Cluster-Management mit der CLI

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Cluster-Management mit der CLI

Administrationsübersicht mit der CLI

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

Sie sollten diese Verfahren unter den folgenden Umständen verwenden:

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

Verwandte Informationen

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

Cluster- und SVM-Administratoren

Cluster- und SVM-Administratoren

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

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

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

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

Management des Zugriffs auf System Manager

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

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

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

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

Was ist der Cluster-Management-Server

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

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

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

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

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

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

SVMs

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

Ein Cluster enthält die folgenden SVMs:

- Admin-SVM

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

- Node-SVM

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

- System-SVM (erweitert)

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

- Daten-SVM

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

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

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

In der CLI werden SVMs als Vserver angezeigt.

Grundlagen der ONTAP Managementoberfläche

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

Greifen Sie über den seriellen Port auf das Cluster zu

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

Schritte

1. Drücken Sie an der Konsole die Eingabetaste.

   Das System antwortet mit der Eingabeaufforderung für die Anmeldung.

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

Zugriff auf das Cluster mit…	Geben Sie den folgenden Kontonamen ein…
Das Standard-Cluster-Konto	**`admin`**
Ein alternatives Administratorkonto	*`username`*

   Das System antwortet mit der Passwort-Eingabeaufforderung.

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

Greifen Sie über SSH auf das Cluster zu

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

Was Sie benötigen

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

  Der `-application` Parameter von `security login` Befehle gibt die Zugriffsmethode für ein Benutzerkonto an. Der `security login` Man-Pages enthalten zusätzliche Informationen.

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

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

Über diese Aufgabe

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

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

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

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

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

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

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

- Ab ONTAP 9.3 können Sie die SSH-Multi-Faktor-Authentifizierung für lokale Administratorkonten aktivieren.

  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 die Multi-Faktor-SSH-Authentifizierung für LDAP- und NIS-Remote-Benutzer aktivieren.

Schritte

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

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

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

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

command Ist für SSH-interaktive Sessions nicht erforderlich.

Beispiele für SSH-Anforderungen

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

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

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

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

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

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

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

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

Verwandte Informationen

"Administratorauthentifizierung und RBAC"

SSH-Anmeldesicherheit

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

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

- Das letzte Mal, wenn Ihr Kontoname angemeldet wurde.
- Die Anzahl der fehlgeschlagenen Anmeldeversuche seit der letzten erfolgreichen Anmeldung.

- Gibt an, ob sich die Rolle seit der letzten Anmeldung geändert hat (z. B. wenn sich die Rolle des Administratorkontos von „admin“ in „Backup“ geändert hat)
- Gibt an, ob die Funktionen zum Hinzufügen, Ändern oder Löschen der Rolle seit der letzten Anmeldung geändert wurden.

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

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

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

Einschränkungen und andere Überlegungen bei der SSH-Anmeldesicherheit

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

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

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

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

Beispiele für Sicherheitsdaten für SSH-Anmeldungen

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

- Diese Meldung wird nach jeder erfolgreichen Anmeldung angezeigt:

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

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

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

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

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

Aktivieren Sie Telnet- oder RSH-Zugriff auf den Cluster

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

Über diese Aufgabe

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

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

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:
   `set advanced`
2. Aktivieren eines Sicherheitsprotokolls (RSH oder Telnet):
   `security protocol modify -application *security_protocol* -enabled true`
3. Erstellen Sie eine neue Management-Firewall-Richtlinie auf der Grundlage von `mgmt` Management-Firewallrichtlinie:
   `system services firewall policy clone -policy mgmt -destination-policy *policy-name*`
4. Aktivieren Sie Telnet oder RSH unter der neuen Management Firewall-Richtlinie:
   `system services firewall policy create -policy *policy-name* -service *security_protocol* -action allow -ip-list *ip_address/netmask*``Um alle IP-Adressen zuzulassen, sollten Sie angeben `-ip-list 0.0.0.0/0`
5. Zuordnen der neuen Richtlinie zu der Cluster-Management-LIF:
   `network interface modify -vserver *cluster_management_LIF* -lif cluster_mgmt -firewall-policy *policy-name*`

Greifen Sie über Telnet auf das Cluster zu

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

Was Sie benötigen

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

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

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

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

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

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

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

Über diese Aufgabe

- Telnet ist kein sicheres Protokoll.

