



Cluster-Management mit der CLI

ONTAP 9

NetApp
February 06, 2026

This PDF was generated from <https://docs.netapp.com/de-de/ontap/system-admin/index.html> on February 06, 2026. Always check docs.netapp.com for the latest.

Inhalt

Cluster-Management mit der CLI	1
Erfahren Sie mehr über die Cluster-Administration mit der ONTAP CLI	1
Cluster- und SVM-Administratoren	1
Erfahren Sie mehr über die Administratorrollen für ONTAP Cluster und SVM	1
Aktivieren oder deaktivieren Sie den Webbrowser-Zugriff auf ONTAP System Manager	1
Erfahren Sie mehr über den ONTAP Cluster Management Server	2
SVMs-Typen in einem ONTAP-Cluster	2
Zugriff auf das Cluster über die CLI (nur Cluster-Administratoren)	3
Greifen Sie über den seriellen Node-Port auf ein ONTAP Cluster zu	3
Zugriff auf einen ONTAP-Cluster mithilfe von SSH-Anforderungen	3
ONTAP SSH-Anmeldesicherheit	6
Aktivieren Sie den Telnet- oder RSH-Zugriff auf einen ONTAP-Cluster	8
Greifen Sie über Telnet-Anforderungen auf einen ONTAP-Cluster zu	10
Greifen Sie über RSH-Anforderungen auf ein ONTAP-Cluster zu	13
Verwenden Sie die ONTAP Befehlszeilenschnittstelle	16
Hier erhalten Sie Informationen zur Befehlszeilenschnittstelle von ONTAP	16
Erfahren Sie mehr über die verschiedenen ONTAP Shells für CLI-Befehle	17
Navigieren durch ONTAP CLI-Befehlsverzeichnisse	19
Verstehen Sie die Regeln zur Angabe von Werten in der ONTAP CLI	19
Zeigen Sie den ONTAP-Befehlsverlauf an, und führen Sie einen beliebigen Befehl aus dem Verlauf erneut aus	20
ONTAP-Tastaturbefehle zum Bearbeiten von CLI-Befehlen	21
Berechtigungsebenen für ONTAP-CLI-Befehle verstehen	23
Legt die Berechtigungsebene in der ONTAP-CLI fest	24
Legen Sie die Anzeigeeinstellungen für die ONTAP-CLI fest	24
Verwenden Sie Abfrageoperatoren in der ONTAP-CLI	25
Verwenden Sie erweiterte Abfragen mit Änderungs- und Löschbefehlen in der ONTAP-CLI	29
Begrenzen Sie die Ausgabe des Befehls ONTAP show mit dem Parameter Fields	30
Verwenden Sie die Positionsparameter der ONTAP-CLI in der Befehlseingabe	31
Zugriff auf die ONTAP CLI-man-Seiten	33
Zeichnen Sie eine ONTAP-CLI-Sitzung auf, und verwalten Sie die aufgezeichneten Sitzungen	34
Notieren Sie eine CLI-Sitzung	34
Befehle zum Verwalten von Datensätzen von CLI-Sitzungen	34
Befehle zum Verwalten der automatischen Zeitüberschreitung von CLI-Sitzungen	35
Cluster-Management (nur Cluster-Administratoren)	35
Zeigen Sie Details auf Node-Ebene in einem ONTAP Cluster an	35
Hier erhalten Sie Details zu ONTAP auf Cluster-Ebene	36
Ändern Sie die Attribute des ONTAP-Clusters	37
Zeigen Sie den Replikationsstatus der ONTAP-Cluster-Ringe an	37
Zustandsbewertungen von ONTAP Clustern anhand von Quorum und Epsilon	38
Zeigen Sie die Storage-Kapazitätsauslastung von System-Volumes in einem ONTAP Cluster an	39
Managen von Nodes	40
Hinzufügen von Nodes zu einem ONTAP-Cluster	40

Entfernen von Nodes aus einem ONTAP-Cluster	43
Zugriff über einen Webbrowser auf ONTAP Node-Protokolle, Core Dumps und MIB-Dateien	47
Zugriff auf die Systemkonsole eines ONTAP Node	48
Management von ONTAP Node Root-Volumes und Root-Aggregaten	50
Starten oder Stoppen eines ONTAP-Node für Wartungsarbeiten oder zur Fehlerbehebung	52
Managen eines ONTAP-Node über das Boot-Menü	55
Anzeigen der Attribute der Nodes in einem ONTAP-Cluster	58
Ändern Sie die Attribute eines ONTAP-Knotens	59
Umbenennen eines ONTAP-Node	60
Management eines Single-Node-ONTAP-Clusters	60
Konfigurieren Sie das SP/BMC-Netzwerk	65
Isolieren Sie den ONTAP-Managementverkehr im Netzwerk	65
Informieren Sie sich über die ONTAP SP/BMC-Netzwerkkonfiguration	66
Aktivieren der automatischen Netzwerkkonfiguration für ONTAP SP/BMC	67
Konfigurieren Sie das ONTAP SP/BMC-Netzwerk manuell	68
Ändern Sie die Konfiguration der ONTAP-Serviceprozessor-API	70
Remote-Verwaltung von Knoten über den SP/BMC	72
Managen Sie einen ONTAP-Knoten per Remote-Zugriff über das SP/BMC	72
Remote-Node-Management mit dem ONTAP Serviceprozessor	72
Verwenden Sie den ONTAP Baseboard-Verwaltungscontroller zur Remote-Verwaltung eines Knotens .	74
Managen von Updates der ONTAP SP/BMC-Firmware	75
ONTAP SP/BMC und die Netzwerkschnittstellen verwenden für Firmware-Updates	76
Greifen Sie über ein Cluster-Benutzerkonto auf den ONTAP Serviceprozessor zu	76
Greifen Sie von einem Administrations-Host aus auf die ONTAP SP/BMC eines Node zu	77
Greifen Sie über die Systemkonsole auf die ONTAP SP/BMC eines Node zu	78
Erfahren Sie, wie ONTAP SP-CLI-, SP-Konsole- und Systemkonsolensitzungen zusammenhängen .	79
Fügen Sie die Administrations-Host-IP-Adresse hinzu, um auf den ONTAP Serviceprozessor zuzugreifen	80
Zeigen Sie die Hilfeinformationen in der ONTAP SP/BMC-CLI an	82
ONTAP-Befehle für das Remote-Node-Management	84
ONTAP Monitoring des Node-Systemzustands mithilfe schwellenwertbasierter Messwerte und Status des SP-Sensors	92
Statuswerte des ONTAP SP-Sensors in der Befehlsausgabe des Befehls „System Sensor“	95
ONTAP-Befehle für das Management des Serviceprozessors	98
ONTAP-Befehle für BMC Management	102
Unterstützte CLI-Befehle für den ONTAP Baseboard-Verwaltungscontroller	103
Management der ONTAP-Cluster-Zeit (nur für Cluster-Administratoren)	104
Befehle zum Verwalten der Cluster-Zeit	105
Verwalten des Banners und der MOTD	107
Erfahren Sie mehr über das ONTAP Anmeldebanner und den Text für die täglichen Nachrichten .	107
Erstellen Sie ein ONTAP-Anmeldebanner	109
Verwalten Sie den Bannertext, der auf ONTAP-Cluster- und SVM-Ebene angezeigt wird	111
Erstellen Sie Text für die Tagesnachricht für ONTAP-Benutzer	112
Managen des Tagestexts, der auf ONTAP-Cluster- und SVM-Ebene angezeigt wird	114
Managen von ONTAP-Jobs und Jobplänen	117

Jobkategorien	117
Befehle zum Verwalten von Jobs	118
Befehle zum Verwalten von Job-Zeitplänen	119
Backup und Restore von Cluster-Konfigurationen (nur Cluster-Administratoren)	120
Erfahren Sie mehr über Backup-Dateien der ONTAP-Konfiguration	120
Erfahren Sie mehr über die Planung von Backups von ONTAP-Cluster- und Node-Konfigurationsdateien	121
ONTAP-Befehle zum Managen der Backup-Zeitpläne für die Konfiguration	121
ONTAP-Befehle zum Managen von Backup-Dateien der Node-Konfiguration	122
Suchen Sie die Backup-Datei für die ONTAP-Node-Konfiguration, um einen Node wiederherzustellen	124
Stellen Sie einen Node mithilfe der Backup-Datei für die ONTAP-Node-Konfiguration wieder her	125
Suchen Sie die Backup-Datei für die ONTAP-Cluster-Konfiguration, um ein Cluster wiederherzustellen	126
Stellen Sie einen Cluster mithilfe der Backup-Datei für die ONTAP-Cluster-Konfiguration wieder her	127
Synchronisieren Sie einen Node mit dem ONTAP-Cluster, um das Cluster-weite Quorum sicherzustellen	130
Management von Node Core Dumps für ein ONTAP-Cluster (nur Cluster-Administratoren)	131
Befehle zum Verwalten von Core Dumps	131

Cluster-Management mit der CLI

Erfahren Sie mehr über die Cluster-Administration mit der ONTAP CLI

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

Sie sollten diese Verfahren unter den folgenden Umständen verwenden:

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

Verwandte Informationen

Details zur CLI-Syntax und -Verwendung finden Sie in der "[ONTAP-Befehlsreferenz](#)" Dokumentation.

Cluster- und SVM-Administratoren

Erfahren Sie mehr über die Administratorrollen für ONTAP Cluster und SVM

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

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

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



Die ONTAP Befehlszeilenschnittstelle (CLI) verwendet in der Ausgabe weiterhin den Begriff „vServer“, und vserver da der Befehl oder Parametername nicht geändert wurde.

Aktivieren oder deaktivieren Sie den Webbrowser-Zugriff auf ONTAP System Manager

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

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

Die Protokollierung durch System Manager wird in den `/mroot/etc/log/mlog/sysmgr.log` Dateien des

Node aufgezeichnet, der die Cluster-Management-LIF hostet, wenn auf System Manager zugegriffen wird. Sie können die Protokolldateien über einen Browser anzeigen. Das Protokoll von System Manager ist auch in AutoSupport Meldungen enthalten.

Erfahren Sie mehr über den ONTAP Cluster Management Server

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

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

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

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

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

Wenn Sie den `vserver show` Befehl ausführen, wird der Cluster-Management-Server in der Ausgabeliste des Befehls angezeigt.

SVMs-Typen in einem ONTAP-Cluster

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

Ein Cluster enthält die folgenden SVMs:

- Admin-SVM

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

- Node-SVM

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

- System-SVM (erweitert)

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

- Data SVM

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

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

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

In der CLI werden SVMs als Vserver angezeigt.

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

Greifen Sie über den seriellen Node-Port auf ein ONTAP Cluster zu

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

Schritte

1. Drücken Sie an der Konsole die Eingabetaste.

Das System antwortet mit der Eingabeaufforderung für die Anmeldung.

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

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

Das System antwortet mit der Passwort-Eingabeaufforderung.

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

Zugriff auf einen ONTAP-Cluster mithilfe von SSH-Anforderungen

Sie können SSH-Anforderungen an ein ONTAP-Cluster ausgeben, um administrative Aufgaben auszuführen. SSH ist standardmäßig aktiviert.

Bevor Sie beginnen

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

Der `-application` Parameter der `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Erfahren Sie mehr über `security login` in der "[ONTAP-Befehlsreferenz](#)".

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

Über diese Aufgabe

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

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

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

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

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

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

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

SSH-Authentifizierungsoptionen

- Ab ONTAP 9.3 können Sie "[Aktivieren Sie SSH-Multi-Faktor-Authentifizierung](#)" lokale Administratorkonten einrichten.

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

- Ab ONTAP 9.4 können Sie "[Aktivieren Sie SSH-Multi-Faktor-Authentifizierung](#)" LDAP- und NIS-Remote-Benutzer verwenden.
- Ab ONTAP 9.13.1 können Sie optional der SSH-Authentifizierung eine Zertifikatsüberprüfung hinzufügen, um die Anmeldesicherheit zu erhöhen. Um dies "[Verknüpfen Sie ein X.509-Zertifikat mit dem öffentlichen Schlüssel](#)" zu tun, die ein Konto verwendet. Wenn Sie sich mit SSH sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem X.509-Zertifikat anmelden, überprüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor Sie sich mit dem öffentlichen SSH-Schlüssel authentifizieren. Die SSH-Anmeldung wird

abgelehnt, wenn das Zertifikat abgelaufen ist oder widerrufen wurde und der öffentliche SSH-Schlüssel automatisch deaktiviert wird.

- Ab ONTAP 9.14.1 können ONTAP Administratoren ["Fügen Sie der SSH-Authentifizierung die zwei-Faktor-Authentifizierung des Cisco Duo hinzu"](#) die Anmeldesicherheit erhöhen. Nach der ersten Anmeldung, nachdem Sie die Cisco Duo-Authentifizierung aktiviert haben, müssen Benutzer ein Gerät registrieren, das als Authentifikator für SSH-Sitzungen dient.
- Ab ONTAP 9.15.1 können Administratoren ["Dynamische Autorisierung konfigurieren"](#) SSH-Benutzern basierend auf der Vertrauensbewertung des Benutzers zusätzliche adaptive Authentifizierung bereitstellen.

Schritte

1. Geben Sie den ssh Befehl von einem Host mit Zugriff auf das Netzwerk des ONTAP Clusters in eines der folgenden Formate ein:

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

Wenn Sie ein AD-Domain-Benutzerkonto verwenden, müssen Sie *username* das Format *domainname \\AD_accountname* (mit doppelten Backslashes nach dem Domänennamen) oder *"domainname\AD_accountname"* (in doppelte Anführungszeichen und mit einem einzigen Backslash nach dem Domänennamen) angeben.

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

command ist für SSH-interaktive Sitzungen nicht erforderlich.

Beispiele für SSH-Anforderungen

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

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

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

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

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

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

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

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

Verwandte Informationen

["Administratorauthentifizierung und RBAC"](#)

ONTAP SSH-Anmeldesicherheit

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

Sicherheitsbezogene Informationen werden angezeigt, wenn Sie sich erfolgreich als SSH-Admin-Benutzer

einloggen. Sie werden über die folgenden Bedingungen benachrichtigt:

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



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

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

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

Einschränkungen und andere Überlegungen bei der SSH-Anmeldesicherheit

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

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

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

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

Beispiele für Sicherheitsdaten für SSH-Anmeldungen

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

- Diese Meldung wird nach jeder erfolgreichen Anmeldung angezeigt:

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

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

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

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

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

Aktivieren Sie den Telnet- oder RSH-Zugriff auf einen ONTAP-Cluster

Aus Sicherheitsgründen sind Telnet und RSH standardmäßig deaktiviert. Damit das Cluster Telnet- oder RSH-Anforderungen akzeptieren kann, müssen Sie den Service in der Standardrichtlinie für den Verwaltungsdienst aktivieren.

Telnet und RSH sind keine sicheren Protokolle. Sie sollten SSH für den Zugriff auf den Cluster in Erwägung ziehen. SSH bietet eine sichere Remote Shell und interaktive Netzwerksitzung. Weitere Informationen finden Sie unter ["Greifen Sie über SSH auf das Cluster zu"](#).

Über diese Aufgabe

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

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

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

- RSH-Befehle erfordern erweiterte Berechtigungen.

ONTAP 9.10.1 oder höher

Schritte

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

```
security protocol show
```

- a. Wenn das RSH- oder Telnet-Sicherheitsprotokoll aktiviert ist, fahren Sie mit dem nächsten Schritt fort.
- b. Wenn das RSH- oder Telnet-Sicherheitsprotokoll nicht aktiviert ist, verwenden Sie den folgenden Befehl, um es zu aktivieren:

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

Erfahren Sie mehr über `security protocol show` und `security protocol modify` in der ["ONTAP-Befehlsreferenz"](#).

2. Vergewissern Sie sich, dass der `management-rsh-server` Service oder `management-telnet-server` auf den Management-LIFs vorhanden ist:

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

Oder

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

Erfahren Sie mehr über `network interface show` in der ["ONTAP-Befehlsreferenz"](#).

- a. Wenn der `management-rsh-server` oder `management-telnet-server`-Dienst vorhanden ist, fahren Sie mit dem nächsten Schritt fort.
- b. Wenn der `management-rsh-server` Dienst oder `management-telnet-server` nicht vorhanden ist, fügen Sie ihn mit dem folgenden Befehl hinzu:

```
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
```

Erfahren Sie mehr über `network interface service-policy add-service` in der ["ONTAP-Befehlsreferenz"](#).

ONTAP 9.9 oder früher

Über diese Aufgabe

ONTAP verhindert, dass Sie vordefinierte Firewallrichtlinien ändern. Sie können jedoch eine neue Richtlinie erstellen, indem Sie die vordefinierte `mgmt` Management-Firewallrichtlinie klonen und anschließend Telnet oder RSH unter der neuen Richtlinie aktivieren.

