht zwischen Groß- und Kleinschreibung unterschieden.

  Wenn Sie beispielsweise Parameterwerte für die `vserver cifs` Befehle eingeben, wird die Groß-/Kleinschreibung ignoriert. Die meisten Parameterwerte, wie etwa die Namen von Nodes, Storage Virtual Machines (SVMs), Aggregaten, Volumes und logischen Schnittstellen, sind jedoch case-sensitiv.

- Wenn der Wert eines Parameters gelöscht werden soll, der eine Text-String oder eine Liste erwartet, wird ein leeres Paar Anführungszeichen ("") oder ein Bindestrich ("-") angegeben.

- Das Hash-Zeichen (`#`, auch bekannt als Pfundzeichen, kennzeichnet einen Kommentar für eine Befehlszeileneingabe; falls es verwendet wird, sollte es nach dem letzten Parameter in einer Befehlszeile stehen.

  Die CLI ignoriert den Text zwischen `#` und dem Zeilenende.

Im folgenden Beispiel wird eine SVM mit einem Textkommentar erstellt. Anschließend wird die SVM so geändert, dass der Kommentar gelöscht wird:

```
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 Befehlszeilenkommentar, der das `#` Zeichen verwendet, an, was der Befehl bewirkt.

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

Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehlsverlauf anzeigen und jeden Befehl aus dem Verlauf erneut ausführen

Jede CLI-Sitzung speichert den Verlauf aller darin ausgeführten Befehle. Der Befehlsverlauf der aktuellen Sitzung kann angezeigt werden. Auch das erneute Ausführen von Befehlen ist möglich.

Um den Befehlsverlauf anzuzeigen, kann der `history` Befehl verwendet werden.

Um einen Befehl erneut auszuführen, kann der `redo` Befehl mit einem der folgenden Argumente verwendet werden:

- Eine Zeichenkette, die mit einem Teil eines vorherigen Befehls übereinstimmt

  Wenn der einzige von Ihnen ausgeführte `volume` Befehl `volume show` war, kann der `redo volume` Befehl verwendet werden, um den Befehl erneut auszuführen.

- Die numerische ID eines vorherigen Befehls, wie sie vom `history` Befehl aufgelistet wird

  Beispielsweise kann der `redo 4` Befehl verwendet werden, um den vierten Befehl in der Befehlsliste erneut auszugeben.

- Ein negativer Offset vom Ende der Verlaufsliste

Beispielsweise kann der `redo -2`-Befehl verwendet werden, um den Befehl erneut auszuführen, der vor zwei Befehlen ausgeführt wurde.

Beispielsweise würde der folgende Befehl eingegeben, um den Befehl, der an dritter Stelle vom Ende der Befehlshistorie steht, zu wiederholen:

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

Verwandte Informationen

- "Geschichte"
- "Wiederholen"
- "Volumen"

ONTAP Tastenkombinationen zum Bearbeiten von CLI-Befehlen

Der aktuell in der Befehlszeile angezeigte Befehl ist der aktive Befehl. Mithilfe von Tastenkombinationen kann der aktive Befehl schnell bearbeitet werden. Diese Tastenkombinationen ähneln denen der UNIX tcsh Shell und des Emacs Editors.

Die folgende Tabelle listet die Tastenkombinationen zum Bearbeiten von CLI-Befehlen auf. `Ctrl-` gibt an, dass die Strg-Taste gedrückt gehalten wird, während das nachfolgende Zeichen eingegeben wird. `Esc-` gibt an, dass die Esc-Taste gedrückt und wieder losgelassen wird und anschließend das nachfolgende Zeichen eingegeben wird.

Wenn Sie möchten…	Verwenden Sie eine dieser Tastenkombinationen…
Den Cursor um ein Zeichen zurückbewegen	• Strg+B • Zurück-Pfeil
Den Cursor um ein Zeichen vorwärts bewegen	• Strg-F • Vorwärtspfeil
Den Cursor um ein Wort zurück bewegen	Esc-B
Den Cursor um ein Wort vorwärts bewegen	Esc-F
Den Cursor an den Anfang der Zeile bewegen	Strg+A
Den Cursor an das Ende der Zeile bewegen.	Strg-E
Entfernen Sie den Inhalt der Befehlszeile vom Zeilenanfang bis zur Cursorposition und speichern Sie ihn im Ausschneidepuffer. Der Ausschneidepuffer fungiert als temporärer Speicher, ähnlich wie die sogenannte Zwischenablage in manchen Programmen.	Strg-U
Entfernen Sie den Inhalt der Befehlszeile vom Cursor bis zum Zeilenende und speichern Sie ihn im Ausschneidepuffer	Strg-K

Wenn Sie möchten…	Verwenden Sie eine dieser Tastenkombinationen…
Entfernen Sie den Inhalt der Befehlszeile vom Cursor bis zum Ende des folgenden Wortes und speichern Sie ihn im Ausschneidepuffer	Esc-D
Das Wort vor dem Cursor wird entfernt und im Ausschneidepuffer gespeichert.	Strg-W
Den Inhalt des Ausschneidepuffers abrufen und an der Cursorposition in die Befehlszeile einfügen	Strg-Y
Das Zeichen vor dem Cursor löschen	• Strg-H • Rücktaste
Das Zeichen an der Cursorposition löschen	Strg-D
Leitung freimachen	Strg+C
Bildschirm löschen	Strg-L
Der aktuelle Inhalt der Befehlszeile wird durch den vorherigen Eintrag in der Verlaufsliste ersetzt. Bei jeder Wiederholung des Tastaturkürzels bewegt sich der Verlaufscursor zum vorherigen Eintrag.	• Strg+P • Esc-P • Pfeil nach oben
Ersetzt den aktuellen Inhalt der Befehlszeile durch den nächsten Eintrag in der Verlaufsliste. Mit jeder Wiederholung des Tastenkürzels bewegt sich der Verlaufscursor zum nächsten Eintrag.	• Strg-N • Esc-N • Pfeil nach unten
Einen teilweise eingegebenen Befehl erweitern oder gültige Eingaben ab der aktuellen Bearbeitungsposition auflisten	• Tab • Strg-I
Kontextsensitive Hilfe anzeigen	?
Die spezielle Zuordnung für das Fragezeichen ? -Zeichen aufheben. Um beispielsweise ein Fragezeichen als Argument in einer Befehlszeile einzugeben, Esc drücken und dann das ?-Zeichen eingeben.	Esc-?
TTY-Ausgabe starten	Strg-Q
TTY-Ausgabe beenden	Strg-S

Die Berechtigungsstufen für ONTAP CLI-Befehle

ONTAP Befehle und Parameter sind auf drei Berechtigungsstufen definiert: *admin*, *advanced* und *diagnostic*. Die Berechtigungsstufen spiegeln die für die Ausführung der Aufgaben erforderlichen Kenntnisse wider.

- **admin**

  Die meisten Befehle und Parameter sind auf dieser Ebene verfügbar. Sie werden für gängige oder routinemäßige Aufgaben verwendet.

- **fortschrittlich**

  Befehle und Parameter auf dieser Ebene werden selten verwendet, erfordern fortgeschrittene Kenntnisse und können bei unsachgemäßer Verwendung Probleme verursachen.

  Erweiterte Befehle oder Parameter werden nur auf Anraten des Supportpersonals verwendet.

- **Diagnostik**

  Diagnosebefehle und -parameter können Störungen verursachen. Sie werden ausschließlich von Supportmitarbeitern zur Diagnose und Behebung von Problemen verwendet.

Die Berechtigungsstufe in der ONTAP CLI festlegen

Sie können die Berechtigungsstufe in der CLI mit dem `set` Befehl festlegen. Änderungen an den Einstellungen der Berechtigungsstufe gelten nur für die aktuelle Sitzung. Sie sind nicht sitzungsübergreifend persistent.

Schritte

1. Um die Berechtigungsstufe in der CLI festzulegen, den `set` Befehl mit dem `-privilege` Parameter verwenden.

Beispiel für die Festlegung der Berechtigungsstufe

Im folgenden Beispiel wird die Berechtigungsstufe zunächst auf „Erweitert“ und anschließend auf „Admin“ gesetzt:

```
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
```

Weitere Informationen zu `set` finden sich in der "ONTAP-Befehlsreferenz".

Anzeigeeinstellungen für die ONTAP CLI festlegen

Sie können die Anzeigeeinstellungen für eine CLI-Sitzung mithilfe des `set` Befehls und des `rows` Befehls festlegen. Die von Ihnen festgelegten Einstellungen gelten nur für die aktuelle Sitzung. Sie sind nicht sitzungsübergreifend persistent.

Über diese Aufgabe

Sie können die folgenden CLI-Anzeigeeinstellungen festlegen:

- Die Berechtigungsstufe der Befehlssitzung
- Ob Bestätigungen für potenziell unterbrechende Befehle erteilt werden
- Ob `show`Befehle alle Felder anzeigen
- Das oder die als Feldtrennzeichen zu verwendenden Zeichen

- Die Standardeinheit bei der Angabe von Datengrößen
- Die Anzahl der Zeilen, die der Bildschirm in der aktuellen CLI-Sitzung anzeigt, bevor die Schnittstelle die Ausgabe pausiert

  Wird die gewünschte Zeilenanzahl nicht angegeben, wird sie automatisch anhand der tatsächlichen Höhe des Terminals angepasst. Ist die tatsächliche Höhe nicht definiert, beträgt die Standardzeilenanzahl 24.
- Die standardmäßige Storage Virtual Machine (SVM) oder der Node
- Ob ein fortlaufender Befehl bei einem Fehler gestoppt werden soll

Schritte

1. Um die Anzeigeeinstellungen der Befehlszeile festzulegen, den `set` Befehl verwenden.

   Um die Anzahl der Zeilen festzulegen, die der Bildschirm in der aktuellen CLI-Sitzung anzeigt, kann auch der `rows` Befehl verwendet werden.

   Weitere Informationen zu `set` und `rows` finden sich in der "ONTAP-Befehlsreferenz".

Beispiel für das Festlegen von Anzeigeeinstellungen in der Befehlszeile

Im folgenden Beispiel wird ein Komma als Feldtrennzeichen festgelegt, `GB` als Standard-Datengrößeneinheit festgelegt und die Anzahl der Zeilen auf 50 gesetzt:

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

Verwandte Informationen

- "anzeigen"
- "Set"
- "Zeilen"

Abfrageoperatoren in der ONTAP CLI verwenden

Die Managementoberfläche unterstützt Abfragen sowie UNIX-typische Muster und Platzhalter, sodass mehrere Werte in Befehlsparameterargumenten abgeglichen werden können.

Die folgende Tabelle beschreibt die unterstützten Abfrageoperatoren:

Operator	Beschreibung
*	Platzhalter, der mit allen Einträgen übereinstimmt. Beispielsweise zeigt der Befehl `volume show -volume *tmp*`eine Liste aller Volumes an, deren Namen die Zeichenkette `tmp`enthalten.
!	NICHT-Operator. Gibt einen Wert an, der nicht abgeglichen werden soll; beispielsweise **`!vs0`** gibt an, dass der Wert `vs0` nicht abgeglichen werden soll.

Operator	Beschreibung
ODER Operator. Trennt zwei Werte, die verglichen werden sollen; zum Beispiel `*vs0	vs2*` passt entweder vs0 oder vs2. Mehrere ODER-Anweisungen können angegeben werden; zum Beispiel `a
b*	*c*` passt auf den Eintrag `a`, auf jeden Eintrag, der mit `b` beginnt, und auf jeden Eintrag, der `c` enthält.
..	Bereichsoperator. Beispielsweise **`5..10`** entspricht jeder Wert von `5` bis `10` einschließlich.
<	Kleiner-als-Operator. Beispielsweise entspricht **`<20`** jeder Wert, der kleiner als `20` ist.
>	Größer-als-Operator. Beispielsweise **`>5`** entspricht jeder Wert, der größer als `5` ist.
<=	Kleiner-gleich-Operator. Beispielsweise entspricht ⇐**`5`** jeder Wert, der kleiner oder gleich `5` ist.
>=	Größer-oder-gleich-Operator. Beispielsweise entspricht **`>=5`** jeder Wert, der größer oder gleich `5` ist.
{`query`}	Erweiterte Abfrage. Eine erweiterte Abfrage muss als erstes Argument nach dem Befehlsnamen, vor allen anderen Parametern, angegeben werden. Beispielsweise setzt der Befehl `volume modify {-volume *tmp*} -state offline`alle Volumes, deren Namen die Zeichenkette `tmp`enthalten, offline.

Wenn Sie Abfragezeichen als Literale parsen möchten, müssen Sie die Zeichen in doppelte Anführungszeichen setzen (zum Beispiel "`<10`", "`0..100`", "`*abc*`", oder "`a|b`"), damit die korrekten Ergebnisse zurückgegeben werden.

Dateinamen müssen in doppelte Anführungszeichen gesetzt werden, 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. Zum Beispiel zeigt der Befehl `volume show -size >1GB -percent-used <50 -vserver !vs1` alle Volumes an, die größer als 1 GB sind, zu weniger als 50 % belegt sind und sich nicht in der Storage Virtual Machine (SVM) mit dem Namen “vs1” befinden.

Verwandte Informationen

"Tastenkombinationen zum Bearbeiten von CLI-Befehlen"

Erweiterte Abfragen mit den Befehlen modify und delete in der ONTAP CLI verwenden

Sie können erweiterte Abfragen verwenden, um Objekte mit bestimmten Werten abzugleichen und Operationen an ihnen durchzuführen.

Erweiterte Abfragen werden durch Einschließen in geschweifte Klammern ({}) angegeben. Eine erweiterte Abfrage muss als erstes Argument nach dem Befehlsnamen, vor allen anderen Parametern, angegeben werden. Beispielsweise wird der folgende Befehl verwendet, um alle Volumes offline zu schalten, deren Namen die Zeichenkette `tmp` enthalten:

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

Erweiterte Abfragen sind im Allgemeinen nur mit `modify` und `delete` Befehlen sinnvoll. Sie haben keine Bedeutung in `create` oder `show` Befehlen.

Die Kombination aus Abfragen und Änderungsoperationen ist ein nützliches Werkzeug. Bei falscher Implementierung kann sie jedoch zu Verwirrung und Fehlern führen. Beispielsweise bewirkt die Verwendung des (erweiterte Berechtigung) `system node image modify` Befehls zum Festlegen des Standard-Software-Images eines Knotens automatisch, dass das andere Software-Image nicht mehr als Standard festgelegt wird. Der Befehl im folgenden Beispiel ist im Grunde eine Nulloperation:

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

Dieser Befehl legt das aktuelle Standardimage als nicht standardmäßiges Image fest und setzt anschließend das neue Standardimage (das vorherige nicht standardmäßige Image) auf das nicht standardmäßige Image, sodass die ursprünglichen Standardeinstellungen erhalten bleiben. Für die korrekte Ausführung des Vorgangs kann der Befehl wie im folgenden Beispiel verwendet werden:

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

Die Ausgabe des ONTAP show-Befehls kann mit dem Parameter fields eingeschränkt werden.

Wenn der `-instance` Parameter mit einem `show` Befehl zur Anzeige von Details verwendet wird, kann die Ausgabe sehr umfangreich sein und mehr Informationen enthalten, als benötigt werden. Der `-fields` Parameter eines `show` Befehls ermöglicht die Anzeige nur der Informationen, die angegeben werden.

Beispielsweise führt das Ausführen von `volume show -instance` wahrscheinlich zu mehreren Informationsseiten. Mit `volume show -fields` *`fieldname[,fieldname…]`* lässt sich die Ausgabe so anpassen, dass nur das angegebene Feld oder die angegebenen Felder enthalten sind (zusätzlich zu den standardmäßig angezeigten Feldern). Mit `-fields ?` lassen sich gültige Felder für einen `show` Befehl

anzeigen.

Das folgende Beispiel zeigt den Unterschied in der Ausgabe zwischen dem `-instance` Parameter und dem `-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::>
```

Die Positionsparameter der ONTAP CLI in der Befehlseingabe verwenden

Sie können die Funktionalität der Positionsparameter der ONTAP CLI nutzen, um die Effizienz der Befehlseingabe zu steigern. Es besteht die Möglichkeit, einen Befehl abzufragen, um die Positionsparameter dieses Befehls zu identifizieren.

Was ein Positionsparameter ist

- Ein Positionsparameter ist ein Parameter, bei dem der Parametername nicht vor der Angabe des Parameterwerts angegeben werden muss.
- Ein Positionsparameter kann im Befehlseingang mit nicht positionsbezogenen Parametern vermischt werden, solange er seine relative Reihenfolge mit anderen Positionsparametern im selben Befehl beachtet, wie in der ***command_name ?*** Ausgabe angezeigt.
- Ein Positionsparameter kann ein erforderlicher oder optionaler Parameter für einen Befehl sein.
- Ein Parameter kann für einen Befehl positionell, für einen anderen jedoch nicht positionell sein.

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

Einen Positionsparameter identifizieren

Ein Positionsparameter kann in der ***command_name ?***-Befehlsausgabe identifiziert werden. Ein Positionsparameter ist durch eckige Klammern um den Parameternamen in einem der folgenden Formate gekennzeichnet:

- [*-parameter_name*] *parameter_value* zeigt einen erforderlichen Parameter an, der positionell ist.
- [[*-parameter_name*] *parameter_value*] zeigt einen optionalen Positionsparameter an.

Wenn der Parameter beispielsweise in der ***command_name ?*** Ausgabe wie folgt angezeigt wird, ist er positionsbezogen für den Befehl, in dem er vorkommt:

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

Wird der Parameter jedoch wie folgt angezeigt, ist er für den Befehl, in dem er vorkommt, nicht positionell:

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

Beispiele für die Verwendung von Positionsparametern

Im folgenden Beispiel zeigt die ***volume create ?*** Ausgabe, dass drei Parameter für den Befehl positionell 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 `volume create` Befehl angegeben, ohne die Funktionalität der Positionsparameter zu nutzen:

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

Die folgenden Beispiele nutzen die Funktionalität der Positionsparameter, um die Effizienz der Befehlseingabe zu erhöhen. Die Positionsparameter sind im `volume create` Befehl zwischen nichtpositionsbezogenen Parametern eingefügt, und die Werte der Positionsparameter werden ohne die Parameternamen angegeben. Die Positionsparameter werden in der gleichen Reihenfolge angegeben, wie sie in der **`volume create ?`** Ausgabe angezeigt wird. Das bedeutet, dass der Wert für `-volume` vor dem von `-aggregate` angegeben wird, welcher wiederum vor dem von `-size` angegeben wird.

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

Zugriff auf die Manpages der ONTAP CLI

ONTAP manuell (man) Seiten erklären, wie ONTAP CLI-Befehle verwendet werden. Diese Seiten sind auf der Befehlszeile verfügbar und werden auch in releasespezifischen *Befehlsreferenzen* veröffentlicht.

An der ONTAP Befehlszeile kann mit dem `man <command_name>` Befehl die Handbuchseite des angegebenen Befehls angezeigt werden. Wird kein Befehlsname angegeben, erscheint das Inhaltsverzeichnis der Handbuchseiten. Mit dem `man man` Befehl lassen sich Informationen zum `man` Befehl selbst anzeigen. Eine Handbuchseite kann durch Eingabe von **`q`** verlassen werden.

Weitere Informationen zu den in Ihrer Version verfügbaren ONTAP-Befehlen auf Administrator- und Expertenebene finden Sie im "ONTAP-Befehlsreferenz".

Eine ONTAP CLI Sitzung aufzeichnen und die aufgezeichneten Sitzungen verwalten

Sie können eine CLI-Sitzung in einer Datei mit einem festgelegten Namen und einer festgelegten Größenbegrenzung aufzeichnen und die Datei anschließend an ein FTP- oder HTTP-Ziel hochladen. Es besteht außerdem die Möglichkeit, Dateien anzuzeigen oder zu löschen, in denen zuvor CLI-Sitzungen aufgezeichnet wurden.

Eine CLI-Sitzung aufzeichnen

Ein Protokoll einer CLI-Sitzung endet, wenn die Aufzeichnung gestoppt oder die CLI-Sitzung beendet wird oder wenn die Datei die festgelegte Größenbeschränkung erreicht. Die standardmäßige Dateigrößenbeschränkung beträgt 1 MB. Die maximale Dateigrößenbeschränkung beträgt 2 GB.

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

Schritte

1. Die aktuelle CLI-Sitzung in einer Datei aufzeichnen:

   ```
   system script start
   ```

   Weitere Informationen zu `system script start` finden sich in der "ONTAP-Befehlsreferenz".

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

2. Fahren Sie mit Ihrer CLI-Sitzung fort.
3. Nach Abschluss die Aufzeichnung der Sitzung beenden:

   ```
   system script stop
   ```

   Weitere Informationen zu `system script stop` finden sich in der "ONTAP-Befehlsreferenz".

   ONTAP beendet die Protokollierung Ihrer CLI-Sitzung.

Befehle zur Verwaltung von Protokollen von CLI-Sitzungen

Sie verwenden die `system script` Befehle, um Aufzeichnungen von CLI-Sitzungen zu verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Die aktuelle CLI-Sitzung in einer angegebenen Datei aufzeichnen.	`system script start`
Die Aufzeichnung der aktuellen CLI-Sitzung wird gestoppt	`system script stop`
Informationen zu Protokollen von CLI-Sitzungen	`system script show`
Einen Protokolleintrag einer CLI-Sitzung an ein FTP- oder HTTP-Ziel hochladen	`system script upload`
Einen Datensatz einer CLI-Sitzung löschen	`system script delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Befehle zur Verwaltung des automatischen Zeitüberschreitungszeitraums von CLI-Sitzungen

Der Zeitüberschreitungswert gibt an, wie lange eine CLI-Sitzung inaktiv bleibt, bevor sie automatisch beendet wird. Der CLI-Zeitüberschreitungswert gilt clusterweit. Das heißt, jeder Node in einem Cluster verwendet denselben CLI-Zeitüberschreitungswert.

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

Die `system timeout` Befehle werden verwendet, um die automatische Zeitüberschreitungsperiode von CLI-Sitzungen zu verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Automatische Zeitüberschreitungsperiode für CLI-Sitzungen	`system timeout show`
Die automatische Zeitüberschreitungsperiode für CLI-Sitzungen anpassen	`system timeout modify`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Clusterverwaltung (nur für Clusteradministratoren)

Details auf Knotenebene in einem ONTAP Cluster

Sie können Knotennamen, den Status der Knoten und deren Eignung zur Teilnahme am Cluster einsehen. Auf der erweiterten Berechtigungsstufe wird außerdem angezeigt, ob ein Knoten über Epsilon verfügt.

Schritte

1. Informationen über die Knoten in einem Cluster sind mit dem `cluster show` Befehl verfügbar.

   Soll in der Ausgabe angezeigt werden, ob ein Knoten Epsilon enthält, ist der Befehl auf dem erweiterten Berechtigungsniveau auszuführen.

   Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele für die Anzeige der Knoten in einem Cluster

Das folgende Beispiel zeigt Informationen über alle Knoten in einem vier Knoten Cluster:

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

Das folgende Beispiel zeigt detaillierte Informationen über den Knoten mit dem Namen “node1” auf der erweiterten Berechtigungsstufe:

```
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
```

ONTAP Cluster-Details auf Clusterebene anzeigen

Es werden die eindeutige Kennung (UUID), der Name, die Seriennummer, der Standort und die Kontaktinformationen eines Clusters angezeigt.

Schritte

1. Die Attribute eines Clusters werden mit dem `cluster identity show` Befehl angezeigt.

Beispiel für die Anzeige von Clusterattributen

Das folgende Beispiel zeigt den Namen, die Seriennummer, den Standort und die Kontaktinformationen eines Clusters.

```
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
```

Weitere Informationen zu `cluster identity show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Clusterattribute ändern

Die Attribute eines Clusters, wie den Clusternamen, den Standort und die Kontaktinformationen, können bei Bedarf angepasst werden.

Über diese Aufgabe

Die UUID eines Clusters kann nicht geändert werden, da sie bei der Erstellung des Clusters festgelegt wird.

Schritte

1. Zum Ändern von Clusterattributen wird der `cluster identity modify` Befehl verwendet.

   Der `-name`Parameter gibt den Namen des Clusters an. Weitere Informationen zu `cluster identity modify`und den Regeln für die Angabe des Clusternamens sind in der "ONTAP-Befehlsreferenz"zu finden.

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

   Der `-contact` Parameter gibt die Kontaktinformationen wie Name oder E-Mail-Adresse an.

Beispiel für die Umbenennung eines Clusters

Der folgende Befehl benennt den aktuellen Cluster (“cluster1”) in “cluster2” um:

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

Den Replikationsstatus der ONTAP Clusterringe anzeigen

Sie können den Status der Replikationsringe des Clusters einsehen, um clusterweite Probleme zu diagnostizieren. Wenn Ihr Cluster Probleme aufweist, kann das Support-Personal Sie bitten, diese Aufgabe durchzuführen, um die Fehlerbehebung zu unterstützen.

Schritte

1. Der Status der Cluster-Replikationsringe lässt sich mit dem `cluster ring show` Befehl auf der Ebene mit erweiterten Berechtigungen anzeigen.

Beispiel für die Anzeige des Cluster Ring-Replikationsstatus

Das folgende Beispiel zeigt den Status des VLDB-Replikationsrings auf einem Knoten mit dem Namen node0:

```
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
```

Weitere Informationen zu `cluster ring show` finden sich in der "ONTAP-Befehlsreferenz".