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

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

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

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

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

Schritte

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

   `telnet` *`hostname_or_IP`*

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

Beispiel für eine Telnet-Anforderung

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

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

Zugriff auf den Cluster über RSH

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

Was Sie benötigen

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

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

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

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

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

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

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

Über diese Aufgabe

- RSH ist kein sicheres Protokoll.

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

- ONTAP unterstützt maximal 50 RSH-Sitzungen pro Node.

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

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

Schritte

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

rsh *hostname_or_IP* -l *username:passwordcommand*

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

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

Beispiel einer RSH-Anforderung

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

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

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

Verwenden Sie die ONTAP Befehlszeilenschnittstelle

Über die ONTAP Befehlszeilenschnittstelle

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

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

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

```
cluster_name::*>
```

Allgemeines zu den verschiedenen Shells für CLI-Befehle (nur Cluster-Administratoren)

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

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

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

  Er stellt alle Befehle bereit, die Sie für die Konfiguration und das Management des Clusters benötigen. Die

clustershell CLI-Hilfe (wird von ausgelöst `?` An der clustershell Eingabeaufforderung) werden verfügbare clustershell-Befehle angezeigt. Der `man command_name` Mit dem Befehl in der clustershell wird die man-Page für den angegebenen clustershell-Befehl angezeigt.

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

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

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

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

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

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

Zugriff von nodeshell Befehlen und Optionen in der clustershell

Nodeshell Befehle und Optionen sind über die nodeshell zugänglich:

`system node run –node nodename`

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

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

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

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

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

Zeigt die verfügbaren nodeshell-Befehle an

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

Schritte

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

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

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

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

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

   [*commandname*] help

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

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

Beispiel für die Anzeige von verfügbaren nodeshell Befehlen

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

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

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

Methoden zur Navigation in CLI-Befehlsverzeichnissen

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

Bei Verwendung der CLI können Sie auf ein Befehlsverzeichnis zugreifen, indem Sie an der Eingabeaufforderung den Namen des Verzeichnisses eingeben und anschließend die Eingabetaste drücken. Der Verzeichnisname wird dann in den Text der Aufforderung enthalten, um anzugeben, dass Sie mit dem entsprechenden Befehlsverzeichnis interagieren. Um sich tiefer in die Befehlshierarchie zu bewegen, geben

Sie den Namen eines Unterverzeichnisses für Befehle ein, gefolgt von der Eingabetaste. Der Unterverzeichnisname wird dann in den Text der Eingabeaufforderung aufgenommen und der Kontext wechselt in das Unterverzeichnis.

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

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

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

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

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

Regeln zum Angeben von Werten in der CLI

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

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

  Einige Parameter akzeptieren eine 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 werden Hiltinformationen für einen bestimmten Befehl angezeigt.
- Einige Text, die Sie in die CLI eingeben, z. B. Befehlsnamen, Parameter und bestimmte Werte, ist nicht zwischen Groß- und Kleinschreibung zu beachten.

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

- Wenn Sie den Wert eines Parameters löschen möchten, der einen String oder eine Liste nimmt, geben Sie einen leeren Satz Anführungszeichen ("") oder einen Strich ("-") an.

- Das Hash-Zeichen („`#`"), auch als Rautzeichen bekannt, gibt einen Kommentar für eine Befehlszeileingabe an. Falls verwendet, sollte es nach dem letzten Parameter in einer Befehlszeile angezeigt werden.

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

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

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

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

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

Methoden zur Anzeige des Befehlsverlaufs und der Neuausgabe von Befehlen

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

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

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

- Eine Zeichenfolge, die einem Teil eines vorherigen Befehls entspricht

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

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

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

- Ein negativer Offset vom Ende der Verlaufsliste

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

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

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

Tastenkombinationen zum Bearbeiten von CLI-Befehlen

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

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

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

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination…
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	Strg-H
Rücktaste	Löschen Sie das Zeichen, in dem sich der Cursor befindet
Strg-D	Löschen Sie die Zeile
Strg-C	Deaktivieren Sie den Bildschirm
Strg-L	Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den vorherigen Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum vorherigen Eintrag.
Strg-P	ESC-P
Nach-oben-Pfeil	Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den nächsten Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum nächsten Eintrag.
Strg-N	ESC-N
Nach-unten-Pfeil	Erweitern Sie einen teilweise eingegebenen Befehl oder eine gültige Eingabe aus der aktuellen Bearbeitungsposition
Registerkarte	Strg-I
Kontextabhängige Hilfe anzeigen	?
Entfliehen Sie dem speziellen Mapping für das Fragezeichen (“?”) character. For instance, to enter a question mark into a command’s argument, press Esc and then the "`?`“ Zeichen.	Esc-?
TTY-Ausgabe starten	Strg-Q