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set advanced
```

2. Aktivieren eines Sicherheitsprotokolls (RSH oder Telnet):

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

3. Erstellen Sie eine neue Management-Firewall `mgmt`-Richtlinie auf der Grundlage der Management-Firewall-Richtlinie:

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

4. Aktivieren Sie Telnet oder RSH unter der neuen Management Firewall-Richtlinie:

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

Um alle IP-Adressen zuzulassen, sollten Sie angeben `-ip-list 0.0.0.0/0`

5. Zuordnen der neuen Richtlinie zu der Cluster-Management-LIF:

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

Erfahren Sie mehr über `network interface modify` in der "[ONTAP-Befehlsreferenz](#)".

Greifen Sie über Telnet-Anforderungen auf einen ONTAP-Cluster zu

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

Telnet und RSH sind keine sicheren Protokolle. Sie sollten SSH für den Zugriff auf den Cluster in Erwägung ziehen. SSH bietet eine sichere Remote Shell und interaktive Netzwerksitzung. Weitere Informationen finden Sie unter "[Greifen Sie über SSH auf das Cluster zu](#)".

Bevor Sie beginnen

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

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

Der `-application` Parameter der `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Erfahren Sie mehr über `security login` in der "[ONTAP-Befehlsreferenz](#)".

Über diese Aufgabe

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

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

Falls die Rate der kommenden Verbindungen mehr als 10 pro Sekunde ist, wird der Dienst vorübergehend

für 60 Sekunden deaktiviert.

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

ONTAP 9.10.1 oder höher

Schritte

1. Vergewissern Sie sich, dass das Telnet-Sicherheitsprotokoll aktiviert ist:

```
security protocol show
```

- a. Wenn das Telnet-Sicherheitsprotokoll aktiviert ist, fahren Sie mit dem nächsten Schritt fort.
- b. Wenn das Telnet-Sicherheitsprotokoll nicht aktiviert ist, verwenden Sie den folgenden Befehl, um es zu aktivieren:

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

Erfahren Sie mehr über `security protocol show` und `security protocol modify` in der ["ONTAP-Befehlsreferenz"](#).

2. Vergewissern Sie sich, dass der `management-telnet-server` Service auf den Management-LIFs vorhanden ist:

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

Erfahren Sie mehr über `network interface show` in der ["ONTAP-Befehlsreferenz"](#).

- a. Wenn der `management-telnet-server` Dienst vorhanden ist, fahren Sie mit dem nächsten Schritt fort.
- b. Wenn der `management-telnet-server` Dienst nicht vorhanden ist, fügen Sie ihn mit dem folgenden Befehl hinzu:

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

Erfahren Sie mehr über `network interface service-policy add-service` in der ["ONTAP-Befehlsreferenz"](#).

ONTAP 9.9 oder früher

Bevor Sie beginnen

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

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

Standardmäßig ist Telnet deaktiviert. Der `system services firewall policy show` Befehl mit dem `-service telnet` Parameter zeigt an, ob Telnet in einer Firewallrichtlinie aktiviert wurde. Erfahren Sie mehr über `system services firewall policy` in der ["ONTAP-Befehlsreferenz"](#).

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

Der `network options ipv6 show` Befehl zeigt an, ob IPv6 aktiviert ist. Erfahren Sie mehr über `network options ipv6 show` in der ["ONTAP-Befehlsreferenz"](#). Der `system services firewall policy show` Befehl zeigt Firewallrichtlinien an.

Schritte

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

```
telnet hostname_or_IP
```

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

Beispiel für eine Telnet-Anforderung

Das folgende Beispiel zeigt, wie der Benutzer mit dem Namen „joe“, der über einen Telnet-Zugriff verfügt, eine Telnet-Anfrage stellen kann, um auf einen Cluster zuzugreifen, dessen Cluster-Management-LIF 10.72.137.28 lautet:

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Greifen Sie über RSH-Anforderungen auf ein ONTAP-Cluster zu

Sie können RSH-Anforderungen an das Cluster ausgeben, um administrative Aufgaben durchzuführen. RSH ist kein sicheres Protokoll und ist standardmäßig deaktiviert.

Telnet und RSH sind keine sicheren Protokolle. Sie sollten SSH für den Zugriff auf den Cluster in Erwägung ziehen. SSH bietet eine sichere Remote Shell und interaktive Netzwerksitzung. Weitere Informationen finden Sie unter ["Greifen Sie über SSH auf das Cluster zu"](#).

Bevor Sie beginnen

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

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

Der `-application` Parameter der `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Erfahren Sie mehr über `security login` in der ["ONTAP-Befehlsreferenz"](#).

Über diese Aufgabe

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

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

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

- RSH-Befehle erfordern erweiterte Berechtigungen.

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, fahren Sie mit dem nächsten Schritt fort.
- b. Wenn das RSH-Sicherheitsprotokoll nicht aktiviert ist, verwenden Sie den folgenden Befehl, um es zu aktivieren:

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

Erfahren Sie mehr über `security protocol show` und `security protocol modify` in der ["ONTAP-Befehlsreferenz"](#).

2. Vergewissern Sie sich, dass der `management-rsh-server` Service auf den Management-LIFs vorhanden ist:

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

Erfahren Sie mehr über `network interface show` in der ["ONTAP-Befehlsreferenz"](#).

- a. Wenn der `management-rsh-server` Dienst vorhanden ist, fahren Sie mit dem nächsten Schritt fort.
- b. Wenn der `management-rsh-server` Dienst nicht vorhanden ist, fügen Sie ihn mit dem folgenden Befehl hinzu:

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

Erfahren Sie mehr über `network interface service-policy add-service` in der ["ONTAP-Befehlsreferenz"](#).

ONTAP 9.9 oder früher

Bevor Sie beginnen

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

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

RSH ist standardmäßig deaktiviert. Der Befehl `System Services Firewall Policy show` mit dem `-service rsh` Parameter zeigt an, ob RSH in einer Firewallrichtlinie aktiviert wurde. Erfahren Sie mehr über `system services firewall policy` in der ["ONTAP-Befehlsreferenz"](#).

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

Der `network options ipv6 show` Befehl zeigt an, ob IPv6 aktiviert ist. Erfahren Sie mehr über `network options ipv6 show` in der ["ONTAP-Befehlsreferenz"](#). Der `system services firewall policy show` Befehl zeigt Firewallrichtlinien an.

Schritte

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

```
rsh hostname_or_IP -l username:password command
```

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

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

Beispiel einer RSH-Anforderung

Das folgende Beispiel zeigt, wie der Benutzer „joe“, der mit RSH-Zugriff eingerichtet wurde, eine RSH-Anforderung zur Ausführung des `cluster show` Befehls ausgeben kann:

```
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$
```

Erfahren Sie mehr über `cluster show` in der ["ONTAP-Befehlsreferenz"](#).

Verwenden Sie die ONTAP Befehlszeilenschnittstelle

Hier erhalten Sie Informationen zur Befehlszeilenschnittstelle von ONTAP

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

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

Wenn Sie die Berechtigungsebene (d. h. den `-privilege` Parameter des `set` Befehls) auf `set advanced`, enthält die Eingabeaufforderung ein Sternchen (*), z. B.:

```
cluster_name::*>
```

Erfahren Sie mehr über `set` in der ["ONTAP-Befehlsreferenz"](#).

Erfahren Sie mehr über die verschiedenen ONTAP Shells für CLI-Befehle

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

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

Er stellt alle Befehle bereit, die Sie für die Konfiguration und das Management des Clusters benötigen. In der Clustershell-CLI-Hilfe (ausgelöst durch `?` die Eingabeaufforderung für *clustershell*) werden verfügbare Clustershell-Befehle angezeigt. Der `man` Befehl in der *clustershell* zeigt die `man`-Seite für den angegebenen *clustershell*-Befehl (`man <command_name>`an`). Erfahren Sie mehr über `'man` in der "[ONTAP-Befehlsreferenz](#)".

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

Die Nodeshell ist über den `system node run` Befehl zugänglich. Erfahren Sie mehr über `system node run` in der "[ONTAP-Befehlsreferenz](#)".

In der nodeshell CLI-Hilfe (ausgelöst durch `?` oder `help` an der nodeshell-Eingabeaufforderung) werden die verfügbaren nodeshell-Befehle angezeigt. Der `man` Befehl im nodeshell zeigt die `man`-Page für den angegebenen nodeshell-Befehl an.

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

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

Die Systemshell und das zugehörige `diag` Konto sind für Low-Level-Diagnosezwecke vorgesehen. Für ihren Zugriff ist die Diagnose-Berechtigungsebene erforderlich und nur für den technischen Support reserviert, um Aufgaben zur Fehlerbehebung auszuführen.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "[ONTAP-Befehlsreferenz](#)".

Zugriff von nodeshell Befehlen und Optionen in der clustershell

Nodeshell Befehle und Optionen sind über die nodeshell zugänglich:

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

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

Die in der Clustershell unterstützten Nodeshell-Optionen können über die folgende Methode aufgerufen werden: `vserver options clustershell` Befehl. Um diese Optionen anzuzeigen, können Sie die Clustershell-CLI mit folgender Abfrage verwenden: `vserver options -vserver nodename_or_clusternode -option-name ?`

Wenn Sie in der *clustershell* einen Befehl oder eine ältere Option eingeben und der Befehl oder die Option einen entsprechenden *clustershell*-Befehl hat, informiert ONTAP Sie über den entsprechenden *clustershell*-Befehl.

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

Zeigt die verfügbaren nodeshell-Befehle an

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

Schritte

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

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

local Ist der Node, den Sie für den Zugriff auf das Cluster verwenden.



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

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

```
[commandname] help
```

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

Sie geben `exit` Strg-D ein, um zur Clustershell-CLI zurückzukehren.

Erfahren Sie mehr über `exit` in der ["ONTAP-Befehlsreferenz"](#).

Beispiel für die Anzeige von verfügbaren nodeshell Befehlen

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

Navigieren durch ONTAP CLI-Befehlsverzeichnisse

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

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

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

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

Erfahren Sie mehr über `storage disk show` in der ["ONTAP-Befehlsreferenz"](#).

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

Mit dem `top` Befehl können Sie zur obersten Ebene der Befehlshierarchie wechseln und mit dem `up` Befehl oder Befehl `..` eine Ebene nach oben in der Befehlshierarchie wechseln.



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

Verwandte Informationen

- ["Oben"](#)
- ["Hoch"](#)

Verstehen Sie die Regeln zur Angabe von Werten in der ONTAP CLI

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

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

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

- Die CLI interpretiert ein Fragezeichen (?) als Befehl, um Hilfeinformationen für einen bestimmten Befehl anzuzeigen.
- Einige Text, die Sie in die CLI eingeben, z. B. Befehlsnamen, Parameter und bestimmte Werte, ist nicht zwischen Groß- und Kleinschreibung zu beachten.

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

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

Die CLI ignoriert den Text zwischen # und dem Zeilenende.

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

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

Im folgenden Beispiel gibt ein Befehlszeilenkommentar, der das Vorzeichen verwendet #, an, was der Befehl tut.

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

Erfahren Sie mehr über security login create in der ["ONTAP-Befehlsreferenz"](#).

Zeigen Sie den ONTAP-Befehlsverlauf an, und führen Sie einen beliebigen Befehl aus dem Verlauf erneut aus

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

können auch Befehle neu ausgeben.

Um den Befehlsverlauf anzuzeigen, können Sie den `history` Befehl verwenden.

Um einen Befehl erneut auszustellen, können Sie den `redo` Befehl mit einem der folgenden Argumente verwenden:

- Eine Zeichenfolge, die einem Teil eines vorherigen Befehls entspricht

Wenn beispielsweise der einzige `volume` Befehl, den Sie ausgeführt haben `volume show`, lautet, können Sie den `redo volume` Befehl verwenden, um den Befehl erneut auszuführen.

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

Sie können beispielsweise den `redo 4` Befehl verwenden, um den vierten Befehl in der Verlaufsliste erneut auszustellen.

- Ein negativer Offset vom Ende der Verlaufsliste

Beispielsweise können Sie mit dem `redo -2` Befehl den Befehl, den Sie vor zwei Befehlen ausgeführt haben, erneut ausgeben.

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

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

Verwandte Informationen

- "[Verlauf](#)"
- "[Wiederholen](#)"
- "[Datenmenge](#)"

ONTAP-Tastaturbefehle zum Bearbeiten von CLI-Befehlen

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

In der folgenden Tabelle werden die Tastaturbefehle zum Bearbeiten von CLI-Befehlen aufgeführt. `Ctrl-B` Zeigt an, dass Sie die Strg-Taste gedrückt halten, während Sie das danach angegebene Zeichen eingeben. `Esc` Zeigt an, dass Sie die Esc-Taste drücken und loslassen und dann das danach angegebene Zeichen eingeben.

Ihr Ziel ist	Verwenden Sie einen dieser Tastenkombinationen...
Bewegen Sie den Cursor um ein Zeichen zurück	<ul style="list-style-type: none">• Strg-B• Hinterpfeil

Ihr Ziel ist	Verwenden Sie einen dieser Tastenkombinationen...
Bewegen Sie den Cursor um ein Zeichen nach vorne	<ul style="list-style-type: none"> • Strg-F • Vorwärtspfeil
Bewegen Sie den Cursor um ein Wort zurück	ESC-B
Bewegen Sie den Cursor um ein Wort nach vorne	ESC-F
Bewegen Sie den Cursor an den Anfang der Zeile	Strg+A
Bewegen Sie den Cursor an das Ende der Zeile	Strg-E
Entfernen Sie den Inhalt der Befehlszeile vom Anfang der Zeile zum Cursor und speichern Sie ihn im Schnittpuffer. Der Cut-Puffer wirkt wie temporärer Speicher, ähnlich dem, was in einigen Programmen als <i>Clipboard</i> bezeichnet wird.	Strg-U
Entfernen Sie den Inhalt der Befehlszeile vom Cursor zum Zeilenende und speichern Sie ihn im Schnittpuffer	Strg-K
Entfernen Sie den Inhalt der Befehlszeile vom Cursor bis zum Ende des folgenden Wortes und speichern Sie ihn im Schnittpuffer	ESC-D
Entfernen Sie das Wort vor dem Cursor, und speichern Sie es im Schnittpuffer	Strg-W
Geben Sie den Inhalt des Schnittbuffers ein, und drücken Sie ihn in die Befehlszeile am Cursor	Strg-Y
Das Zeichen vor dem Cursor löschen	<ul style="list-style-type: none"> • Strg-H • Rücktaste
Löschen Sie das Zeichen, in dem sich der Cursor befindet	Strg-D
Löschen Sie die Zeile	Strg-C
Deaktivieren Sie den Bildschirm	Strg-L

Ihr Ziel ist	Verwenden Sie einen dieser Tastenkombinationen...
Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den vorherigen Eintrag in der Verlaufsliste.	<ul style="list-style-type: none"> • Strg-P • ESC-P • Nach-oben-Pfeil
Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum vorherigen Eintrag.	
Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den nächsten Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum nächsten Eintrag.	<ul style="list-style-type: none"> • Strg-N • ESC-N • Nach-unten-Pfeil
Erweitern Sie einen teilweise eingegebenen Befehl oder eine gültige Eingabe aus der aktuellen Bearbeitungsposition	<ul style="list-style-type: none"> • Registerkarte • Strg-I
Kontextabhängige Hilfe anzeigen	?
Escape die spezielle Zuordnung für das Fragezeichen (?) Zeichen. Um z. B. ein Fragezeichen in das Argument eines Befehls einzugeben, drücken Sie die Esc-Taste und anschließend das ? Zeichen.	Esc-?
TTY-Ausgabe starten	Strg-Q
TTY-Ausgang stoppen	Strg-S

Berechtigungsebenen für ONTAP-CLI-Befehle verstehen

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

- * Admin*

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

- * Fortgeschrittene *

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

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

- **Diagnose**

Diagnosebefehle und Parameter unterbrechen potenziell den Betrieb. Sie werden nur vom Support-

Personal eingesetzt, um Probleme zu diagnostizieren und zu beheben.

Legt die Berechtigungsebene in der ONTAP-CLI fest

Sie können die Berechtigungsebene in der CLI mit dem `set` Befehl festlegen. Änderungen an Einstellungen auf Berechtigungsebene gelten nur für die Sitzung, in der Sie sich befinden. Sie sind nicht über Sitzungen hinweg persistent.

Schritte

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

Beispiel zum Festlegen der Berechtigungsebene

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

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

Erfahren Sie mehr über `set` in der ["ONTAP-Befehlsreferenz"](#).

Legen Sie die Anzeigeeinstellungen für die ONTAP-CLI fest

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

Über diese Aufgabe

Sie können die folgenden CLI-Anzeigeeinstellungen festlegen:

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

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

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

Schritte

1. Verwenden Sie zum Festlegen der Anzeigeeinstellungen für `set` die CLI den Befehl.

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

Erfahren Sie mehr über `set` und `rows` in der "[ONTAP-Befehlsreferenz](#)".

Beispiel zum Festlegen von Anzeigeeinstellungen in der CLI

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

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

Verwandte Informationen

- "[Anzeigen](#)"
- "[Einstellen](#)"
- "[Zeilen](#)"

Verwenden Sie Abfrageoperatoren in der ONTAP-CLI

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

In der folgenden Tabelle werden die unterstützten Abfrageoperatoren beschrieben:

Operator	Beschreibung
*	Platzhalter, der allen Einträgen entspricht. Der Befehl <code>volume show -volume *tmp*</code> zeigt beispielsweise eine Liste aller Volumes an, deren Namen den String enthalten <code>tmp</code> .
!	KEIN Operator. Gibt einen Wert an, der nicht abgeglichen werden soll; <code>!vs0</code> zeigt z. B. an, dass er nicht mit dem Wert übereinstimmt <code>vs0</code> .
.	Oder Operator. Trennt zwei Werte, die verglichen werden sollen, z. B. <code>.*vs0</code>

Operator	Beschreibung
vs2* entspricht entweder vs0 oder vs2. Sie können mehrere ODER Anweisun gen angeben; zum Beispiel, 'a	b*
c passt der Eintrag a, jeder Eintrag, der mit beginnt b, und jeder Eintrag, der enthält c.	..
Bereichs bediener. Zum Beispiel, 5 .. 10 entspricht einem beliebige n Wert von 5 bis 10, einschlie ßlich.	<

Operator	Beschreibung
Kleiner als Operator.	> Zum Beispiel, <code><20</code> entspricht jedem Wert, der kleiner als ist 20. .
Greater-than Operator.	<code><=</code> `*> 5*` Entspricht z. B. einem Wert, der größer ist als `5`. .

Operator	Beschreibung
<p>Kleiner als oder gleich dem Operator.</p> <p>Zum Beispiel, ≤ 5 entspricht einem Wert, der kleiner oder gleich ist 5.</p>	<p>\geq</p>
<p>Größer als oder gleich dem Operator.</p> <div data-bbox="133 967 257 1917" style="border: 1px solid black; padding: 5px; width: 75px;"> \star \geq $=5$ \star \leq En tsp ric ht z. B. ein em Wer t, der grö ßer ode r gle ich ist \star 5 \star \cdot </div>	<p>{query}</p>

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

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

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

Verwandte Informationen

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

Verwenden Sie erweiterte Abfragen mit Änderungs- und Löschbefehlen in der ONTAP-CLI

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

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

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

Erweiterte Abfragen sind in der Regel nur mit `modify` und `delete` Befehlen nützlich. Sie haben keine Bedeutung in `create` oder `show` Befehlen.

Die Kombination von Abfragen und Änderungsvorgängen ist ein nützliches Werkzeug. Es kann jedoch zu Verwirrung und Fehlern führen, wenn es falsch umgesetzt wird. `system node image modify` Wenn Sie beispielsweise mit dem Befehl (erweiterte Berechtigung) das Standard-Software-Image eines Node festlegen, wird das andere Software-Image automatisch nicht als Standard festgelegt. Der Befehl im folgenden Beispiel ist effektiv ein null Vorgang:

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

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

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

Begrenzen Sie die Ausgabe des Befehls ONTAP show mit dem Parameter Fields

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

Zum Beispiel `volume show -instance` führt die Ausführung wahrscheinlich zu mehreren Informationsbildschirmen. Mit können Sie `volume show -fields fieldname[,fieldname...]` die Ausgabe so anpassen, dass sie nur das angegebene Feld oder die Felder enthält (zusätzlich zu den immer angezeigten Standardfeldern). Mit können Sie `-fields ?` gültige Felder für einen `show` Befehl anzeigen.

Das folgende Beispiel zeigt die Ausgabedifferenz zwischen dem `-instance` `-fields` Parameter und dem 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::>