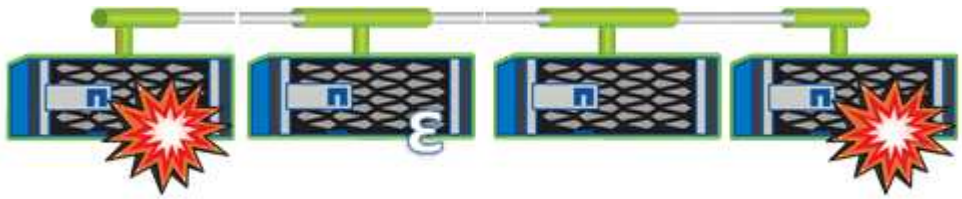
ONTAP Cluster-Gesundheitsbewertungen mithilfe von Quorum und Epsilon

Quorum und Epsilon sind wichtige Kennzahlen für die Gesundheit und Funktionsfähigkeit eines Clusters, die zusammen angeben, wie Cluster potenzielle Kommunikations- und Konnektivitätsherausforderungen adressieren.

Quorum ist eine Grundvoraussetzung für einen voll funktionsfähigen Cluster. Befindet sich ein Cluster im Quorum, ist die einfache Mehrheit der Knoten fehlerfrei und kann miteinander kommunizieren. Geht das Quorum verloren, verliert der Cluster die Fähigkeit, normale Clusteroperationen durchzuführen. Nur eine Knotengruppe kann zu einem bestimmten Zeitpunkt ein Quorum aufweisen, da alle Knoten gemeinsam eine einheitliche Datensicht nutzen. Wenn daher zwei nicht kommunizierende Knoten die Daten auf unterschiedliche Weise verändern, ist es nicht mehr möglich, die Daten zu einer einheitlichen Datensicht zusammenzuführen.

Jeder Knoten im Cluster nimmt an einem Abstimmungsprotokoll teil, das einen Knoten als *primär* wählt; jeder verbleibende Knoten ist ein *sekundär*. Der primäre Knoten ist für die Synchronisierung von Informationen im gesamten Cluster verantwortlich. Wenn ein Quorum gebildet ist, wird es durch fortlaufende Abstimmung aufrechterhalten. Wenn der primäre Knoten offline geht und der Cluster weiterhin im Quorum ist, wird von den verbleibenden Knoten, die online bleiben, ein neuer primärer Knoten gewählt.

Da in einem Cluster mit einer geraden Anzahl von Knoten ein Stimmengleichstand möglich ist, besitzt ein Knoten ein zusätzliches, bruchstückhaftes Stimmgewicht namens *epsilon*. Fällt die Verbindung zwischen zwei gleich großen Teilen eines großen Clusters aus, bleibt die Gruppe der Knoten mit *epsilon* beschlussfähig, vorausgesetzt, alle Knoten sind funktionsfähig. Die folgende Abbildung zeigt beispielsweise ein Vier-Node-Cluster, in dem zwei der Knoten ausgefallen sind. Da jedoch einer der verbleibenden Knoten *epsilon* hält, bleibt der Cluster beschlussfähig, obwohl keine einfache Mehrheit funktionsfähiger Knoten vorhanden ist.



Epsilon wird beim Erstellen des Clusters automatisch dem ersten Knoten zugewiesen. Wenn der Knoten, der Epsilon enthält, fehlerhaft wird, seinen Hochverfügbarkeitspartner übernimmt oder von seinem Hochverfügbarkeitspartner übernommen wird, wird Epsilon automatisch einem fehlerfreien Knoten in einem anderen HA-Paar neu zugewiesen.

Das Offline-Nehmen eines Knotens kann die Fähigkeit des Clusters beeinträchtigen, im Quorum zu bleiben. Daher gibt ONTAP eine Warnmeldung aus, wenn ein Vorgang versucht wird, der entweder den Cluster aus dem Quorum bringt oder ihn eine Störung vom Verlust des Quorums entfernt. Die Quorum-Warnmeldungen können mit dem `cluster quorum-service options modify` Befehl auf der Stufe „Erweiterte Berechtigungen“ deaktiviert werden. Weitere Informationen zu `cluster quorum-service options modify` finden sich in der "ONTAP-Befehlsreferenz".

Im Allgemeinen gilt: Bei zuverlässiger Verbindung zwischen den Knoten des Clusters ist ein größerer Cluster stabiler als ein kleinerer. Die Quorumsanforderung einer einfachen Mehrheit (die Hälfte der Knoten plus Epsilon) lässt sich in einem Cluster mit 24 Knoten leichter erfüllen als in einem Zwei-Node-Cluster.

Ein Zwei-Node-Cluster stellt einige besondere Herausforderungen für die Aufrechterhaltung des Quorums dar.

Zwei-Node-Cluster verwenden Cluster-HA, bei der keiner der Knoten Epsilon hält; stattdessen werden beide Knoten kontinuierlich abgefragt, um sicherzustellen, dass im Falle eines Ausfalls eines Knotens der andere vollständigen Lese- und Schreibzugriff auf die Daten sowie Zugriff auf logische Schnittstellen und Verwaltungsfunktionen hat.

Kapazitätsauslastung der Systemvolumes in einem ONTAP Cluster anzeigen

Systemvolumes sind FlexVol Volumes, die spezielle Metadaten enthalten, beispielsweise Metadaten für die Überwachungsprotokolle von Dateidiensten. Diese Volumes sind im Cluster sichtbar, sodass die Speichernutzung im Cluster vollständig nachvollzogen werden kann.

Systemvolumes gehören dem Cluster-Management-Server (auch Admin-SVM genannt) und werden automatisch erstellt, wenn die Überwachung der Dateidienste aktiviert ist.

Systemvolumes können mit dem `volume show` Befehl angezeigt werden, die meisten anderen Volume-Operationen sind jedoch nicht zulässig. Beispielsweise kann ein Systemvolume nicht mit dem `volume modify` Befehl geändert werden.

Dieses Beispiel zeigt vier Systemvolumes auf der Admin-SVM, die automatisch erstellt wurden, als die Dateidienstüberwachung für eine Daten-SVM im Cluster aktiviert wurde:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
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.
```

Knoten verwalten

Knoten zu einem ONTAP Cluster hinzufügen

Nachdem ein Cluster erstellt wurde, kann es durch das Hinzufügen von Knoten erweitert werden. Es wird jeweils nur ein Knoten hinzugefügt.

Bevor Sie beginnen

- Installieren und konfigurieren Sie Ihr neues Speichersystem, indem Sie die Hardwareanforderungen prüfen, Ihren Standort vorbereiten und die Hardwarekomponenten (Controller, Storage Shelves und Switches) installieren und verkabeln. Siehe die folgende ONTAP-Hardwaresystemdokumentation für Details:
  - "AFF A-Serien-Systeme"
  - "AFF C-Serien-Systeme"
  - "AFX-Systeme"
  - "ASA R2-Systeme"
  - "FAS-Systeme"
- Prüfen Sie die Verkabelungs- und Konfigurationsanforderungen Ihres Cluster-Switch-Modells für die Cluster-Ports Ihres neuen Speichersystems. Siehe die "Switch-Dokumentation für ONTAP Hardware-Systeme"
  a. Wählen Sie die **Cluster Switches** oder **Shared Switches** in der Kachel **Unterstützte Switches** aus.
  b. Wählen Sie die **Install**-Dokumentation für Ihr Switch-Modell aus.
  c. Suchen Sie nach dem Thema **Review cabling and configuration considerations** und überprüfen Sie es für Ihr Speichersystem.
- Wenn Sie einem Cluster mit mehreren Knoten weitere Knoten hinzufügen, müssen alle vorhandenen Knoten im Cluster fehlerfrei sein (erkennbar an `cluster show`). Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".
- Wenn Sie einem Cluster ohne Switches mit zwei Knoten weitere Knoten hinzufügen, muss das Cluster ohne Switches mit zwei Knoten mithilfe eines von NetApp unterstützten Cluster-Switches in ein Cluster mit Switch-Anschluss umgewandelt werden.

Switch-Modell	Migrationsverfahren
Broadcom BES-53248	"Migration zu einer switched NetApp Cluster-Umgebung"
Cisco Nexus 9336C-FX2	"Migration zu einem Zwei-Knoten-Switched-Cluster"
Cisco Nexus 9336C-FX2 (Gemeinsames Cluster+Storage)	"Migrieren Sie von einem Cluster ohne Switches mit direkt angeschlossenem Speicher"
NVIDIA SN2100	"Migrieren Sie zu einem Zwei-Knoten-Cluster mit NVIDIA SN2100-Clusterswitches"

- Wenn einem Einzelknotencluster ein zweiter Knoten hinzugefügt wird, muss der zweite Knoten installiert und das Clusternetzwerk konfiguriert sein.
- Wenn im Cluster die automatische SP-Konfiguration aktiviert ist, muss das für den SP angegebene Subnetz über verfügbare Ressourcen verfügen, damit der beitretende Knoten das angegebene Subnetz zur automatischen Konfiguration des SP verwenden kann.
- Folgende Informationen für das Node-Management-LIF des neuen Knotens müssen vorliegen:
  - Port
  - IP-Adresse
  - Netzmaske
  - Standardgateway

Über diese Aufgabe

Die Anzahl der Knoten muss gerade sein, damit sie HA-Paare bilden können. Nachdem mit dem Hinzufügen eines Knotens zum Cluster begonnen wurde, muss der Vorgang abgeschlossen werden. Der Knoten muss Teil des Clusters sein, bevor ein weiterer Knoten hinzugefügt werden kann.

Schritte

1. Der Knoten, der dem Cluster hinzugefügt werden soll, wird eingeschaltet.

   Der Knoten wird hochgefahren und der Knoteneinrichtungsassistent startet auf der Konsole.

   ```
   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. Den Node Setup-Assistenten beenden: `exit`

   Der Node Setup-Assistent wird beendet, und es erscheint eine Anmeldeaufforderung mit dem Hinweis, dass die Einrichtungsaufgaben nicht abgeschlossen wurden.

   Weitere Informationen zu `exit` finden sich in der "ONTAP-Befehlsreferenz".

3. Melden Sie sich beim Administratorkonto mit dem `admin`Benutzernamen an.
4. Den Cluster Setup-Assistenten starten:

   ```
   ::> 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 mithilfe der Setup-GUI finden Sie in der "Dokumentation zur Knotenverwaltung". Weitere Informationen zu `cluster setup` finden sich in der "ONTAP-Befehlsreferenz".

5. Drücken Sie die Eingabetaste, um diese Aufgabe über die Befehlszeilenschnittstelle (CLI) abzuschließen. Wenn Sie aufgefordert werden, einen neuen Cluster zu erstellen oder einem bestehenden beizutreten, geben Sie **`join`** ein.

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

   Wenn die auf dem neuen Knoten ausgeführte ONTAP-Version von der Version auf dem bestehenden Cluster abweicht, meldet das System einen `System checks Error: Cluster join operation cannot be performed at this time` Fehler. Dies ist das erwartete Verhalten. Zum Fortfahren wird der `cluster add-node -allow-mixed-version-join true -cluster-ips <IP address> -node-names <new_node_name>` Befehl auf einem vorhandenen Knoten im Cluster mit erweitertem Berechtigungsniveau ausgeführt.

6. Folgen Sie den Anweisungen, um den Knoten einzurichten und ihn dem Cluster hinzuzufügen:
   - Um den Standardwert für eine Eingabeaufforderung zu übernehmen, die Eingabetaste drücken.
   - Zum Eingeben eines eigenen Werts für eine Eingabeaufforderung den Wert eingeben und anschließend die Eingabetaste drücken.
7. Die vorhergehenden Schritte sind für jeden weiteren Knoten zu wiederholen, den Sie hinzufügen möchten.

Nachdem Sie fertig sind

Nach dem Hinzufügen von Knoten zum Cluster sollte das Storage-Failover für jedes HA-Paar aktiviert werden.

Verwandte Informationen

- "Unterstützung für Cluster mit gemischten Versionen bei ONTAP Software-Upgrades"
- "Cluster Node hinzufügen"

Knoten aus einem ONTAP Cluster entfernen

Sie können unerwünschte Knoten aus einem Cluster entfernen, jeweils einen nach dem anderen. Nach der Entfernung eines Knotens muss auch dessen Failover-Partner entfernt werden. Wenn ein Knoten entfernt wird, sind dessen Daten nicht mehr zugänglich oder werden gelöscht.

Bevor Sie beginnen

Bevor Sie Knoten aus dem Cluster entfernen, müssen folgende Bedingungen erfüllt sein:

- Mehr als die Hälfte der Knoten im Cluster muss fehlerfrei sein.

- Sämtliche Daten, Volumes und Nicht-Root-Aggregate müssen vom Node verschoben oder entfernt werden.
  - Alle Daten auf dem Node, den Sie entfernen möchten, müssen evakuiert worden sein. Dies kann "Daten aus einem verschlüsselten Volume entfernen" umfassen.
  - Alle Nicht-Root-Volumes wurden "verschoben" aus Aggregaten entfernt, die dem Node gehören.
  - Alle Nicht-Root-Aggregate wurden "gelöscht" vom Node entfernt.
- Alle LIFs und VLANs wurden vom Node verschoben oder entfernt.
  - Daten-LIFs wurden "gelöscht" oder "verschoben" vom Node entfernt.
  - Die Cluster-Management-LIFs wurden "verschoben" vom Node entfernt und die Home-Ports geändert.
  - Alle Intercluster-LIFs wurden "Entfernung". Beim Entfernen von Intercluster-LIFs wird eine Warnung angezeigt, die ignoriert werden kann.
  - Alle VLANs auf dem Knoten wurden "gelöscht".
- Der Knoten ist an keiner Failover-Beziehung beteiligt.
  - Storage-Failover wurde für den Knoten "deaktiviert" aktiviert.
  - Alle LIF-Failover-Regeln wurden "modifiziert" zur Entfernung von Ports auf dem Node angepasst.
- Wenn der Knoten über Federal Information Processing Standards (FIPS) Datenträger oder selbstverschlüsselnde Datenträger (SEDs) verfügt, "Die Festplattenverschlüsselung wurde entfernt" indem die Datenträger in den ungeschützten Modus zurückversetzt werden.
  - Möglicherweise besteht auch Interesse daran, "FIPS-Laufwerke oder SEDs löschen".
- Wenn sich auf dem zu entfernenden Knoten LUNs befinden, sollten Sie "die Liste der Reporting-Nodes der Selective LUN Map (SLM) ändern" entfernen, bevor Sie den Knoten entfernen.

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

Es wird empfohlen, eine AutoSupport-Nachricht zu senden, um den NetApp technischen Support darüber zu informieren, dass die Entfernung eines Node im Gange ist.

Operationen wie `cluster remove-node`, `cluster unjoin` und `node rename` sollten nicht durchgeführt werden, wenn ein automatisiertes ONTAP Upgrade im Gange ist.

Über diese Aufgabe

- Wenn Sie einen Cluster mit gemischten Versionen betreiben, kann der letzte Node mit niedriger Version mithilfe eines der erweiterten Berechtigungsbefehle ab ONTAP 9.3 entfernt werden:
  - 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 zwei Knoten aus einem vier-Knoten-Cluster entfernen, wird Cluster HA automatisch auf den beiden verbleibenden Knoten aktiviert.

Alle System- und Benutzerdaten von allen mit dem Knoten verbundenen Festplatten müssen für die Benutzer unzugänglich gemacht werden, bevor ein Knoten aus dem Cluster entfernt wird.

Falls ein Knoten fälschlicherweise aus einem Cluster entfernt wurde, wenden Sie sich an den NetApp Support, um Unterstützung bei den Wiederherstellungsoptionen zu erhalten.

Schritte

1. Ändern Sie die Berechtigungsstufe auf „advanced“:

```
set -privilege advanced
```

2. Identifizieren Sie den Knoten im Cluster, der epsilon hat:

```
cluster show
```

Im folgenden Beispiel hält "node0" derzeit epsilon:

```
cluster::*>
Node                  Health  Eligibility  Epsilon
--------------------- ------- ------------ ------------
node0                 true    true         true
node1                 true    true         false
node2                 true    true         false
node3                 true    true         false
```

3. Wenn der Knoten, den Sie entfernen, Epsilon enthält:
   a. Verschiebe epsilon von dem Knoten, den du entfernst:

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

   b. Verschieben Sie epsilon auf einen Knoten, den Sie nicht entfernen:

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

4. Aktueller primärer Knoten identifizieren:

```
cluster ring show
```

Der primäre Knoten ist der Knoten, der Prozesse wie `mgmt`, `vldb`, `vifmgr`, `bcomd` und `crs` enthält.

5. Falls der zu entfernende Knoten der aktuelle primäre Knoten ist, kann ein anderer Knoten im Cluster als primärer Knoten gewählt werden:
   a. Den aktuellen primären Knoten für die Teilnahme am Cluster als nicht berechtigt markieren:

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

Der Knoten wird als fehlerhaft markiert, bis seine Eignung wiederhergestellt ist. Wenn der primäre Knoten seine Eignung verliert, wählt das Cluster-Quorum einen der verbleibenden Knoten als neuen primären Knoten.

> Wenn Sie diesen Schritt auf dem ersten Knoten eines HA-Paares durchführen, sollten Sie nur diesen Knoten als nicht geeignet markieren. Ändern Sie nicht den Status des HA-Partners.
>
> Wird der Partnerknoten als neuer primärer Knoten ausgewählt, muss vor seiner Deaktivierung überprüft werden, ob er Epsilon enthält. Wenn der Partnerknoten Epsilon enthält, muss Epsilon auf einen anderen, im Cluster verbleibenden Knoten verschoben werden, bevor er deaktiviert wird. Dies geschieht, wenn diese Schritte zum Entfernen des Partnerknotens wiederholt werden.

a. Den vorherigen primären Knoten wieder für die Teilnahme am Cluster berechtigen:

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

6. Melden Sie sich bei der Remote-Knotenverwaltungs-LIF oder der Clusterverwaltungs-LIF auf einem Knoten an, den Sie nicht aus dem Cluster entfernen.
7. Entfernen Sie die Knoten aus dem Cluster:

Für diese ONTAP Version…	Verwenden Sie diesen Befehl…
ONTAP 9.3	`cluster unjoin`

ONTAP 9.4 und höher	Mit Node-Name:
	`cluster remove-node -node <node_name>`
	Mit Node-IP:
	`cluster remove-node -cluster_ip <node_ip>`

Wenn Sie einen Cluster mit gemischten Versionen haben und den letzten Knoten mit der niedrigeren Version entfernen, sollte der `-skip-last-low-version-node-check` Parameter bei diesen Befehlen verwendet werden.

Das System informiert Sie über Folgendes:

- Außerdem ist der Failover-Partner des Knotens aus dem Cluster zu entfernen.
- Nachdem der Node entfernt wurde und bevor er wieder einem Cluster beitreten kann, müssen Sie die Bootmenüoption **(4) Clean configuration and initialize all disks** oder die Option **(9) Configure Advanced Drive Partitioning** verwenden, um die Konfiguration des Node zu löschen und alle

Datenträger zu initialisieren.

Eine Fehlermeldung wird generiert, wenn Bedingungen vorliegen, die Sie vor dem Entfernen des Knotens beheben müssen. Die Meldung kann beispielsweise darauf hinweisen, dass der Knoten gemeinsam genutzte Ressourcen hat, die entfernt werden müssen, oder dass sich der Knoten in einer Cluster HA-Konfiguration oder einer Storage Failover-Konfiguration befindet, die deaktiviert werden muss.

Wenn der Knoten der primäre Quorumknoten ist, verliert der Cluster kurzzeitig das Quorum und stellt es anschließend wieder her. Dieser Quorumverlust ist vorübergehend und hat keine Auswirkungen auf Datenoperationen.

8. Wenn eine Fehlermeldung auf Fehlerbedingungen hinweist, sollten diese Bedingungen behoben und der `cluster remove-node` oder `cluster unjoin` Befehl erneut ausgeführt werden.

   Der Knoten startet nach erfolgreicher Entfernung aus dem Cluster automatisch neu.

9. Wenn der Node für einen anderen Zweck verwendet wird, werden die Node-Konfiguration gelöscht und alle Festplatten initialisiert:
   a. Während des Bootvorgangs Strg+C drücken, um das Bootmenü anzuzeigen, wenn dazu aufgefordert wird.
   b. Wählen Sie die Bootmenü-Option **(4) Konfiguration bereinigen und alle Festplatten initialisieren**.
10. Zurück zur Administrator-Berechtigungsstufe:

    ```
    set -privilege admin
    ```

11. Wiederholen Sie die Schritte 1 bis 9, um den Failover-Partner aus dem Cluster zu entfernen.

Verwandte Informationen

- "cluster remove-node"

ONTAP-Knotenprotokolle, Core-Dumps und MIB-Dateien können mit einem Webbrowser abgerufen werden

Der Webdienst der Service Processor Infrastructure (`spi` ist standardmäßig aktiviert, um einem Webbrowser den Zugriff auf die Protokoll-, Core-Dump- und MIB-Dateien eines Knotens im Cluster zu ermöglichen. Die Dateien bleiben auch dann zugänglich, wenn der Knoten ausgefallen ist, sofern der Knoten von seinem Partner übernommen wird.

Bevor Sie beginnen

- Der Cluster-Management-LIF muss aktiv sein.

  Sie können die Management-LIF des Clusters oder eines Knotens verwenden, um auf den `spi` Webdienst zuzugreifen. Es wird jedoch empfohlen, die Cluster-Management-LIF zu verwenden.

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

  Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

- Sie müssen ein lokales Benutzerkonto verwenden, um auf den `spi` Webdienst zuzugreifen, Domänenbenutzerkonten werden nicht unterstützt.
- Falls Ihr Benutzerkonto nicht über die `admin` Rolle verfügt (die standardmäßig Zugriff auf den `spi` Webdienst hat), muss Ihrer Zugriffskontrollrolle Zugriff auf den `spi` Webdienst gewährt werden.

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

- Wenn Sie das `admin` Benutzerkonto nicht verwenden (das `http` Zugriffsmethode standardmäßig beinhaltet), muss Ihr Benutzerkonto mit der `http` Zugriffsmethode eingerichtet sein.

  Der `security login show`Befehl zeigt die Zugriffs- und Anmeldemethoden der Benutzerkonten sowie deren Zugriffskontrollrollen.

  Weitere Informationen zu `security login show` finden sich in der "ONTAP-Befehlsreferenz".

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

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

Über diese Aufgabe

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

Die `admin`Rolle erhält standardmäßig Zugriff auf den `spi`Webdienst, und der Zugriff kann manuell deaktiviert werden (`services web access delete -vserver *cluster_name* -name spi -role admin`.

Schritte

1. Den Webbrowser auf die `spi` Webdienst-URL in einem der folgenden Formate richten:
   - `http://`*`cluster-mgmt-LIF`*`/spi/`
   - `https://`*`cluster-mgmt-LIF`*`/spi/`

     `cluster-mgmt-LIF` ist die IP-Adresse des Cluster-Management-LIF.
2. Wenn der Browser dazu auffordert, Benutzerkonto und Passwort eingeben.

   Nach der Authentifizierung Ihres Kontos zeigt der Browser Links zu den `/mroot/etc/log/`, `/mroot/etc/crash/` und `/mroot/etc/mib/` Verzeichnissen jedes Knotens im Cluster an.

Zugriff auf die Systemkonsole eines ONTAP Knotens

Wenn ein Knoten im Bootmenü oder an der Bootumgebungs-Eingabeaufforderung hängen bleibt, kann darauf nur über die Systemkonsole (auch als serielle Konsole bezeichnet) zugegriffen werden. Die Systemkonsole eines Knotens ist über eine SSH-Verbindung zum SP oder zum Cluster zugänglich.

Über diese Aufgabe

Sowohl SP als auch ONTAP bieten Befehle, mit denen Sie auf die Systemkonsole zugreifen können. Vom SP aus ist jedoch nur die Systemkonsole des eigenen Knotens zugänglich. Vom Cluster aus kann auf die Systemkonsole jedes anderen Knotens im Cluster (außer dem lokalen Knoten) zugegriffen werden.

Schritte

1. Zugriff auf die Systemkonsole eines Knotens:

Wenn Sie sich in der… befinden	Geben Sie diesen Befehl ein…
SP CLI des Knotens	`system console`
ONTAP CLI	`system node run-console`

2. Melden Sie sich an der Systemkonsole an, wenn Sie dazu aufgefordert werden.
3. Zum Verlassen der Systemkonsole Strg+D drücken.

Beispiele für den Zugriff auf die Systemkonsole

Das folgende Beispiel zeigt das Ergebnis der Eingabe des `system console` Befehls an der Eingabeaufforderung „`SP node2`“. Die Systemkonsole zeigt an, dass node2 an der Bootumgebungs-Eingabeaufforderung hängt. Der `boot_ontap` Befehl wird an der Konsole eingegeben, um den Node auf ONTAP zu booten. Anschließend wird Strg+D 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 wird gedrückt, 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` Befehls aus ONTAP, um auf die Systemkonsole von node2 zuzugreifen, die an der Boot-Umgebungs-Eingabeaufforderung hängt. Der `boot_ontap` Befehl wird an der Konsole eingegeben, um node2 in ONTAP zu starten. Anschließend wird Strg+D gedrückt, um die Konsole zu verlassen und zu 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 wird gedrückt, um die Systemkonsole zu verlassen.)