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination…
TTY-Ausgang stoppen	Strg-S

Verwendung von administrativen Berechtigungsebenen

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

- * Admin*

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

- * Fortgeschrittene *

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

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

- **Diagnose**

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

Legen Sie die Berechtigungsebene in der CLI fest

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

Schritte

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

Beispiel zum Festlegen der Berechtigungsebene

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

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

Legen Sie die Anzeigeeinstellungen in der CLI fest

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

Über diese Aufgabe

Sie können die folgenden CLI-Anzeigeeinstellungen festlegen:

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

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

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

Schritte

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

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

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

Beispiel zum Festlegen von Anzeigeeinstellungen in der CLI

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

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

Methoden zur Verwendung von Abfrageoperatoren

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

In der folgenden Tabelle werden die unterstützten Abfrageoperatoren beschrieben:

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

Operator	Beschreibung
Bereichsbediener. Beispiel: **`5..10`** Entspricht jedem Wert von `5` Bis `10`, Inklusive.	<
Kleiner als Operator. Beispiel: **`<20`** Entspricht jedem Wert, der kleiner ist als `20`.	>
Greater-than Operator. Beispiel: **`>5`** Entspricht jedem Wert, der größer ist als `5`.	<=
Kleiner als oder gleich dem Operator. Beispiel: **⇐`5`** Entspricht jedem Wert, der kleiner oder gleich ist `5`.	>=

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

Wenn Sie Abfragezeichen als Literale analysieren möchten, müssen Sie die Zeichen in doppelte Anführungszeichen einschließen (z. B. „^“, „`".`", "*", or "€`“) für die richtigen Ergebnisse zurückgegeben werden.

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

Methoden zur Verwendung erweiterter Abfragen

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

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

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

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

Die Kombination von Abfragen und Änderungsvorgängen ist ein nützliches Werkzeug. Es kann jedoch zu Verwirrung und Fehlern führen, wenn es falsch umgesetzt wird. Beispiel: Verwenden der (erweiterten Berechtigung) `system node image modify` Befehl zum Festlegen des Standard-Software-Images eines Node wird automatisch das andere Software-Image als nicht das Standard festgelegt. Der Befehl im folgenden Beispiel ist effektiv ein null Vorgang:

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

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

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

Methoden zur Anpassung der Show-Befehlsausgabe mithilfe von Feldern

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

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

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

```
cluster1::> volume show -instance

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

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

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

Informationen zu Positionsparametern

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

Was ist ein Positionsparameter

- Ein Positionsparameter ist ein Parameter, der nicht erfordert, dass Sie den Parameternamen angeben müssen, bevor Sie den Parameterwert angeben.
- Ein Positionsparameter kann in der Befehlseingabe mit nonpositionellen Parametern interspert werden, solange er seine relative Sequenz mit anderen Positionsparametern im selben Befehl, wie im angegeben,

beobachtet ***command_name ?*** Ausgabe:

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

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

Einen Positionsparameter identifizieren

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

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

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

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

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

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

Beispiele für die Verwendung von Positionsparametern

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

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

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

```
cluster1::> volume create -vserver svm1 -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 mit nonpositionellen Parametern interspert `volume create` Befehl, und die Positionsparameterwerte werden ohne die Parameternamen angegeben. Die Positionsparameter werden in der gleichen Reihenfolge angegeben, die vom angegeben wird **`volume create ?`** Ausgabe: Das ist der Wert für `-volume` Wird vor dem von angegeben `-aggregate`, Die wiederum vor der von angegeben ist `-size`.

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

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

Methoden für den Zugriff auf ONTAP man-Pages

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

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

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

Managen von CLI-Sitzungen (nur Cluster-Administratoren)

Verwalten von Datensätzen von CLI-Sitzungen

Verwalten von Datensätzen der CLI-Sitzungen – Übersicht

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.

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.

Notieren Sie eine CLI-Sitzung

Sie können das verwenden `system script start` Und `system script stop` Befehle zum Aufzeichnen einer CLI-Sitzung.