```

Verwenden Sie die Positionsparameter der ONTAP-CLI in der Befehlseingabe

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

Was ist ein Positionsparameter

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

solange er seine relative Reihenfolge mit anderen Positionsparametern im selben Befehl beobachtet, wie in der **command_name** ?Ausgabe angegeben.

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



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

Einen Positionsparameter identifizieren

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

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

Wenn z. B. in der **command_name** ? Ausgabe als folgender Parameter angezeigt wird, ist der Parameter für den Befehl positioniert, in dem er angezeigt wird:

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

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

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

Beispiele für die Verwendung von Positionsparametern

Im folgenden Beispiel **volume create** ? zeigt die Ausgabe, dass drei Parameter für den Befehl `-volume` , `-aggregate` und positioniert sind `-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 `volume create` wird der Befehl angegeben, ohne die Funktionen der Positionsparameter zu nutzen:

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

In den folgenden Beispielen wird die Positionsparameterfunktion verwendet, um die Effizienz der Befehlseingabe zu erhöhen. Die Positionsparameter werden im `volume create` Befehl mit nicht-Positionsparametern intersert, und die Positionsparameterwerte werden ohne Parameternamen angegeben. Die Positionsparameter werden in der gleichen Reihenfolge angegeben `volume create ?`, die vom Ausgang angezeigt wird. Das heißt, der Wert für `-volume` wird vor dem von angegeben `-aggregate`, was wiederum vor dem von angegeben ist `-size`.

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

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

Zugriff auf die ONTAP CLI-man-Seiten

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

Verwenden Sie in der ONTAP-Befehlszeile den `man <command_name>` Befehl, um die manuelle Seite des angegebenen Befehls anzuzeigen. Wenn Sie keinen Befehlsnamen angeben, wird der manuelle Seitenindex angezeigt. Sie können mit dem `man man` Befehl Informationen zum `man` Befehl selbst anzeigen. Sie können eine man-Page verlassen, indem `q` Sie eingeben.

Weitere Informationen zu den ONTAP-Befehlen auf Administratorebene und erweiterten Ebenen finden Sie in Ihrer Version im ["ONTAP-Befehlsreferenz"](#).

Zeichnen Sie eine ONTAP-CLI-Sitzung auf, und verwalten Sie die aufgezeichneten Sitzungen

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

Notieren Sie eine CLI-Sitzung

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

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

Schritte

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

```
system script start
```

Erfahren Sie mehr über `system script start` 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. Wenn Sie fertig sind, beenden Sie die Aufzeichnung der Sitzung:

```
system script stop
```

Erfahren Sie mehr über `system script stop` in der ["ONTAP-Befehlsreferenz"](#).

ONTAP beendet die Aufzeichnung Ihrer CLI-Sitzung.

Befehle zum Verwalten von Datensätzen von CLI-Sitzungen

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

Ihr Ziel ist	Befehl
Starten Sie die Aufzeichnung der aktuellen CLI-Sitzung in einer bestimmten Datei	<code>system script start</code>
Aufzeichnung der aktuellen CLI-Sitzung beenden	<code>system script stop</code>

Ihr Ziel ist	Befehl
Zeigt Informationen zu Datensätzen von CLI-Sitzungen an	system script show
Laden Sie einen Datensatz einer CLI-Sitzung auf ein FTP- oder HTTP-Ziel hoch	system script upload
Löschen eines Datensatzes einer CLI-Sitzung	system script delete

Verwandte Informationen

["ONTAP-Befehlsreferenz"](#)

Befehle zum Verwalten der automatischen Zeitüberschreitung von CLI-Sitzungen

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

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

Sie verwenden die `system timeout` Befehle, um die automatische Zeitüberschreitung von CLI-Sitzungen zu verwalten.

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

Verwandte Informationen

["ONTAP-Befehlsreferenz"](#)

Cluster-Management (nur Cluster-Administratoren)

Zeigen Sie Details auf Node-Ebene in einem ONTAP Cluster an

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

Schritte

- Um Informationen zu den Nodes in einem Cluster anzuzeigen, verwenden Sie den `cluster show` Befehl.

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

Erfahren Sie mehr über `cluster show` in der "[ONTAP-Befehlsreferenz](#)".

Beispiele zum Anzeigen der Nodes in einem Cluster

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

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

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

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

cluster1::*> cluster show -node node1

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

Hier erhalten Sie Details zu ONTAP auf Cluster-Ebene

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

Schritte

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

Beispiel zum Anzeigen von Cluster-Attributen

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

```
cluster1::> cluster identity show

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

Erfahren Sie mehr über `cluster identity show` in der "[ONTAP-Befehlsreferenz](#)".

Ändern Sie die Attribute des ONTAP-Clusters

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

Über diese Aufgabe

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

Schritte

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

Der `-name` Parameter gibt den Namen des Clusters an. Erfahren Sie mehr über `cluster identity modify` und die Regeln zum Angeben des Cluster-Namens in der "[ONTAP-Befehlsreferenz](#)".

Der `-location` Parameter gibt den Standort des Clusters an.

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

Beispiel für die Umbenennung eines Clusters

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

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

Zeigen Sie den Replikationsstatus der ONTAP-Cluster-Ringe an

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

Schritte

1. Um den Status der Cluster-Replizierungsringe anzuzeigen, verwenden Sie den `cluster ring show` Befehl auf der erweiterten Berechtigungsebene.

Beispiel zum Anzeigen des Status von Cluster-Ring-Replizierung

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

angezeigt:

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

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

Erfahren Sie mehr über `cluster ring show` in der "[ONTAP-Befehlsreferenz](#)".

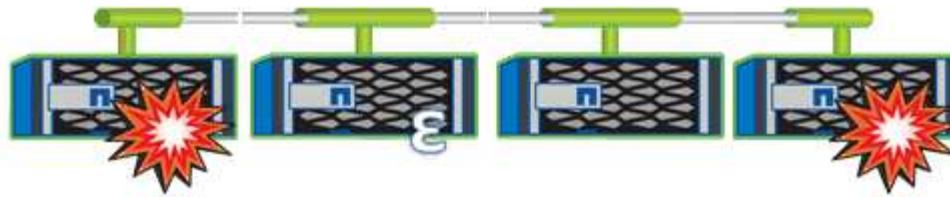
Zustandsbewertungen von ONTAP Clustern anhand von Quorum und Epsilon

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

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

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

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



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

Wenn ein Node offline geschaltet wird, kann sich dies darauf auswirken, dass das Cluster im Quorum bleibt. Daher gibt ONTAP eine Warnmeldung aus, wenn Sie versuchen, einen Vorgang durchzuführen, der entweder das Cluster aus dem Quorum entfernt, oder wenn es ein Ausfall von dem Verlust des Quorums entfernt wird. Sie können die Quorum-Warnmeldungen deaktivieren, indem Sie den `cluster quorum-service options modify` Befehl auf der erweiterten Berechtigungsebene verwenden. Erfahren Sie mehr über `cluster quorum-service options modify` in der ["ONTAP-Befehlsreferenz"](#).

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

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

Zeigen Sie die Storage-Kapazitätsauslastung von System-Volumes in einem ONTAP Cluster an

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

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

Sie können System-Volumes mit dem `volume show` Befehl anzeigen, die meisten anderen Volume-Vorgänge sind jedoch nicht zulässig. Beispielsweise können Sie ein System-Volume nicht mit dem `volume modify` Befehl ändern.

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

```

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

```

Managen von Nodes

Hinzufügen von Nodes zu einem ONTAP-Cluster

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

Bevor Sie beginnen

- Wenn Sie einem Cluster mit mehreren Nodes hinzufügen, müssen alle vorhandenen Nodes im Cluster in einem ordnungsgemäßen Zustand sein (angezeigt durch `cluster show`). Erfahren Sie mehr über `cluster show` in der ["ONTAP-Befehlsreferenz"](#).
- Wenn Sie einem 2-Node-Cluster ohne Switches Nodes hinzufügen, müssen Sie das 2-Node-Cluster ohne Switches mit einem von NetApp unterstützten Cluster Switch in ein Switch-Attached-Cluster konvertieren.

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

- Wenn Sie einem Single-Node-Cluster einen zweiten Node hinzufügen, muss der zweite Node installiert sein und das Cluster-Netzwerk konfiguriert sein.
- Wenn für das Cluster die automatische SP-Konfiguration aktiviert ist, muss das für den SP angegebene Subnetz über verfügbare Ressourcen verfügen, damit der beigetreten Node das angegebene Subnetz verwenden kann, um den SP automatisch zu konfigurieren.
- Sie müssen die folgenden Informationen für die Node-Management-LIF des neuen Node gesammelt haben:
 - Port
 - IP-Adresse
 - Netzmaske

- Standard-Gateway

Über diese Aufgabe

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

Schritte

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

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

```
Welcome to node setup.
```

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

```
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the setup wizard.
```

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

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

```
Enter the node management interface port [e0M]:
```

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

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

Erfahren Sie mehr über `exit` in der ["ONTAP-Befehlsreferenz"](#).

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

```
::> 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 im ["Dokumentation zur Knotenverwaltung"](#). Erfahren Sie mehr über `cluster setup` in der ["ONTAP-Befehlsreferenz"](#).

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

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

Wenn sich die auf dem neuen Node ausgeführte ONTAP-Version von der auf dem vorhandenen Cluster ausgeführten Version unterscheidet, meldet das System eine System checks Error: Cluster join operation cannot be performed at this time Fehlermeldung. Dies ist das erwartete Verhalten. Führen Sie den `cluster add-node -allow-mixed-version-join true -cluster-ips <IP address> -node-names <new_node_name>` Befehl von einem vorhandenen Node im Cluster aus auf der erweiterten Berechtigungsebene aus, um fortzufahren.

6. Befolgen Sie die Anweisungen, um den Node einzurichten und mit dem Cluster zu verbinden:
 - Um den Standardwert für eine Eingabeaufforderung zu akzeptieren, drücken Sie die Eingabetaste.
 - Um Ihren eigenen Wert für eine Eingabeaufforderung einzugeben, geben Sie den Wert ein, und drücken Sie dann die Eingabetaste.
7. Wiederholen Sie die vorherigen Schritte für jeden weiteren Node, den Sie hinzufügen möchten.

Nachdem Sie fertig sind

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

Verwandte Informationen

- ["Cluster mit gemischten Versionen werden von ONTAP Software-Upgrades unterstützt"](#)
- ["Cluster-Add-Knoten"](#)

Entfernen von Nodes aus einem ONTAP-Cluster

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

Bevor Sie beginnen

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

- Mehr als die Hälfte der Nodes im Cluster muss sich in einem ordnungsgemäßen Zustand befinden.
- Sämtliche Daten, Volumes und Nicht-Root-Aggregate müssen vom Knoten verschoben oder entfernt werden.
 - Alle Daten auf dem Node, den Sie entfernen möchten, müssen evakuiert worden sein. Dazu kann gehören ["Daten werden aus einem verschlüsselten Volume entfernt"](#).
 - Alle nicht-Root-Volumes wurden ["Verschoben"](#) von Aggregaten verwendet, die dem Node gehören.
 - Alle nicht-Root-Aggregate wurden ["Gelöscht"](#) vom Node entfernt.
- Alle LIFs und VLANs wurden verschoben oder vom Node entfernt.
 - Daten-LIFs wurden ["Gelöscht"](#) ["Umgezogen"](#) von oder vom Node verwendet.
 - Cluster-Management-LIFs wurden ["Umgezogen"](#) vom Node entfernt, und die Home Ports wurden geändert.
 - Alle Intercluster-Schnittstellen waren ["Entfernt"](#). Wenn Sie Intercluster LIFs entfernen, wird eine Warnung angezeigt, die ignoriert werden kann.
 - Alle VLANs auf dem Knoten waren ["Gelöscht"](#).
- Der Knoten ist nicht an Failover-Beziehungen beteiligt.
 - Speicher-Failover wurde ["Deaktiviert"](#) für den Node durchgeführt.
 - Alle LIF-Failover-Regeln wurden ["Geändert"](#) zum Entfernen von Ports auf dem Node verwendet.
- Wenn der Node über FIPS-Festplatten (Federal Information Processing Standards) oder SEDs (Self-Encrypting Drives) verfügt, ["Die Festplattenverschlüsselung wurde entfernt"](#) indem die Festplatten wieder in den ungeschützten Modus versetzt werden.
 - Vielleicht möchten Sie auch ["FIPS-Laufwerke oder SEDs reinigen"](#).
- Wenn auf dem Node LUNs vorhanden sind, die entfernt werden sollen, sollten Sie ["Ändern Sie die Liste Selective LUN Map \(SLM\) Reporting-Nodes"](#), bevor Sie den Node entfernen.

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

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



Führen Sie keine Vorgänge wie `cluster remove-node`, `cluster unjoin` und `node rename` aus, wenn ein automatisiertes ONTAP-Upgrade ausgeführt wird.