```
Connection to 123.12.123.12 closed.
cluster1::>
```

ONTAP Node-Root-Volumes und Root-Aggregate verwalten

Das Root-Volume eines Knotens ist ein FlexVol Volume, das werkseitig oder durch Installationssoftware eingerichtet wird. Es ist für Systemdateien, Protokolldateien und Core-Dateien reserviert. Der Verzeichnisname ist `/mroot`, der nur über die Systemshell durch den technischen Support zugänglich ist. Die Mindestgröße des Root-Volumes eines Knotens hängt vom Plattformmodell ab.

Überblick über die Regeln für Node-Root-Volumes und Root-Aggregate

Das Root-Volume eines Nodes enthält spezielle Verzeichnisse und Dateien für diesen Node. Das Root-Aggregat enthält das Root-Volume. Für das Root-Volume und das Root-Aggregat eines Nodes gelten einige Regeln.

- Für das Root-Volume des Knotens gelten folgende Regeln:
  - Ändern Sie weder die Konfiguration noch den Inhalt des Root-Volumes, es sei denn, Sie werden vom technischen Support dazu aufgefordert.
  - Benutzerdaten dürfen nicht im Root-Volume gespeichert werden.

    Das Speichern von Benutzerdaten im Root-Volume erhöht die Speicherrückgabezeit zwischen den Knoten in einem HA-Paar.
  - Sie können das Root-Volume in ein anderes Aggregat verschieben. Siehe Root-Volumes auf neue Aggregate verschieben.
- Das Root-Aggregat ist ausschließlich dem Root-Volume des Knotens zugeordnet.

ONTAP verhindert die Erstellung weiterer Volumes im Root-Aggregat.

"NetApp Hardware Universe"

Speicherplatz auf dem Root-Volume eines Knotens freigeben

Eine Warnmeldung erscheint, wenn das Root-Volume eines Knotens voll oder fast voll ist. Der Knoten kann nicht ordnungsgemäß funktionieren, wenn sein Root-Volume voll ist. Sie können Speicherplatz auf dem Root-Volume eines Knotens freigeben, indem Sie Core-Dump-Dateien, Paket-Trace-Dateien und Root-Volume-Snapshots löschen.

Schritte

1. Die Core-Dump-Dateien des Knotens und deren Namen werden angezeigt:

   `system node coredump show`

2. Unerwünschte Core-Dump-Dateien vom Node löschen:

   `system node coredump delete`

3. Zugriff auf die Nodeshell:

   system node run -node *nodename*

   nodename ist der Name des Knotens, dessen Root-Volume-Speicherplatz Sie freigeben möchten.

4. Zur erweiterten Berechtigungsstufe der NodeShell wechseln:

   priv set advanced

5. Anzeige und Löschung der Paketverfolgungsdateien des Knotens über die Nodeshell:
   a. Alle Dateien im Root-Volume des Knotens anzeigen:

      ls /etc

   b. Wenn sich Paketverfolgungsdateien (`*.trc` im Root-Volume des Knotens befinden, sollten diese einzeln gelöscht werden:

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

6. Die Snapshots des Root-Volumes des Knotens können über die Nodeshell identifiziert und gelöscht werden:
   a. Den Namen des Root-Volumes identifizieren:

      vol status

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

      Im folgenden Beispiel ist das Root-Volume `vol0`:

```
node1*> vol status

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

a. Snapshots des Root-Volumes anzeigen:

```
snap list root_vol_name
```

b. Unerwünschte Root-Volume-Snapshots löschen:

```
snap delete root_vol_namesnapshot_name
```

7. Beenden Sie die Nodeshell und kehren Sie zur Clustershell zurück:

```
exit
```

Root-Volumes auf neue Aggregate verschieben

Das Root-Ersatzverfahren migriert das aktuelle Root-Aggregat ohne Unterbrechung auf einen anderen Satz von Festplatten.

Über diese Aufgabe

Die Speicherausfallsicherung muss aktiviert sein, um Root-Volumes zu verschieben. Mit dem `storage failover modify -node` *`nodename`* `-enable true` Befehl kann die Ausfallsicherung aktiviert werden.

Der Speicherort des Root-Volumes kann in den folgenden Szenarien auf ein neues Aggregat geändert werden:

- Wenn sich die Root-Aggregate nicht auf der bevorzugten Festplatte befinden
- Wenn die an den Knoten angeschlossenen Festplatten neu angeordnet werden sollen
- Bei einem Austausch der EOS-Festplattengehäuse

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set privilege advanced
```

2. Das Root-Aggregat verschieben:

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

   - **-Knoten**

     Gibt den Knoten an, dem das Root-Aggregat gehört, das migriert werden soll.

   - **-disklist**

     Gibt die Liste der Datenträger an, auf denen das neue Root-Aggregat erstellt wird. Alle Datenträger müssen Ersatzdatenträger sein und demselben Knoten zugeordnet sein. Die Mindestanzahl der

benötigten Datenträger hängt vom RAID-Typ ab.

- **-RAID-Typ**

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

3. Den Fortschritt des Jobs überwachen:

   `job show -id jobid -instance`

Ergebnisse

Wenn alle Vorabprüfungen erfolgreich sind, startet der Befehl einen Root-Volume-Ersetzungsvorgang und beendet sich. Es ist zu erwarten, dass der Knoten neu startet.

Verwandte Informationen

- "storage failover modify"

Einen ONTAP Knoten für Wartungs- oder Fehlerbehebungszwecke starten oder stoppen

Möglicherweise müssen Sie einen Knoten aus Wartungs- oder Fehlerbehebungsgründen starten oder stoppen. Dies ist über die ONTAP CLI, die Boot-Umgebungseingabeaufforderung oder die SP CLI möglich.

Die Verwendung des SP CLI-Befehls `system power off` oder `system power cycle` zum Ausschalten oder Neustarten eines Knotens kann zu einem unsachgemäßen Herunterfahren des Knotens (auch als *dirty shutdown* bezeichnet) führen und ist kein Ersatz für ein ordnungsgemäßes Herunterfahren mit dem ONTAP `system node halt` Befehl.

Einen Node an der Systemaufforderung neu starten

Ein Knoten kann im normalen Modus über die Systemeingabeaufforderung neu gestartet werden. Ein Knoten ist so konfiguriert, dass er vom Boot-Gerät, wie einer PC CompactFlash Karte, startet.

Schritte

1. Wenn der Cluster vier oder mehr Knoten enthält, ist zu überprüfen, dass der neu zu startende Knoten kein Epsilon hält:

   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

      `set -privilege advanced`

   b. Ermitteln Sie, welcher Knoten Epsilon enthält:

      `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 neu zu startende Knoten Epsilon enthält, ist Epsilon vom Knoten zu entfernen:

cluster modify -node *node_name* -epsilon false

b. Epsilon einem anderen Knoten zuweisen, der aktiv bleibt:

cluster modify -node *node_name* -epsilon true

c. Zurück zur Administrator-Privilegstufe:

set -privilege admin

2. Mit dem `system node reboot` Befehl wird der Node neu gestartet.

Wenn der `-skip-lif-migration` Parameter nicht angegeben wird, versucht der Befehl, Daten- und Cluster-Management-LIFs vor dem Neustart synchron auf einen anderen Knoten zu migrieren. Wenn die LIF-Migration fehlschlägt oder eine Zeitüberschreitung auftritt, wird der Neustartvorgang abgebrochen und ONTAP zeigt eine Fehlermeldung an, die auf den Fehler bei der LIF-Migration hinweist.

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

Der Knoten startet den Neustartvorgang. Die ONTAP Anmeldeaufforderung erscheint und zeigt damit an, dass der Neustartvorgang abgeschlossen ist.

ONTAP an der Eingabeaufforderung der Startumgebung starten

Die aktuelle Version oder die Backup-Version von ONTAP kann gestartet werden, wenn Sie sich an der Boot-Umgebungs-Eingabeaufforderung eines Knotens befinden.

Schritte

1. Auf die Bootumgebungs-Eingabeaufforderung kann von der Storage-System-Konsole aus mit dem `system node halt` Befehl zugegriffen werden.

Die Storage-System-Konsole zeigt die Eingabeaufforderung für die Startumgebung an.

2. An der Eingabeaufforderung der Bootumgebung einen der folgenden Befehle eingeben:

Und obendrein …	Eingeben…
Die aktuelle Version von ONTAP	`boot_ontap`
Das primäre ONTAP Image vom Boot-Gerät	`boot_primary`
Das ONTAP Backup-Image vom Boot-Gerät	`boot_backup`

Wenn Sie sich nicht sicher sind, welches Image Sie verwenden sollen, sollte `boot_ontap` in der ersten Instanz verwendet werden.

Einen Knoten herunterfahren

Sie können einen Knoten herunterfahren, wenn er nicht mehr reagiert oder wenn das Supportpersonal Sie im Rahmen der Fehlerbehebung dazu auffordert.

Schritte

1. Wenn der Cluster vier oder mehr Knoten enthält, ist zu überprüfen, ob der Knoten, der heruntergefahren werden soll, kein Epsilon hält:

   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

      `set -privilege advanced`

   b. Ermitteln Sie, welcher Knoten Epsilon enthält:

      `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 abzuschaltende Knoten Epsilon enthält, dann Epsilon aus dem Knoten entfernen:

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

   b. Epsilon einem anderen Knoten zuweisen, der aktiv bleibt:

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

   c. Zurück zur Administrator-Privilegstufe:

      `set -privilege admin`

2. Der `system node halt` Befehl dient zum Herunterfahren des Knotens.

   Wenn der `-skip-lif-migration` Parameter nicht angegeben wird, versucht der Befehl, Daten- und Cluster-Management-LIFs vor dem Herunterfahren synchron auf einen anderen Knoten zu migrieren. Wenn die LIF-Migration fehlschlägt oder ein Timeout auftritt, wird der Herunterfahrvorgang abgebrochen und ONTAP zeigt eine Fehlermeldung an, die auf den Fehler bei der LIF-Migration hinweist.

   Sie können beim Herunterfahren manuell einen Core-Dump auslösen, indem Sie den `-dump` Parameter

verwenden.

Das folgende Beispiel fährt den Knoten mit dem Namen “node1” für Hardwarewartungsarbeiten herunter:

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

Einen ONTAP-Knoten über das Bootmenü verwalten

Über das Bootmenü können Sie Konfigurationsprobleme auf einem Knoten beheben, das Administratorpasswort zurücksetzen, Festplatten initialisieren, die Knotenkonfiguration zurücksetzen und die Knotenkonfigurationsinformationen auf das Bootgerät wiederherstellen.

Wenn ein HA-Paar "Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)" verwendet wird, müssen Sie die Anweisungen im Thema "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus" für alle Laufwerke innerhalb des HA-Paares befolgen, bevor Sie das System initialisieren (Boot-Optionen 4 oder 9). Andernfalls kann es in Zukunft zu Datenverlust kommen, wenn die Laufwerke wiederverwendet werden.

Schritte

1. Der Knoten kann neu gestartet werden, um über den `system node reboot` Befehl an der Systemeingabeaufforderung auf das Boot-Menü zuzugreifen.

   Der Knoten startet den Neustartvorgang.

2. Während des Neustartvorgangs Strg+C drücken, um das Startmenü anzuzeigen, wenn dazu aufgefordert wird.

   Der Knoten zeigt die folgenden Optionen für das Bootmenü an:

```
(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-Menü Option (2) Booten ohne /etc/rc ist veraltet und hat keine Auswirkung auf das System.

3. Eine der folgenden Optionen kann durch Eingabe der entsprechenden Nummer ausgewählt werden:

Zu…	Auswählen…
Der Knoten wird im normalen Modus weiter hochgefahren.	1) Normaler Startvorgang
Das Passwort des Knotens ändern, das gleichzeitig das Passwort des „admin“-Kontos ist	3) Passwort ändern
Die Festplatten des Knotens werden initialisiert und ein Root-Volume für den Knoten erstellt.	4) Konfiguration bereinigen und alle Festplatten initialisieren Diese Menüoption löscht alle Daten auf den Festplatten des Knotens und setzt die Knotenkonfiguration auf die Werkseinstellungen zurück. Wählen Sie diesen Menüpunkt nur aus, nachdem der Knoten aus einem Cluster entfernt wurde und nicht einem anderen Cluster beigetreten ist. Bei einem Knoten mit internen oder externen Festplattengehäusen wird das Root-Volume auf den internen Festplatten initialisiert. Sind keine internen Festplattengehäuse vorhanden, wird das Root-Volume auf den externen Festplatten initialisiert. Wenn der Knoten, den Sie initialisieren möchten, über Festplatten verfügt, die für Root-Datenpartitionierung partitioniert sind, müssen die Festplatten vor der Initialisierung des Knotens entpartitioniert werden, siehe **9) Configure Advanced Drive Partitioning** und "Festplatten- und Aggregatverwaltung".
Wartungsarbeiten an Aggregaten und Festplatten sowie detaillierte Informationen zu Aggregaten und Festplatten sind möglich.	5) Start im Wartungsmodus Sie beenden den Wartungsmodus mit dem `halt` Befehl.
Die Konfigurationsinformationen werden vom Root-Volume des Knotens auf das Boot-Gerät, wie eine PC CompactFlash Karte, wiederhergestellt.	6) Flash aus der Backup-Konfiguration aktualisieren ONTAP speichert einige Konfigurationsinformationen des Knotens auf dem Boot-Gerät. Beim Neustart des Knotens werden die Informationen auf dem Boot-Gerät automatisch auf das Root-Volume des Knotens gesichert. Wenn das Boot-Gerät beschädigt ist oder ersetzt werden muss, ist diese Menüoption zu verwenden, um die Konfigurationsinformationen vom Root-Volume des Knotens auf das Boot-Gerät wiederherzustellen.

Zu…	Auswählen…
Neue Software auf dem Knoten installieren	7) Zuerst die neue Software installieren Falls die ONTAP Software auf dem Boot-Gerät keine Unterstützung für das Storage Array bietet, das Sie für das Root-Volume verwenden möchten, kann über diese Menüoption eine Version der Software bezogen werden, die Ihr Storage Array unterstützt, und diese auf dem Node installiert werden. Diese Menüoption dient ausschließlich der Installation einer neueren Version der ONTAP Software auf einem Knoten, auf dem kein Root-Volume installiert ist. Diese Menüoption ist *nicht* für das Upgrade von ONTAP zu verwenden.
Den Knoten neu starten	8) Neustart des Knotens

Alle Festplatten entpartitionieren und deren Besitzerinformationen entfernen oder die Konfiguration bereinigen und das System mit ganzen oder partitionierten Festplatten initialisieren	9) Erweiterte Laufwerkspartitionierung konfigurieren
	
	Die Option „Erweiterte Laufwerkspartitionierung“ bietet zusätzliche Verwaltungsfunktionen für Datenträger, die für Root-Data- oder Root-Data-Data-Partitionierung konfiguriert sind. Die folgenden Optionen sind über Boot Option 9 verfügbar:
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

Die Attribute der Knoten in einem ONTAP Cluster anzeigen

Sie können die Attribute eines oder mehrerer Knoten im Cluster anzeigen, zum Beispiel Name, Besitzer, Standort, Modellnummer, Seriennummer, Betriebsdauer des Knotens, Gesundheitszustand und Berechtigung zur Teilnahme an einem Cluster.

Schritte

1. Um die Attribute eines bestimmten Knotens oder aller Knoten in einem Cluster anzuzeigen, den `system node show` Befehl verwenden.

Beispiel für die Anzeige von Informationen über einen Knoten

Das folgende Beispiel zeigt detaillierte Informationen zu node1:

```
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
```

Attribute eines ONTAP Knotens ändern

Sie können die Attribute eines Knotens nach Bedarf ändern. Zu den Attributen, die geändert werden können, gehören die Eigentümerinformationen des Knotens, Standortinformationen, Asset-Tag und die Berechtigung zur Teilnahme am Cluster.

Über diese Aufgabe

Die Teilnahmeberechtigung eines Knotens am Cluster kann auf der Ebene erweiterter Berechtigungen mithilfe des `-eligibility` Parameters des `system node modify` oder `cluster modify` Befehls geändert werden. Wenn die Teilnahmeberechtigung eines Knotens auf `false` gesetzt wird, wird der Knoten im Cluster inaktiv.

> Die Knotenberechtigung kann nicht lokal geändert werden. Sie muss von einem anderen Knoten aus geändert werden. Die Knotenberechtigung kann auch nicht mit einer Cluster HA-Konfiguration geändert werden.

> Sie sollten die Berechtigung eines Knotens nicht auf `false` setzen, außer in Situationen wie der Wiederherstellung der Knotenkonfiguration oder längerer Wartung des Knotens. Der SAN- und NAS-Datenzugriff auf den Knoten kann beeinträchtigt sein, wenn der Knoten nicht berechtigt ist.

Schritte

1. Mit dem `system node modify` Befehl lassen sich die Attribute eines Knotens ändern.

Beispiel für die Änderung von Knotenattributen

Der folgende Befehl ändert die Attribute des Knotens “node1”. Der Besitzer des Knotens wird auf “Joe Smith” und das Asset-Tag auf “js1234” gesetzt:

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

Verwandte Informationen

- "system node modify"
- "cluster modify"

Umbenennen eines ONTAP Knotens

Sie können den Namen eines Knotens nach Bedarf ändern.

Schritte

1. Um einen Node umzubenennen, wird der `system node rename` Befehl verwendet.

   Der `-newname` Parameter gibt den neuen Namen für den Node an. Weitere Informationen zu `system node rename` finden sich in der "ONTAP-Befehlsreferenz".

   Wenn Sie mehrere Knoten im Cluster umbenennen möchten, muss der Befehl für jeden Knoten einzeln ausgeführt werden.

   Der Knotenname darf nicht “all” lauten, da “all” ein vom System reservierter Name ist.

Beispiel für das Umbenennen eines Knotens

Der folgende Befehl benennt den Knoten “node1” in “node1a” um:

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

Verwaltung eines ONTAP Clusters mit einem einzelnen Knoten

Ein Einzelknoten-Cluster ist eine spezielle Implementierung eines Clusters, der auf einem einzelnen Knoten läuft. Einzelknoten-Cluster sind nicht empfehlenswert, da sie keine Redundanz bieten. Fällt der Knoten aus, geht der Datenzugriff verloren.

Für Fehlertoleranz und unterbrechungsfreien Betrieb wird dringend empfohlen, den Cluster mit "Hochverfügbarkeit (HA Paare)" zu konfigurieren.

Wenn Sie einen Einzelknoten-Cluster konfigurieren oder aktualisieren, ist Folgendes zu beachten:

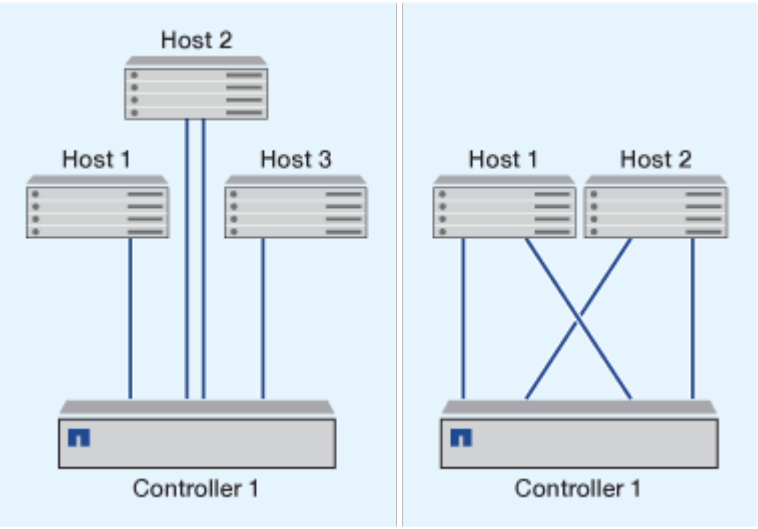
- Die Verschlüsselung des Root-Volumes wird auf Single-Node-Clustern nicht unterstützt.
- Wenn Sie Knoten entfernen, um einen Einzelknoten-Cluster zu erhalten, sollten die Cluster-Ports so modifiziert werden, dass sie den Datenverkehr bedienen, indem die Cluster-Ports in Daten-Ports umgewandelt und anschließend Daten-LIFs auf den Daten-Ports erstellt werden.
- Bei Einzelknotenclustern kann das Ziel für die Konfigurationssicherung während der Softwareinstallation festgelegt werden. Nach der Installation können diese Einstellungen mit ONTAP Befehlen geändert werden.
- Sind mehrere Hosts mit dem Knoten verbunden, kann jeder Host mit einem anderen Betriebssystem wie Windows oder Linux konfiguriert werden. Bestehen mehrere Pfade vom Host zum Controller, muss ALUA auf dem Host aktiviert sein.

Möglichkeiten zur Konfiguration von iSCSI SAN Hosts mit einzelnen Knoten

Sie können iSCSI SAN Hosts so konfigurieren, dass sie entweder direkt mit einem einzelnen Knoten oder über einen oder mehrere IP Switches verbunden werden. Der Knoten kann mehrere iSCSI Verbindungen zum Switch haben.

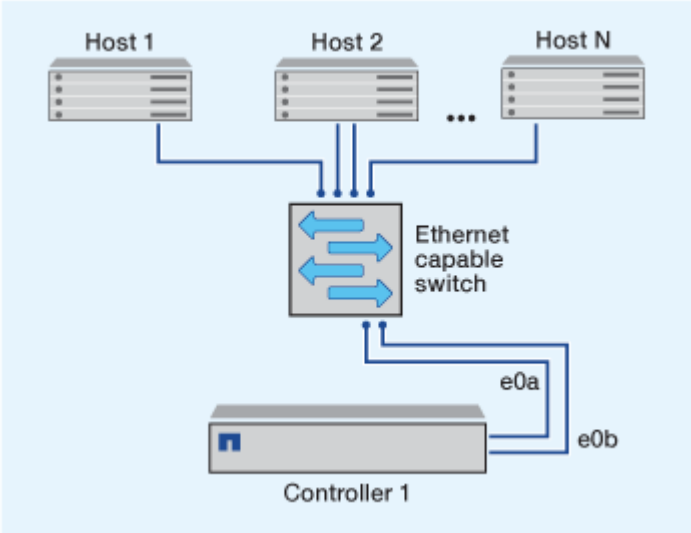
Direkt angeschlossene Single-Node Konfigurationen

Bei direkt angeschlossenen Single-Node-Konfigurationen sind ein oder mehrere Hosts direkt mit dem Node verbunden.



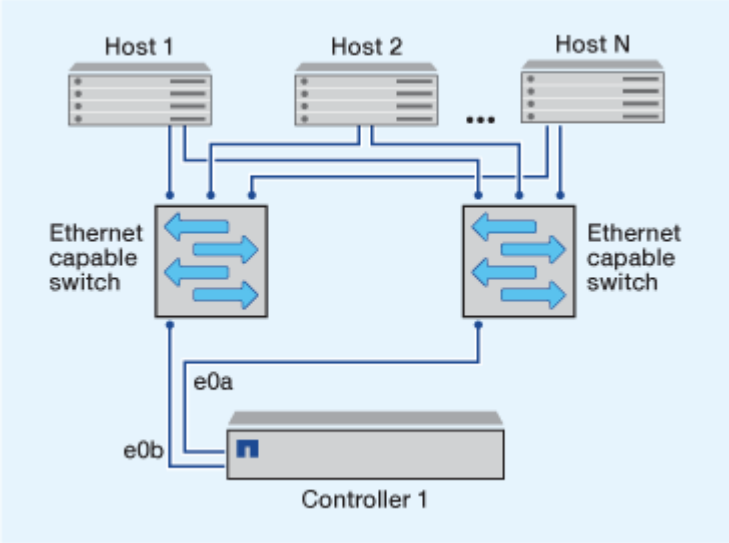
Single-network Single-Node-Konfigurationen

In Konfigurationen mit einem einzigen Netzwerk und einem einzigen Knoten verbindet ein Switch einen einzelnen Knoten mit einem oder mehreren Hosts. Da nur ein einziger Switch verwendet wird, ist diese Konfiguration nicht vollständig redundant.



Multi-Network Single-Node-Konfigurationen

In Multi-Netzwerk-Einzelknotenkonfigurationen verbinden zwei oder mehr Switches einen einzelnen Knoten mit einem oder mehreren Hosts. Da mehrere Switches vorhanden sind, ist diese Konfiguration vollständig redundant.



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

FC- und FC-NVMe SAN-Hosts können über ein oder mehrere Fabrics mit einzelnen Knoten konfiguriert werden. N-Port ID Virtualisierung (NPIV) ist erforderlich und muss auf allen FC-Switches im Fabric aktiviert sein. FC- oder FC-NVMe SAN-Hosts können nicht ohne FC-Switch direkt an einzelne Knoten angebunden werden.

Single-fabric Single-Node-Konfigurationen

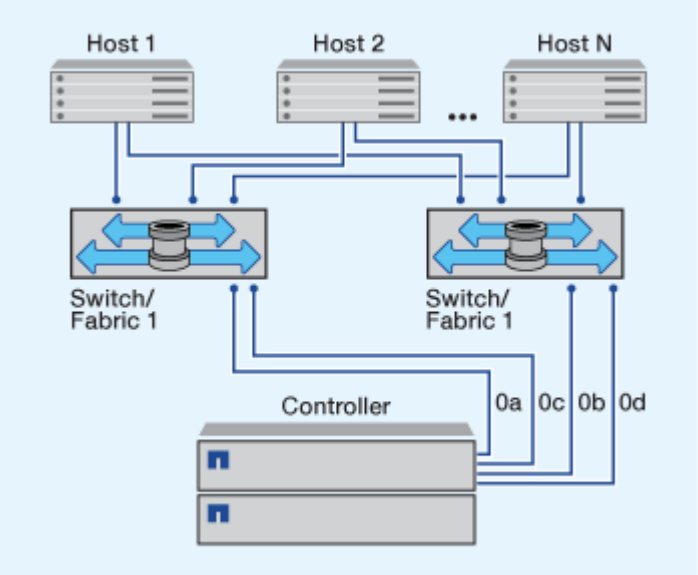
In Single Fabric Single Node Konfigurationen verbindet ein einzelner Switch einen Knoten mit einem oder mehreren Hosts. Da nur ein einziger Switch verwendet wird, ist diese Konfiguration nicht vollständig redundant.