Schritte

1. Um mit der Aufzeichnung der aktuellen CLI-Sitzung in einer Datei zu beginnen, verwenden Sie den `system script start` Befehl.

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

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

2. Fahren Sie mit Ihrer CLI-Sitzung fort.
3. Um die Aufzeichnung der Sitzung zu beenden, verwenden Sie den `system script stop` Befehl.

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

   ONTAP beendet die Aufzeichnung Ihrer CLI-Sitzung.

Befehle zum Verwalten von Datensätzen von CLI-Sitzungen

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

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

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 9-Befehle"

Befehle zum Verwalten der automatischen Zeitüberschreitung von CLI-Sitzungen

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

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

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

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

Verwandte Informationen

"ONTAP 9-Befehle"

Über die ONTAP Befehlszeilenschnittstelle

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

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

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

```
cluster_name::*>
```

Allgemeines zu den verschiedenen Shells für CLI-Befehle (nur Cluster-Administratoren)

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

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

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

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

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

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

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

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

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

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

Zugriff von nodeshell Befehlen und Optionen in der clustershell

Nodeshell Befehle und Optionen sind über die nodeshell zugänglich:

`system node run –node nodename`

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

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

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

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

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

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

Zeigt die verfügbaren nodeshell-Befehle an

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

Schritte

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

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

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

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

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

   `[`*`commandname`*`] help`

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

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

Beispiel für die Anzeige von verfügbaren nodeshell Befehlen

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

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

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

Methoden zur Navigation in CLI-Befehlsverzeichnissen

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

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

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

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

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

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

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

Regeln zum Angeben von Werten in der CLI

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

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

  Einige Parameter akzeptieren eine 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 werden Hiltinformationen für einen bestimmten Befehl angezeigt.
- Einige Text, die Sie in die CLI eingeben, z. B. Befehlsnamen, Parameter und bestimmte Werte, ist nicht zwischen Groß- und Kleinschreibung zu beachten.

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

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

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

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

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

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

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

Methoden zur Anzeige des Befehlsverlaufs und der Neuausgabe von Befehlen

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

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

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

- Eine Zeichenfolge, die einem Teil eines vorherigen Befehls entspricht

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

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

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

- Ein negativer Offset vom Ende der Verlaufsliste

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

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

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

Tastenkombinationen zum Bearbeiten von CLI-Befehlen

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

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

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination…
Bewegen Sie den Cursor um ein Zeichen zurück	Strg-B
Hinterpfeil	Bewegen Sie den Cursor um ein Zeichen nach vorne
Strg-F	Vorwärtspfeil

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination…
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 *Clipboard* 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	Strg-H
Rücktaste	Löschen Sie das Zeichen, in dem sich der Cursor befindet
Strg-D	Löschen Sie die Zeile
Strg-C	Deaktivieren Sie den Bildschirm
Strg-L	Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den vorherigen Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum vorherigen Eintrag.
Strg-P	ESC-P

Ihr Ziel ist	Verwenden Sie die folgende Tastenkombination…
Nach-oben-Pfeil	Ersetzen Sie den aktuellen Inhalt der Befehlszeile durch den nächsten Eintrag in der Verlaufsliste. Bei jeder Wiederholung der Tastenkombination wechselt der Verlaufscursor zum nächsten Eintrag.
Strg-N	ESC-N
Nach-unten-Pfeil	Erweitern Sie einen teilweise eingegebenen Befehl oder eine gültige Eingabe aus der aktuellen Bearbeitungsposition
Registerkarte	Strg-I
Kontextabhängige Hilfe anzeigen	?
Entfliehen Sie dem speziellen Mapping für das Fragezeichen (“?”) character. For instance, to enter a question mark into a command’s argument, press Esc and then the "`?`“ Zeichen.	Esc-?
TTY-Ausgabe starten	Strg-Q
TTY-Ausgang stoppen	Strg-S

Verwendung von administrativen Berechtigungsebenen

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

- * Admin*

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

- * Fortgeschrittene *

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

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

- **Diagnose**

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

Legen Sie die Berechtigungsebene in der CLI fest

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

Schritte

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

Beispiel zum Festlegen der Berechtigungsebene

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

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

Legen Sie die Anzeigeeinstellungen in der CLI fest

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

Über diese Aufgabe

Sie können die folgenden CLI-Anzeigeeinstellungen festlegen:

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

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

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

Schritte

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

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

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

Beispiel zum Festlegen von Anzeigeeinstellungen in der CLI

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

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

Methoden zur Verwendung von Abfrageoperatoren

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

In der folgenden Tabelle werden die unterstützten Abfrageoperatoren beschrieben:

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

Operator	Beschreibung
c` Entspricht dem Eintrag `a`, Jeder Eintrag, der mit beginnt `b`, Und jeder Eintrag, der beinhaltet `c`.	..
Bereichsbediener. Beispiel: **`5..10`** Entspricht jedem Wert von `5` Bis `10`, Inklusive.	<
Kleiner als Operator. Beispiel: **`<20`** Entspricht jedem Wert, der kleiner ist als `20`.	>
Greater-than Operator. Beispiel: **`>5`** Entspricht jedem Wert, der größer ist als `5`.	<=

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

Wenn Sie Abfragezeichen als Literale analysieren möchten, müssen Sie die Zeichen in doppelte Anführungszeichen einschließen (z. B. „^“, „`".`", "*", or "€`“) für die richtigen Ergebnisse zurückgegeben werden.

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

Methoden zur Verwendung erweiterter Abfragen

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

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

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

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

Die Kombination von Abfragen und Änderungsvorgängen ist ein nützliches Werkzeug. Es kann jedoch zu Verwirrung und Fehlern führen, wenn es falsch umgesetzt wird. Beispiel: Verwenden der (erweiterten Berechtigung) `system node image modify` Befehl zum Festlegen des Standard-Software-Images eines Node wird automatisch das andere Software-Image als nicht das Standard festgelegt. Der Befehl im folgenden Beispiel ist effektiv ein null Vorgang:

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

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

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

Methoden zur Anpassung der Show-Befehlsausgabe mithilfe von Feldern

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

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

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

```
cluster1::> volume show -instance

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

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

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

Informationen zu Positionsparametern

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

Was ist ein Positionsparameter

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

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

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

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

Einen Positionsparameter identifizieren

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

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

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

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

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

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

Beispiele für die Verwendung von Positionsparametern

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

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

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

```
cluster1::> volume create -vserver svm1 -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 mit nonpositionellen Parametern interspert `volume create` Befehl, und die Positionsparameterwerte werden ohne die Parameternamen angegeben. Die Positionsparameter werden in der gleichen Reihenfolge angegeben, die vom angegeben wird **`volume create ?`** Ausgabe: Das ist der Wert für `-volume` Wird vor dem von angegeben `-aggregate`, Die wiederum vor der von angegeben ist `-size`.

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

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

Methoden für den Zugriff auf ONTAP man-Pages

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

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

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

Grundlagen des Cluster-Managements (nur Cluster-Administratoren)