Über diese Aufgabe

- Wenn Sie ein Cluster mit gemischten Versionen ausführen, können Sie den letzten Node niedriger Versionen mithilfe eines der erweiterten Berechtigungsbefehle, beginnend mit ONTAP 9.3, entfernen:
 - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
 - ONTAP 9.4 und höher: `cluster remove-node -skip-last-low-version-node-check`
- Wenn Sie 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 Berechtigungsebene in erweitert:

```
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. Den aktuellen Master-Knoten identifizieren:

```
cluster ring show
```

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

5. Wenn der Knoten, den Sie entfernen, der aktuelle Master-Knoten ist, aktivieren Sie einen anderen Knoten im Cluster, damit er als Master-Knoten gewählt werden kann:

- a. Machen Sie den aktuellen Master-Node zur Teilnahme am Cluster nicht berechtigt:

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

Der Knoten wird als fehlerhaft markiert, bis die Eignung wiederhergestellt ist. Wenn der Master-Knoten seine Eignung verliert, wird einer der verbleibenden Knoten vom Cluster-Quorum zum neuen Master gewählt.

Wenn Sie diesen Schritt auf dem ersten Knoten eines HA-Paars durchführen, sollten Sie nur diesen Knoten als nicht geeignet markieren. Ändern Sie nicht den Status des HA-Partners.



Wenn der Partnerknoten als neuer Master ausgewählt wird, müssen Sie überprüfen, ob er Epsilon hält, bevor Sie ihn für nicht berechtigt erklären. Wenn der Partnerknoten Epsilon hält, müssen Sie Epsilon auf einen anderen, im Cluster verbleibenden Knoten verschieben, bevor Sie ihn für nicht berechtigt erklären. Sie tun dies, wenn Sie diese Schritte wiederholen, um den Partnerknoten zu entfernen.

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

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

6. Melden Sie sich bei der Remote-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...	Befehl
ONTAP 9,3	<pre>cluster unjoin</pre>

Für diese ONTAP-Version...	Befehl
ONTAP 9.4 und höher	<p>Mit Node-Name:</p> <pre data-bbox="878 255 1323 329">cluster remove-node -node <node_name></pre> <p>Mit Node-IP:</p> <pre data-bbox="878 498 1428 572">cluster remove-node -cluster_ip <node_ip></pre>

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

Das System informiert Sie über Folgendes:

- Außerdem müssen Sie den Failover-Partner des Node aus dem Cluster entfernen.
- Nachdem der Node entfernt wurde und bevor er 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.

Wenn die Bedingungen angegeben sind, die Sie vor dem Entfernen des Node berücksichtigen müssen, wird eine Fehlermeldung generiert. Beispielsweise könnte die Meldung angeben, dass der Node über gemeinsam genutzte Ressourcen verfügt, die Sie entfernen müssen, oder dass sich der Node in einer Cluster HA-Konfiguration oder in einer Storage-Failover-Konfiguration befindet, die Sie deaktivieren müssen.

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

8. Wenn eine Fehlermeldung auf Fehlerbedingungen hinweist, beheben Sie diese Bedingungen und führen Sie den `cluster remove-node cluster unjoin` Befehl oder erneut aus.

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

9. Löschen Sie bei einer Neuzuordnung des Node die Node-Konfiguration und initialisieren Sie alle Festplatten:

- a. Drücken Sie während des Bootens Strg-C, um das Boot-Menü anzuzeigen, wenn Sie dazu aufgefordert werden.
- b. Wählen Sie die 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"](#)

Zugriff über einen Webbrowser auf ONTAP Node-Protokolle, Core Dumps und MIB-Dateien

Der (`spi`Webdienst Service Processor Infrastructure) ist standardmäßig aktiviert, um einen Webbrowser zu ermöglichen, auf die Protokoll-, Core Dump- und MIB-Dateien eines Knotens im Cluster zuzugreifen. Der Zugriff auf die Dateien bleibt auch dann möglich, wenn der Node ausfällt, wenn der Node vom Partner übernommen wird.

Bevor Sie beginnen

- Die Cluster-Management-LIF muss aktiv sein.

Sie können die Management-LIF des Clusters oder einen Node für den Zugriff auf den `spi` Web-Service verwenden. Allerdings wird die Verwendung der Cluster-Management-LIF empfohlen.

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

Erfahren Sie mehr über `network interface show` in der ["ONTAP-Befehlsreferenz"](#).

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

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

- Wenn Sie nicht die `admin` Benutzerkonto (einschließlich der `http` Zugriffsmethode standardmäßig), muss Ihr Benutzerkonto mit der `http` Zugriffsmethode.

Der `security login show` Befehl zeigt die Zugriffs- und Anmeldemethoden von Benutzerkonten und ihre Zugriffskontrollrollen an.

Erfahren Sie mehr über `security login show` in der ["ONTAP-Befehlsreferenz"](#).

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

Mit dem `system services web show` Befehl wird die Konfiguration der Web-Protokoll-Engine auf Cluster-Ebene angezeigt.

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`).

Der `admin` Rolle wird Zugriff auf die `spi` Webdienst standardmäßig und der Zugriff kann manuell deaktiviert werden (`services web access delete -vserver cluster_name -name spi -role admin`).

Schritte

1. Zeigen Sie im Webbrowser spi in einem der folgenden Formate auf die Webservice-URL:
 - `http://cluster-mgmt-LIF/spi/`
 - `https://cluster-mgmt-LIF/spi/`

cluster-mgmt-LIF ist die IP-Adresse der Cluster-Management-LIF.
2. Wenn Sie vom Browser dazu aufgefordert werden, geben Sie Ihr Benutzerkonto und Ihr Passwort ein.

Nachdem Ihr Konto authentifiziert wurde, zeigt der Browser Links zu den `/mroot/etc/log/` `/mroot/etc/crash/` `/mroot/etc/mib/` Verzeichnissen, und der einzelnen Knoten im Cluster an.

Zugriff auf die Systemkonsole eines ONTAP Node

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

Über diese Aufgabe

Sowohl der SP als auch die ONTAP bieten Befehle, mit denen Sie auf die Systemkonsole zugreifen können. Über den SP können Sie jedoch nur auf die Systemkonsole seines eigenen Node zugreifen. Vom Cluster aus können Sie auf die Systemkonsole eines beliebigen anderen Node im Cluster (außer dem lokalen Node) zugreifen.

Schritte

1. Zugriff auf die Systemkonsole eines Node:

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

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

Beispiele für den Zugriff auf die Systemkonsole

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

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

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

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

```
Connection to 123.12.123.12 closed.
```

```
SP node2>
```

Im folgenden Beispiel wird das Ergebnis angezeigt, wenn Sie den `system node run-console` Befehl von ONTAP zum Zugriff auf die Systemkonsole von node2 eingeben, die an der Eingabeaufforderung der Boot-Umgebung hängt. Der `boot_ontap` Befehl wird an der Konsole eingegeben, um node2 zu ONTAP zu booten. Strg-D wird dann gedrückt, um die Konsole zu verlassen und zur ONTAP zurückzukehren.

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

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

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

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

Management von ONTAP Node Root-Volumes und Root-Aggregaten

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

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

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

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

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

- Sie können das Root-Volume zu einem anderen Aggregat verschieben. Siehe [\[relocate-root\]](#).

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

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

"NetApp Hardware Universe"

Geben Sie Speicherplatz im Root-Volume eines Node frei

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

Schritte

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

```
system node coredump show
```

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

```
system node coredump delete
```

3. Zugriff auf die Hölle:

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

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

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

```
priv set advanced
```

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

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

```
ls /etc
```

b. Wenn (*.trc` sich irgendwelche Packet Trace Dateien im Root Volume des Knotens befinden, löschen Sie sie einzeln:

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

6. Identifizieren und löschen Sie die Root-Volume-Snapshots des Node über die nodeshell:

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

```
vol status
```

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

Im folgenden Beispiel lautet das Root-Volume vol0:

```
node1*> vol status

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

a. Root-Volume-Snapshots anzeigen:

```
snap list root_vol_name
```

b. Unerwünschte Root-Volume-Snapshots löschen:

```
snap delete root_vol_name snapshot_name
```

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

```
exit
```

Verschieben von Root-Volumes in neue Aggregate

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

Über diese Aufgabe

Storage-Failover muss aktiviert sein, um Root-Volumes zu verschieben. Sie können den storage failover

`modify -node nodename -enable true` Befehl zum Aktivieren des Failover verwenden.

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set privilege advanced
```

2. Verschieben des Root-Aggregats:

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

- **-Node**

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

- **-disklist**

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

- **-RAID-Typ**

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

3. Überwachen des Fortschritts des Jobs:

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

Ergebnisse

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

Verwandte Informationen

- ["Speicherfailover ändern"](#)

Starten oder Stoppen eines ONTAP-Node für Wartungsarbeiten oder zur Fehlerbehebung

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

Mit dem SP-CLI-Befehl `system power off` oder `system power cycle` zum aus- und Wiedereinschalten eines Node kann ein Node zu einem nicht ordnungsgemäßen Herunterfahren des Node führen (dies wird auch

„Dirty shutdown“ genannt) und ist kein Ersatz für ein ordnungsgemäßes Herunterfahren mit dem ONTAP-`system node halt` Befehl.

Booten Sie einen Node an der Eingabeaufforderung des Systems neu

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

Schritte

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

- a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

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

```
cluster show
```

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

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

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

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

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

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

- c. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. `system node reboot` Booten Sie den Node mit dem Befehl neu.

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

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

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

Starten Sie ONTAP an der Eingabeaufforderung der Boot-Umgebung

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

Schritte

1. Greifen Sie über die Eingabeaufforderung des Speichersystems mit dem `system node halt` Befehl auf die Eingabeaufforderung für die Startumgebung zu.

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

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

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

Wenn Sie sich nicht sicher sind, welches Bild verwendet werden soll, sollten Sie `boot_ontap` es zunächst verwenden.

Fahren Sie einen Node herunter

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

Schritte

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

- a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

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

```
cluster show
```

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

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

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

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

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

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

- c. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

2. Fahren Sie `system node halt` den Node mit dem Befehl herunter.

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

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

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

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

Managen eines ONTAP-Node über das Boot-Menü

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



Wenn ein HA-Paar verwendet "Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)", müssen Sie die Anweisungen im Thema "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren" für alle Laufwerke innerhalb des HA-Paars befolgen, bevor Sie das System initialisieren (Startoptionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Schritte

1. Booten Sie den Node neu, um auf das Boot-Menü zuzugreifen `system node reboot`, indem Sie den Befehl an der Systemaufforderung verwenden.

Der Node startet den Neubootvorgang.

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

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