Bei Konfigurationen mit einem einzigen Fabric und einem einzelnen Knoten ist Multipathing-Software nicht erforderlich, wenn Sie nur einen einzigen Pfad vom Host zum Knoten haben.

Multifabric Einzelknoten-Konfigurationen

In Multifabric Single-Node-Konfigurationen verbinden zwei oder mehr Switches einen einzelnen Knoten mit einem oder mehreren Hosts. Zur Vereinfachung zeigt die folgende Abbildung eine Multifabric Single-Node-Konfiguration mit nur zwei Fabrics, jedoch sind in jeder Multifabric-Konfiguration zwei oder mehr Fabrics möglich. In dieser Abbildung ist der Storage Controller im oberen Chassis montiert, und das untere Chassis kann leer sein oder, wie in diesem Beispiel, ein IOMX-Modul enthalten.

Die FC-Zielports (0a, 0c, 0b, 0d) in den Abbildungen sind Beispiele. Die tatsächlichen Portnummern variieren je nach Modell Ihres Speicherknotens und ob Erweiterungsadapter verwendet werden.



Verwandte Informationen

"NetApp Technical Report 4684: Implementierung und Konfiguration moderner SANs mit NVMe-oF"

ONTAP Upgrade für Einzelknoten-Cluster

Sie können die ONTAP CLI verwenden, um ein automatisiertes Update eines Einzelknotenclusters durchzuführen. Einzelknotencluster weisen keine Redundanz auf, das bedeutet, dass Updates immer unterbrechungsfrei sind. Unterbrechende Upgrades können nicht mit System Manager durchgeführt werden.

Bevor Sie beginnen

Das Upgrade-"Vorbereitung"Schritte müssen abgeschlossen werden.

Schritte

1. Das vorherige ONTAP Softwarepaket löschen:

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

2. Das gewünschte ONTAP Softwarepaket herunterladen:

```
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. Es sollte sichergestellt sein, dass das Softwarepaket im Cluster-Paket-Repository 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. Es sollte überprüft werden, ob der Cluster für das Upgrade bereit 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. Fortschritt der Validierung überwachen:

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

6. Alle im Rahmen der Validierung identifizierten erforderlichen Aktionen müssen abgeschlossen werden.
7. Optional kann eine Kostenschätzung für ein Software-Upgrade erstellt werden:

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

Die Kostenschätzung für das Software-Upgrade enthält Details zu jeder zu aktualisierenden Komponente und die geschätzte Dauer des Upgrades.

8. Das Software-Upgrade ausführen:

```
cluster image update -version <package_version_number>
```



Wenn ein Problem auftritt, wird das Update angehalten und Sie werden aufgefordert, eine Korrekturmaßnahme zu ergreifen. Mit dem Befehl cluster image show-update-progress lassen sich Details zu etwaigen Problemen und dem Fortschritt des Updates anzeigen. Nach Behebung des Problems lässt sich das Update mit dem Befehl cluster image resume-update fortsetzen.

9. Fortschritt der Clusteraktualisierung anzeigen:

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

Der Knoten wird im Rahmen des Updates neu gestartet und ist während des Neustarts nicht erreichbar.

10. Benachrichtigung auslösen:

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

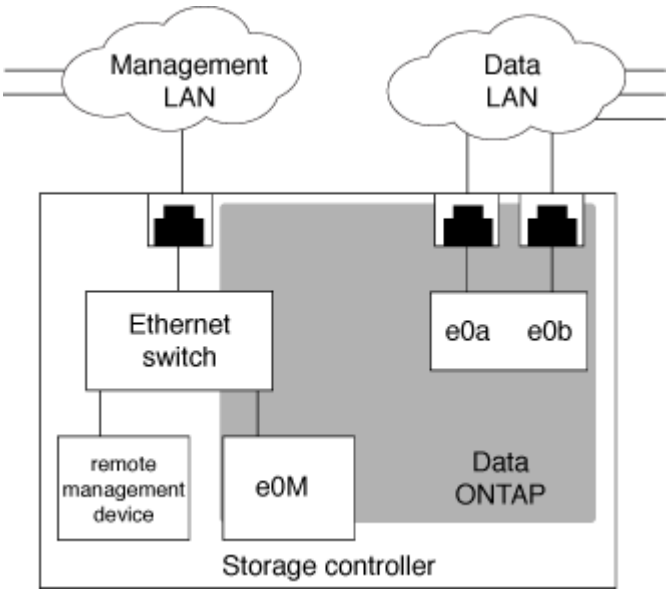
Wenn Ihr Cluster nicht für den Versand von Nachrichten konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

Das SP/BMC-Netzwerk konfigurieren

ONTAP Verwaltungsdatenverkehr im Netzwerk isolieren

Es gilt als Best Practice, SP/BMC und die e0M Managementoberfläche in einem Subnetz zu konfigurieren, das ausschließlich für den Management-Datenverkehr vorgesehen ist. Die Übertragung von Datenverkehr über das Managementnetzwerk kann zu Leistungseinbußen und Routing-Problemen führen.

Der Management-Ethernet-Port der meisten Storage Controller (gekennzeichnet durch ein Schraubenschlüssel-Symbol auf der Rückseite des Gehäuses) ist mit einem internen Ethernet-Switch verbunden. Der interne Switch stellt die Verbindung zu SP/BMC und zur e0M Managementoberfläche her, die für den Zugriff auf das Speichersystem über TCP/IP-Protokolle wie Telnet, SSH und SNMP genutzt werden kann.



Wenn Sie sowohl das Fernverwaltungsgerät als auch e0M verwenden möchten, müssen Sie diese im selben IP-Subnetz konfigurieren. Da es sich um Schnittstellen mit geringer Bandbreite handelt, ist es am besten, SP/BMC und e0M in einem für den Managementdatenverkehr reservierten Subnetz zu konfigurieren.

Wenn Sie den Management-Datenverkehr nicht isolieren können oder Ihr dediziertes Management-Netzwerk

ungewöhnlich groß ist, sollte das Netzwerkverkehrsaufkommen so gering wie möglich gehalten werden. Übermäßiger eingehender Broadcast- oder Multicast-Datenverkehr kann die Leistung von SP/BMC beeinträchtigen.

Einige Storage-Controller, wie beispielsweise der AFF A800, verfügen über zwei externe Ports, einen für BMC und den anderen für e0M. Für diese Controller besteht keine Anforderung, BMC und e0M im selben IP-Subnetz zu konfigurieren.

Informationen zur ONTAP SP/ BMC Netzwerkkonfiguration

Sie können die automatische Netzwerkkonfiguration auf Clusterebene für den SP (empfohlen) aktivieren. Es besteht auch die Möglichkeit, die automatische Netzwerkkonfiguration des SP deaktiviert zu lassen (Standardeinstellung) und die SP-Netzwerkkonfiguration manuell auf Knotenebene zu verwalten. Für beide Fälle sind einige Aspekte zu berücksichtigen.

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

Die automatische SP-Netzwerkkonfiguration ermöglicht es dem SP, Adressressourcen (einschließlich IP-Adresse, Subnetzmaske und Gateway-Adresse) aus dem angegebenen Subnetz zu verwenden, um sein Netzwerk automatisch einzurichten. Mit der automatischen SP-Netzwerkkonfiguration ist keine manuelle Zuweisung von IP-Adressen für den SP jedes Knotens erforderlich. Standardmäßig ist die automatische SP-Netzwerkkonfiguration deaktiviert, da für die Aktivierung zunächst das für die Konfiguration zu verwendende Subnetz im Cluster definiert sein muss.

Wenn die SP automatische Netzwerkkonfiguration aktiviert wird, gelten die folgenden Szenarien und Überlegungen:

- Wenn der SP noch nie konfiguriert wurde, wird das SP-Netzwerk automatisch auf Basis des für die automatische SP-Netzwerkkonfiguration angegebenen Subnetzes konfiguriert.
- Wenn der SP zuvor manuell konfiguriert wurde oder die bestehende SP-Netzwerkkonfiguration auf einem anderen Subnetz basiert, wird das SP-Netzwerk aller Knoten im Cluster auf Grundlage des Subnetzes neu konfiguriert, das Sie in der automatischen SP-Netzwerkkonfiguration angeben.

  Die Neukonfiguration kann dazu führen, dass dem SP eine andere Adresse zugewiesen wird, was Auswirkungen auf Ihre DNS-Konfiguration und deren Fähigkeit zur Auflösung von SP-Hostnamen haben kann. Infolgedessen könnte eine Aktualisierung Ihrer DNS-Konfiguration erforderlich sein.

- Ein Knoten, der dem Cluster beitritt, verwendet das angegebene Subnetz, um sein SP-Netzwerk automatisch zu konfigurieren.
- Der `system service-processor network modify`Befehl ermöglicht keine Änderung der SP IP-Adresse.

  Wenn die automatische SP Netzwerkkonfiguration aktiviert ist, erlaubt der Befehl nur das Aktivieren oder Deaktivieren der SP Netzwerkschnittstelle.

  - Wenn die automatische SP-Netzwerkkonfiguration zuvor aktiviert war, führt das Deaktivieren der SP-Netzwerkschnittstelle dazu, dass die zugewiesene Adressressource freigegeben und dem Subnetz zurückgegeben wird.
  - Wenn die SP-Netzwerkschnittstelle deaktiviert und anschließend wieder aktiviert wird, kann der SP möglicherweise mit einer anderen Adresse neu konfiguriert werden.

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

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

  Ein Knoten, der dem Cluster beitritt, verwendet standardmäßig ebenfalls IPv4 DHCP für seine SP-Netzwerkkonfiguration.

- Der `system service-processor network modify`Befehl ermöglicht die Konfiguration der SP-IP-Adresse eines Knotens.

  Eine Warnmeldung erscheint, wenn versucht wird, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind. Das Ignorieren der Warnung und das Fortfahren mit der manuellen Adresszuweisung kann zu einer Situation mit doppelten Adressen führen.

Wenn die SP automatische Netzwerkkonfiguration nach vorheriger Aktivierung deaktiviert wird, gelten die folgenden Szenarien und Überlegungen:

- Wenn die automatische SP-Netzwerkkonfiguration die IPv4-Adressfamilie deaktiviert hat, verwendet das SP IPv4-Netzwerk standardmäßig DHCP, und der `system service-processor network modify` Befehl ermöglicht die Anpassung der SP IPv4-Konfiguration für einzelne Knoten.
- Wenn die automatische SP-Netzwerkkonfiguration die IPv6-Adressfamilie deaktiviert hat, ist auch das SP IPv6-Netzwerk deaktiviert, und der `system service-processor network modify` Befehl ermöglicht das Aktivieren und Ändern der SP IPv6-Konfiguration für einzelne Nodes.

Automatische Netzwerkkonfiguration für ONTAP SP/BMC aktivieren

Die Aktivierung der automatischen Netzwerkkonfiguration für den SP wird gegenüber der manuellen Konfiguration des SP Netzwerks bevorzugt. Da die automatische Netzwerkkonfiguration des SP clusterweit gilt, ist keine manuelle Verwaltung des SP Netzwerks für einzelne Knoten erforderlich.

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

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

  Der `network subnet show` Befehl zeigt Subnetzinformationen für den Cluster an.

  Weitere Informationen zu `network subnet show` finden sich in der "ONTAP-Befehlsreferenz".

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

- Wenn IPv6-Verbindungen für den SP verwendet werden sollen, muss IPv6 für ONTAP bereits konfiguriert und aktiviert sein.

  Der `network options ipv6 show` Befehl zeigt den aktuellen Status der IPv6-Einstellungen für ONTAP an. Weitere Informationen zu `network options ipv6 show` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Geben Sie die IPv4- oder IPv6-Adressfamilie und den Namen des Subnetzes an, das der SP verwenden soll, indem Sie den `system service-processor network auto-configuration enable` Befehl verwenden.
2. Die automatische SP-Netzwerkkonfiguration kann mit dem `system service-processor network auto-configuration show` Befehl angezeigt werden.
3. Wenn anschließend die SP IPv4 oder IPv6 Netzwerkschnittstelle für alle Knoten, die sich im Quorum befinden, deaktiviert oder wieder aktiviert werden soll, ist der `system service-processor network modify` Befehl mit den Parametern `-address-family` [`IPv4`|`IPv6`] und `-enable` [`true`|`false`] zu verwenden.

   Wenn die automatische SP-Netzwerkkonfiguration aktiviert ist, kann die SP-IP-Adresse eines Knotens, der sich im Quorum befindet, nicht geändert werden. Es kann lediglich die SP-IPv4- oder SP-IPv6-Netzwerkschnittstelle aktiviert oder deaktiviert werden.

   Befindet sich ein Knoten außerhalb des Quorums, kann die SP-Netzwerkkonfiguration des Knotens, einschließlich der SP-IP-Adresse, durch Ausführen von `system service-processor network modify` auf dem Knoten geändert werden, wobei zu bestätigen ist, dass die automatische SP-Netzwerkkonfiguration für den Knoten überschrieben werden soll. Wenn der Knoten dem Quorum wieder beitritt, erfolgt die automatische SP-Neukonfiguration für den Knoten basierend auf dem angegebenen Subnetz.

Das ONTAP SP/BMC Netzwerk manuell konfigurieren

Wenn keine automatische Netzwerkkonfiguration für den SP eingerichtet ist, muss das SP Netzwerk eines Knotens manuell konfiguriert werden, damit der SP über eine IP-Adresse erreichbar ist.

Bevor Sie beginnen

Wenn IPv6-Verbindungen für den SP verwendet werden sollen, muss IPv6 für ONTAP bereits konfiguriert und aktiviert sein. Die `network options ipv6` Befehle verwalten die IPv6-Einstellungen für ONTAP. Weitere Informationen zu `network options ipv6` finden sich in der "ONTAP-Befehlsreferenz".

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

Der SP kann so konfiguriert werden, dass er IPv4, IPv6 oder beides verwendet. Die SP IPv4 Konfiguration unterstützt statische und DHCP-Adressierung, und die SP IPv6 Konfiguration unterstützt nur statische Adressierung.

Wenn die automatische SP-Netzwerkkonfiguration eingerichtet ist, ist keine manuelle Konfiguration des SP-Netzwerks für einzelne Knoten erforderlich, und der `system service-processor network modify` Befehl ermöglicht lediglich das Aktivieren oder Deaktivieren der SP-Netzwerkschnittstelle.

Schritte

1. Das SP Netzwerk für einen Node kann mit dem `system service-processor network modify` Befehl konfiguriert werden.
   - Der `-address-family`Parameter gibt an, ob die IPv4- oder die IPv6-Konfiguration des SP geändert wird.
   - Der `-enable` Parameter aktiviert die Netzwerkschnittstelle der angegebenen IP-Adressfamilie.

- Der `-dhcp`Parameter gibt an, ob die Netzwerkkonfiguration vom DHCP-Server oder die von Ihnen angegebene Netzwerkadresse verwendet wird.

  DHCP kann (durch Einstellen von `-dhcp` auf `v4`) nur aktiviert werden, wenn IPv4 verwendet wird. DHCP kann für IPv6-Konfigurationen nicht aktiviert werden.

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

  Eine Warnmeldung erscheint, wenn versucht wird, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind. Das Ignorieren der Warnung und das Fortsetzen der manuellen Adresszuweisung kann zu einer doppelten Adresszuweisung führen.

- Der `-netmask`Parameter gibt die Subnetzmaske für den SP (bei Verwendung von IPv4) an.
- Der `-prefix-length` Parameter gibt die Netzwerkpräfixlänge der Subnetzmaske für den SP (bei Verwendung von IPv6) an.
- Der `-gateway`Parameter gibt die Gateway-IP-Adresse für den SP an.

2. Das SP Netzwerk für die verbleibenden Knoten im Cluster wird konfiguriert, indem Schritt 1 wiederholt wird.
3. Die SP-Netzwerkkonfiguration kann angezeigt und der SP Einrichtungsstatus überprüft werden, indem der `system service-processor network show` Befehl mit den `-instance` oder `-field setup-status` Parametern verwendet wird.

   Der SP Setup-Status für einen Knoten kann einer der folgenden sein:

   - `not-setup` — Nicht konfiguriert
   - `succeeded` — Konfiguration erfolgreich
   - `in-progress` Konfiguration läuft
   - `failed` — Konfiguration fehlgeschlagen

Beispiel für die Konfiguration des SP Netzwerks

Das folgende Beispiel konfiguriert den SP eines Knotens für die Verwendung von IPv4, aktiviert den SP und zeigt die SP Netzwerkkonfiguration an, 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::>
```

Die ONTAP Service Processor API-Konfiguration anpassen

Die SP-API ist eine sichere Netzwerk-API, die ONTAP die Kommunikation mit dem SP über das Netzwerk ermöglicht. Es besteht die Möglichkeit, den vom SP-API-Service verwendeten Port zu ändern, die für die interne Kommunikation genutzten Zertifikate zu erneuern oder den Service vollständig zu deaktivieren. Eine Änderung der Konfiguration ist nur in seltenen Fällen erforderlich.

Über diese Aufgabe

- Der SP API-Service verwendet standardmäßig Port `50000`.

  Sie können den Portwert ändern, wenn Sie sich beispielsweise in einer Netzwerkumgebung befinden, in der Port `50000` von einer anderen Netzwerkanwendung für die Kommunikation verwendet wird oder wenn Sie zwischen dem Datenverkehr anderer Anwendungen und dem vom SP API-Service erzeugten Datenverkehr unterscheiden möchten.

- Die für den SP API-Service verwendeten SSL- und SSH-Zertifikate sind intern im Cluster und werden nicht extern verteilt.

  Im unwahrscheinlichen Fall, dass die Zertifikate kompromittiert werden, ist eine Erneuerung möglich.

- Der SP API-Service ist standardmäßig aktiviert.

  Das Deaktivieren des SP API-Service ist nur in seltenen Fällen erforderlich, beispielsweise in einem privaten LAN, in dem der SP nicht konfiguriert oder verwendet wird und der Dienst deaktiviert werden soll.

  Wenn der SP API-Service deaktiviert ist, akzeptiert die API keine eingehenden Verbindungen. Zusätzlich stehen Funktionen wie netzwerkbasierte SP-Firmware-Updates und die netzwerkbasierte SP „down system“-Revisionsprotokollsammlung nicht mehr zur Verfügung. Das System wechselt zur Verwendung der seriellen Schnittstelle.

Schritte

1. Zur erweiterten Berechtigungsstufe wird mit dem `set -privilege advanced` Befehl gewechselt.

2. Die SP API-Service-Konfiguration anpassen:

Wenn Sie möchten…	Der folgende Befehl kann verwendet werden…
Den vom SP API-Service verwendeten Port ändern	`system service-processor api-service modify` mit dem `-port {49152..65535}` Parameter
Die SSL- und SSH-Zertifikate, die vom SP API-Service für die interne Kommunikation verwendet werden, erneuern.	• Für ONTAP 9.5 oder höher verwenden `system service-processor api-service renew-internal-certificate` • Für ONTAP 9.4 und frühere Versionen • `system service-processor api-service renew-certificates` Wird kein Parameter angegeben, werden nur die Hostzertifikate (einschließlich der Client- und Serverzertifikate) erneuert. Wenn der `-renew-all true` Parameter angegeben wird, werden sowohl die Hostzertifikate als auch das Root-CA-Zertifikat erneuert.
Kommunikation	
Deaktivieren oder erneutes Aktivieren des SP API-Service	`system service-processor api-service modify` mit dem `-is-enabled {true`

3. Die SP API-Service-Konfiguration wird mit dem `system service-processor api-service show` Befehl angezeigt.

Knoten aus der Ferne mit dem SP/BMC verwalten

Einen ONTAP Knoten remote mit dem SP/BMC verwalten

Ein Knoten kann mithilfe eines integrierten Controllers, dem sogenannten Service Processor (SP) oder Baseboard Management Controller (BMC), remote verwaltet werden. Dieser Remote-Management-Controller ist in allen aktuellen Plattformmodellen enthalten. Der Controller bleibt unabhängig vom Betriebszustand des Knotens funktionsfähig.

Eine vollständige Übersicht über die Unterstützung von Plattform SP und BMC ist im "Support-Matrix" auf der NetApp Support-Website zu finden.

Remote-Knotenverwaltung mit dem ONTAP Service Processor

Der Service Processor (SP) ist ein Fernverwaltungsgerät, das den Fernzugriff, die Überwachung und die Fehlerbehebung eines Knotens ermöglicht.

Zu den wichtigsten Funktionen des SP zählen die folgenden:

- Mit dem SP können Sie unabhängig vom Zustand des Knotencontrollers remote auf einen Knoten zugreifen, um ihn zu diagnostizieren, herunterzufahren, einen Power-Cycle durchzuführen oder neu zu starten.

  Der SP wird über eine Standby-Spannung versorgt, die so lange verfügbar ist, wie der Knoten von mindestens einem seiner Netzteile mit Eingangsspannung versorgt wird.

  Sie können sich mit einer Secure Shell-Clientanwendung von einem Administrationshost am SP anmelden. Anschließend kann die SP-CLI verwendet werden, um den Knoten remote zu überwachen und Fehler zu beheben. Zusätzlich kann der SP genutzt werden, um auf die serielle Konsole zuzugreifen und ONTAP-Befehle remote auszuführen.

  Sie können auf den SP über die serielle Konsole zugreifen oder von dem SP auf die serielle Konsole zugreifen. Der SP ermöglicht es, sowohl eine SP-CLI-Sitzung als auch eine separate Konsolensitzung gleichzeitig zu öffnen.

  Wenn beispielsweise ein Temperatursensor einen kritischen Wert erreicht (zu hoch oder zu niedrig), löst ONTAP aus, dass der SP das Motherboard ordnungsgemäß herunterfährt. Die serielle Konsole reagiert dann nicht mehr, aber mit Strg+G auf der Konsole ist weiterhin Zugriff auf die SP CLI möglich. Anschließend kann der `system power on`- oder `system power cycle`-Befehl vom SP verwendet werden, um den Knoten einzuschalten oder einen Power-Cycle durchzuführen.

- Der SP überwacht Umweltsensoren und protokolliert Ereignisse, was eine zeitnahe und effektive Durchführung von Servicemaßnahmen ermöglicht.

  Der SP überwacht Umgebungssensoren wie Knotentemperaturen, Spannungen, Ströme und Lüfterdrehzahlen. Wenn ein Umgebungssensor einen anomalen Zustand erreicht, protokolliert der SP die abweichenden Messwerte, benachrichtigt ONTAP über das Problem und sendet bei Bedarf Warnmeldungen und „down system“-Benachrichtigungen über eine AutoSupport-Nachricht, unabhängig davon, ob der Knoten AutoSupport-Nachrichten senden kann.

  Der SP protokolliert außerdem Ereignisse wie den Bootvorgang, Änderungen an Field Replaceable Units (FRU), von ONTAP generierte Ereignisse und den SP-Befehlsverlauf. Eine AutoSupport-Meldung kann manuell ausgelöst werden, um die von einem bestimmten Knoten erfassten SP-Protokolldateien einzubinden.

  Abgesehen davon, dass diese Meldungen im Auftrag eines ausgefallenen Knotens generiert und zusätzliche Diagnoseinformationen an AutoSupport-Meldungen angehängt werden, hat der SP keinen Einfluss auf die AutoSupport-Funktionalität. Die AutoSupport-Konfigurationseinstellungen und das Verhalten des Meldungsinhalts werden von ONTAP übernommen.

  > Der SP ist nicht auf die `-transport` Parametereinstellung des `system node autosupport modify` Befehls angewiesen, um Benachrichtigungen zu senden. Der SP verwendet ausschließlich das Simple Mail Transport Protocol (SMTP) und erfordert, dass die AutoSupport-Konfiguration seines Hosts Informationen zum Mail-Host enthält.

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

- Der SP verfügt über einen nichtflüchtigen Speicherpuffer, der bis zu 4.000 Ereignisse in einem Systemereignisprotokoll (SEL) speichert, um bei der Diagnose von Problemen zu unterstützen.

  Das SEL speichert jeden Revisionsprotokoll-Eintrag als Audit-Ereignis. Es wird im internen Flash-Speicher des SP gespeichert. Die Ereignisliste aus dem SEL wird vom SP automatisch per AutoSupport-Nachricht

an die festgelegten Empfänger gesendet.

Das SEL enthält die folgenden Informationen:

- Vom SP erkannte Hardware-Ereignisse, beispielsweise Sensorstatus zu Netzteilen, Spannung oder anderen Komponenten
- Vom SP erkannte Fehler, beispielsweise ein Kommunikationsfehler, ein Lüfterausfall oder ein Speicher- oder CPU-Fehler
- Kritische Softwareereignisse, die vom Knoten an den SP gesendet werden, zum Beispiel ein Systemabsturz, ein Kommunikationsfehler, ein Startfehler oder ein vom Benutzer ausgelöstes „down system“ infolge der Ausführung des SP `system reset` oder `system power cycle`-Befehls

- Der SP überwacht die serielle Konsole, unabhängig davon, ob Administratoren angemeldet oder mit der Konsole verbunden sind.