Zeigt Informationen über die Nodes in einem Cluster an

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

Schritte

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

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

Beispiele zum Anzeigen der Nodes in einem Cluster

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

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

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

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

cluster1::*> cluster show -node node1

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

Zeigt Cluster-Attribute an

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

Schritte

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

Beispiel zum Anzeigen von Cluster-Attributen

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

```
cluster1::> cluster identity show

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

Cluster-Attribute ändern

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

Über diese Aufgabe

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

Schritte

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

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

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

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

Beispiel für die Umbenennung eines Clusters

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

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

Zeigt den Status von Cluster-Replikationsringen an

Sie können den Status von Cluster-Replizierungsringen anzeigen, um Ihnen bei der

Diagnose von Problemen im gesamten Cluster zu helfen. Wenn im Cluster Probleme auftreten, werden Sie möglicherweise von dem Support-Personal gebeten, diese Aufgabe auszuführen, um die Fehlerbehebung zu unterstützen.

Schritte

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

Beispiel zum Anzeigen des Status von Cluster-Ring-Replizierung

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

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

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

Über Quorum und Epsilon

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

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

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

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

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

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

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

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

Welche System-Volumes sind

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

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

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

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

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

Zeigen Sie Node-Attribute an

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

Schritte

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

Beispiel zum Anzeigen von Informationen über einen Node

Im folgenden Beispiel werden ausführliche Informationen über node1 angezeigt:

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

Ändern von Node-Attributen

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

Über diese Aufgabe

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

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

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

Schritte

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

Beispiel zum Ändern von Node-Attributen

Mit dem folgenden Befehl werden die Attribute des Node „`node1`“ geändert. Der Eigentümer des Knotens ist

auf „`Joe Smith`“ eingestellt und die Asset-Tag-Nummer ist auf „`js1234`“ eingestellt:

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

Benennen Sie einen Node um

Sie können den Namen eines Node nach Bedarf ändern.

Schritte

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

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

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

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

Beispiel für die Umbenennung eines Node

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

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

Fügen Sie dem Cluster Nodes hinzu

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

Was Sie benötigen

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

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

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

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

  Ein Node, der dem Cluster hinzugefügt wird, verwendet das angegebene Subnetz, um die automatische

Konfiguration für den SP durchzuführen.

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

Über diese Aufgabe

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

Schritte

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

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

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

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

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

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

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

3. Loggen Sie sich mit dem beim Administratorkonto ein `admin` Benutzername:
4. Starten Sie den Cluster Setup-Assistenten:

   `cluster setup`

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

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

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

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

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

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

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

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

Nachdem Sie fertig sind

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

Entfernen Sie die Nodes aus dem Cluster

Sie können nicht benötigte Nodes gleichzeitig von einem Cluster und einem Node entfernen. Nachdem Sie einen Node entfernt haben, müssen Sie auch seinen Failover-

Partner entfernen. Wenn Sie einen Node entfernen, können seine Daten auf nicht mehr zugegriffen oder gelöscht werden.

Bevor Sie beginnen

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

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

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

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

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

Über diese Aufgabe

Wenn Sie ein Cluster mit gemischten Versionen ausführen, können Sie den letzten Node niedriger Versionen mithilfe eines der erweiterten Berechtigungsbefehle, beginnend mit ONTAP 9.3, entfernen:

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

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

Schritte

1. Ändern Sie die Berechtigungsebene in erweitert:

   `set -privilege advanced`

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

   `cluster modify –eligibility false`

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

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

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

Für diese ONTAP-Version…	Befehl
ONTAP 9.3	**`cluster unjoin`**
ONTAP 9.4 und höher	**`cluster remove-node`**

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

   Das System informiert Sie über Folgendes:

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

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

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

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

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

6. Löschen Sie bei einer 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 Startmenü-Option **(4) Konfiguration reinigen und initialisieren Sie alle Festplatten**.
7. Zurück zur Administrator-Berechtigungsebene:

   ```
   set -privilege admin
   ```

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

Nachdem Sie fertig sind

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

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

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

Was Sie benötigen

- Die Cluster-Management-LIF muss aktiv sein.

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

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

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

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

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

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

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

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

Über diese Aufgabe

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

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

Schritte

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

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

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

Greifen Sie auf die Systemkonsole eines Node zu

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

Über diese Aufgabe

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

Schritte

1. Zugriff auf die Systemkonsole eines Node:

Wenn Sie im…	Diesen Befehl eingeben…
SP-CLI des Node	`system console`
CLI VON ONTAP	`system node run-console`

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

Beispiele für den Zugriff auf die Systemkonsole

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

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

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

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

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

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

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

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

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

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

Regeln für Root-Volumes und Root-Aggregate der Nodes

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

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

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

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

    Das Speichern von Benutzerdaten im Root-Volume erhöht die Storage-Giveback zwischen Nodes in einem HA-Paar.
  - Sie können das Root-Volume zu einem anderen Aggregat verschieben.

    Verschieben von Root-Volumes in neue Aggregate
- Das Root-Aggregat ist nur dem Root-Volumen des Knotens zugewiesen.

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

"NetApp Hardware Universe"

Freier Speicherplatz auf dem Root-Volume eines Knotens

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

Schritte

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

3. Zugriff auf die Hölle:

   system node run -node *nodename*

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

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

   priv set advanced

5. Die Paketverfolgungsdateien des Knotens über die nodeshell anzeigen und löschen:
   a. Alle Dateien im Root-Volume des Nodes anzeigen:

      ls /etc

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

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

6. Root-Volume-Snapshot-Kopien des Node über den Knotenpunkt ermitteln und löschen:
   a. Geben Sie den Namen des Root-Volumes an:

      vol status

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

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