```
(1) Normal Boot.  
(2) Boot without /etc/rc.  
(3) Change password.  
(4) Clean configuration and initialize all disks.  
(5) Maintenance mode boot.  
(6) Update flash from backup config.  
(7) Install new software first.  
(8) Reboot node.  
(9) Configure Advanced Drive Partitioning.  
(10) Set onboard key management recovery secrets.  
(11) Configure node for external key management.  
Selection (1-11) ?
```



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

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

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

An...	Auswählen...
<p>Initialisieren Sie die Festplatten des Node und erstellen Sie ein Root-Volume für den Node</p>	<p>4) Reinigen Sie die Konfiguration und initialisieren Sie alle Festplatten</p> <p> Mit dieser Menüoption werden alle Daten auf den Festplatten des Knotens gelöscht und die Knotenkonfiguration auf die werkseitigen Standardeinstellungen zurückgesetzt.</p> <p>Wählen Sie diesen Menüpunkt nur aus, nachdem der Knoten aus einem Cluster entfernt wurde und nicht einem anderen Cluster beigetreten ist.</p> <p>Bei einem Node mit internen oder externen Festplatten-Shelfs wird das Root-Volume auf den internen Festplatten initialisiert. Wenn keine internen Festplatten-Shelfs vorhanden sind, wird das Root-Volume auf den externen Festplatten initialisiert.</p> <p>Wenn der Node, den Sie initialisieren möchten, über Laufwerke verfügt, die für die Root-Daten-Partitionierung partitioniert sind, müssen die Laufwerke unpartitioniert werden, bevor der Node initialisiert werden kann, siehe 9) Konfigurieren der erweiterten Laufwerkpartitionierung und "Festplatten- und Aggregatmanagement".</p>
<p>Führen Sie Wartungsvorgänge für Aggregate und Festplatten durch und erhalten Sie detaillierte Aggregat- und Festplatteninformationen.</p>	<p>5) Bootvorgang im Wartungsmodus</p> <p>Sie beenden den Wartungsmodus mit dem <code>halt</code> Befehl.</p>
<p>Stellen Sie die Konfigurationsinformationen vom Root-Volume des Node auf das Boot-Gerät, z. B. eine PC CompactFlash Card, wieder her</p>	<p>6) Flash aus Backup-Konfiguration aktualisieren</p> <p>ONTAP speichert einige Node-Konfigurationsinformationen auf dem Boot-Gerät. Beim Neubooten des Node werden die Informationen zum Boot-Gerät automatisch auf dem Root-Volume des Node gesichert. Wenn das Startgerät beschädigt wird oder ersetzt werden muss, müssen Sie diese Menüoption verwenden, um die Konfigurationsinformationen aus dem Stammvolumen des Knotens wieder auf das Startgerät wiederherzustellen.</p>

An...	Auswählen...
Installieren Sie auf dem Node neue Software	<p>7) Neue Software zuerst installieren</p> <p>Wenn die ONTAP-Software auf dem Boot-Gerät keine Unterstützung für das Speicher-Array bietet, das Sie für das Root-Volume verwenden möchten, können Sie mit dieser Menüoption eine Version der Software erhalten, die Ihr Speicher-Array unterstützt und auf dem Knoten installieren.</p> <p>Diese Menüoption dient nur zur Installation einer neueren Version der ONTAP-Software auf einem Knoten, auf dem kein Root-Volume installiert ist. Do_Non_Use Verwenden Sie diese Menüoption, um ONTAP zu aktualisieren.</p>
Booten Sie den Node neu	8) Node neu booten
Heben Sie die Partitionierung aller Festplatten auf, entfernen Sie deren Besitzinformationen oder reinigen Sie die Konfiguration und initialisieren Sie das System mit ganzen oder partitionierten Festplatten	<p>9) Konfigurieren Der Erweiterten Laufwerkpartitionierung</p> <p>Die Option „Erweiterte Laufwerkpartitionierung“ bietet zusätzliche Verwaltungsfunktionen für Datenträger, die für die Root-Daten- oder Root-Daten-Daten-Partitionierung konfiguriert sind. Die folgenden Optionen sind über die Boot-Option 9 verfügbar:</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information. (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.</p> </div>

Anzeigen der Attribute der Nodes in einem ONTAP-Cluster

Sie können die Attribute eines oder mehrerer Nodes im Cluster anzeigen, z. B. den Namen, Besitzer, Standort, Modellnummer, Seriennummer, wie lange der Node ausgeführt wurde, den Systemzustand und die Berechtigung, an einem Cluster teilzunehmen.

Schritte

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

Beispiel zum Anzeigen von Informationen über einen Node

Im folgenden Beispiel werden ausführliche Informationen über node1 angezeigt:

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

Ändern Sie die Attribute eines ONTAP-Knotens

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

Über diese Aufgabe

Die Berechtigung eines Node zur Teilnahme an dem Cluster kann auf der erweiterten Berechtigungsebene mit dem `-eligibility` Parameter des `system node modify cluster modify` Befehls oder geändert werden. Wenn Sie die Berechtigung eines Knotens auf festlegen `false`, wird der Knoten im Cluster inaktiv.



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



Sie sollten die Berechtigung eines Knotens nicht auf setzen `false`, außer in Situationen wie dem Wiederherstellen der Knotenkonfiguration oder einer längeren Wartung des Knotens. DER SAN- und NAS-Datenzugriff auf den Node kann davon betroffen sein, wenn der Node nicht verfügbar ist.

Schritte

1. Verwenden Sie den `system node modify` Befehl, um die Attribute eines Knotens zu ändern.

Beispiel zum Ändern von Node-Attributen

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

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

Verwandte Informationen

- ["System-Node ändern"](#)
- ["Cluster ändern"](#)

Umbenennen eines ONTAP-Node

Sie können den Namen eines Node nach Bedarf ändern.

Schritte

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

Der `-newname` Parameter gibt den neuen Namen für den Node an. Erfahren Sie mehr über `system node rename` in der ["ONTAP-Befehlsreferenz"](#).

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



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

Beispiel für die Umbenennung eines Node

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

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

Management eines Single-Node-ONTAP-Clusters

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



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

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

- Die Root-Volume-Verschlüsselung wird auf Single-Node-Clustern nicht unterstützt.
- Wenn Sie Nodes entfernen, um ein Single-Node-Cluster zu besitzen, sollten Sie die Cluster-Ports für den Datenverkehr ändern. Dazu ändern Sie die Cluster-Ports als Daten-Ports und erstellen anschließend Daten-LIFs an den Daten-Ports.
- Für Single-Node-Cluster können Sie das Konfigurations-Backup-Ziel während der Software-Einrichtung angeben. Nach dem Setup können diese Einstellungen mit ONTAP Befehlen geändert werden.

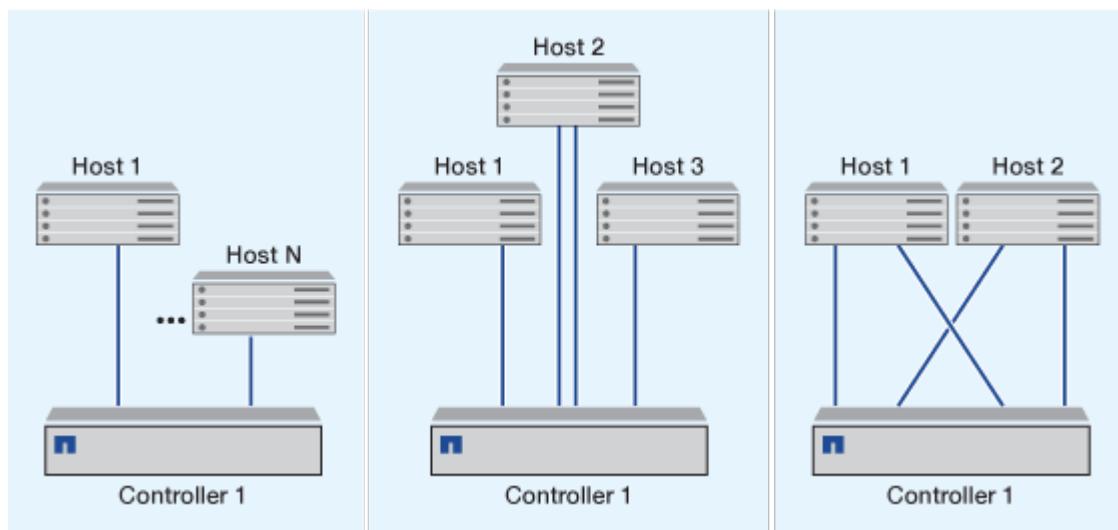
- Wenn mehrere Hosts mit dem Knoten verbunden sind, kann jeder Host mit einem anderen Betriebssystem wie Windows oder Linux konfiguriert werden. Wenn mehrere Pfade vom Host zum Controller vorhanden sind, muss ALUA auf dem Host aktiviert sein.

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

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

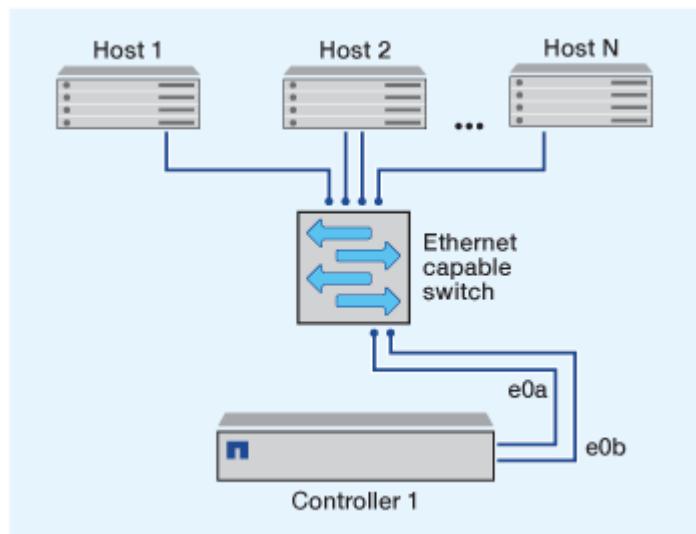
Direct-Attached Single Node-Konfigurationen

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



Single-Network-Konfiguration mit Single Node-Konfiguration

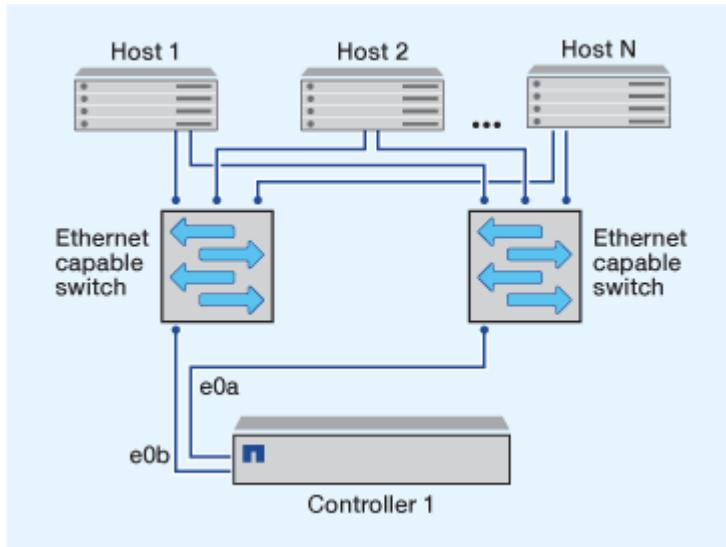
In Single-Network-Konfigurationen mit einem oder mehreren Hosts wird über einen Switch ein Node mit einem oder mehreren Hosts verbunden. Da es einen einzelnen Switch gibt, ist diese Konfiguration nicht vollständig redundant.



Single Node-Konfigurationen in mehreren Netzwerken

Bei Konfigurationen mit einem einzigen Netzwerk mit mehreren Nodes werden mindestens zwei Switches

einen einzelnen Node mit einem oder mehreren Hosts verbunden. Da es mehrere Switches gibt, ist diese Konfiguration vollständig redundant.



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

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

Single-Fabric-Single-Node-Konfigurationen

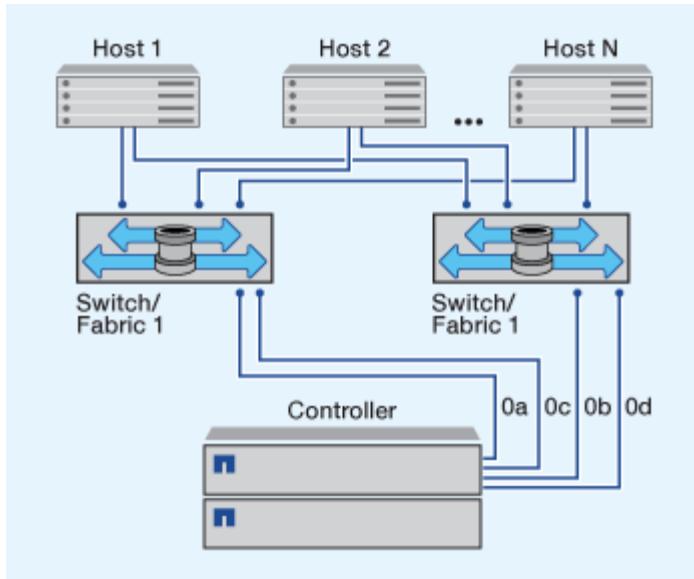
Bei Single-Fabric-Konfigurationen mit einem Node kann ein Switch einen einzelnen Node mit einem oder mehreren Hosts verbinden. Da es einen einzelnen Switch gibt, ist diese Konfiguration nicht vollständig redundant.

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

Single Node-Konfigurationen in MultiFabric-Architektur

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

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



Verwandte Informationen

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

ONTAP Upgrade für Single-Node-Cluster

Mit der ONTAP CLI können Sie ein automatisiertes Update eines Single-Node-Clusters durchführen. Single-Node-Cluster verfügen über keine Redundanz, daher sind Updates immer störend. Mit System Manager können Sie keine störenden Upgrades durchführen.

Bevor Sie beginnen

Sie müssen die Upgrade-["Vorbereitung"](#) Schritte ausführen.

Schritte

1. Löschen Sie das frühere ONTAP-Softwarepaket:

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

2. Laden Sie das ONTAP-Zielsoftwarepaket herunter:

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

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

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

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

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

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

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

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

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

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

5. Überwachen Sie den Fortschritt der Validierung:

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

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

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

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

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

8. Durchführen des Software-Updates:

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



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

9. Zeigt den Status des Cluster-Updates an:

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

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

10. Auslösen einer Benachrichtigung:

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

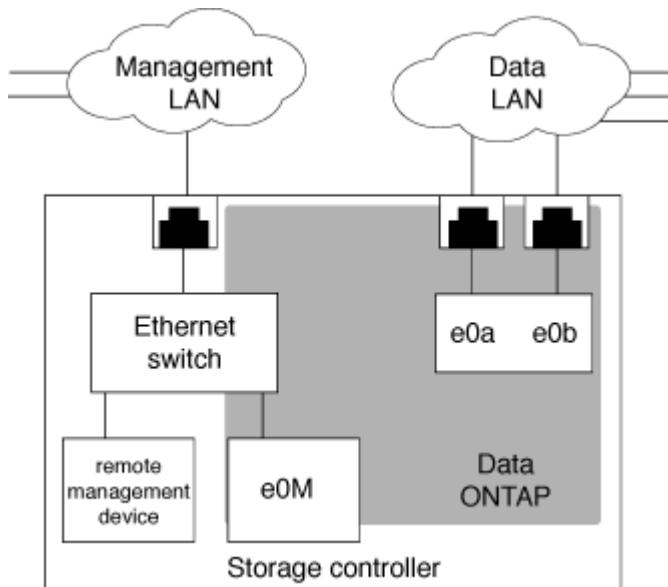
Wenn Ihr Cluster nicht für das Senden von Meldungen konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

Konfigurieren Sie das SP/BMC-Netzwerk

Isolieren Sie den ONTAP-Managementverkehr im Netzwerk

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

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



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

Wenn Sie den Verwaltungsdatenverkehr nicht isolieren können oder wenn Ihr dediziertes Managementnetzwerk ungewöhnlich groß ist, sollten Sie versuchen, das Volumen des Netzwerkdatenverkehrs

so gering wie möglich zu halten. Übermäßiger Ingress-Broadcast- oder Multicast-Datenverkehr kann die SP/BMC-Leistung beeinträchtigen.



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

Informieren Sie sich über die ONTAP SP/BMC-Netzwerkkonfiguration

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



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

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

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

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

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

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

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

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

Wenn die automatische SP-Netzwerkkonfiguration deaktiviert ist (standardmäßig), gelten die folgenden

Szenarien und Überlegungen:

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

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

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

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

Wenn die automatische SP-Netzwerkkonfiguration nach erfolgter Aktivierung deaktiviert ist, gelten die folgenden Szenarien und Überlegungen:

- Wenn für die automatische Netzwerkkonfiguration `system service-processor network modify` von SP die IPv4-Adressenfamilie deaktiviert ist, wird im SP-IPv4-Netzwerk standardmäßig DHCP verwendet, und mit dem Befehl können Sie die SP-IPv4-Konfiguration für einzelne Nodes ändern.
- Wenn für die automatische Netzwerkkonfiguration `system service-processor network modify` von SP die IPv6-Adressenfamilie deaktiviert ist, wird auch das SP-IPv6-Netzwerk deaktiviert, und mit dem Befehl können Sie die SP-IPv6-Konfiguration für einzelne Knoten aktivieren und ändern.

Aktivieren der automatischen Netzwerkkonfiguration für ONTAP SP/BMC

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



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

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

Der `network subnet show` Befehl zeigt Subnetz-Informationen für das Cluster an.

Erfahren Sie mehr über `network subnet show` in der "[ONTAP-Befehlsreferenz](#)".

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

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

Der `network options ipv6 show` Befehl zeigt den aktuellen Status der IPv6-Einstellungen für ONTAP an. Erfahren Sie mehr über `network options ipv6 show` in der "[ONTAP-Befehlsreferenz](#)".

Schritte

1. Geben Sie mit dem `system service-processor network auto-configuration enable` Befehl die IPv4- oder IPv6-Adressenfamilie und den Namen für das Subnetz an, das die SP verwenden soll.
2. Zeigt die automatische Netzwerkkonfiguration von SP mit dem `system service-processor network auto-configuration show` Befehl an.
3. Wenn Sie anschließend die SP IPv4- oder IPv6-Netzwerkschnittstelle für alle Knoten deaktivieren oder wieder aktivieren möchten, die sich im Quorum befinden, verwenden Sie den `system service-processor network modify` Befehl mit den `-address-family [IPv4|IPv6 -enable [true|`false`Parameters] und]`.

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

Wenn ein Knoten nicht über das Quorum verfügt, können Sie die SP-Netzwerkkonfiguration des Node, einschließlich der SP-IP-Adresse, ändern, indem `system service-processor network modify` Sie über den Node ausführen und bestätigen, dass Sie die automatische SP-Netzwerkkonfiguration für den Node überschreiben möchten. Wenn der Node jedoch dem Quorum Beitritt, erfolgt die automatische SP-Neukonfiguration für den Node auf Grundlage des angegebenen Subnetzes.

Konfigurieren Sie das ONTAP SP/BMC-Netzwerk manuell

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

Bevor Sie beginnen

Wenn Sie IPv6-Verbindungen für den SP verwenden möchten, muss IPv6 bereits für ONTAP konfiguriert und aktiviert sein. Die `network options ipv6` Befehle verwalten IPv6-Einstellungen für ONTAP. Erfahren Sie mehr über `network options ipv6` in der ["ONTAP-Befehlsreferenz"](#).



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

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

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

Schritte

1. Konfigurieren Sie mit dem `system service-processor network modify` Befehl das SP-Netzwerk für einen Node.
 - Der `-address-family` Parameter gibt an, ob die IPv4- oder IPv6-Konfiguration der SP geändert werden soll.
 - 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 werden soll.

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

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

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

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

2. Konfigurieren Sie das SP-Netzwerk für die im Cluster verbliebenen Nodes, indem Sie den Schritt 1 wiederholen.
3. Zeigen Sie die SP-Netzwerkkonfiguration an und überprüfen Sie den SP Setup-Status mithilfe des `system service-processor network show` Befehls mit den `-instance -field setup-status` Parametern oder.

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

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

Beispiel für das Konfigurieren des SP-Netzwerks

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

```

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

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

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

1 entries were displayed.