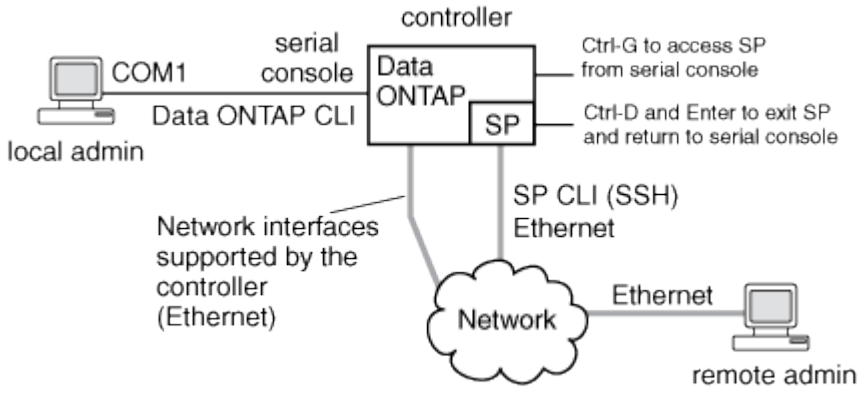
  Wenn Meldungen an die Konsole gesendet werden, speichert der SP diese im Konsole-Protokoll. Das Konsole-Protokoll bleibt so lange erhalten, wie der SP von einem der Knotennetzteile mit Strom versorgt wird. Da der SP mit Standby-Strom arbeitet, bleibt er auch dann verfügbar, wenn der Knoten neu gestartet oder ausgeschaltet wird.

- Eine hardwaregestützte Übernahme ist verfügbar, wenn der SP konfiguriert ist.
- Der SP API-Service ermöglicht ONTAP die Kommunikation mit dem SP über das Netzwerk.

  Der Dienst verbessert die ONTAP Verwaltung des SP durch die Unterstützung netzwerkbasierter Funktionen wie die Verwendung der Netzwerkschnittstelle für das SP Firmware-Update, die Möglichkeit, dass ein Knoten auf die SP-Funktionalität oder die Systemkonsole eines anderen Knotens zugreift, sowie das Hochladen des SP-Protokolls von einem anderen Knoten.

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

Das folgende Diagramm veranschaulicht den Zugriff auf ONTAP und den SP eines Knotens. Auf die SP-Schnittstelle wird über den Ethernet-Port zugegriffen (gekennzeichnet durch ein Schraubenschlüssel-Symbol auf der Rückseite des Gehäuses):



Der ONTAP Baseboard Management Controller ermöglicht die Remoteverwaltung eines Knotens.

Auf bestimmten Hardwareplattformen wird die Software angepasst, um einen neuen

Onboard-Controller im Baseboard Management Controller (BMC) zu unterstützen. Der BMC verfügt über Befehlszeilenbefehle (CLI), mit denen das Gerät remote verwaltet werden kann.

Der BMC funktioniert ähnlich wie der Service Processor (SP) und verwendet viele der gleichen Befehle. Der BMC ermöglicht Folgendes:

- Die BMC-Netzwerkeinstellungen konfigurieren.
- Aus der Ferne kann auf einen Knoten zugegriffen und Knotenverwaltungsaufgaben wie Diagnose, Herunterfahren, Stromzyklus oder Neustart des Knotens durchgeführt werden.

Es bestehen einige Unterschiede zwischen SP und BMC:

- Das BMC steuert die Umgebungsüberwachung von Stromversorgungselementen, Kühlkomponenten, Temperatursensoren, Spannungssensoren und Stromsensoren vollständig. Das BMC meldet Sensordaten über IPMI an ONTAP.
- Einige der Befehle für Hochverfügbarkeit (HA) und Storage unterscheiden sich.
- Das BMC sendet keine AutoSupport-Nachrichten.

Automatische Firmware-Updates sind auch verfügbar, wenn ONTAP mit den folgenden Voraussetzungen betrieben wird:

- Die BMC-Firmware-Revision 1.15 oder höher muss installiert sein.

  Für ein Upgrade der BMC Firmware von Version 1.12 auf 1.15 oder höher ist ein manuelles Update erforderlich.

- BMC startet nach Abschluss eines Firmware-Updates automatisch neu.

  Knotenoperationen werden während eines BMC Neustarts nicht beeinträchtigt.

ONTAP SP/BMC-Firmware-Updates verwalten

ONTAP enthält ein SP Firmware-Image, das als *Baseline-Image* bezeichnet wird. Wenn eine neue Version der SP Firmware später verfügbar ist, besteht die Möglichkeit, diese herunterzuladen und die SP Firmware auf die heruntergeladene Version zu aktualisieren, ohne die ONTAP Version zu aktualisieren.

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

ONTAP bietet die folgenden Methoden zur Verwaltung von SP Firmware-Updates:

- Die automatische Update-Funktionalität des SP ist standardmäßig aktiviert, wodurch die SP-Firmware in den folgenden Szenarien automatisch aktualisiert wird:
  - Beim Upgrade auf eine neue Version von ONTAP

    Der ONTAP Upgrade-Prozess umfasst automatisch das SP Firmware-Update, sofern die mit ONTAP gebündelte SP Firmware-Version neuer ist als die auf dem Knoten ausgeführte SP-Version.

ONTAP erkennt ein fehlgeschlagenes automatisches SP-Update und leitet eine Korrekturmaßnahme ein, um das automatische SP-Update bis zu dreimal zu wiederholen. Wenn alle drei Wiederholungsversuche fehlschlagen, siehe "NetApp Knowledge Base: Health Monitor SPAutoUpgradeFailedMajorAlert SP Upgrade fehlgeschlagen - AutoSupport Message".

- Wenn eine Version der SP Firmware von der NetApp Support-Website heruntergeladen wird und die heruntergeladene Version neuer ist als die Version, die aktuell auf dem SP ausgeführt wird
- Beim Downgrade oder der Rückkehr zu einer früheren Version von ONTAP

  Die SP Firmware wird automatisch auf die neueste kompatible Version aktualisiert, die von der ONTAP Version unterstützt wird, auf die Sie zurückgesetzt oder herabgestuft wurden. Eine manuelle Aktualisierung der SP Firmware ist nicht erforderlich.

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

- ONTAP ermöglicht es Ihnen, ein SP Update manuell auszulösen und mithilfe des `system service-processor image update` Befehls festzulegen, wie das Update durchgeführt werden soll.

  Folgende Optionen können angegeben werden:

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

    Sie können die SP-Firmware auf ein heruntergeladenes Paket aktualisieren, indem Sie den Paketdateinamen angeben. Der `system image package show`Befehl zeigt alle auf einem Knoten verfügbaren Paketdateien an (einschließlich der Dateien für das SP-Firmware-Paket).

  - Ob das Basis SP Firmwarepaket für das SP Update verwendet werden soll (`-baseline`)

    Sie können die SP Firmware auf die Basisversion aktualisieren, die mit der aktuell laufenden Version von ONTAP gebündelt ist.

  Wenn einige der erweiterten Aktualisierungsoptionen oder Parameter verwendet werden, können die Konfigurationseinstellungen des BMC vorübergehend gelöscht werden. Nach dem Neustart kann es bis zu 10 Minuten dauern, bis ONTAP die BMC Konfiguration wiederherstellt.

- ONTAP ermöglicht die Anzeige des Status des neuesten SP-Firmware-Updates, das von ONTAP mit dem `system service-processor image update-progress show` Befehl ausgelöst wurde.

Jegliche bestehende Verbindung zum SP wird getrennt, wenn die SP Firmware aktualisiert wird. Dies ist sowohl bei einer automatisch als auch bei einer manuell ausgelösten SP Firmware-Aktualisierung der Fall.

Verwandte Informationen

"NetApp Downloads: System Firmware und Diagnose"

ONTAP SP/BMC und Netzwerkschnittstelle für Firmware-Updates

Ein SP Firmware-Update, das von ONTAP ausgelöst wird und bei dem auf dem SP die

Version 1.5, 2.5, 3.1 oder höher ausgeführt wird, unterstützt die Verwendung eines IP-basierten Dateiübertragungsmechanismus über die SP Netzwerkschnittstelle.

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

Ein SP-Firmware-Update über die Netzwerkschnittstelle ist schneller als ein Update über die serielle Schnittstelle. Dadurch verkürzt sich das Wartungsfenster, während das SP-Firmware-Update durchgeführt wird, und der ONTAP-Betrieb bleibt zudem unterbrechungsfrei. Die SP Versionen, die diese Funktion unterstützen, sind in ONTAP enthalten. Sie sind außerdem auf der NetApp Support Site verfügbar und können auf Controllern installiert werden, die eine kompatible Version von ONTAP ausführen.

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

- Ein SP-Firmware-Update, das *automatisch* von ONTAP ausgelöst wird, verwendet standardmäßig die Netzwerkschnittstelle für das Update; das automatische SP-Update wechselt jedoch zur Verwendung der seriellen Schnittstelle für das Firmware-Update, wenn eine der folgenden Bedingungen eintritt:
  - Die SP-Netzwerkschnittstelle ist nicht konfiguriert oder nicht verfügbar.
  - Die IP-basierte Dateiübertragung schlägt fehl.
  - Der SP API-Service ist deaktiviert.

Unabhängig von der verwendeten SP-Version nutzt ein über die SP-CLI ausgelöstes SP-Firmware-Update immer die SP Netzwerkschnittstelle für das Update.

Verwandte Informationen

"NetApp Downloads: System Firmware und Diagnose"

Zugriff auf den ONTAP Service Processor mit einem Cluster-Benutzerkonto

Beim Versuch, auf den SP zuzugreifen, wird zur Eingabe von Anmeldeinformationen aufgefordert. Cluster-Benutzerkonten, die mit dem `service-processor` Anwendungstyp erstellt wurden, haben Zugriff auf die SP-CLI auf jedem Knoten des Clusters. SP-Benutzerkonten werden von ONTAP verwaltet und durch Passwort authentifiziert. Ab ONTAP 9.15.1 können SP-Benutzerkonten optional die Zwei-Faktor-Authentifizierung mit einem öffentlichen Schlüssel als zweitem Authentifizierungsverfahren verwenden. Ab ONTAP 9.9.1 müssen SP-Benutzerkonten die `admin` Rolle besitzen.

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 `-application` Parameter des `security login create` Befehls auf `service-processor` gesetzt und der `-authmethod` Parameter auf `password` gesetzt ist. Ab ONTAP 9.15.1 kann optional eine Zwei-Faktor-Authentifizierung für ein SP-Konto konfiguriert werden, indem das zweite Authentifizierungsverfahren auf `publickey` mit dem `security login modify` Befehl gesetzt und anschließend der öffentliche Schlüssel mit dem `security login publickey create` Befehl verknüpft wird.

Sie müssen den `-role` Parameter bei der Erstellung eines SP Benutzerkontos angeben.

- In ONTAP 9.9.1 und späteren Versionen muss `admin` für den `-role` Parameter angegeben werden, und

jede Änderung an einem Konto erfordert die `admin` Rolle. Aus Sicherheitsgründen sind andere Rollen nicht mehr zulässig.

  - Wenn ein Upgrade auf ONTAP 9.9.1 oder eine spätere Version durchgeführt wird, siehe "Änderung der Benutzerkonten, die auf den Service Processor zugreifen können".
  - Wenn auf ONTAP 9.8 oder frühere Versionen zurückgegangen wird, siehe "Benutzerkonten, die auf den Serviceprozessor zugreifen können, überprüfen".

- In ONTAP 9.8 und früheren Versionen kann jede Rolle auf den SP zugreifen, aber `admin` wird empfohlen.

Standardmäßig umfasst das Cluster-Benutzerkonto mit dem Namen “admin” den `service-processor` Anwendungstyp und hat Zugriff auf den SP.

ONTAP verhindert die Erstellung von Benutzerkonten mit für das System reservierten Namen (wie „root“ und „naroot“). Ein für das System reservierter Name kann nicht für den Zugriff auf den Cluster oder den SP verwendet werden.

Die aktuellen SP Benutzerkonten lassen sich mit dem `-application service-processor`Parameter des `security login show`Befehls anzeigen.

Weitere Informationen zu `security login modify`, `security login publickey create` und `security login show` finden sich in der ONTAP Befehlsreferenz.

Zugriff auf das ONTAP SP/BMC eines Knotens von einem Administrationshost

Sie können sich von einem Administrationshost aus beim SP eines Knotens anmelden, um Knotenverwaltungsaufgaben remote durchzuführen.

Bevor Sie beginnen

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.

  Um auf den SP zuzugreifen, muss Ihr Benutzerkonto mit dem `-application` Parameter des `security login create` Befehls auf `service-processor` und dem `-authmethod` Parameter auf `password` erstellt worden sein.

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

Wenn der SP für die Verwendung einer IPv4- oder IPv6-Adresse konfiguriert ist und fünf SSH-Anmeldeversuche von einem Host innerhalb von 10 Minuten fehlschlagen, weist der SP die SSH-Anmeldeanfragen zurück und setzt die Kommunikation mit der IP-Adresse des Hosts für 15 Minuten aus. Nach 15 Minuten wird die Kommunikation wieder aufgenommen, und ein erneuter Anmeldeversuch beim SP ist möglich.

ONTAP verhindert die Erstellung oder Verwendung von systemreservierten Namen (wie “root” und “naroot”) für den Zugriff auf den Cluster oder den SP.

Schritte

1. Vom Administrationshost aus beim SP anmelden:

   `ssh username@SP_IP_address`

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

   Die SP-Eingabeaufforderung erscheint, was anzeigt, dass Sie Zugriff auf die SP CLI haben.

Beispiele für SP Zugriff von einem Administrationshost

Das folgende Beispiel zeigt, wie Sie sich beim SP mit einem Benutzerkonto `joe` anmelden, das für den Zugriff auf den SP eingerichtet wurde.

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

Die folgenden Beispiele zeigen, wie die globale IPv6-Adresse oder die vom Router angekündigte IPv6-Adresse verwendet werden kann, um sich beim SP auf einem Node anzumelden, auf dem SSH für IPv6 eingerichtet ist und der SP für IPv6 konfiguriert ist.

```
[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>
```

Zugriff auf das ONTAP SP/BMC eines Knotens von der Systemkonsole

Auf den SP kann über die Systemkonsole (auch serielle Konsole genannt) zugegriffen werden, um Überwachungs- oder Fehlerbehebungsaufgaben durchzuführen.

Über diese Aufgabe

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

Schritte

1. Auf die SP CLI kann über die Systemkonsole zugegriffen werden, indem an der Eingabeaufforderung Strg+G gedrückt wird.
2. Melden Sie sich bei der SP CLI an, wenn Sie dazu aufgefordert werden.

   Die SP-Eingabeaufforderung erscheint, was anzeigt, dass Sie Zugriff auf die SP CLI haben.

3. Die SP CLI wird beendet und zur Systemkonsole zurückgekehrt, indem Strg+D gedrückt und anschließend die Eingabetaste betätigt wird.

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

Das folgende Beispiel zeigt das Ergebnis des Drückens von Strg+G in der Systemkonsole, um auf die SP CLI zuzugreifen. Der `help system power` Befehl wird an der SP Eingabeaufforderung eingegeben, gefolgt von Strg+D und anschließend der Eingabetaste, um zur Systemkonsole zurückzukehren.

```
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 dann die Eingabetaste, um zur Systemkonsole zurückzukehren.)

```
cluster1::>
```

Wie die ONTAP SP CLI, SP Konsole und Systemkonsolensitzungen zusammenhängen

Sie können eine SP-CLI-Sitzung öffnen, um einen Knoten remote zu verwalten, und eine separate SP-Konsolensitzung öffnen, um auf die Konsole des Knotens zuzugreifen. Die SP-Konsolensitzung spiegelt die Ausgabe wider, die in einer gleichzeitig laufenden Systemkonsolensitzung angezeigt wird. Der SP und die Systemkonsole verfügen über unabhängige Shell-Umgebungen mit unabhängiger Authentifizierung.

Das Verständnis, wie die SP-CLI-, SP-Konsolen- und Systemkonsolen-Sitzungen miteinander zusammenhängen, unterstützt bei der Remoteverwaltung eines Knotens. Im Folgenden wird die Beziehung zwischen den Sitzungen beschrieben:

- Nur ein Administrator kann sich gleichzeitig in die SP CLI-Sitzung einloggen; jedoch ermöglicht der SP, sowohl eine SP CLI-Sitzung als auch eine separate SP-Konsolensitzung gleichzeitig zu öffnen.

  Die SP CLI wird durch die SP-Eingabeaufforderung (`SP>` angezeigt. Aus einer SP CLI-Sitzung kann mit dem SP `system console`-Befehl eine SP-Konsolensitzung initiiert werden. Gleichzeitig kann eine separate SP CLI-Sitzung über SSH gestartet werden. Beim Drücken von Strg+D zum Beenden der SP-Konsolensitzung erfolgt automatisch die Rückkehr zur SP CLI-Sitzung. Falls bereits eine SP CLI-Sitzung besteht, erscheint eine Meldung mit der Nachfrage, ob die bestehende SP CLI-Sitzung beendet werden soll. Bei Eingabe von „y“ wird die bestehende SP CLI-Sitzung beendet, sodass eine Rückkehr von der SP Konsole zur SP CLI möglich ist. Diese Aktion wird im SP-Ereignisprotokoll aufgezeichnet.

  In einer ONTAP CLI-Sitzung, die über SSH verbunden ist, kann zur Systemkonsole eines Knotens gewechselt werden, indem der ONTAP `system node run-console` Befehl von einem anderen Knoten ausgeführt wird.

- Aus Sicherheitsgründen verfügen die SP CLI-Sitzung und die Systemkonsolensitzung über eine unabhängige Authentifizierung.

  Wenn eine SP-Konsolensitzung von der SP-CLI (mithilfe des SP `system console` Befehls) initiiert wird, erfolgt eine Aufforderung zur Eingabe der Systemkonsolen-Anmeldeinformationen. Beim Zugriff auf die SP-CLI aus einer Systemkonsolensitzung (durch Drücken von Strg+G) erfolgt eine Aufforderung zur Eingabe der SP-CLI-Anmeldeinformationen.

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

  Die SP-Konsolensitzung spiegelt die Ausgabe einer gleichzeitig laufenden Systemkonsolensitzung wider. Die gleichzeitig laufende Systemkonsolensitzung spiegelt jedoch nicht die SP-Konsolensitzung wider.

  Die SP-Konsolensitzung spiegelt die Ausgabe gleichzeitig laufender SSH-Sitzungen nicht wider.

Die IP-Adresse des Administrationshosts wird hinzugefügt, um auf den ONTAP Service Processor zuzugreifen.

Standardmäßig akzeptiert der SP SSH-Verbindungsanfragen von Administrationshosts mit beliebigen IP-Adressen. Der SP kann so konfiguriert werden, dass er SSH-Verbindungsanfragen nur von Administrationshosts mit den von Ihnen angegebenen IP-Adressen akzeptiert. Die vorgenommenen Änderungen gelten für den SSH-Zugriff auf den SP aller Knoten im Cluster.

Schritte

1. SP-Zugriff wird nur den von Ihnen angegebenen IP-Adressen gewährt, indem der `system service-processor ssh add-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter verwendet wird.
   - Der Wert des `-allowed-addresses` Parameters muss im Format `address/netmask` angegeben werden, und mehrere `address/netmask` Paare müssen durch Kommas getrennt werden, zum Beispiel `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

     Das Setzen des `-allowed-addresses`Parameters auf `0.0.0.0/0, ::/0`ermöglicht allen IP-Adressen den Zugriff auf den SP (Standard).

   - Wenn die Standardeinstellung geändert wird, indem der SP-Zugriff auf nur die von Ihnen angegebenen IP-Adressen beschränkt wird, fordert ONTAP Sie auf zu bestätigen, dass die angegebenen IP-Adressen die Standardeinstellung „`allow all`“ ersetzen (`0.0.0.0/0, ::/0`).
   - Der `system service-processor ssh show`Befehl zeigt die IP-Adressen an, die auf den SP zugreifen können.
2. Wenn eine bestimmte IP-Adresse vom Zugriff auf den SP ausgeschlossen werden soll, ist der `system service-processor ssh remove-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter zu verwenden.

   Wenn alle IP-Adressen vom Zugriff auf den SP ausgeschlossen werden, ist der SP von keinem Administrationshost mehr erreichbar.

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

Die folgenden Beispiele zeigen die Standardeinstellung für den SSH-Zugriff auf den SP, die Standardeinstellung wird geändert, indem der SP-Zugriff auf nur die angegebenen IP-Adressen beschränkt wird, die angegebenen IP-Adressen aus der Zugriffsliste entfernt werden und anschließend 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
```

Die Hilfeinformationen in der ONTAP SP/BMC CLI anzeigen

Die Online-Hilfe zeigt die SP/BMC CLI-Befehle und Optionen an.

Über diese Aufgabe

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

Schritte

1. Hilfeinformationen zu den SP/BMC-Befehlen werden mit folgendem Befehl angezeigt:

Um auf die SP-Hilfe zuzugreifen…	Um auf die BMC-Hilfe zuzugreifen…
Geben Sie `help` an der SP-Eingabeaufforderung ein.	Geben Sie `system` an der BMC-Eingabeaufforderung ein.

Das folgende Beispiel zeigt die Online-Hilfe der SP CLI.

```
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 Online-Hilfe der BMC CLI.

```
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 Hilfeinformationen zu einer Option eines SP/BMC-Befehls anzuzeigen, `help` vor oder nach dem SP/BMC-Befehl eingeben.