cluster1::>

```

Ändern Sie die Konfiguration der ONTAP-Serviceprozessor-API

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

Über diese Aufgabe

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

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

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

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

- Der SP-API-Service ist standardmäßig aktiviert.

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

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

Schritte

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

Ihr Ziel ist	Verwenden Sie den folgenden Befehl...
Ändern Sie den Port, der vom SP-API-Service verwendet wird	<code>system service-processor api-service modify Mit dem -port {49152..65535} Parameter .}</code>
Erneuern der vom SP-API-Service verwendeten SSL- und SSH-Zertifikate für die interne Kommunikation	<ul style="list-style-type: none"> • Für ONTAP 9.5 oder spätere Verwendung <code>system service-processor api-service renew-internal-certificate</code> • Für ONTAP 9.4 und frühere Verwendung <code>system service-processor api-service renew-certificates</code> <p>Wenn kein Parameter angegeben wird, werden nur die Host-Zertifikate (einschließlich der Client- und Server-Zertifikate) erneuert.</p> <p>Wenn der <code>-renew-all true</code> Parameter angegeben wird, werden sowohl die Hostzertifikate als auch das Stammzertifizierungsstellenzertifikat erneuert.</p>
komm	
Deaktiviert bzw. reaktiviert den SP-API-Service	<code>system service-processor api-service modify Mit dem -is-enabled {true}</code>

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

Remote-Verwaltung von Knoten über den SP/BMC

Managen Sie einen ONTAP-Knoten per Remote-Zugriff über das SP/BMC

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

Eine vollständige Aufschlüsselung der Unterstützung von Plattform-SP und BMC finden Sie auf der NetApp Support Site im "[Support-Matrix](#)".

Remote-Node-Management mit dem ONTAP Serviceprozessor

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

Zu den wichtigsten Funktionen des SP gehören:

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

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

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

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

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

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

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

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

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



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

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

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

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

Das SEL enthält die folgenden Informationen:

- Vom SP erkannte Hardware-Events, beispielsweise Sensorstatus zu Netzteilen, Spannung oder anderen Komponenten
 - Vom SP erkannte Fehler, beispielsweise ein Kommunikationsfehler, ein Ausfall des Lüfters oder ein Arbeitsspeicher- oder CPU-Fehler
 - Vom Node an die SP gesendete kritische Softwareereignisse – beispielsweise Panic, ein Kommunikationsfehler, ein Boot-Fehler oder ein vom Benutzer ausgelöster „down System“ als Ergebnis der Ausgabe 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 sie im Konsole-Protokoll. Das Konsole-Protokoll bleibt gespeichert, solange der SP von einem der Netzteile des Node mit Strom versorgt wird. Da der SP mit Standby-Strom betrieben wird, bleibt er auch dann verfügbar, wenn der Node aus- und wieder eingeschaltet oder ganz ausgeschaltet wird.

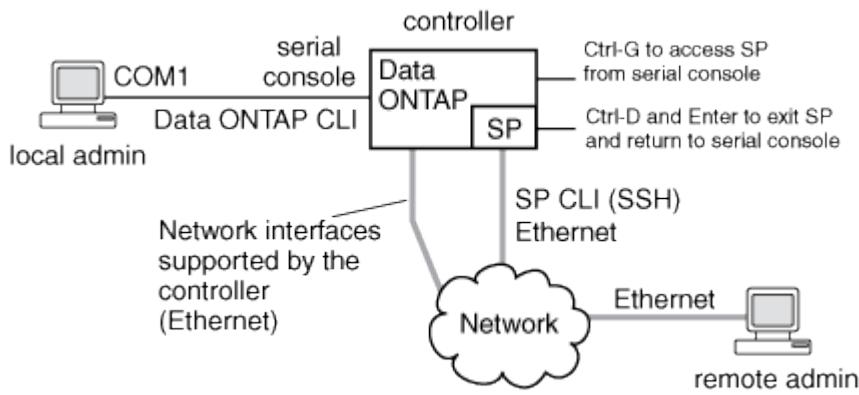
- Die Hardware-gestützte Übernahme ist verfügbar, wenn der SP konfiguriert ist.
- Der SP-API-Service ermöglicht die Kommunikation zwischen ONTAP und dem SP über das Netzwerk.

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

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

Das folgende Diagramm zeigt den Zugriff auf ONTAP und den SP eines Node. Auf die SP-Schnittstelle ist über den Ethernet-Port zugegriffen (wird durch ein Schraubenschlüsselsymbol auf der Rückseite des Chassis

angezeigt):



Verwenden Sie den ONTAP Baseboard-Verwaltungscontroller zur Remote-Verwaltung eines Knotens

Auf bestimmten Hardwareplattformen wird die Software so angepasst, dass sie einen neuen Onboard-Controller im Baseboard-Verwaltungscontroller (BMC) unterstützt. Der BMC verfügt über CLI-Befehle (Command Line Interface), mit denen Sie das Gerät Remote managen können.

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

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

Es gibt einige Unterschiede zwischen SP und BMC:

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

Automatische Firmware-Updates sind auch beim Ausführen von ONTAP mit den folgenden Anforderungen verfügbar:

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



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

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



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

Managen von Updates der ONTAP SP/BMC-Firmware

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



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

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

- Die Funktion für die automatische Aktualisierung des SP ist standardmäßig aktiviert, sodass die SP-Firmware in folgenden Szenarien automatisch aktualisiert werden kann:

- Wenn Sie ein Upgrade auf eine neue Version von ONTAP durchführen

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



ONTAP erkennt ein fehlgeschlagenes automatisches SP Update und löst eine Korrekturmaßnahme aus, um das automatische SP Update bis zu dreimal zu wiederholen. Wenn alle drei Versuche fehlgeschlagen, lesen Sie die "[NetApp Knowledge Base: Health Monitor SPAutoUpgradeFailedMajorAlert SP Upgrade schlägt fehl – AutoSupport Meldung](#)".

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

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

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

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

Sie können die folgenden Optionen angeben:

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

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

- Ob das SP-Firmware-Paket für das SP-Update verwendet (`-baseline` werden soll)

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



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

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

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

Verwandte Informationen

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

ONTAP SP/BMC und die Netzwerkschnittstellen verwenden für Firmware-Updates

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



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

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

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

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

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

Verwandte Informationen

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

Greifen Sie über ein Cluster-Benutzerkonto auf den ONTAP Serviceprozessor zu

Wenn Sie versuchen, auf den SP zuzugreifen, werden Sie nach Berechtigungen gefragt.

Cluster-Benutzerkonten, die mit dem `service-processor` Applikationstyp erstellt werden, haben Zugriff auf die SP-CLI auf einem beliebigen Node des Clusters. SP-Benutzerkonten werden über ONTAP verwaltet und per Passwort authentifiziert. 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 die SP zugreifen, wenn es mit dem `-application` Parameter des `security login create` Befehls set to `service-processor` und dem `-authmethod` Parameter set to erstellt wird `password`. Der SP unterstützt nur die Passwort-Authentifizierung.

Sie müssen den `-role` Parameter angeben, wenn Sie ein SP-Benutzerkonto erstellen.

- In Versionen von ONTAP 9.9.1 und neueren Versionen müssen Sie `admin` für den `-role` Parameter angeben, und alle Änderungen an einem Konto erfordern die `admin` Rolle. Andere Rollen sind aus Sicherheitsgründen nicht mehr zulässig.
 - Wenn Sie ein Upgrade auf ONTAP 9.9.1 oder höhere Versionen durchführen, finden Sie unter "[Ändern von Benutzerkonten, die auf den Service Processor zugreifen können](#)".
 - Wenn Sie auf ONTAP 9.8 oder frühere Versionen zurückkehren, siehe "[Überprüfen Sie, ob Benutzerkonten, die auf den Service Processor zugreifen können](#)".
- In ONTAP 9.8 und früheren Versionen kann jede Rolle auf das SP zugreifen, `admin` wird aber empfohlen.

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

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

Sie können mit dem `-application` `service-processor` Parameter des `security login show` Befehls aktuelle SP-Benutzerkonten anzeigen.

Erfahren Sie mehr über `security login show` in der "[ONTAP-Befehlsreferenz](#)".

Greifen Sie von einem Administrations-Host aus auf die ONTAP SP/BMC eines Node zu

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

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



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

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

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

Schritte

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

```
ssh username@SP_IP_address
```

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

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

Beispiele für SP-Zugriff von einem Administrationshost aus

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

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

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

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

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

Greifen Sie über die Systemkonsole auf die ONTAP SP/BMC eines Node zu

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

```
cluster1::>
```

Erfahren Sie, wie ONTAP SP-CLI-, SP-Konsole- und Systemkonsolensitzungen zusammenhängen

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

Umgebungen mit unabhängiger Anmeldeauthentifizierung.

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

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

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

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

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

Wenn Sie eine SP-Konsolensitzung über die SP-CLI starten (mit dem `system console` Befehl SP), werden Sie nach den Berechtigungen für die Systemkonsole gefragt. Wenn Sie über eine Systemkonsolensession auf die SP-CLI zugreifen (durch Drücken von Strg-G), werden Sie nach den SP-CLI-Berechtigungen gefragt.

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

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

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

Fügen Sie die Administrations-Host-IP-Adresse hinzu, um auf den ONTAP Serviceprozessor zuzugreifen

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

Schritte

1. Gewähren Sie SP-Zugriff nur auf die IP-Adressen, die Sie mit dem `system service-processor ssh add-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter angeben.
 - Der Wert des `-allowed-addresses` Parameters muss im Format angegeben werden `address /netmask`, und mehrere `address/netmask` Paare müssen durch Kommas getrennt werden, zum Beispiel `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Wenn Sie den `-allowed-addresses` Parameter auf `0.0.0.0/0, ::/0` festlegen, können alle IP-Adressen auf die SP zugreifen (Standardeinstellung).

- Wenn Sie die Standardeinstellung ändern, indem Sie den SP-Zugriff auf die von Ihnen angegebenen IP-Adressen beschränken, fordert ONTAP Sie auf zu bestätigen, dass die angegebene IP-Adresse die Standardeinstellung „allow all“ ersetzen soll(`0.0.0.0/0, ::/0.`)
 - Mit dem `system service-processor ssh show` Befehl werden die IP-Adressen angezeigt, die auf die SP zugreifen können.
2. Wenn Sie den Zugriff einer angegebenen IP-Adresse auf die SP blockieren möchten, verwenden Sie den `system service-processor ssh remove-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter.

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

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

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

```

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

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

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

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

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

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

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

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

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

```

Zeigen Sie die Hilfeinformationen in der ONTAP SP/BMC-CLI an

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

Über diese Aufgabe

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

Schritte

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

Um auf die SP-Hilfe zuzugreifen...	Um auf die BMC-Hilfe zuzugreifen...
Geben Sie <code>help</code> an der SP-Eingabeaufforderung ein.	Geben Sie <code>system</code> an der BMC-Eingabeaufforderung ein.

Das folgende Beispiel zeigt die SP CLI Online-Hilfe.

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

Das folgende Beispiel zeigt die BMC CLI Online-Hilfe.

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

BMC>
```

2. Um Hilfeinformationen für die Option eines Befehls „SP/BMC help“ anzuzeigen, geben Sie vor oder nach dem Befehl „SP/BMC“ ein.

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

```
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
```

Im folgenden Beispiel wird die BMC-CLI-Online-Hilfe für den `system power` Befehl BMC angezeigt.

```
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>
```

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "[ONTAP-Befehlsreferenz](#)".

Verwandte Informationen

- "[Veranstaltungen](#)"
- "[Stromversorgung des Systems](#)"

ONTAP-Befehle für das Remote-Node-Management

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 ausgeführte Remote-Knotenverwaltungsaufgaben können Sie auch ONTAP -Befehle von einem anderen Knoten im Cluster verwenden. 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 Aufrufen 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 verfügbar in "[Zeigen Sie die Hilfeinformationen in der ONTAP SP/BMC-CLI an](#)".

Erfahren Sie mehr über die entsprechende ONTAP BMC CLI in "[Unterstützte CLI-Befehle für den ONTAP Baseboard-Verwaltungscontroller](#)".

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
Verfügbare Befehle oder Unterbefehle eines angegebenen Befehls für SP/ BMC/ ONTAP anzeigen	help [command]	help [command]	1. A.
Anzeige der aktuellen Berechtigungsstufe für die SP/ BMC/ ONTAP CLI	priv show	priv show	1. A.
Legen Sie die Berechtigungsebene für den Zugriff auf den angegebenen Modus für die SP/ BMC/ ONTAP -CLI fest	priv set {admin	advanced	diag }
priv set {admin	advanced	diag	test }
1. A.	Zeigt Datum und Uhrzeit des Systems an	date	date
date	Zeigt Ereignisse an, die vom SP/ BMC/ ONTAP protokolliert werden	events {all	info
newest number	oldest number	search keyword}	events {all
info	newest	oldest	search }
1. A.	Anzeige des SP/ BMC/ ONTAP -Status und der Netzwerkkonfigurationsinformationen	sp status [-v	* Der -v Option zeigt SP Statistiken in ausführlicher Form an. * Der -d Option fügt das SP Debug-Protokoll zur Anzeige hinzu.

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
bmc status [-v]	-d] * Der -v Option zeigt SP Statistiken in ausführlicher Form an. * Der -d Option fügt das SP Debug-Protokoll zur Anzeige hinzu.	system service-processor show	Zeigt die Zeitspanne an, in der SP/ BMC/ ONTAP aktiv war, sowie die durchschnittliche Anzahl der Jobs in der Ausführungswarteschlange in den letzten 1, 5 und 15 Minuten.
sp uptime	bmc uptime	1. A.	Zeigt Protokolle der Systemkonsole an
system log	system log [-a]	system log (druckt Systemkonsolenprotokolle)	Anzeige der SP/ BMC/ ONTAP Log-Archive 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 }]
1. A.	Zeigt den Stromstatus des Controllers eines Node an	system power status	system power status
system node power show	Zeigt Informationen zur Batterie an	system battery show	system battery show
1. A.	Zeigen Sie ACP-Informationen oder den Status von Expander-Sensoren an	system acp [show	sensors show]
1. A.	1. A.	Listen Sie alle System-FRUs und ihre IDs auf	system fru list
system fru list	1. A.	Zeigt Produktinformationen für die angegebene FRU an	system fru show fru_id

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
system fru show [show <id>]	1. A.	Zeigt das FRU-Datenhistorie-Protokoll an	system fru log show (Erweiterte Berechtigungsebene)
system fru log show	1. A.	Zeigt den Status der Umgebungssensoren an, einschließlich ihrer Status und aktuellen Werte	system sensors Oder system sensors show
system sensors {show	filter <sensor_string>}	system node environment sensors show	Status und Details für den angegebenen Sensor anzeigen
system sensors get sensor_name Sie können die sensor_name mit dem system sensors system sensors show Befehl oder abrufen.	system sensors [get]	1. A.	Zeigen Sie die Informationen zur SP/ BMC/ ONTAP -Firmware -Version an
version	version	system service-processor image show	Zeigen Sie den SP/ BMC/ ONTAP -Befehlsverlauf an
sp log audit (Erweiterte Berechtigungsebene)	bmc log audit (Erweiterte Berechtigungsebene)	1. A.	Zeigen Sie die SP/ BMC/ ONTAP -Debuginformationen an
sp log debug (Erweiterte Berechtigungsebene)	bmc log debug (Erweiterte Berechtigungsebene)	1. A.	Zeigen Sie die SP/ BMC/ ONTAP -Nachrichtendatei an

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
sp log messages (Erweiterte Berechtigungsebene)	bmc log messages (Erweiterte Berechtigungsebene)	1. A.	Anzeigen der Einstellungen für das Sammeln der Systemforensik bei einem Watchdog-Reset-Ereignis, Anzeigen der Systemforensik-Informationen, die während eines Watchdog-Reset-Ereignisses gesammelt wurden, oder Löschen der gesammelten Informationen zur Systemforensik
system forensics [show	log dump	log clear]	1. A.
1. A.	Melden Sie sich bei der Systemkonsole an	system console	system console
system node run-console	Drücken Sie Strg-D, um die Systemkonsolensitzung zu beenden.	Schalten Sie den Knoten ein oder aus, oder führen Sie ein aus- und wieder ein (aus- und wieder einschalten).	system power on
system power on	system node power on (Erweiterte Berechtigungsebene)	system power off	system power off
1. A.	system power cycle	system power cycle	1. A.

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
<p>Die Standby-Stromversorgung bleibt eingeschaltet, damit der SP unterbrechungsfrei betrieben wird. Während des Einschaltzyklus erfolgt eine kurze Pause, bevor der Strom wieder eingeschaltet wird.</p> <p> Wenn der Node mit diesen Befehlen aus- und wieder eingeschaltet wird, kann dies zu einem nicht ordnungsgemäßen Herunterfahren des Node führen (das auch „<i>Dirty shutdown</i>“ genannt system node halt wird) und ist kein Ersatz für ein ordnungsgemäßes Herunterfahren mit dem Befehl ONTAP.</p>	<p>Erstellen Sie einen Core Dump, und setzen Sie den Node zurück</p>	<p><code>system core [-f]</code></p> <p>Die <code>-f</code> Option erzwingt das Erstellen eines Core Dump und das Zurücksetzen des Node.</p>	<p><code>system core</code></p>

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

Ihr Ziel ist		Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
	<p>Dieser Vorgang bewirkt ein nicht ordnungsgemäßes Herunterfahren des Node.</p> <p>Wenn kein BIOS-Firmware-Image angegeben wird, wird das aktuelle Image für das Neubooten verwendet. Der SP bleibt betriebsbereit, solange die Input-Stromversorgung des Node nicht unterbrochen wird.</p>	<p>Vergleicht das aktuelle Akku-Firmware-Image mit einem angegebenen Firmware-Image</p>	<p><code>system battery verify [image_URL]</code> (Erweiterte Berechtigungsebene)</p> <p>Wenn <code>image_URL</code> nicht angegeben wird, wird das Standard-Image der Akku-Firmware zum Vergleich verwendet.</p>	<p><code>system battery verify [image_URL]</code> (Erweiterte Berechtigungsebene)</p> <p>Wenn <code>image_URL</code> nicht angegeben wird, wird das Standard-Image der Akku-Firmware zum Vergleich verwendet.</p>
1. A.		<p>Aktualisieren Sie die Akku-Firmware vom Image am angegebenen Speicherort</p>	<p><code>system battery flash [image_URL]</code> (Erweiterte Berechtigungsebene)</p> <p>Sie verwenden diesen Befehl, wenn das automatische Update der Akku-Firmware aus einem bestimmten Grund fehlgeschlagen ist.</p>	1. A.
1. A.		<p>Aktualisieren Sie die SP/ BMC/ ONTAP -Firmware mithilfe des Images am angegebenen Speicherort</p>	<p><code>sp update</code> <code>image_URL</code> `image_URL` darf 200 Zeichen nicht überschreiten.</p>	<p><code>bmc update</code> <code>image_URL</code> `image_URL` darf 200 Zeichen nicht überschreiten.</p>
system service-processor image update		Starten Sie SP/ BMC/ ONTAP	<code>sp reboot</code>	<code>bmc reboot</code>

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl...	Verwenden Sie diesen BMC-Befehl...	Verwenden Sie diesen ONTAP -Befehl ...
system service-processor reboot-sp	Löscht den NVRAM-Flash-Inhalt	system nvram flash clear (Erweiterte Berechtigungsebene) Dieser Befehl kann nicht gestartet werden, wenn die Steuerung ausgeschaltet ist (system power off).	1. A.
1. A.	Beenden Sie die SP/ BMC/ ONTAP CLI	exit	exit

Verwandte Informationen

- ["ONTAP-Befehlsreferenz"](#)

ONTAP Monitoring des Node-Systemzustands mithilfe schwellenwertbasierter Messwerte und Status des SP-Sensors

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

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

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

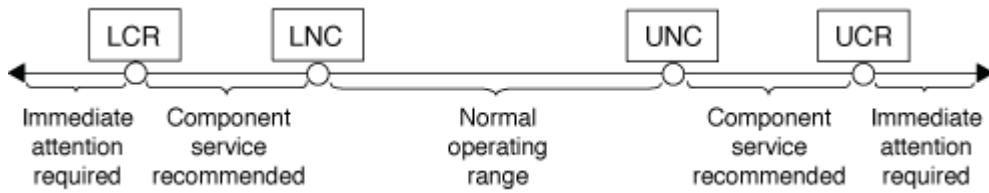
Schwellenwertbasierte Sensoren verfügen über die folgenden Schwellenwerte, die in der Ausgabe des `system sensors` Befehls SP angezeigt werden:

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

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

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

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



Sie können den Messwert eines schwellenwertbasierten Sensors `Current` in der Spalte der `system sensors` Befehlsausgabe des Befehls finden. Mit dem `system sensors get sensor_name` Befehl werden weitere Details für den angegebenen Sensor angezeigt. Wenn der Messwert eines schwellenwertbasierten Sensors den nicht kritischen und kritischen Schwellenwert überschreitet, meldet der Sensor ein Problem mit dem größer werdenden Schweregrad. Wenn der Messwert einen Grenzwert überschreitet, `system sensors` wird `ok` `nc` `cr` je nach Überschreitung des Schwellenwerts der Status des Sensors in der Befehlsausgabe von `in` (nicht kritisch) oder `(kritisch)` geändert, und eine Event-Meldung wird im SEL-Ereignisprotokoll protokolliert.

Manche schwellenwertbasierten Sensoren weisen nicht alle vier Schwellenwertstufen auf. Bei diesen Sensoren werden die fehlenden Schwellenwerte `na` als Grenzwert in der `system sensors` Befehlsausgabe angezeigt. Dies bedeutet, dass der jeweilige Sensor keinen Grenzwert für den angegebenen Schwellenwert hat und dass der SP den Sensor für diesen Schwellenwert nicht überwacht.

Beispiel der Befehlsausgabe des Befehls „System Sensors“

Im folgenden Beispiel werden einige der Informationen angezeigt, die mit dem `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 der Befehlausgabe des Befehls „System Sensors“ 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+
```

Statuswerte des ONTAP SP-Sensors in der Befehlsausgabe des Befehls „System Sensor“

Diskrete Sensoren verfügen über keine Schwellenwerte. Ihre Messwerte, die in der Current Spalte der `system sensors` Befehlsausgabe des SP CLI-Befehls angezeigt werden, haben keine tatsächlichen Bedeutungen und werden daher von der SP ignoriert. In der Status Spalte der `system sensors` Befehlsausgabe der Befehlsausgabe werden die Statuswerte der diskreten Sensoren im Hexadezimalformat angezeigt.

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

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

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID          : 7.97
Sensor Type (Discrete): Temperature
States Asserted     : Digital State
                           [State Deasserted]
```

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

Obwohl der `system sensors get sensor_name` Befehl die Statusinformationen für die meisten diskreten Sensoren anzeigt, stellt er keine Statusinformationen für die diskreten Sensoren „System_FW_Status“, „System_Watchdog“, „PSU1_Input_Type“ und „PSU2_Input_Type“ bereit. Sie können die folgenden Informationen nutzen, um die Statuswerte dieser Sensoren zu interpretieren.

„System_FW_Status“

Der Zustand des Sensors „System_FW_Status 0xAABB“ erscheint im Format . Sie können die Informationen von AA und kombinieren BB, um den Zustand des Sensors zu ermitteln.

AA Kann einen der folgenden Werte haben:

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

BB Kann einen der folgenden Werte haben:

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

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

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

„System_Watchdog“

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

- **0x0080**

Der Zustand dieses Sensors hat sich nicht geändert

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

Werte	Zustand des Sensors
0x0880	Aus- und wieder einschalten

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

PSU1_Input_Type und PSU2_Input_Type

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

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

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

ONTAP-Befehle für das Management des Serviceprozessors

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

Befehle zum Verwalten der SP-Netzwerkkonfiguration

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

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

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

Befehle zum Verwalten des SP-Firmware-Images

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

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus...
Laden Sie manuell ein SP-Firmware-Image auf einem Node herunter	<pre>system node image get</pre> <p> Bevor Sie die <code>system node image</code> Befehle ausführen, müssen Sie die Berechtigungsebene auf Advanced setzen (<code>set -privilege advanced</code>) und bei Aufforderung y eingeben.</p> <p>Das SP-Firmware-Image ist mit ONTAP verpackt. Sie müssen die SP-Firmware nur manuell herunterladen, es sei denn, Sie möchten eine SP-Firmware-Version verwenden, die sich von der des ONTAP-Paketen unterscheidet.</p>
<p>Zeigt den Status für das aktuelle, von ONTAP ausgelöste Firmware-Update an, einschließlich der folgenden Informationen:</p> <ul style="list-style-type: none"> Die Start- und Endzeit für das aktuelle SP-Firmware-Update Ob ein Update ausgeführt wird und der Prozentsatz, der abgeschlossen ist 	<pre>system service-processor image update-progress show</pre>

Befehle zum Verwalten von SSH-Zugriff auf den SP

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

Befehle für die allgemeine SP-Administration

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

Verwandte Informationen

["ONTAP-Befehlsreferenz"](#)

ONTAP-Befehle für BMC Management

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

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

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

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

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

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

Verwandte Informationen

- ["Serviceprozessor des Systems"](#)

Unterstützte CLI-Befehle für den ONTAP Baseboard-Verwaltungscontroller

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

Befehl	Funktion
System	Zeigt eine Liste aller Befehle an.
Systemkonsole	Stellt eine Verbindung mit der Konsole des Systems her. Verwenden Sie Ctrl+D , um die Sitzung zu beenden.
Systemkern	Gibt einen Dump des Systemkerns aus und setzt ihn zurück.

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

Management der ONTAP-Cluster-Zeit (nur für Cluster-Administratoren)

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

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

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

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

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

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

- Auf der erweiterten Berechtigungsebene können Sie einen externen NTP-Server angeben, der mit dem Cluster verbunden ist und als primäre Datenquelle für die Korrektur und Anpassung der Cluster-Zeit

dient.

- Sie können die NTP-Server anzeigen, die dem Cluster zugeordnet sind (`cluster time-service ntp server show`).
- Sie können die NTP-Konfiguration des Clusters ändern (`cluster time-service ntp server modify`).
- Sie können die Zuordnung des Clusters zu einem externen NTP-Server aufheben (`cluster time-service ntp server delete`).
- Auf der erweiterten Berechtigungsebene können Sie die Konfiguration zurücksetzen, indem Sie die Zuordnung aller externen NTP-Server zum Cluster aufheben (`cluster time-service ntp server reset`).

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

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

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

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

 Job-Zeitpläne passen nicht auf manuelle Cluster-Datums- und -Zeitänderungen an. Diese Jobs werden planmäßig ausgeführt, basierend auf der aktuellen Cluster-Zeit, zu der der Job erstellt wurde oder zum Zeitpunkt der letzten Ausführung des Jobs. Wenn Sie daher das Datum oder die Uhrzeit des Clusters manuell ändern, müssen Sie mithilfe der `job show job history show` Befehle und überprüfen, ob alle geplanten Jobs gemäß Ihren Anforderungen in die Warteschlange verschoben und abgeschlossen wurden.

Befehle zum Verwalten der Cluster-Zeit

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

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

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

Ihr Ziel ist	Befehl
Verbinden Sie das Cluster ohne symmetrische Authentifizierung mit einem externen NTP-Server	<code>cluster time-service ntp server create -server server_name</code>

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

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

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

Verwandte Informationen

- ["Cluster-Datum wird angezeigt"](#)
- ["Ändern des Cluster-Datums"](#)
- ["Cluster Time Service ntp"](#)
- ["Jobanzeigen"](#)

Verwalten des Banners und der MOTD

Erfahren Sie mehr über das ONTAP Anmeldebanner und den Text für die täglichen Nachrichten

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

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

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

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

```
Password:
```

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

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

Sie können den Inhalt des Banners oder der MOTD mit dem `security login banner modify` `security login motd modify` Befehl oder wie folgt erstellen oder ändern:

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

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

Der nicht-interaktive Modus, in dem der `-message` Parameter zum Angeben der Meldungszeichenfolge verwendet wird, unterstützt keine Zeilenumbrüche.

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

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

- Cluster-Name, Node-Name oder SVM-Name
- Cluster-Datum und -Uhrzeit
- Name des Benutzers, der sich anmeldet
- Letzte Anmeldung für den Benutzer auf einem beliebigen Node im Cluster
- Anmeldename oder IP-Adresse
- Der Name des Betriebssystems
- Softwareversion
- Effektive Cluster-Versionszeichenfolge

Das Banner unterstützt keine dynamischen Inhalte. Erfahren Sie mehr über `security login motd modify` und die Escape-Sequenzen, mit denen Sie die MOTD aktivieren können, um dynamisch generierte Inhalte in der anzuzeigen "[ONTAP-Befehlsreferenz](#)".

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

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

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

die angegebene SVM überschrieben.

- Folgende Fakten gelten für die MOTD:

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

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

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

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

Erstellen Sie ein ONTAP-Anmeldebanner

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

Schritte

1. `security login banner modify` Erstellen Sie mit dem Befehl ein Banner für das Cluster oder die SVM:

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

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

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

Das für das Cluster erstellte Banner wird auch für alle SVMs angezeigt, die über kein vorhandenes Banner verfügen. Jedes nachträglich erstellte Banner für eine SVM überschreibt das Banner auf Cluster-Ebene für diese SVM. Durch Angabe des `-message` Parameters mit einem Bindestrich in doppelten Anführungszeichen ("") für die SVM wird die SVM zurückgesetzt, um das Cluster-Level Banner zu verwenden.

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

Wenn Sie den `-message` Parameter mit einem leeren String angeben (" "), werden Banner angezeigt, die keinen Inhalt haben.

Durch Angabe des `-message` Parameters mit `"-"` werden alle (admin oder Data) SVMs ohne konfiguriertes Banner angezeigt.

Beispiele für die Erstellung von Bannern

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

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

Im folgenden Beispiel wird im interaktiven Modus ein Banner für die SVM `svm1` erstellt:

```
cluster1::> security login banner modify -vserver svm1  
  
Enter the message of the day for Vserver "svm1".  
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to  
abort.  
0 1 2 3 4 5 6 7  
8  
1234567890123456789012345678901234567890123456789012345678901234  
567890  
The svm1 SVM is reserved for authorized users only!
```

```
cluster1::>
```

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

```

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

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

2 entries were displayed.

cluster1::>

```

Verwandte Informationen

- [Verwalten des Banners](#)
- ["Sicherheits-Login-Banner ändern"](#)
- ["Sicherheits-Login-Banner anzeigen"](#)

Verwalten Sie den Bannertext, der auf ONTAP-Cluster- und SVM-Ebene angezeigt wird

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

Wahlmöglichkeiten

- Managen Sie das Banner auf Cluster-Ebene:

Ihr Ziel ist	Dann...
Erstellen Sie ein Banner, das für alle Anmeldesitzungen angezeigt werden soll	Setzen Sie ein Banner auf Cluster-Ebene: `security login banner modify -vserver <cluster_name> { [-message "text"]
[-uri <ftp_or_http_addr>] {	Entfernen Sie das Banner für alle Anmeldungen (Cluster und SVM)

Ihr Ziel ist	Dann...
Setzen Sie das Banner auf eine leere Zeichenfolge (`): <code>security login banner modify -vserver * -message</code>	Überschreiben eines Banners, das von einem SVM-Administrator erstellt wurde
Ändern der SVM-Banner-Meldung: <code>`security login banner modify -vserver <svm_name> { [-message "<text>"]</code>	<code>[-uri <ftp_or_http_addr>] }`</code>

- Banner auf SVM-Ebene managen:

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

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

Verwandte Informationen

- ["Sicherheits-Login-Banner ändern"](#)

Erstellen Sie Text für die Tagesnachricht für ONTAP-Benutzer

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

Schritte

1. Verwenden Sie den `security login motd modify` Befehl, um eine MOTD für den Cluster oder die SVM zu erstellen:

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

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

`Security login motd modify` Beschreibt die Escape-Sequenzen, mit denen Sie die MOTD aktivieren können, um dynamisch generierte Inhalte anzuzeigen.

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

Standardmäßig wird auch für alle SVM-Anmeldungen ein für das Cluster erstellter MOTD angezeigt sowie eine MOTD auf SVM-Ebene, die Sie separat für eine bestimmte SVM erstellen können. Wenn der `-is-cluster-message-enabled` Parameter `false` für eine SVM auf gesetzt wird, wird die MOTD auf Clusterebene für diese SVM nicht angezeigt.

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

Festlegen der `-message` Der Parameter mit einer leeren Zeichenfolge (``) zeigt MOTDs an, die nicht konfiguriert sind oder keinen Inhalt haben.

Erfahren Sie mehr über `security login motd modify` und Parameter, mit denen die MOTD dynamisch generierte Inhalte im anzeigen kann "[ONTAP-Befehlsreferenz](#)".

Beispiele für die Erstellung von MOTDs

Das folgende Beispiel verwendet den nicht-interaktiven Modus, um ein MOTD für das `cluster1` Cluster:

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

Das folgende Beispiel verwendet den interaktiven Modus, um ein MOTD für das `svm1` SVM, das Escape-Sequenzen verwendet, um dynamisch generierte Inhalte anzuzeigen:

```

cluster1::> security login motd modify -vserver svml

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

```

Im folgenden Beispiel werden die erstellten MOTDs angezeigt:

```

cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Greetings!

Vserver: svml
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.

```

Erfahren Sie mehr über `security login motd show` in der "[ONTAP-Befehlsreferenz](#)".

Managen des Tagestexts, der auf ONTAP-Cluster- und SVM-Ebene angezeigt wird

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

Erfahren Sie mehr über die "[Escape-Sequenzen](#)", mit denen Sie in der ONTAP-Befehlsreferenz dynamisch Inhalte für die MOTD generieren können.

Wahlmöglichkeiten

- Verwalten Sie die MOTD auf Clusterebene:

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

Ihr Ziel ist	Dann...
<pre data-bbox="186 164 512 196">[-uri <ftp_or_http_addr>] }</pre> <p data-bbox="186 234 279 266">[NOTE]</p> <p data-bbox="186 276 251 297">=====</p> <p data-bbox="186 308 806 473">Wenn Sie den interaktiven Modus verwenden, werden Sie von der CLI aufgefordert, die MOTD einzeln für das Cluster und jede SVM einzugeben. Sie können dieselbe MOTD in jede Instanz einfügen, wenn Sie dazu aufgefordert werden.</p> <p data-bbox="186 515 251 536">=====</p>	<p data-bbox="848 164 1455 261">Ein MOTD auf Cluster-Ebene steht optional allen SVMs zur Verfügung, soll aber nicht, dass der MOTD für Cluster-Anmeldungen angezeigt wird</p>
<p data-bbox="186 572 832 635">Legen Sie eine MOTD auf Cluster-Ebene fest, deaktivieren Sie jedoch die Anzeige für das Cluster:</p> <pre data-bbox="186 671 659 734">`security login motd modify -vserver <cluster_name> { [-message "<text>"] }</pre>	<pre data-bbox="848 572 1421 625">[-uri <ftp_or_http_addr>] -is-cluster-message -enabled false`</pre>
<p data-bbox="186 789 780 882">Entfernen Sie alle MODs auf Cluster- und SVM-Ebene, wenn nur einige SVMs über MOTDs auf Cluster-Ebene und SVM-Ebene verfügen</p>	<p data-bbox="848 789 1478 853">Legen Sie den Cluster und alle SVMs so fest, dass für die MOTD ein leerer String verwendet wird:</p> <pre data-bbox="848 889 1470 952">security login motd modify -vserver * -message ""</pre>
<p data-bbox="186 1022 796 1142">Ändern Sie die MOTD nur für die SVMs mit einer nicht leeren Zeichenfolge, wenn andere SVMs einen leeren String verwenden und wenn auf Clusterebene ein anderes MOTD verwendet wird</p>	<p data-bbox="848 1022 1478 1085">Verwenden Sie erweiterte Abfragen, um die MOTD selektiv zu ändern:</p> <pre data-bbox="848 1121 1421 1205">`security login motd modify { -vserver !<cluster_name> -message !"" } { [-message "<text>"] }</pre>
<pre data-bbox="186 1262 512 1294">[-uri <ftp_or_http_addr>] }</pre>	<p data-bbox="848 1262 1494 1427">Alle MOTDs anzeigen, die an beliebiger Stelle in einer ein- oder mehrzeiligen Nachricht einen bestimmten Text enthalten (z. B. „Januar“ gefolgt von „2015“), auch wenn der Text auf mehrere Zeilen verteilt ist</p>
<p data-bbox="186 1486 698 1550">Verwenden Sie eine Abfrage, um MOTDs anzuzeigen:</p> <div data-bbox="213 1613 796 1681" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <pre data-bbox="213 1613 796 1681">`security login motd show -message *"January"*"2015"*</pre> </div>	<p data-bbox="848 1486 1494 1579">Erstellen Sie interaktiv ein MOTD, das mehrere und aufeinanderfolgende Zeilen enthält (auch als Zeilenende oder EOLs bezeichnet).</p>

- Management von MOTD auf SVM-Ebene:

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

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

Verwandte Informationen

- ["Sicherheitsanmeldung motd modify"](#)
- ["Sicherheits-Login-Motd-Show"](#)

Managen von ONTAP-Jobs und Jobplänen

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

Jobkategorien

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

Ein Job kann in einer der folgenden Kategorien sein:

- **Server-verbundene Jobs**

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

- **Cluster-verbundene Jobs**

Diese Jobs werden vom Management-Framework in die Warteschlange für jeden Node im auszulaufenden

Cluster verschoben.