   Das folgende Beispiel zeigt die SP CLI Online-Hilfe für den SP `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 BMC CLI Online-Hilfe 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>
```

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Ereignisse"
- "Systemstromversorgung"

ONTAP Befehle für die Remote-Knotenverwaltung

Sie können Knotenverwaltungsaufgaben remote ausführen, indem Sie entweder auf den SP zugreifen und SP-CLI-Befehle ausführen oder auf den BMC zugreifen und BMC-CLI-Befehle ausführen. Für mehrere häufig durchgeführte Remote-Knotenverwaltungsaufgaben können auch ONTAP-Befehle von einem anderen Knoten im Cluster verwendet werden. Einige SP- und BMC-Befehle sind plattformspezifisch und möglicherweise auf Ihrer Plattform nicht verfügbar.

Bestimmte Befehlstypen können sowohl in SP als auch in BMC Befehlssätzen verwendet werden. Die Unterschiede zwischen ihnen werden beim Eingeben der Befehlszeile angezeigt.

Beispiele

- Der `help` Befehl in SP: `SP> help`
- Der `help` Befehl in BMC: `BMC> help`

Erfahren Sie mehr über die `help` Befehlsoptionen für SP und BMC in "Die Hilfeinformationen in der ONTAP SP/BMC CLI anzeigen".

Erfahren Sie mehr über die entsprechende ONTAP BMC CLI in "Unterstützte CLI-Befehle für den ONTAP Baseboard Management Controller".

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
Verfügbare Befehle oder Unterbefehle eines bestimmten Befehls für SP/BMC/ONTAP	`help` [`command`]	`help` [`command`]	k. A.
Die aktuelle Berechtigungsstufe für die SP/BMC/ONTAP CLI anzeigen	`priv show`	`priv show`	k. A.
Die Berechtigungsstufe wird festgelegt, um Zugriff auf den angegebenen Modus für die SP/BMC/ONTAP Befehlszeile zu erhalten.	`priv set` {`admin`	`advanced`	`diag`}
`priv set` {`admin`	`advanced`	`diag`	`test`}
k. A.	Systemdatum und -uhrzeit anzeigen	`date`	`date`
`date`	Anzeige von Ereignissen, die vom SP/BMC/ONTAP protokolliert werden	`events` {`all`	`info`
`newest number`	`oldest number`	`search keyword`}	`events` {`all`
`info`	`newest`	`oldest`	`search` }
k. A.	SP/BMC/ONTAP Status und Netzwerkkonfigurationsinformationen	`sp status` [`-v`	`-d`] * Die `-v` Option zeigt SP Statistiken in ausführlicher Form an. * Die `-d` Option fügt das SP Debug-Protokoll zur Anzeige hinzu.
`bmc status` [`-v`	`-d`] * Die `-v` Option zeigt SP Statistiken in ausführlicher Form an. * Die `-d` Option fügt das SP Debug-Protokoll zur Anzeige hinzu.	`system service-processor show`	Die Laufzeit des SP/BMC/ONTAP und die durchschnittliche Anzahl der Aufträge in der Ausführungswarteschlange während der letzten 1, 5 und 15 Minuten werden angezeigt.
`sp uptime`	`bmc uptime`	k. A.	Systemkonsolenprotokolle anzeigen

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
`system log`	`system log` [`-a`]	`system log` (gibt Systemkonsolenprotokolle aus)	Anzeige der SP/BMC/ONTAP-Protokollarchive oder der Dateien in einem Archiv
`sp log history show` [`-archive {latest`	{`all`	`archive-name}] [-dump {all`	`file-name}]`
`bmc log history show` [`-archive {latest`	{`all`	`archive-name}] [-dump {all`	`file-name}]`
k. A.	Den Energiestatus des Controllers eines Knotens anzeigen	`system power status`	`system power status`
`system node power show`	Akkuinformationen	`system battery show`	`system battery show`
k. A.	Anzeige von ACP-Informationen oder dem Status von Expandersensoren	`system acp` [`show`	`sensors show]`
k. A.	k. A.	Alle System-FRUs und deren IDs auflisten	`system fru list`
`system fru list`	k. A.	Produktinformationen für die angegebene FRU werden angezeigt	`system fru show fru_id`
`system fru show` [`show <id>]`	k. A.	FRU-Datenverlaufsprotokoll anzeigen	`system fru log show` (Erweiterte Berechtigungsstufe)

`system fru log show`	k. A.	Der Status der Umweltsensoren wird angezeigt, einschließlich ihrer Zustände und aktuellen Werte	`system sensors`
			
			oder
			
			`system sensors show`

`system sensors` {`show`	`filter <sensor_string> }`	`system node environment sensors show`	Status und Details des angegebenen Sensors anzeigen

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
`system sensors get sensor_name` Sie können `sensor_name` mit dem `system sensors`- oder dem `system sensors show`-Befehl erhalten.	`system sensors` [`get`]	k. A.	Anzeige der SP/BMC/ONTAP-Firmware-Versionsinformationen
`version`	`version`	`system service-processor image show`	SP/BMC/ONTAP-Befehlsverlauf anzeigen
`sp log audit` (Erweiterte Berechtigungsstufe)	`bmc log audit` (Erweiterte Berechtigungsstufe)	k. A.	SP/BMC/ONTAP-Debug-Informationen anzeigen
`sp log debug` (Erweiterte Berechtigungsstufe)	`bmc log debug` (Erweiterte Berechtigungsstufe)	k. A.	Die Datei mit den SP/BMC/ONTAP-Meldungen anzeigen
`sp log messages` (Erweiterte Berechtigungsstufe)	`bmc log messages` (Erweiterte Berechtigungsstufe)	k. A.	Die Einstellungen für die Erfassung von Systemforensikdaten bei einem Watchdog-Reset-Ereignis anzeigen, die während eines Watchdog-Reset-Ereignisses erfassten Systemforensikdaten anzeigen oder die erfassten Systemforensikdaten löschen
`system forensics` [`show`	`log dump`	`log clear`]	k. A.
k. A.	Anmeldung an der Systemkonsole	`system console`	`system console`
`system node run-console`	Zum Beenden der Systemkonsolensitzung sollte Strg+D gedrückt werden.	Den Knoten ein- oder ausschalten oder einen Neustart durchführen (die Stromzufuhr ausschalten und dann wieder einschalten)	`system power on`

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
`system power on`	`system node power on` (Erweiterte Berechtigungsstufe)	`system power off`	`system power off`
k. A.	`system power cycle`	`system power cycle`	k. A.

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
Die Standby-Stromversorgung bleibt eingeschaltet, um den SP ohne Unterbrechung in Betrieb zu halten. Während des Power-Cycles tritt eine kurze Pause auf, bevor die Stromversorgung wieder eingeschaltet wird. Die Verwendung dieser Befehle zum Ausschalten oder Neustarten des Knotens kann zu einem unsachgemäßen Herunterfahren des Knotens (auch als *dirty shutdown* bezeichnet) führen und ist kein Ersatz für ein ordnungsgemäßes Herunterfahren mit dem ONTAP `system node halt` Befehl.	Einen Core Dump erstellen und den Knoten zurücksetzen	`system core [-f]` Die `-f` Option erzwingt die Erstellung eines Core-Dumps und das Zurücksetzen des Knotens.	`system core`

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
`system node coredump trigger` (Erweiterte Berechtigungsstufe)	Diese Befehle haben dieselbe Wirkung wie das Drücken der Non-maskable Interrupt (NMI) Taste an einem Knoten, was ein unsauberes Herunterfahren des Knotens verursacht und beim Anhalten des Knotens einen Speicherauszug der Core-Dateien erzwingt. Diese Befehle sind hilfreich, wenn ONTAP auf dem Knoten hängt oder nicht auf Befehle wie `system node shutdown` reagiert. Die generierten Core-Dump-Dateien werden in der Ausgabe des `system node coredump show` Befehls angezeigt. Der SP bleibt betriebsbereit, solange die Stromversorgung des Knotens nicht unterbrochen wird.	Der Knoten kann mit einem optional angegebenen BIOS-Firmware-Image (primär, Backup oder aktuell) neu gestartet werden, um Probleme wie ein beschädigtes Image des Boot-Geräts des Knotens zu beheben.	`system reset` {`primary`
`backup`	`current`}	`system reset` { `current`	`primary`
`backup` }	`system node reset` mit dem `-firmware {primary`	`backup`	`current`} Parameter (Erweiterte Berechtigungsstufe)

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
Dieser Vorgang führt zu einem unsauberen Herunterfahren des Knotens. Wird kein BIOS-Firmware-Image angegeben, wird das aktuelle Image für den Neustart verwendet. Der SP bleibt betriebsbereit, solange die Stromversorgung des Knotens nicht unterbrochen wird.	Das aktuelle Battery Firmware Image mit einem angegebenen Firmware Image vergleichen	`system battery verify` [`image_URL`] (Erweiterte Berechtigungsstufe) Wenn `image_URL` nicht angegeben ist, wird zum Vergleich das Standard-Batterie-Firmware-Image verwendet.	`system battery verify` [`image_URL`] (Erweiterte Berechtigungsstufe) Wenn `image_URL` nicht angegeben ist, wird zum Vergleich das Standard-Batterie-Firmware-Image verwendet.
k. A.	Die Batterie-Firmware wird mit dem Image am angegebenen Speicherort aktualisiert	`system battery flash` [`image_URL`] (Erweiterte Berechtigungsstufe) Dieser Befehl wird verwendet, wenn der automatische Firmware-Aktualisierungsprozess für den Akku aus irgendeinem Grund fehlgeschlagen ist.	k. A.

k. A.	Die SP/BMC/ONTAP-Firmware wird mithilfe des Images am angegebenen Speicherort aktualisiert.	`sp update`
		
		`image_URL`
		
		`image_URL` darf 200 Zeichen nicht überschreiten.
			`bmc update`
			
			`image_URL`
			
			`image_URL` darf 200 Zeichen nicht überschreiten.

`system service-processor image update`	SP/BMC/ONTAP neu starten	`sp reboot`	`bmc reboot`

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
`system service-processor reboot-sp`	Den Inhalt des NVRAM-Flashspeichers löschen	`system nvram flash clear` (Erweiterte Berechtigungsstufe) Dieser Befehl kann nicht ausgeführt werden, wenn die Stromversorgung des Controllers ausgeschaltet ist (`system power off`).	k. A.
k. A.	Die SP/BMC/ONTAP-CLI verlassen	`exit`	`exit`

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

ONTAP Knotenzustandsüberwachung anhand schwellenwertbasierter SP Sensormesswerte und Status

Schwellenwertbasierte Sensoren erfassen regelmäßig Messwerte verschiedener Systemkomponenten. Das SP vergleicht den Messwert eines schwellenwertbasierten Sensors mit seinen voreingestellten Schwellenwerten, die die zulässigen Betriebsbedingungen einer Komponente definieren.

Basierend auf den Sensormesswerten zeigt das SP den Sensorstatus an, um die Überwachung des Zustands der Komponente zu unterstützen.

Beispiele für schwellenwertbasierte Sensoren sind Sensoren für Systemtemperaturen, Spannungen, Ströme und Lüfterdrehzahlen. Die genaue Liste der schwellenwertbasierten Sensoren hängt von der jeweiligen Plattform ab.

Schwellenwertbasierte Sensoren haben die folgenden Schwellenwerte, die in der Ausgabe des SP `system sensors`-Befehls angezeigt werden:

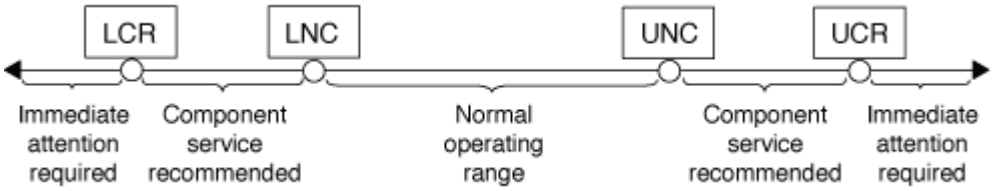
- Untere kritische Grenze (LCR)
- Niedriger nichtkritischer (LNC)
- Oberer nichtkritischer Bereich (UNC)
- Oberer kritischer Wert (UCR)

Ein Messwert zwischen LNC und LCR oder zwischen UNC und UCR bedeutet, dass die Komponente Anzeichen eines Problems zeigt und ein Systemausfall als Folge auftreten könnte. Daher sollte eine Wartung der Komponente in naher Zukunft eingeplant werden.

Ein Messwert unterhalb des LCR-Werts oder oberhalb des UCR-Werts bedeutet, dass die Komponente fehlerhaft arbeitet und ein Systemausfall unmittelbar bevorsteht. Daher erfordert die Komponente sofortige

Aufmerksamkeit.

Das folgende Diagramm veranschaulicht die durch die Schwellenwerte festgelegten Schweregrade:



Die Messwerte eines schwellenwertbasierten Sensors sind unter der `Current` Spalte in der `system sensors` Befehlsausgabe zu finden. Der `system sensors get sensor_name` Befehl zeigt zusätzliche Details für den angegebenen Sensor an. Wenn der Messwert eines schwellenwertbasierten Sensors die nichtkritischen und kritischen Schwellenwertbereiche überschreitet, meldet der Sensor ein Problem mit zunehmendem Schweregrad. Wenn der Messwert einen Schwellenwert überschreitet, ändert sich der Status des Sensors in der `system sensors` Befehlsausgabe von `ok` auf `nc` (nichtkritisch) oder `cr` (kritisch), abhängig vom überschrittenen Schwellenwert, und eine Ereignismeldung wird im SEL-Ereignisprotokoll protokolliert.

Einige schwellenwertbasierte Sensoren verfügen nicht über alle vier Schwellenwerte. Bei diesen Sensoren werden die fehlenden Schwellenwerte als `na` Grenzwerte in der `system sensors` Befehlsausgabe angezeigt, was darauf hinweist, dass für den jeweiligen Sensor hinsichtlich des angegebenen Schwellenwerts kein Grenzwert oder Schweregrad besteht und der SP den Sensor für diesen Schwellenwert nicht überwacht.

Beispiel für die Befehlsausgabe des system sensors-Kommandos

Das folgende Beispiel zeigt einige der Informationen, die vom `system sensors` Befehl in der SP CLI angezeigt werden:

```
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 für die Ausgabe des Befehls system sensors sensor_name für einen schwellenwertbasierten Sensor

Das folgende Beispiel zeigt das Ergebnis der Eingabe `system sensors get sensor_name` in die 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+
```

ONTAP SP Sensorstatuswerte in der Systemsensor-Befehlsausgabe

Diskrete Sensoren haben keine Schwellenwerte. Ihre Messwerte, die unter der `Current` Spalte in der SP-CLI `system sensors`-Befehlsausgabe angezeigt werden, haben keine tatsächliche Bedeutung und werden daher vom SP ignoriert. Die `Status` Spalte in der

`system sensors`-Befehlsausgabe zeigt die Statuswerte diskreter Sensoren im Hexadezimalformat an.

Beispiele für diskrete Sensoren sind Sensoren für Lüfterfehler, Netzteilfehler (PSU) und Systemfehler. Die genaue Liste der diskreten Sensoren hängt von der Plattform ab.

Sie können den SP CLI `system sensors get sensor_name` Befehl zur Unterstützung bei der Interpretation der Statuswerte der meisten diskreten Sensoren verwenden. Die folgenden Beispiele zeigen die Ergebnisse der Eingabe von `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` Befehl die Statusinformationen für die meisten diskreten Sensoren anzeigt, liefert er keine Statusinformationen für die diskreten Sensoren System_FW_Status, System_Watchdog, PSU1_Input_Type und PSU2_Input_Type. Die folgenden Informationen dienen zur Interpretation der Statuswerte dieser Sensoren.

System_FW_Status

Der Zustand des Sensors System_FW_Status wird in Form von `0xAABB` angezeigt. Die Informationen von `AA` und `BB` können kombiniert werden, um den Zustand des Sensors zu bestimmen.

`AA` kann einen der folgenden Werte annehmen:

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

`BB` kann einen der folgenden Werte annehmen:

Werte	Zustand des Sensors
00	Die Systemsoftware wurde ordnungsgemäß heruntergefahren
01	Speicherinitialisierung läuft
02	NVMEM-Initialisierung läuft (wenn NVMEM vorhanden ist)
04	Wiederherstellen der Werte des Speichercontroller-Hubs (MCH) (wenn NVMEM vorhanden ist)
05	Benutzer hat Setup aufgerufen
13	Starten des Betriebssystems oder des LOADER
1F	BIOS wird gestartet
20	LOADER läuft
21	Der LOADER programmiert die primäre BIOS-Firmware. Das System darf nicht heruntergefahren werden.
22	Der LOADER programmiert die alternative BIOS-Firmware. Das System darf nicht heruntergefahren werden.
2F	ONTAP läuft
60	SP hat das System ausgeschaltet
61	SP hat das System eingeschaltet
62	SP hat das System zurückgesetzt
63	SP Watchdog Power Cycle
64	SP Watchdog Kaltreset

Beispielsweise bedeutet der System_FW_Status Sensorstatus 0x042F „System-Firmware-Fortschritt (04), ONTAP läuft (2F)“.

System_Watchdog

Der System_Watchdog Sensor kann einen der folgenden Zustände aufweisen:

- **0x0080**

  Der Zustand dieses Sensors hat sich nicht geändert

Werte	Zustand des Sensors
0x0081	Timer-Interrupt
0x0180	Zeitüberschreitung
0x0280	Hard Reset
0x0480	Strom abschalten
0x0880	Stromkreislauf

Beispielsweise bedeutet der System_Watchdog Sensorstatus 0x0880, dass eine Watchdog Zeitüberschreitung

auftritt und einen Systemneustart auslöst.

PSU1_Input_Type und PSU2_Input_Type

Bei Gleichstromnetzteilen (DC) sind die Sensoren PSU1_Input_Type und PSU2_Input_Type nicht relevant. Bei Wechselstromnetzteilen (AC) können die Sensoren einen der folgenden Statuswerte annehmen:

Werte	Zustand des Sensors
0x01 xx	220V Netzteiltyp
0x02 xx	110V Netzteiltyp

Beispielsweise bedeutet der Sensorstatus PSU1_Input_Type 0x0280, dass der Sensor meldet, dass der Netzteiltyp 110V ist.

ONTAP Befehle für das Service Processor Management

ONTAP stellt Befehle zur Verwaltung des SP bereit, einschließlich der SP Netzwerkkonfiguration, SP Firmware Image, des SSH Zugriffs auf den SP und der allgemeinen SP Administration.

Befehle zur Verwaltung der SP Netzwerkkonfiguration

Wenn Sie möchten…	Diesen ONTAP Befehl ausführen…
Die SP automatische Netzwerkkonfiguration ermöglicht dem SP die Nutzung der IPv4 oder IPv6 Adressfamilie des angegebenen Subnetzes.	`system service-processor network auto-configuration enable`
Die automatische SP Netzwerkkonfiguration für die IPv4- oder IPv6-Adressfamilie des für den SP angegebenen Subnetzes deaktivieren	`system service-processor network auto-configuration disable`
Anzeige der automatischen SP-Netzwerkkonfiguration	`system service-processor network auto-configuration show`
Das SP Netzwerk für einen Knoten kann manuell konfiguriert werden, einschließlich Folgendem: • Die IP-Adressfamilie (IPv4 oder IPv6) • Ob die Netzwerkschnittstelle der angegebenen IP-Adressfamilie aktiviert werden sollte • Wenn Sie IPv4 verwenden, ob die Netzwerkkonfiguration vom DHCP-Server oder die von Ihnen angegebene Netzwerkadresse verwendet wird • Die öffentliche IP-Adresse für den SP • Die Netzmaske für den SP (bei Verwendung von IPv4) • Die Netzwerkpräfixlänge der Subnetzmaske für den SP (bei Verwendung von IPv6) • Die Gateway-IP-Adresse für den SP	`system service-processor network modify`

Wenn Sie möchten…	Diesen ONTAP Befehl ausführen…
Die SP Netzwerkkonfiguration wird angezeigt, einschließlich der folgenden: • Die konfigurierte Adressfamilie (IPv4 oder IPv6) und ob sie aktiviert ist • Der Typ des Fernverwaltungsgeräts • Der aktuelle SP Status und Verbindungsstatus • Netzwerkkonfiguration, wie z. B. IP-Adresse, MAC-Adresse, Netzmaske, Präfixlänge der Subnetzmaske, vom Router zugewiesene IP-Adresse, Link-Local-IP-Adresse und Gateway-IP-Adresse • Zeitpunkt der letzten Aktualisierung des SP • Der Name des Subnetzes, das für die automatische SP-Konfiguration verwendet wird • Ob die vom IPv6-Router zugewiesene IP-Adresse aktiviert ist • SP Netzwerk-Setup-Status • Grund für das Fehlschlagen der SP-Netzwerkeinrichtung	`system service-processor network show` Die vollständigen SP Netzwerkdetails werden angezeigt, wenn der `-instance` Parameter verwendet wird.
Die SP API-Service-Konfiguration einschließlich der folgenden Punkte anpassen: • Ändern des vom SP API-Service verwendeten Ports • Aktivieren oder Deaktivieren des SP API-Service	`system service-processor api-service modify` (Erweiterte Berechtigungsstufe)
Anzeigen der SP API-Service-Konfiguration	`system service-processor api-service show` (Erweiterte Berechtigungsstufe)
Die SSL- und SSH-Zertifikate, die vom SP API-Service für die interne Kommunikation verwendet werden, erneuern.	• Für ONTAP 9.5 oder höher: `system service-processor api-service renew-internal-certificates` • Für ONTAP 9.4 oder älter: `system service-processor api-service renew-certificates` (Erweiterte Berechtigungsstufe)

Befehle zur Verwaltung des SP Firmware-Images

Wenn Sie möchten…	Diesen ONTAP Befehl ausführen…
Die Details des aktuell installierten SP-Firmware-Images werden angezeigt, einschließlich der folgenden: • Der Typ des Fernverwaltungsgeräts • Das Image (primär oder Backup), von dem der SP gebootet wird, sein Status und die Firmware-Version • Ob die automatische Firmware-Aktualisierung aktiviert ist und der letzte Aktualisierungsstatus	`system service-processor image show` Der `-is-current`Parameter gibt das Image (primär oder Backup) an, von dem der SP aktuell gebootet ist, nicht ob die installierte Firmware-Version die aktuellste ist.
Automatische Firmware-Aktualisierung für SP aktivieren oder deaktivieren	`system service-processor image modify` Standardmäßig wird die SP-Firmware automatisch mit der Aktualisierung von ONTAP oder beim manuellen Herunterladen einer neuen Version der SP-Firmware aktualisiert. Es wird nicht empfohlen, die automatische Aktualisierung zu deaktivieren, da dies zu suboptimalen oder nicht qualifizierten Kombinationen zwischen dem ONTAP Image und dem SP Firmware-Image führen kann.
Manuelles Herunterladen eines SP-Firmware-Images auf einen Knoten	`system node image get` Bevor Sie die `system node image`Befehle ausführen, muss die Berechtigungsstufe auf „`advanced (`set -privilege advanced`“ gesetzt werden, wobei bei entsprechender Aufforderung **y** einzugeben ist, um fortzufahren. Das SP Firmware-Image ist mit ONTAP gebündelt. Ein manueller Download der SP Firmware ist nicht erforderlich, es sei denn, eine andere SP Firmware-Version als die mit ONTAP gebündelte soll verwendet werden.
Der Status des neuesten von ONTAP ausgelösten SP-Firmware-Updates wird angezeigt, einschließlich der folgenden Informationen: • Start- und Endzeitpunkt des neuesten SP Firmware-Updates • Ob ein Update läuft und der Prozentsatz des Abschlusses	`system service-processor image update-progress show`

Befehle zur Verwaltung des SSH-Zugriffs auf den SP

Wenn Sie möchten…	Diesen ONTAP Befehl ausführen…
SP erhält nur für die angegebenen IP-Adressen Zugriff.	`system service-processor ssh add-allowed-addresses`
Der Zugriff der angegebenen IP-Adressen auf den SP wird blockiert	`system service-processor ssh remove-allowed-addresses`
Die IP-Adressen, die auf den SP zugreifen können, anzeigen	`system service-processor ssh show`

Befehle für die allgemeine SP Verwaltung

Wenn Sie möchten…	Diesen ONTAP Befehl ausführen…
Allgemeine SP-Informationen, einschließlich der folgenden, werden angezeigt: • Der Typ des Fernverwaltungsgeräts • Der aktuelle SP Status • Ob das SP Netzwerk konfiguriert ist • Netzwerkinformationen, wie die öffentliche IP-Adresse und die MAC-Adresse • Die SP-Firmware-Version und die Intelligent Platform Management Interface (IPMI)-Version • Ob die automatische SP-Firmware-Aktualisierung aktiviert ist	`system service-processor show`Die Anzeige vollständiger SP-Informationen erfordert den `-instance`Parameter.
Der SP auf einem Knoten wird neu gestartet.	`system service-processor reboot-sp`
Eine AutoSupport-Nachricht generieren und senden, die die vom angegebenen Node erfassten SP-Protokolldateien enthält	`system node autosupport invoke-splog`
Die Zuordnungskarte der gesammelten SP-Protokolldateien im Cluster wird angezeigt, einschließlich der Sequenznummern der SP-Protokolldateien, die sich auf jedem Sammelknoten befinden.	`system service-processor log show-allocations`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

ONTAP Befehle für BMC Management

Diese ONTAP Befehle sind auf dem Baseboard Management Controller (BMC) verfügbar.

Der BMC verwendet einige der gleichen Befehle wie der Service Processor (SP). Die folgenden SP-Befehle werden auf dem BMC unterstützt.

Wenn Sie möchten…	Verwenden Sie diesen Befehl
BMC-Informationen anzeigen	**`system service-processor show`**

Wenn Sie möchten…	Verwenden Sie diesen Befehl
BMC Netzwerkkonfiguration anzeigen/ändern	**system service-processor network show/modify**
Den BMC zurücksetzen	**system service-processor reboot-sp**
Details des aktuell installierten BMC-Firmware-Images anzeigen/ändern	**system service-processor image show/modify**
BMC Firmware aktualisieren	**system service-processor image update**
Status des neuesten BMC Firmware-Updates anzeigen	**system service-processor image update-progress show**
Die automatische Netzwerkkonfiguration für den BMC aktivieren, um eine IPv4- oder IPv6-Adresse im angegebenen Subnetz zu verwenden.	**system service-processor network auto-configuration enable**
Die automatische Netzwerkkonfiguration für eine IPv4- oder IPv6-Adresse im für den BMC angegebenen Subnetz deaktivieren	**system service-processor network auto-configuration disable**
Anzeige der automatischen BMC-Netzwerkkonfiguration	**system service-processor network auto-configuration show**

Für Befehle, die von der BMC Firmware nicht unterstützt werden, wird die folgende Fehlermeldung zurückgegeben.

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

Verwandte Informationen

- "System Service Processor"

Unterstützte CLI-Befehle für den ONTAP Baseboard Management Controller

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

Befehl	Funktion
System	Eine Liste aller Befehle wird angezeigt.
Systemkonsole	Mit der Systemkonsole verbinden. `Ctrl+D` zum Beenden der Sitzung verwenden.
Systemkern	Systemkern sichern und zurücksetzen.
System Power Cycle	Das System wird ausgeschaltet und anschließend wieder eingeschaltet.
System ausschalten	Das System ausschalten.
System einschalten	Das System einschalten.
Systemstromstatus	Systemstromstatus drucken.
System zurücksetzen	Das System zurücksetzen.

Befehl	Funktion
Systemprotokoll	Systemkonsolenprotokolle drucken
system fru show [id]	Alle oder ausgewählte Field Replacable Unit (FRU) Informationen ausgeben.

ONTAP Clusterzeit verwalten (nur für Clusteradministratoren)

Probleme können auftreten, wenn die Clusterzeit ungenau ist. Obwohl ONTAP die manuelle Einstellung von Zeitzone, Datum und Uhrzeit im Cluster ermöglicht, wird empfohlen, die Network Time Protocol (NTP)-Server zu konfigurieren, um die Clusterzeit zu synchronisieren.

Ab ONTAP 9.5 kann der NTP-Server mit symmetrischer Authentifizierung konfiguriert werden.

NTP ist immer aktiviert. Dennoch ist eine Konfiguration erforderlich, damit der Cluster mit einer externen Zeitquelle synchronisiert wird. ONTAP ermöglicht die Verwaltung der NTP-Konfiguration des Clusters auf folgende Weise:

- Sie können maximal 10 externe NTP-Server mit dem Cluster verknüpfen (`cluster time-service ntp server create`).
  - Zur Gewährleistung von Redundanz und Qualität des Zeitdienstes sollten mindestens drei externe NTP-Server mit dem Cluster verbunden werden.
  - Ein NTP-Server kann über seine IPv4- oder IPv6-Adresse oder seinen vollqualifizierten Hostnamen angegeben werden.
  - Die zu verwendende NTP-Version (v3 oder v4) kann manuell angegeben werden.

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

  Wenn die von Ihnen angegebene NTP-Version vom NTP-Server nicht unterstützt wird, kann kein Zeitaustausch stattfinden.
  - Auf der erweiterten Berechtigungsstufe kann ein externer NTP-Server, der mit dem Cluster verknüpft ist, als primäre Zeitquelle für die Korrektur und Anpassung der Clusterzeit angegeben werden.
- Sie können die mit dem Cluster verbundenen NTP-Server anzeigen (`cluster time-service ntp server show`.
- Sie können die NTP-Konfiguration des Clusters ändern (`cluster time-service ntp server modify`).
- Sie können den Cluster von einem externen NTP-Server trennen (`cluster time-service ntp server delete`).
- Auf der erweiterten Berechtigungsstufe kann die Konfiguration zurückgesetzt werden, indem die Verbindung aller externen NTP-Server mit dem Cluster aufgehoben wird (`cluster time-service ntp server reset`).

Ein Knoten, der einem Cluster beitritt, übernimmt automatisch die NTP-Konfiguration des Clusters.

Neben der Verwendung von NTP ermöglicht ONTAP auch die manuelle Verwaltung der Clusterzeit. Diese Funktion ist hilfreich, wenn fehlerhafte Zeitangaben korrigiert werden müssen (zum Beispiel wenn die Zeit eines Knotens nach einem Neustart erheblich falsch ist). In diesem Fall kann eine ungefähre Zeit für den Cluster angegeben werden, bis NTP mit einem externen Zeitserver synchronisieren kann. Die manuell festgelegte Zeit gilt für alle Knoten im Cluster.

Sie können die Clusterzeit auf folgende Weise manuell verwalten:

- Sie können die Zeitzone, das Datum und die Uhrzeit im Cluster festlegen oder ändern (`cluster date modify`).
- Sie können die aktuelle Zeitzone, das Datum und die Uhrzeiteinstellungen des Clusters anzeigen (`cluster date show`).

> Jobpläne werden nicht an manuelle Änderungen von Datum und Uhrzeit des Clusters angepasst. Diese Jobs werden basierend auf der aktuellen Clusterzeit geplant, die zum Zeitpunkt der Erstellung des Jobs oder der letzten Ausführung galt. Wenn Datum oder Uhrzeit des Clusters manuell geändert werden, sind die `job show` und `job history show` Befehle zu verwenden, um zu überprüfen, ob alle geplanten Jobs entsprechend Ihren Anforderungen in die Warteschlange gestellt und abgeschlossen werden.

Befehle zur Verwaltung der Clusterzeit

Sie verwenden die `cluster time-service ntp server` Befehle, um die NTP-Server für den Cluster zu verwalten. Sie verwenden die `cluster date` Befehle, um die Clusterzeit manuell zu verwalten.

Ab ONTAP 9.5 kann der NTP-Server mit symmetrischer Authentifizierung konfiguriert werden.

Mit den folgenden Befehlen ist die Verwaltung der NTP-Server für den Cluster möglich:

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Den Cluster mit einem externen NTP-Server ohne symmetrische Authentifizierung verknüpfen	`cluster time-service ntp server create -server server_name`
Den Cluster mit einem externen NTP-Server mit symmetrischer authenticationAvailable in ONTAP 9.5 oder höher verknüpfen	`cluster time-service ntp server create -server server_ip_address -key-id key_id` Der `key_id` muss auf einen vorhandenen gemeinsam genutzten Schlüssel verweisen, der mit ``cluster time-service ntp key' konfiguriert ist.
Symmetrische Authentifizierung für einen bestehenden NTP serverAn Server aktivieren. Ein bestehender NTP Server kann modifiziert werden, um die Authentifizierung durch Hinzufügen der erforderlichen Schlüssel-ID zu ermöglichen. Verfügbar in ONTAP 9.5 oder höher	`cluster time-service ntp server modify -server server_name -key-id key_id`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Symmetrische Authentifizierung deaktivieren	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`
Einen gemeinsamen NTP-Schlüssel konfigurieren	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Gemeinsame Schlüssel werden über eine ID referenziert. Die ID, ihr Typ und ihr Wert müssen sowohl auf dem Knoten als auch auf dem NTP Server identisch sein.
Informationen zu den mit dem Cluster verbundenen NTP-Servern	`cluster time-service ntp server show`
Die Konfiguration eines externen NTP-Servers, der mit dem Cluster verbunden ist, anpassen	`cluster time-service ntp server modify`
Einen NTP-Server vom Cluster trennen	`cluster time-service ntp server delete`
Die Konfiguration wird zurückgesetzt, indem die Zuordnung aller externen NTP-Server zum Cluster entfernt wird.	`cluster time-service ntp server reset` Für diesen Befehl ist die erweiterte Berechtigungsebene erforderlich.

Mit den folgenden Befehlen ist eine manuelle Verwaltung der Clusterzeit möglich:

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Zeitzone, Datum und Uhrzeit festlegen oder ändern	`cluster date modify`
Zeitzonen-, Datums- und Uhrzeiteinstellungen für den Cluster anzeigen	`cluster date show`

Verwandte Informationen

- "cluster date show"
- "cluster date modify"
- "Cluster Zeitdienst NTP"
- "Job anzeigen"

Banner und MOTD verwalten

Informationen zum ONTAP Anmeldebanner und zum Text der Nachricht des Tages

ONTAP ermöglicht die Konfiguration eines Anmeldebanners oder einer Nachricht des Tages (MOTD), um administrative Informationen an System Manager und CLI-Benutzer des Clusters oder der Storage Virtual Machine (SVM) zu kommunizieren.

In einer Konsolensitzung (nur für Clusterzugriff) oder einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) wird ein Banner angezeigt, bevor ein Benutzer zur Authentifizierung wie zum Beispiel einem Passwort aufgefordert wird. Das Banner kann beispielsweise dazu verwendet werden, einer Person, die versucht, sich am System anzumelden, eine Warnmeldung wie die folgende anzuzeigen:

```
$ ssh admin@cluster1-01

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

Password:
```

Eine MOTD (Meldung des Tages) wird in einer Konsolensitzung (nur für Clusterzugriff) oder einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, nachdem ein Benutzer authentifiziert wurde, aber bevor die Clustershell-Eingabeaufforderung erscheint. Zum Beispiel kann die MOTD verwendet werden, um eine Willkommens- oder Informationsnachricht wie die folgende anzuzeigen, 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 `security login banner modify` oder `security login motd modify` Befehl jeweils auf folgende Weise erstellen oder ändern:

- Sie können die CLI interaktiv oder nichtinteraktiv verwenden, um den Text für das Banner oder die MOTD festzulegen.

  Der interaktive Modus, der beim Aufruf des Befehls ohne den `-message` oder `-uri` Parameter gestartet wird, ermöglicht die Verwendung von Zeilenumbrüchen (auch bekannt als Zeilenenden) in der Nachricht.

  Der nichtinteraktive Modus, der den `-message` Parameter zur Angabe der Nachrichtenzeichenfolge verwendet, unterstützt keine Zeilenumbrüche.

- Es besteht die Möglichkeit, Inhalte von einem FTP- oder HTTP-Speicherort hochzuladen und für das Banner oder die MOTD zu nutzen.
- Die MOTD kann so konfiguriert werden, dass dynamische Inhalte angezeigt werden.

  Beispiele für die dynamische Anzeige der MOTD, die konfiguriert werden können, sind unter anderem die folgenden:

  - Clustername, Node-Name oder SVM-Name
  - Datum und Uhrzeit des Clusters
  - Name des Benutzers, der sich anmeldet

- Letzter Login des Benutzers auf einem beliebigen Node im Cluster
- Anmeldegerätname oder IP-Adresse
- Name des Betriebssystems
- Software Release Version
- Effektive Clusterversion-Zeichenfolge

Das Banner unterstützt keine dynamischen Inhalte. Weitere Informationen zu `security login motd modify` und den Escape-Sequenzen, mit denen die MOTD so konfiguriert werden kann, dass dynamisch generierte Inhalte angezeigt werden, finden Sie im "ONTAP-Befehlsreferenz".

Das Banner und die MOTD lassen sich auf Cluster- oder SVM-Ebene verwalten:

- Die folgenden Fakten gelten für das Banner:
  - Das für den Cluster konfigurierte Banner wird auch für alle SVMs verwendet, für die keine Banner-Nachricht definiert ist.
  - Für jede SVM kann ein Banner auf SVM-Ebene konfiguriert werden.

    Wenn ein Banner auf Clusterebene konfiguriert wurde, wird es durch das Banner auf SVM-Ebene für die jeweilige SVM überschrieben.
- Für die MOTD gelten folgende Fakten:
  - Standardmäßig ist die für den Cluster konfigurierte MOTD auch für alle SVMs aktiviert.
  - Zusätzlich kann auf SVM-Ebene für jede SVM eine MOTD konfiguriert werden.

    In diesem Fall sehen Benutzer, die sich bei der SVM anmelden, zwei MOTDs, eine auf Cluster-Ebene und die andere auf SVM-Ebene.
  - Die MOTD auf Clusterebene kann vom Cluster-Administrator für jede SVM aktiviert oder deaktiviert werden.

    Wenn der Clusteradministrator die MOTD auf Clusterebene für eine SVM deaktiviert, sieht ein Benutzer, der sich bei der SVM anmeldet, die MOTD auf Clusterebene nicht.

Ein ONTAP Anmeldebanner erstellen

Es besteht die Möglichkeit, ein Banner zu erstellen, das eine Nachricht für Personen anzeigt, die versuchen, auf den Cluster oder die SVM zuzugreifen. Das Banner wird in einer Konsolensitzung (nur für den Clusterzugriff) oder einer SSH-Sitzung (für den Cluster- oder SVM-Zugriff) angezeigt, bevor ein Benutzer zur Authentifizierung aufgefordert wird.

Schritte

1. Mit dem `security login banner modify` Befehl lässt sich ein Banner für den Cluster oder die SVM erstellen:

Wenn Sie möchten…	Dann…
Eine Nachricht angeben, die eine einzelne Zeile ist	Verwenden Sie den `-message „<text>“` Parameter, um den Text anzugeben.

Wenn Sie möchten…	Dann…
Zeilenumbrüche (auch bekannt als Zeilenenden) in die Nachricht einbeziehen	Der Befehl kann ohne den `-message`- oder `-uri` -Parameter verwendet werden, um den interaktiven Modus zum Bearbeiten des Banners zu starten.
Inhalte von einem Speicherort hochladen, um sie für das Banner zu verwenden	Der `-uri`Parameter gibt den FTP- oder HTTP-Speicherort des Inhalts an.

Die maximale Größe für ein Banner beträgt 2.048 Bytes, einschließlich Zeilenumbrüchen.

Ein mit dem `-uri` Parameter erstelltes Banner ist statisch. Sie wird nicht automatisch aktualisiert, um nachfolgende Änderungen des Quellinhalts widerzuspiegeln.

Das für den Cluster erstellte Banner wird auch für alle SVMs angezeigt, die kein vorhandenes Banner haben. Jedes nachfolgend erstellte Banner für eine SVM überschreibt das Banner auf Cluster-Ebene für diese SVM. Die Angabe des `-message` Parameters mit einem Bindestrich in Anführungszeichen (`"-"` für die SVM setzt die SVM zurück, sodass das Banner auf Cluster-Ebene verwendet wird.

2. Es kann überprüft werden, ob das Banner erstellt wurde, indem es mit dem `security login banner show` Befehl angezeigt wird.

   Die Angabe des `-message` Parameters mit einer leeren Zeichenkette (`""` zeigt Banner ohne Inhalt an.

   Durch Angabe des `-message` Parameters mit `"-"` werden alle (Admin- oder Daten-)SVMs angezeigt, für die kein Banner konfiguriert ist.

Beispiele für die Erstellung von Bannern

Das folgende Beispiel verwendet den nicht-interaktiven Modus, um ein Banner für den Cluster “cluster1” zu erstellen:

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

cluster1::>
```

Das folgende Beispiel verwendet den interaktiven Modus, um ein Banner für die `svm1` SVM zu erstellen:

```
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
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!
```

```
cluster1::>
```

Das folgende Beispiel zeigt die erstellten Banner:

```
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
- "security login banner ändern"
- "Sicherheitsanmeldebanner anzeigen"

Der Bannertext, der auf ONTAP Cluster- und SVM-Ebene angezeigt wird, kann verwaltet werden.

Sie können das Banner auf Cluster- oder SVM-Ebene verwalten. Das für den Cluster konfigurierte Banner wird auch für alle SVMs verwendet, für die keine Banner-Nachricht definiert ist. Ein später für eine SVM erstelltes Banner überschreibt das Cluster-Banner für diese SVM.

Auswahlmöglichkeiten

- Das Banner auf Clusterebene verwalten:

Wenn Sie möchten…	Dann…
Ein Banner für alle Anmeldesitzungen anzeigen lassen	Banner auf Clusterebene festlegen: `security login banner modify -vserver <cluster_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	Das Banner für alle (Cluster- und SVM-)Logins entfernen

Wenn Sie möchten…	Dann…
Setzen Sie das Banner auf eine leere Zeichenkette (``): `security login banner modify -vserver * -message`	Ein von einem SVM-Administrator erstelltes Banner überschreiben
Die SVM-Bannernachricht ändern: `security login banner modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }`

- Das Banner auf SVM-Ebene verwalten:

  Die Angabe von `-vserver <svm_name>` ist im SVM Kontext nicht erforderlich.

Wenn Sie möchten…	Dann…
Das vom Clusteradministrator bereitgestellte Banner kann durch ein anderes Banner für die SVM ersetzt werden.	Ein Banner für die SVM erstellen: `security login banner modify -vserver <svm_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	Das vom Clusteradministrator bereitgestellte Banner wird unterdrückt, sodass für die SVM kein Banner angezeigt wird.
Das SVM-Banner für die SVM auf eine leere Zeichenkette setzen: `security login banner modify -vserver <svm_name> -message`	Das Banner auf Cluster-Ebene wird verwendet, wenn die SVM derzeit ein Banner auf SVM-Ebene verwendet.

Verwandte Informationen

- "security login banner ändern"

Nachrichtentext für ONTAP Benutzer für den Message-of-the-Day erstellen

Es besteht die Möglichkeit, eine Nachricht des Tages (MOTD) zu erstellen, um Informationen an authentifizierte CLI-Benutzer weiterzugeben. Die MOTD wird in einer Konsolensitzung (nur für Clusterzugriff) oder einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, nachdem ein Benutzer authentifiziert wurde, jedoch bevor die Clustershell-Eingabeaufforderung erscheint.

Schritte

1. Mit dem `security login motd modify` Befehl lässt sich eine MOTD für den Cluster oder die SVM erstellen:

Wenn Sie möchten…	Dann…
Eine Nachricht angeben, die eine einzelne Zeile ist	Verwenden Sie den `-message` „`text`“ Parameter, um den Text anzugeben.

Wenn Sie möchten…	Dann…
Zeilenumbrüche (auch bekannt als Zeilenenden) einbeziehen	Der Befehl kann ohne den `-message`- oder `-uri` -Parameter verwendet werden, um den interaktiven Modus zum Bearbeiten der MOTD zu starten.
Inhalte von einem Speicherort hochladen, um sie für die MOTD zu verwenden	Der `-uri`Parameter gibt den FTP- oder HTTP-Speicherort des Inhalts an.

Die maximale Größe für eine MOTD beträgt 2.048 Bytes, einschließlich Zeilenumbrüchen.

`Security login motd modify`beschreibt die Escape-Sequenzen, die verwendet werden können, um die MOTD so zu konfigurieren, dass dynamisch generierte Inhalte angezeigt werden.

Eine mit dem `-uri` Parameter erstellte MOTD ist statisch. Sie wird nicht automatisch aktualisiert, um nachfolgende Änderungen des Quellinhalts widerzuspiegeln.

Eine für den Cluster erstellte MOTD wird standardmäßig auch für alle SVM-Logins angezeigt, zusammen mit einer auf SVM-Ebene erstellten MOTD, die separat für eine bestimmte SVM erstellt werden kann. Das Setzen des `-is-cluster-message-enabled`Parameters auf `false`für eine SVM verhindert, dass die MOTD auf Cluster-Ebene für diese SVM angezeigt wird.

2. Es kann überprüft werden, ob die MOTD erstellt wurde, indem sie mit dem `security login motd show` Befehl angezeigt wird.

   Wird der `-message` Parameter mit einer leeren Zeichenkette (``) angegeben, werden MOTDs angezeigt, die nicht konfiguriert sind oder keinen Inhalt haben.

   Weitere Informationen zu `security login motd modify` und Parametern, mit denen das MOTD dynamisch generierte Inhalte im "ONTAP-Befehlsreferenz" anzeigen kann.

Beispiele für das Erstellen von MOTDs

Das folgende Beispiel verwendet den nicht-interaktiven Modus, um eine MOTD für das `cluster1` Cluster zu erstellen:

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

Das folgende Beispiel verwendet den interaktiven Modus, um eine MOTD für die `svm1` SVM zu erstellen, die Escape-Sequenzen verwendet, um dynamisch generierte Inhalte anzuzeigen:

```
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
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
```

```
was \L.
```

Das folgende Beispiel zeigt die erstellten MOTDs:

```
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.
```

Weitere Informationen zu `security login motd show` finden sich in der "ONTAP-Befehlsreferenz".

Die Verwaltung des Message-of-the-Day-Textes, der auf ONTAP Cluster- und SVM-Ebene angezeigt wird

Sie können die Nachricht des Tages (MOTD) auf Cluster- oder SVM-Ebene verwalten. Standardmäßig ist die für den Cluster konfigurierte MOTD auch für alle SVMs aktiviert. Zusätzlich kann auf SVM-Ebene für jede SVM eine MOTD konfiguriert werden. Die MOTD auf Cluster-Ebene kann vom Clusteradministrator für jede SVM aktiviert oder deaktiviert werden.

Weitere Informationen zu den "Fluchtsequenzen"Funktionen, die zur dynamischen Generierung von Inhalten für die MOTD in der ONTAP-Befehlsreferenz verwendet werden können.

Auswahlmöglichkeiten

- Die MOTD auf Clusterebene verwalten:

Wenn Sie möchten…	Dann…
Eine MOTD für alle Anmeldungen erstellen, wenn noch keine MOTD vorhanden ist.	Eine MOTD auf Clusterebene festlegen: `security login motd modify -vserver <cluster_name> { [-message "<text>"]

Wenn Sie möchten…	Dann…
[-uri <ftp_or_http_addr>] }`	Die MOTD für alle Anmeldungen wird geändert, wenn keine MOTDs auf SVM-Ebene konfiguriert sind.
Die MOTD auf Clusterebene ändern: `security login motd modify -vserver <cluster_name> { [-message "<text>"] }	[-uri <ftp_or_http_addr>] }`
Die MOTD für alle Anmeldungen wird entfernt, wenn keine MOTDs auf SVM-Ebene konfiguriert sind.	Setzen der MOTD auf Clusterebene auf eine leere Zeichenkette (""): `security login motd modify -vserver <cluster_name> -message ""`
Jede SVM zeigt die MOTD auf Clusterebene an, anstatt die MOTD auf SVM-Ebene zu verwenden.	Eine MOTD auf Clusterebene festlegen und anschließend alle MOTDs auf SVM-Ebene auf eine leere Zeichenkette setzen, wobei die MOTD auf Clusterebene aktiviert ist: a. `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` .. `security login motd modify { -vserver !"<cluster_name>" } -message "" -is -cluster-message-enabled true`	Eine MOTD wird nur für ausgewählte SVMs angezeigt, ohne eine MOTD auf Clusterebene zu verwenden.
Die MOTD auf Clusterebene wird auf eine leere Zeichenkette gesetzt, anschließend werden die MOTDs auf SVM-Ebene für die ausgewählten SVMs festgelegt: a. `security login motd modify -vserver <cluster_name> -message ""` b. `security login motd modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }` + Diesen Schritt können Sie bei Bedarf für jede SVM wiederholen.
Die gleiche SVM-Ebene-MOTD wird für alle (Daten- und Verwaltungs-)SVMs verwendet.	Den Cluster und alle SVMs so einstellen, dass dasselbe MOTD verwendet wird: `security login motd modify -vserver * { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` [NOTE] ==== Im interaktiven Modus fordert die CLI dazu auf, die MOTD für den Cluster und jede SVM einzeln einzugeben. Die gleiche MOTD kann in jede Instanz eingefügt werden, wenn die entsprechende Aufforderung erscheint. ====	Eine MOTD auf Clusterebene soll optional für alle SVMs verfügbar sein, aber nicht bei Cluster-Logins angezeigt werden.

Wenn Sie möchten…	Dann…
Eine MOTD auf Clusterebene festlegen, aber deren Anzeige für den Cluster deaktivieren: `security login motd modify -vserver <cluster_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] } -is-cluster-message -enabled false`
Entfernen aller MOTDs auf Cluster- und SVM-Ebene, wenn nur einige SVMs sowohl MOTDs auf Cluster- als auch auf SVM-Ebene haben	Für den Cluster und alle SVMs wird eine leere Zeichenkette als MOTD verwendet: `security login motd modify -vserver * -message ""`
Die MOTD wird nur für die SVMs geändert, die eine nicht-leere Zeichenkette haben, wenn andere SVMs eine leere Zeichenkette verwenden und auf Clusterebene eine andere MOTD genutzt wird.	Erweiterte Abfragen ermöglichen eine gezielte Änderung der MOTD: `security login motd modify { -vserver !"<cluster_name>" -message !"" } { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	Alle MOTDs, die bestimmten Text enthalten (zum Beispiel „Januar“ gefolgt von „2015“), werden überall in einer ein- oder mehrzeiligen Nachricht angezeigt, selbst wenn der Text auf verschiedene Zeilen verteilt ist.
Eine Abfrage zeigt MOTDs an: `security login motd show -message *"January"*"2015"*`	Interaktiv eine MOTD erstellen, die mehrere und aufeinanderfolgende Zeilenumbrüche (auch bekannt als End-of-Line oder EOLs) enthält

- Das MOTD auf SVM-Ebene verwalten:

  Die Angabe von `-vserver <svm_name>` ist im SVM Kontext nicht erforderlich.

Wenn Sie möchten…	Dann…
Eine andere SVM-Level-MOTD verwenden, wenn die SVM bereits eine vorhandene SVM-Level-MOTD hat	Die MOTD auf SVM-Ebene ändern: `security login motd modify -vserver <svm_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	Nur die Cluster-Ebene MOTD für die SVM verwenden, wenn die SVM bereits eine SVM-Ebene MOTD hat.

Wenn Sie möchten…	Dann…
Die MOTD auf SVM-Ebene wird auf eine leere Zeichenfolge gesetzt, danach kann der Clusteradministrator die MOTD auf Clusterebene für die SVM aktivieren: a. `security login motd modify -vserver <svm_name> -message ""` b. (Für den Cluster-Administrator) `security login motd modify -vserver <svm_name> -is-cluster-message -enabled true`	Keine MOTD für die SVM anzeigen, wenn sowohl die MOTD auf Cluster-Ebene als auch auf SVM-Ebene derzeit für die SVM angezeigt werden.

Verwandte Informationen

- "security login motd modify"
- "security login motd show"

ONTAP Jobs und Jobpläne verwalten

Aufträge werden in eine Auftragswarteschlange gestellt und im Hintergrund ausgeführt, sobald Ressourcen verfügbar sind. Wenn ein Auftrag zu viele Clusterressourcen verbraucht, kann er gestoppt oder pausiert werden, bis die Auslastung des Clusters sinkt. Auch die Überwachung und das erneute Starten von Aufträgen ist möglich.

Stellenkategorien

Es gibt drei Kategorien von Jobs, die Sie verwalten können: server-affiliierte, cluster-affiliierte und private Jobs.

Ein Job kann in eine der folgenden Kategorien fallen:

- **Serverbezogene Jobs**

  Diese Aufträge werden vom Management-Framework einem bestimmten Knoten zur Ausführung zugewiesen.

- **Cluster-zugeordnete Jobs**

  Diese Aufträge werden vom Management-Framework in eine Warteschlange gestellt, um auf einem beliebigen Knoten im Cluster ausgeführt zu werden.

- **Private Aufträge**

  Diese Jobs sind knotenspezifisch und nutzen weder die replizierte Datenbank (RDB) noch andere Clustermechanismen. Die Befehle zur Verwaltung privater Jobs erfordern die Berechtigungsstufe Advanced oder höher.

Befehle zur Verwaltung von Jobs

Wenn Sie einen Befehl eingeben, der einen Job startet, informiert der Befehl Sie normalerweise darüber, dass der Job in die Warteschlange gestellt wurde, und kehrt dann zur CLI-Befehlszeile zurück. Einige Befehle

zeigen jedoch stattdessen den Fortschritt des Jobs an und kehren erst zur CLI-Befehlszeile zurück, wenn der Job abgeschlossen ist. In diesen Fällen kann mit Strg+C der Job in den Hintergrund verschoben werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu allen Jobs	`job show`
Informationen zu Jobs auf Knotenbasis anzeigen	`job show bynode`
Informationen zu clusterbezogenen Jobs	`job show-cluster`
Informationen zu abgeschlossenen Aufträgen anzeigen	`job show-completed`
Informationen zur Auftragsverlaufshistorie anzeigen	`job history show` Für jeden Knoten im Cluster werden bis zu 25.000 Auftragsdatensätze gespeichert. Daher kann die Anzeige des vollständigen Auftragsverlaufs längere Zeit in Anspruch nehmen. Um potenziell lange Wartezeiten zu vermeiden, empfiehlt es sich, die Aufträge nach Knoten, Storage Virtual Machine (SVM) oder Datensatz-ID anzuzeigen.
Die Liste der privaten Jobs anzeigen	`job private show` (Erweiterte Berechtigungsstufe)
Informationen zu abgeschlossenen privaten Aufträgen	`job private show-completed` (Erweiterte Berechtigungsstufe)
Informationen zum Initialisierungsstatus für Jobmanager	`job initstate show` (Erweiterte Berechtigungsstufe)
Den Fortschritt eines Auftrags überwachen	`job watch-progress`
Den Fortschritt eines privaten Jobs überwachen	`job private watch-progress` (Erweiterte Berechtigungsstufe)
Einen Job pausieren	`job pause`
Einen privaten Auftrag pausieren	`job private pause` (Erweiterte Berechtigungsstufe)
Einen pausierten Job wieder aufnehmen	`job resume`
Einen pausierten privaten Job wieder aufnehmen	`job private resume` (Erweiterte Berechtigungsstufe)
Einen Job stoppen	`job stop`
Einen privaten Job stoppen	`job private stop` (Erweiterte Berechtigungsstufe)
Einen Job löschen	`job delete`
Einen privaten Job löschen	`job private delete` (Erweiterte Berechtigungsstufe)
Einen einem Cluster zugeordneten Auftrag von einem nicht verfügbaren Knoten, dem er zugeordnet ist, trennen, sodass ein anderer Knoten die Zuständigkeit für diesen Auftrag übernehmen kann	`job unclaim` (Erweiterte Berechtigungsstufe)

Sie können den `event log show` Befehl verwenden, um das Ergebnis eines abgeschlossenen Auftrags zu bestimmen. Weitere Informationen zu `event log show` finden sich in der "ONTAP-Befehlsreferenz".

Befehle zur Verwaltung von Arbeitsplänen

Viele Aufgaben – beispielsweise Volume-Snapshots – können so konfiguriert werden, dass sie nach festgelegten Zeitplänen ausgeführt werden. Zeitpläne, die zu bestimmten Zeiten ausgeführt werden, werden als *Cron-Schedules* (ähnlich wie UNIX `cron`-Schedules) bezeichnet. Zeitpläne, die in Intervallen ausgeführt werden, werden als *Intervall-Schedules* bezeichnet. Sie verwenden die `job schedule` Befehle, um Job-Schedules zu verwalten.

Jobpläne passen sich nicht an manuelle Änderungen von Datum und Uhrzeit des Clusters an. Diese Jobs werden basierend auf der aktuellen Clusterzeit geplant, die zum Zeitpunkt der Erstellung des Jobs oder der letzten Ausführung galt. Daher empfiehlt es sich, bei manuellen Änderungen von Datum oder Uhrzeit des Clusters die `job show` und `job history show` Befehle zu verwenden, um zu überprüfen, ob alle geplanten Jobs entsprechend Ihren Anforderungen in die Warteschlange gestellt und abgeschlossen wurden.

Wenn der Cluster Teil einer MetroCluster Konfiguration ist, müssen die Jobpläne auf beiden Clustern identisch sein. Daher ist bei Erstellung, Änderung oder Löschung eines Jobplans derselbe Vorgang auch auf dem Remote-Cluster durchzuführen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu allen Zeitplänen anzeigen	`job schedule show`
Anzeige der Liste der Jobs nach Zeitplan	`job schedule show-jobs`
Informationen zu Cron-Schedules anzeigen	`job schedule cron show`
Informationen zu Intervallplänen	`job schedule interval show`
Einen Cron-Schedule erstellen	`job schedule cron create` Ab ONTAP 9.10.1 kann die SVM in den Jobplan aufgenommen werden.
Intervallplan erstellen	`job schedule interval create` Mindestens einer der folgenden Parameter muss angegeben werden: `-days`, `-hours`, `-minutes` oder `-seconds`.
Einen Cron-Schedule ändern	`job schedule cron modify`
Einen Intervallplan modifizieren	`job schedule interval modify`
Einen Zeitplan löschen	`job schedule delete`
Einen Cron-Schedule löschen	`job schedule cron delete`
Löschen eines Intervallplans	`job schedule interval delete`

Verwandte Informationen

- "Job"

Sichern und Wiederherstellen von Cluster-Konfigurationen (nur für Clusteradministratoren)

Informationen zu ONTAP Konfigurationssicherungsdateien

Konfigurationssicherungsdateien sind Archivdateien (.7z), die Informationen zu allen konfigurierbaren Optionen enthalten, die für den ordnungsgemäßen Betrieb des Clusters und der darin enthaltenen Nodes erforderlich sind.

Diese Dateien speichern die lokale Konfiguration jedes Knotens sowie die clusterweite replizierte Konfiguration. Konfigurationssicherungsdateien werden verwendet, um die Konfiguration des Clusters zu sichern und wiederherzustellen.

Es gibt zwei Arten von Konfigurationssicherungsdateien:

- **Node-Konfigurationssicherungsdatei**

  Jeder fehlerfreie Knoten im Cluster verfügt über eine Sicherungsdatei der Knotenkonfiguration, die alle Konfigurationsinformationen und Metadaten enthält, die für den fehlerfreien Betrieb des Knotens im Cluster erforderlich sind.

- **Sicherungsdatei für die Cluster-Konfiguration**

  Diese Dateien enthalten ein Archiv aller Node-Konfigurationssicherungsdateien im Cluster sowie die replizierten Clusterkonfigurationsinformationen (die replizierte Datenbank oder RDB-Datei). Clusterkonfigurationssicherungsdateien ermöglichen die Wiederherstellung der Konfiguration des gesamten Clusters oder eines beliebigen Node im Cluster. Die Clusterkonfigurationssicherungspläne erstellen diese Dateien automatisch und speichern sie auf mehreren Nodes im Cluster.

> Konfigurationssicherungsdateien enthalten ausschließlich Konfigurationsinformationen. Sie enthalten keine Benutzerdaten. Informationen zur Wiederherstellung von Benutzerdaten sind unter "Datensicherung" zu finden.

Informationen zur Planung von Backups der ONTAP Cluster- und Knotenkonfigurationsdateien

Drei separate Zeitpläne erstellen automatisch Sicherungsdateien für die Cluster- und Knotenkonfiguration und replizieren sie zwischen den Knoten im Cluster.

Die Konfigurationssicherungsdateien werden automatisch nach folgenden Zeitplänen erstellt:

- Alle 8 Stunden
- Täglich
- Wöchentlich

Zu jedem dieser Zeitpunkte wird auf jedem fehlerfreien Knoten im Cluster eine Sicherungsdatei der Knotenkonfiguration erstellt. Alle diese Sicherungsdateien der Knotenkonfiguration werden anschließend zusammen mit der replizierten Clusterkonfiguration in einer einzigen Clusterkonfigurations-Sicherungsdatei zusammengefasst und auf einem oder mehreren Knoten im Cluster gespeichert.

ONTAP Befehle zur Verwaltung von Konfigurationssicherungszeitplänen

Sie können die `system configuration backup settings` Befehle verwenden, um Sicherungspläne für die Konfiguration zu verwalten.

Diese Befehle sind auf der Zugangsstufe „Erweitert“ verfügbar.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Die Einstellungen für einen Konfigurationssicherungsplan ändern: • Geben Sie eine Remote-URL (HTTP, HTTPS, FTP oder FTPS) an, unter der die Konfigurationssicherungsdateien zusätzlich zu den Standardspeicherorten im Cluster hochgeladen werden. • Ein Benutzername, der für die Anmeldung an der Remote-URL verwendet wird, ist anzugeben. • Die Anzahl der aufzubewahrenden Backups für jeden Konfigurations-Backup-Zeitplan festlegen	`system configuration backup settings modify` Wenn Sie HTTPS in der Remote-URL verwenden, kann die `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatsvalidierung verwendet werden. Die Zertifikatsvalidierung ist standardmäßig deaktiviert. Der Webserver, auf den Sie die Konfigurationssicherungsdatei hochladen, muss PUT-Operationen für HTTP und POST-Operationen für HTTPS aktiviert haben. Weitere Informationen enthält die Dokumentation Ihres Webservers.
Das Passwort festlegen, das für die Anmeldung an der Remote-URL verwendet wird.	`system configuration backup settings set-password`
Die Einstellungen für den Konfigurationssicherungsplan	`system configuration backup settings show` Sie legen den `-instance` Parameter fest, um den Benutzernamen und die Anzahl der aufzubewahrenden Backups für jeden Zeitplan anzuzeigen.

ONTAP Befehle zur Verwaltung von Sicherungsdateien für die Knotenkonfiguration

Sie verwenden die `system configuration backup` Befehle, um Sicherungsdateien für die Cluster- und Knotenkonfiguration zu verwalten.

Diese Befehle sind auf der Zugangsstufe „Erweitert“ verfügbar.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine neue Sicherungsdatei für die Knoten- oder Clusterkonfiguration erstellen	`system configuration backup create`
Kopieren einer Konfigurationssicherungsdatei von einem Knoten auf einen anderen Knoten im Cluster	`system configuration backup copy`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Konfigurationssicherungsdatei von einem Knoten im Cluster auf eine Remote-URL (FTP, HTTP, HTTPS oder FTPS) hochladen	`system configuration backup upload` Wenn Sie HTTPS in der Remote-URL verwenden, kann die `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatsvalidierung verwendet werden. Die Zertifikatsvalidierung ist standardmäßig deaktiviert. Der Webserver, auf den Sie die Konfigurationssicherungsdatei hochladen, muss PUT-Operationen für HTTP und POST-Operationen für HTTPS aktiviert haben. Auf manchen Webservern ist möglicherweise ein zusätzliches Modul erforderlich. Weitere Informationen enthält die Dokumentation Ihres Webservers. Die unterstützten URL-Formate variieren je nach ONTAP Version. Weitere Informationen zu Systemkonfigurationsbefehlen finden Sie im "ONTAP-Befehlsreferenz".
Eine Konfigurationssicherungsdatei kann von einer Remote-URL auf einen Knoten im Cluster heruntergeladen und, falls angegeben, das digitale Zertifikat validiert werden.	`system configuration backup download` Wenn Sie HTTPS in der Remote-URL verwenden, kann die `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatsvalidierung verwendet werden. Die Zertifikatsvalidierung ist standardmäßig deaktiviert.
Eine Konfigurationssicherungsdatei auf einem Knoten im Cluster umbenennen	`system configuration backup rename`
Sicherungsdateien der Knoten- und Clusterkonfiguration für einen oder mehrere Knoten im Cluster anzeigen	`system configuration backup show`
Löschen einer Konfigurationssicherungsdatei auf einem Node	`system configuration backup delete` Dieser Befehl löscht die Konfigurationssicherungsdatei nur auf dem angegebenen Knoten. Wenn die Konfigurationssicherungsdatei auch auf anderen Knoten im Cluster vorhanden ist, bleibt sie auf diesen Knoten erhalten.

Verwandte Informationen

- "Sicherung der Systemkonfiguration"

Die ONTAP Knotenkonfigurationssicherungsdatei zum Wiederherstellen eines Knotens finden.

Eine Konfigurationssicherungsdatei, die sich an einer Remote-URL oder auf einem Knoten im Cluster befindet, wird verwendet, um eine Knotenkonfiguration wiederherzustellen.

Über diese Aufgabe

Sie können entweder eine Cluster- oder eine Knoten-Konfigurationssicherungsdatei verwenden, um eine Knoten-Konfiguration wiederherzustellen.

Schritt

1. Die Konfigurationssicherungsdatei muss dem Knoten zur Verfügung stehen, für den die Konfiguration wiederhergestellt werden soll.

Wenn sich die Konfigurationssicherungsdatei befindet…	Dann…
Unter einer entfernten URL	Der `system configuration backup download`-Befehl auf der erweiterten Berechtigungsebene kann verwendet werden, um ihn auf den wiederherzustellenden Node herunterzuladen.
Auf einem Knoten im Cluster	a. Mit dem `system configuration backup show` Befehl auf der Ebene erweiterter Berechtigungen lässt sich die Liste der im Cluster verfügbaren Konfigurationssicherungsdateien anzeigen, die die Konfiguration des wiederherzustellenden Knotens enthalten. b. Falls die von Ihnen angegebene Konfigurationssicherungsdatei auf dem wiederherzustellenden Knoten nicht vorhanden ist, kann der `system configuration backup copy` Befehl verwendet werden, um sie auf den wiederherzustellenden Knoten zu kopieren.

Wenn Sie den Cluster zuvor neu erstellt haben, sollten Sie eine Konfigurationssicherungsdatei wählen, die nach der Neuerstellung des Clusters erstellt wurde. Falls Sie eine Konfigurationssicherungsdatei verwenden müssen, die vor der Neuerstellung des Clusters erstellt wurde, muss der Cluster nach der Wiederherstellung des Knotens erneut erstellt werden.

Verwandte Informationen

- "Sicherungskopie der Systemkonfiguration"

Einen Node mithilfe der ONTAP Node-Konfigurationssicherungsdatei wiederherstellen

Die Node-Konfiguration wird mithilfe der Konfigurationssicherungsdatei wiederhergestellt, die identifiziert und dem wiederherzustellenden Node zur Verfügung gestellt wurde.

Über diese Aufgabe

Diese Aufgabe sollte nur durchgeführt werden, um sich von einem Desaster zu erholen, das zum Verlust der lokalen Konfigurationsdateien des Knotens geführt hat.

Schritte

1. Wechsel zur erweiterten Berechtigungsstufe:

   ```
   set -privilege advanced
   ```

2. Wenn der Knoten fehlerfrei ist, kann auf der erweiterten Berechtigungsstufe eines anderen Knotens der `cluster modify` Befehl mit den Parametern `-node` und `-eligibility` verwendet werden, um ihn als nicht berechtigt zu markieren und vom Cluster zu isolieren.

   Wenn der Node nicht in Ordnung ist, sollte dieser Schritt übersprungen werden.

   Dieses Beispiel ändert node2 so, dass es nicht mehr für die Teilnahme am Cluster infrage kommt, damit seine Konfiguration wiederhergestellt werden kann:

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

   Weitere Informationen zu `cluster modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Der `system configuration recovery node restore` Befehl auf der erweiterten Berechtigungsebene stellt die Konfiguration des Node aus einer Konfigurationssicherungsdatei wieder her.

   Wenn der Knoten seine Identität, einschließlich seines Namens, verloren hat, sollte der `-nodename-in -backup` Parameter verwendet werden, um den Node-Name in der Konfigurationssicherungsdatei anzugeben.

   Dieses Beispiel stellt die Konfiguration des Knotens mithilfe einer der auf dem Knoten gespeicherten Konfigurationssicherungsdateien wieder her:

   ```
   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 gestartet.

4. Wenn der Node als nicht geeignet markiert wurde, kann der Node mit dem `system configuration recovery cluster sync` Befehl als geeignet markiert und mit dem Cluster synchronisiert werden.
5. In einer SAN-Umgebung kann der `system node reboot` Befehl verwendet werden, um den Node neu zu starten und das SAN-Quorum wiederherzustellen.

Nachdem Sie fertig sind

Wenn der Cluster zuvor neu erstellt wurde und die Node-Konfiguration mithilfe einer Konfigurationssicherungsdatei wiederhergestellt wird, die vor dieser Neuerstellung des Clusters erstellt wurde, muss der Cluster erneut erstellt werden.

Die Sicherungsdatei der ONTAP Clusterkonfiguration zum Wiederherstellen eines Clusters finden

Zur Wiederherstellung eines Clusters wird die Konfiguration entweder von einem Knoten im Cluster oder aus einer Clusterkonfigurationssicherungsdatei verwendet.

Schritte

1. Wählen Sie einen Konfigurationstyp aus, um den Cluster wiederherzustellen.

   - Ein Knoten im Cluster

     Besteht der Cluster aus mehr als einem Knoten und verfügt einer der Knoten über eine Clusterkonfiguration aus der Zeit, als sich der Cluster in der gewünschten Konfiguration befand, kann der Cluster mithilfe der auf diesem Knoten gespeicherten Konfiguration wiederhergestellt werden.

     In den meisten Fällen ist der Knoten mit dem Replikationsring mit der aktuellsten Transaktions-ID am besten für die Wiederherstellung der Cluster-Konfiguration geeignet. Der `cluster ring show` Befehl auf der erweiterten Berechtigungsstufe ermöglicht die Anzeige einer Liste der auf jedem Knoten im Cluster verfügbaren Replikationsringe.

   - Eine Clusterkonfiguration-Sicherungsdatei

     Wenn Sie keinen Knoten mit der korrekten Clusterkonfiguration identifizieren können oder wenn der Cluster nur aus einem einzigen Knoten besteht, kann eine Sicherungsdatei der Clusterkonfiguration zur Wiederherstellung des Clusters verwendet werden.

   Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, gehen alle seit der Sicherung vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Konfigurationssicherungsdatei und der aktuellen Konfiguration behoben werden. Siehe "NetApp Knowledge Base: ONTAP Konfigurationssicherungs-Resolution Guide" für Hinweise zur Fehlerbehebung.

2. Wenn Sie sich für die Verwendung einer Clusterkonfigurations-Sicherungsdatei entschieden haben, muss die Datei dem Knoten zur Verfügung stehen, den Sie zur Wiederherstellung des Clusters verwenden möchten.

Wenn sich die Konfigurationssicherungsdatei befindet…	**Dann…**
Unter einer entfernten URL	Der `system configuration backup download`-Befehl auf der erweiterten Berechtigungsebene kann verwendet werden, um ihn auf den wiederherzustellenden Node herunterzuladen.

Wenn sich die Konfigurationssicherungsdatei befindet…	Dann…
Auf einem Knoten im Cluster	a. Der `system configuration backup show` Befehl auf der Ebene mit erweiterten Berechtigungen ermöglicht das Auffinden einer Cluster-Konfigurationssicherungsdatei, die erstellt wurde, als sich der Cluster in der gewünschten Konfiguration befand. b. Falls sich die Sicherungsdatei der Clusterkonfiguration nicht auf dem Knoten befindet, den Sie für die Wiederherstellung des Clusters verwenden möchten, dann kann der `system configuration backup copy` Befehl verwendet werden, um sie auf den wiederherzustellenden Knoten zu kopieren.

Verwandte Informationen

- "cluster ring show"
- "Sicherungskopie der Systemkonfiguration"

Einen Cluster mithilfe der ONTAP Clusterkonfigurations-Sicherungsdatei wiederherstellen

Um nach einem Clusterausfall eine Clusterkonfiguration aus einer bestehenden Konfiguration wiederherzustellen, wird der Cluster mithilfe der ausgewählten und dem wiederherstellenden Node zur Verfügung gestellten Clusterkonfiguration neu erstellt, und anschließend wird jeder zusätzliche Node dem neuen Cluster wieder hinzugefügt.

Über diese Aufgabe

Diese Aufgabe sollte nur durchgeführt werden, um sich von einem Desaster zu erholen, das zum Verlust der Cluster-Konfiguration geführt hat.

> Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei neu erstellen, muss der technische Support kontaktiert werden, um etwaige Diskrepanzen zwischen der Konfigurationssicherungsdatei und der im Cluster vorhandenen Konfiguration zu klären.
>
> Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, gehen alle seit der Sicherung vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Konfigurationssicherungsdatei und der aktuellen Konfiguration behoben werden. Siehe "NetApp Knowledge Base: ONTAP Konfigurationssicherungs-Resolution Guide" für Hinweise zur Fehlerbehebung.

Schritte

1. Storage-Failover für jedes HA-Paar deaktivieren:

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

   Das Speicher-Failover muss nur einmal pro HA-Paar deaktiviert werden. Wenn das Speicher-Failover für einen Knoten deaktiviert wird, ist es auch auf dem Partnerknoten deaktiviert.

2. Jeden Knoten außer dem sich erholenden Knoten anhalten:

   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. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   set -privilege advanced

4. Auf dem wiederherstellenden Knoten kann der Cluster mit dem **system configuration recovery cluster recreate** Befehl neu erstellt werden.

   Dieses Beispiel erstellt das Cluster mithilfe der auf dem wiederherstellenden Node gespeicherten Konfigurationsinformationen neu:

   ```
   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 neuer Cluster erstellt.

5. Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, überprüfen Sie, ob die Clusterwiederherstellung noch läuft:

   system configuration recovery cluster show

   Sie müssen den Wiederherstellungsstatus des Clusters nicht überprüfen, wenn Sie den Cluster von einem fehlerfreien Node aus neu erstellen.

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

6. Jeder Node, der dem neu erstellten Cluster wieder beitreten muss, wird neu gestartet.

   Die Knoten müssen einzeln neu gestartet werden.

7. Für jeden Node, der dem neu erstellten Cluster hinzugefügt werden soll, ist Folgendes zu beachten:

a. Von einem fehlerfreien Node im neu erstellten Cluster aus erfolgt der erneute Beitritt des Ziel-Node:

system configuration recovery cluster rejoin -node *node_name*

Dieses Beispiel fügt den Ziel-Node “node2” dem neu erstellten Cluster wieder hinzu:

```
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 Zielknoten startet neu und tritt anschließend dem Cluster bei.

b. Es sollte sichergestellt werden, dass der Zielknoten fehlerfrei funktioniert und ein Quorum mit den übrigen Knoten im Cluster gebildet wurde:

cluster show -eligibility true

Der Zielknoten muss dem neu erstellten Cluster wieder beitreten, bevor Sie einen anderen Knoten wieder 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 den Cluster aus einer Konfigurationssicherungsdatei neu erstellt haben, den Wiederherstellungsstatus auf „Abgeschlossen“ setzen:

system configuration recovery cluster modify -recovery-status complete

9. Zurück zur Administrator-Privilegstufe:

set -privilege admin

10. Besteht der Cluster nur aus zwei Knoten, kann der **cluster ha modify** Befehl zum erneuten Aktivieren von Cluster-HA verwendet werden.
11. Mit dem `**storage failover modify**`Befehl lässt sich das Storage-Failover für jedes HA-Paar wieder aktivieren.

Nachdem Sie fertig sind

Wenn der Cluster SnapMirror Peer-Beziehungen aufweist, müssen diese Beziehungen ebenfalls neu erstellt werden. Weitere Informationen finden sich unter "Datensicherung".

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "storage failover modify"

Einen Node mit dem ONTAP Cluster synchronisieren, damit das clusterweite Quorum gewährleistet ist.

Wenn ein clusterweites Quorum vorhanden ist, aber ein oder mehrere Knoten nicht mit dem Cluster synchron sind, muss der Knoten synchronisiert werden, um die replizierte Datenbank (RDB) auf dem Knoten wiederherzustellen und ihn in das Quorum zu bringen.

Schritt

1. Von einem fehlerfreien Knoten aus kann mit dem `system configuration recovery cluster sync` Befehl auf der Ebene mit erweiterten Berechtigungen der Knoten synchronisiert werden, der nicht mit der Clusterkonfiguration übereinstimmt.

   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 auf den Knoten repliziert, und der Knoten ist somit berechtigt, am Cluster teilzunehmen.

Knoten-Core-Dumps für einen ONTAP Cluster verwalten (nur für Cluster-Administratoren)

Wenn ein Knoten abstürzt, tritt ein Core-Dump auf und das System erstellt eine Core-Dump-Datei, die der technische Support zur Fehlerbehebung verwenden kann. Es besteht die Möglichkeit, die Attribute des Core-Dumps zu konfigurieren oder anzuzeigen. Eine Core-Dump-Datei kann außerdem gespeichert, angezeigt, segmentiert, hochgeladen oder gelöscht werden.

Core Dumps können auf folgende Weise verwaltet werden:

- Konfiguration von Core Dumps und Anzeige der Konfigurationseinstellungen
- Anzeige von grundlegenden Informationen, dem Status und den Attributen von Core Dumps

  Core-Dump-Dateien und Berichte werden im `/mroot/etc/crash/` Verzeichnis eines Knotens gespeichert. Der Verzeichnisinhalt kann mit den `system node coredump` Befehlen oder einem Webbrowser angezeigt werden.

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

  ONTAP verhindert das Initiieren des Speicherns einer Core-Dump-Datei während einer Übernahme, einer Aggregatverlagerung oder einer Rückgabe.

- Löschen nicht mehr benötigter Core Dump-Dateien

Befehle zur Verwaltung von Core Dumps

Sie verwenden die `system node coredump config` Befehle zur Verwaltung der Konfiguration von Core Dumps, die `system node coredump` Befehle zur Verwaltung der Core Dump-Dateien und die `system node coredump reports` Befehle zur Verwaltung von Application Core Reports.

Weitere Informationen zu den in diesem Thema beschriebenen Befehlen finden Sie in der "ONTAP-Befehlsreferenz".

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Core Dumps konfigurieren	`system node coredump config modify`
Konfigurationseinstellungen für Core Dumps anzeigen	`system node coredump config show`
Grundlegende Informationen zu Core Dumps	`system node coredump show`
Manuelles Auslösen eines Core Dumps beim Neustart eines Knotens	`system node reboot` mit sowohl dem `-dump` als auch dem `-skip-lif-migration-before -reboot` Parameter Der Parameter `skip-lif-migration-before-reboot`link: gibt an, dass die LIF-Migration vor einem Neustart übersprungen wird.
Manuelles Auslösen eines Core Dump beim Herunterfahren eines Knotens	`system node halt` mit sowohl dem `-dump` als auch dem `-skip-lif-migration-before -shutdown` Parameter Der Parameter `skip-lif-migration-before-shutdown` gibt an, dass die LIF-Migration vor einem Herunterfahren übersprungen wird.
Einen bestimmten Core Dump speichern	`system node coredump save`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Alle nicht gespeicherten Core-Dumps auf einem bestimmten Knoten speichern	`system node coredump save-all`
Eine AutoSupport-Nachricht mit einer von Ihnen angegebenen Core-Dump-Datei generieren und senden	`system node autosupport invoke-core-upload` Der `-uri`optionale Parameter gibt ein alternatives Ziel für die AutoSupport-Nachricht an.
Statusinformationen zu Core Dumps anzeigen	`system node coredump status`
Löschen eines bestimmten Core Dumps	`system node coredump delete`
Alle ungespeicherten Core-Dumps oder alle gespeicherten Core-Dateien auf einem Knoten löschen	`system node coredump delete-all`
Anwendungs-Core-Dump-Berichte anzeigen	`system node coredump reports show`
Löschen eines Application Core Dump-Berichts	`system node coredump reports delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Copyright-Informationen

Copyright © 2026 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 IRGENDEINER 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.