- **Privatjobs**

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

Befehle zum Verwalten von Jobs

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

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

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



Mit dem `event log show` Befehl können Sie das Ergebnis eines abgeschlossenen Jobs bestimmen. Erfahren Sie mehr über `event log show` in der ["ONTAP-Befehlsreferenz"](#).

Befehle zum Verwalten von Job-Zeitplänen

Viele Aufgaben - zum Beispiel Volume Snapshots - können so konfiguriert werden, dass sie nach bestimmten Zeitplänen ausgeführt werden. Zeitpläne, die zu bestimmten Zeitpunkten ausgeführt werden, werden `cron`-Zeitpläne genannt (ähnlich wie `UNIX`cron`-Zeitpläne). Zeitpläne, die in Intervallen ausgeführt werden, werden als „`interval`“-Zeitpläne bezeichnet. Sie verwenden die `job schedule` Befehle zum Verwalten von Job-Zeitplänen.

Job-Zeitpläne passen nicht auf manuelle Änderungen am Cluster-Datum und -Uhrzeit an. Diese Jobs werden planmäßig ausgeführt, basierend auf der aktuellen Cluster-Zeit, zu der der Job erstellt wurde oder zum Zeitpunkt der letzten Ausführung des Jobs. Wenn Sie daher das Datum oder die Uhrzeit des Clusters manuell ändern, sollten Sie mit den `job show` und `job history show` Befehlen und überprüfen, ob alle geplanten Jobs gemäß Ihren Anforderungen in die Warteschlange eingereiht und abgeschlossen sind.

Wenn das Cluster Teil einer MetroCluster-Konfiguration ist, müssen die Job-Zeitpläne auf beiden Clustern

identisch sein. Wenn Sie einen Job-Zeitplan erstellen, ändern oder löschen, müssen Sie diesen Vorgang auf dem Remote-Cluster ausführen.

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

Verwandte Informationen

- ["Job"](#)

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

Erfahren Sie mehr über Backup-Dateien der ONTAP-Konfiguration

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

werden.

Diese Dateien speichern die lokale Konfiguration jedes Nodes sowie die clusterweite replizierte Konfiguration. Sie verwenden Konfigurations-Backup-Dateien, um ein Backup der Cluster-Konfiguration durchzuführen und wiederherzustellen.

Es gibt zwei Arten von Konfigurations-Backup-Dateien:

- **Knoten Konfiguration Backup-Datei**

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

- **Sicherungsdatei der Clusterkonfiguration**

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



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

Erfahren Sie mehr über die Planung von Backups von ONTAP-Cluster- und Node-Konfigurationsdateien

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

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

- Alle 8 Stunden
- Täglich
- Wöchentlich

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

ONTAP-Befehle zum Managen der Backup-Zeitpläne für die Konfiguration

Sie können die `system configuration backup settings` Befehle verwenden, um Backup-Zeitpläne für die Konfiguration zu verwalten.

Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

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

ONTAP-Befehle zum Managen von Backup-Dateien der Node-Konfiguration

Mit den `system configuration backup` Befehlen verwalten Sie Backup-Dateien für die Cluster- und Node-Konfiguration.

Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

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

Ihr Ziel ist	Befehl
Laden Sie eine Konfigurationssicherungsdatei von einem Knoten im Cluster auf eine Remote-URL (FTP, HTTP, HTTPS oder FTPS) hoch.	<pre>system configuration backup upload</pre> <p>Wenn Sie HTTPS in der Remote-URL verwenden, -validate-certification aktivieren oder deaktivieren Sie die digitale Zertifikatvalidierung mit der Option. Die Zertifikatvalidierung ist standardmäßig deaktiviert.</p> <p></p> <p>Auf dem Webserver, auf den Sie die Konfigurationssicherungsdatei hochladen, müssen PUT-Vorgänge für HTTP und POST-Vorgänge für HTTPS aktiviert sein. Auf einigen Webservern müssen Sie möglicherweise ein zusätzliches Modul installieren. Weitere Informationen finden Sie in der Dokumentation Ihres Webservers. Die unterstützten URL-Formate variieren je nach ONTAP Version. Erfahren Sie mehr über Systemkonfigurationsbefehle im "ONTAP-Befehlsreferenz".</p>
Laden Sie eine Sicherungsdatei der Konfiguration von einer Remote-URL auf einen Node im Cluster herunter, und validieren Sie, falls angegeben, das digitale Zertifikat	<pre>system configuration backup download</pre> <p>Wenn Sie HTTPS in der Remote-URL verwenden, -validate-certification aktivieren oder deaktivieren Sie die digitale Zertifikatvalidierung mit der Option. Die Zertifikatvalidierung ist standardmäßig deaktiviert.</p>
Benennen Sie eine Sicherungsdatei für die Konfiguration auf einem Node im Cluster um	<pre>system configuration backup rename</pre>
Zeigen Sie die Backup-Dateien für einen oder mehrere Nodes im Cluster an, die für eine oder mehrere Nodes konfiguriert sind	<pre>system configuration backup show</pre>
Löschen einer Backup-Konfigurationsdatei auf einem Knoten	<pre>system configuration backup delete</pre> <p></p> <p>Mit diesem Befehl wird nur die Backup-Datei der Konfiguration auf dem angegebenen Node gelöscht. Wenn auch die Backup-Datei der Konfiguration auf anderen Knoten im Cluster vorhanden ist, bleibt sie auf diesen Knoten.</p>

Verwandte Informationen

- ["Sicherung der Systemkonfiguration"](#)

Suchen Sie die Backup-Datei für die ONTAP-Node-Konfiguration, um einen Node wiederherzustellen

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

Über diese Aufgabe

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

Schritt

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

Wenn sich die Backup-Datei der Konfiguration befindet...	Dann...
Unter einer Remote-URL	<pre>`system configuration backup download` Laden Sie den Node mit dem Befehl auf der erweiterten Berechtigungsebene auf den Recovery-Node herunter.</pre>
Auf einem Node im Cluster	<ol style="list-style-type: none">a. Verwenden Sie den <code>system configuration backup show</code> Befehl auf der Ebene der erweiterten Berechtigungen, um die Liste der im Cluster verfügbaren Konfigurations-Backup-Dateien anzuzeigen, die die Konfiguration des Recovery-Node enthält.b. Wenn die von Ihnen identifizierte Konfigurations-Backup-Datei auf dem Node für die Wiederherstellung nicht vorhanden ist, <code>system configuration backup copy</code> kopieren Sie sie mit dem Befehl auf den Node für die Wiederherstellung.

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

Verwandte Informationen

- ["Sicherungskopie der Systemkonfiguration"](#)

Stellen Sie einen Node mithilfe der Backup-Datei für die ONTAP-Node-Konfiguration wieder her

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

Über diese Aufgabe

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Wenn sich der Node in einem ordnungsgemäßen Zustand `cluster modify -node -eligibility` befindet, verwenden Sie auf der erweiterten Berechtigungsebene eines anderen Node den Befehl mit den Parametern und, um ihn als nicht zulässig zu markieren und ihn vom Cluster zu isolieren.

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

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

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

Erfahren Sie mehr über `cluster modify` in der ["ONTAP-Befehlsreferenz"](#).

3. Verwenden Sie den `system configuration recovery node restore` Befehl auf der erweiterten Berechtigungsebene, um die Konfiguration des Node aus einer Backup-Konfigurationsdatei wiederherzustellen.

Wenn der Node seine Identität einschließlich seines Namens verloren `-nodename-in-backup` hat, sollten Sie den Node-Namen in der Konfigurations-Backup-Datei mit dem Parameter angeben.

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

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

```
Warning: This command overwrites local configuration files with
files contained in the specified backup file. Use this
command only to recover from a disaster that resulted
in the loss of the local configuration files.

The node will reboot after restoring the local configuration.

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

Die Konfiguration wird wiederhergestellt und der Node wird neu gebootet.

4. Wenn Sie den Node als nicht zulässig markiert haben, verwenden Sie `system configuration recovery cluster sync` den Befehl, um den Node als berechtigt zu markieren und ihn mit dem Cluster zu synchronisieren.
5. Wenn Sie in einer SAN-Umgebung arbeiten, verwenden Sie den `system node reboot` Befehl, um den Node neu zu booten und das SAN-Quorum wiederherzustellen.

Nachdem Sie fertig sind

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

Suchen Sie die Backup-Datei für die ONTAP-Cluster-Konfiguration, um ein Cluster wiederherzustellen

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

Schritte

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

- Ein Node im Cluster

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

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

- Eine Backup-Datei für die Cluster-Konfiguration

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

Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, gehen alle Konfigurationsänderungen verloren, die seit der Erstellung der Sicherung vorgenommen wurden. Sie müssen alle Abweichungen zwischen der Konfigurationssicherungsdatei und der aktuellen Konfiguration nach der Wiederherstellung beheben. Siehe die "[NetApp Knowledge Base: Leitfaden zur Lösung von ONTAP -Konfigurationssicherungen](#)" zur Anleitung zur Fehlerbehebung.

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

Wenn sich die Backup-Datei der Konfiguration befindet...	Dann...
Unter einer Remote-URL	<pre>`system configuration backup download` Laden Sie den Node mit dem Befehl auf der erweiterten Berechtigungsebene auf den Recovery-Node herunter.</pre>
Auf einem Node im Cluster	<ol style="list-style-type: none"> <li data-bbox="850 502 1486 713">a. Verwenden Sie den <code>system configuration backup show</code> Befehl auf der erweiterten Berechtigungsebene, um eine Backup-Datei für die Cluster-Konfiguration zu suchen, die erstellt wurde, als sich das Cluster in der gewünschten Konfiguration befand. <li data-bbox="850 734 1486 967">b. Wenn sich die Backup-Datei für die Cluster-Konfiguration nicht auf dem Node befindet, den Sie zum Wiederherstellen des Clusters verwenden möchten, <code>system configuration backup copy</code> kopieren Sie sie mit dem Befehl auf den Wiederherstellungsknoten.

Verwandte Informationen

- ["Cluster-Ring-Show"](#)
- ["Sicherungskopie der Systemkonfiguration"](#)

Stellen Sie einen Cluster mithilfe der Backup-Datei für die ONTAP-Cluster-Konfiguration wieder her

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

Über diese Aufgabe

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

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



Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, gehen alle Konfigurationsänderungen verloren, die seit der Erstellung der Sicherung vorgenommen wurden. Sie müssen alle Abweichungen zwischen der Konfigurationssicherungsdatei und der aktuellen Konfiguration nach der Wiederherstellung beheben. Siehe die ["NetApp Knowledge Base: Leitfaden zur Lösung von ONTAP -Konfigurationssicherungen"](#) zur Anleitung zur Fehlerbehebung.

Schritte

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

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

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

2. Anhalten jedes Knotens mit Ausnahme des wiederherrenden Knotens:

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

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

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

3. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

4. Verwenden Sie auf dem Recovery-Node den **system configuration recovery cluster recreate** Befehl, um das Cluster erneut zu erstellen.

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

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

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

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

Auf dem wiederherstellenden Node wird ein neues Cluster erstellt.

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

```
system configuration recovery cluster show
```

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

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

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

Sie müssen die Nodes nacheinander neu booten.

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

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

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

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

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

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

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

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

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

```
cluster show -eligibility true
```

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

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

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

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

9. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

10. Wenn das Cluster nur aus zwei Nodes besteht, **cluster ha modify** aktivieren Sie Cluster HA mit dem Befehl erneut.
11. Verwenden Sie den **storage failover modify** Befehl, um Storage Failover für jedes HA-Paar erneut zu aktivieren.

Nachdem Sie fertig sind

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

Verwandte Informationen

- "[ONTAP-Befehlsreferenz](#)"
- "[Speicherfailover ändern](#)"

Synchronisieren Sie einen Node mit dem ONTAP-Cluster, um das Cluster-weite Quorum sicherzustellen

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

Schritt

1. Verwenden Sie in einem funktionstüchtigen Node den **system configuration recovery cluster sync** Befehl auf der erweiterten Berechtigungsebene, um den Node zu synchronisieren, der nicht mit der Cluster-Konfiguration synchronisiert ist.

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

```

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

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

Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.

```

Ergebnis

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

Management von Node Core Dumps für ein ONTAP-Cluster (nur Cluster-Administratoren)

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

Sie haben folgende Möglichkeiten, Core Dumps zu verwalten:

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

Core Dump-Dateien und -Berichte werden im `/mroot/etc/crash/` Verzeichnis eines Node gespeichert. Sie können den Verzeichnisinhalt mit den `system node coredump` Befehlen oder einem Webbrowser anzeigen.

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

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

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

Befehle zum Verwalten von Core Dumps

Sie verwenden die `system node coredump config` Befehle zum Verwalten der Konfiguration von Core Dumps, die `system node coredump` Befehle zum Managen der Core Dump-Dateien und die `system node`

coredump reports Befehle zum Managen von Core-Berichten der Applikation.

Erfahren Sie mehr über die in diesem Thema beschriebenen Befehle im ["ONTAP-Befehlsreferenz"](#).

Ihr Ziel ist	Befehl
Konfigurieren von Core Dumps	system node coredump config modify
Zeigt die Konfigurationseinstellungen für Core Dumps an	system node coredump config show
Zeigt grundlegende Informationen zu Core Dumps an	system node coredump show
Lösen Sie manuell einen Core Dump aus, wenn Sie einen Node neu booten	system node reboot Mit den -dump -skip-lif -migration-before-reboot Parametern und  Der Parameter Link: https://docs.NetApp.com/US-en/ONTAP-cli/System-Node-reboot.HTML#Parameters[skip-lif-migration-before-reboot^] gibt an, dass die LIF-Migration vor einem Neustart übersprungen wird.
Lösen Sie beim Herunterfahren eines Node manuell einen Core Dump aus	system node halt Mit den -dump -skip-lif -migration-before-shutdown Parametern und  Der Parameter Link: https://docs.NetApp.com/US-en/ONTAP-cli/System-Node-halt.HTML#Parameters[skip-lif-migration-before-shutdown^] gibt an, dass die LIF-Migration vor dem Herunterfahren übersprungen wird.
Speichern eines angegebenen Core Dump	system node coredump save
Speichern Sie alle nicht gespeicherten Core Dumps auf einem angegebenen Node	system node coredump save-all
Generieren und senden Sie eine AutoSupport-Nachricht mithilfe einer Core Dump-Datei, die Sie angeben	system node autosupport invoke-core-upload  Der -uri optionale Parameter gibt ein alternatives Ziel für die AutoSupport Meldung an.

Ihr Ziel ist	Befehl
Zeigt Statusinformationen zu Core Dumps an	system node coredump status
Löschen eines angegebenen Core Dump	system node coredump delete
Löschen Sie alle nicht gespeicherten Core Dumps oder alle gespeicherten Core-Dateien auf einem Node	system node coredump delete-all
Zeigt die Berichte zum Anwendungs-Core-Dump an	system node coredump reports show
Löschen eines Core Dump-Berichts der Anwendung	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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 VERTRÄGLICH 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.