```
node1*> vol status

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

   a. Anzeige von Root-Volume Snapshot Kopien:

      snap list root_vol_name

   b. Löschen unerwünschter Root-Volume Snapshot Kopien:

      snap delete root_vol_namesnapshot_name

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

   exit

Verschieben von Root-Volumes in neue Aggregate

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

Über diese Aufgabe

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

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

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set privilege advanced`

2. Verschieben des Root-Aggregats:

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

   - **-Node**

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

   - **-disklist**

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

   - **-RAID-Typ**

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

3. Überwachen des Fortschritts des Jobs:

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

Ergebnisse

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

Starten oder stoppen Sie einen Node

Starten oder Stoppen einer Knotenübersicht

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

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

Booten Sie einen Node an der Eingabeaufforderung des Systems neu

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

Schritte

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

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

      `set -privilege advanced`

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

      `cluster show`

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

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

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

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

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

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

   c. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

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

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

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

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

Starten Sie ONTAP an der Eingabeaufforderung der Boot-Umgebung

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

Schritte

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

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

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

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

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

Fahren Sie einen Node herunter

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

Schritte

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

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

set -privilege advanced

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

cluster show

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

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

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

cluster modify -node *node_name* -epsilon false

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

cluster modify -node *node_name* -epsilon true

c. Zurück zur Administratorberechtigungsebene:

set -privilege admin

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

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

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

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

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

Verwalten Sie einen Knoten über das Startmenü

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

wiederherstellen.

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

Schritte

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

   Der Node startet den Neubootvorgang.

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

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

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

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

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

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

An…	Auswählen…
Initialisieren Sie die Festplatten des Node und erstellen Sie ein Root-Volume für den Node	4) Reinigen Sie die Konfiguration und initialisieren Sie alle Festplatten Mit dieser Menüoption werden alle Daten auf den Festplatten des Knotens gelöscht und die Knotenkonfiguration auf die werkseitigen Standardeinstellungen zurückgesetzt. Wählen Sie dieses Menüelement nur aus, nachdem der Knoten aus einem Cluster entfernt wurde (nicht verbunden) und nicht mit einem anderen Cluster verbunden ist. 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. Bei einem System, auf dem die FlexArray-Virtualisierung mit internen oder externen Festplatten-Shelfs ausgeführt wird, werden die Array-LUNs nicht initialisiert. Alle nativen Festplatten auf internen oder externen Shelfs werden initialisiert. Für ein System, auf dem die FlexArray-Virtualisierung mit nur Array-LUNS ausgeführt wird und keine internen oder externen Festplatten-Shelfs, wird das Root-Volume im Speicher-Array-LUNS initialisiert. Siehe "FlexArray wird installiert". Wenn der Knoten, den Sie initialisieren möchten, über Festplatten verfügt, die für die Root-Daten-Partitionierung partitioniert wurden, müssen die Festplatten unpartitioniert werden, bevor der Knoten initialisiert werden kann, siehe **9) Erweiterte Laufwerkpartitionierung konfigurieren** und "Festplatten- und Aggregatmanagement".
Führen Sie Wartungsvorgänge für Aggregate und Festplatten durch und erhalten Sie detaillierte Aggregat- und Festplatteninformationen.	5) Bootvorgang im Wartungsmodus Sie beenden den Wartungsmodus mit `halt` Befehl.
Stellen Sie die Konfigurationsinformationen vom Root-Volume des Node auf das Boot-Gerät, z. B. eine PC CompactFlash Card, wieder her	6) Flash aus Backup-Konfiguration aktualisieren 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.

An…	Auswählen…
Installieren Sie auf dem Node neue Software	7) Neue Software zuerst installieren 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. Diese Menüoption dient nur zur Installation einer neueren Version der ONTAP-Software auf einem Knoten, auf dem kein Root-Volume installiert ist. Do_Not_ Verwenden Sie diese Menüoption, um ONTAP zu aktualisieren.
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	9) Konfigurieren Der Erweiterten Laufwerkpartitionierung
	
	Ab ONTAP 9.2 bietet die Option „Advanced Drive Partitioning“ zusätzliche Managementfunktionen für Festplatten, die für Root-Daten oder Root-Daten-Partitionierung konfiguriert sind. Die folgenden Optionen sind über die Boot-Option 9 verfügbar:
	
	`(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.`

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

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

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

Die folgenden Plattformen unterstützen BMC anstelle des SP:

- FAS 8700
- FAS 8300
- FAS27x0

- AFF A800
- AFF A700s
- AFF A400
- AFF A320
- AFF A220
- AFF C 190

Allgemeines zum SP

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

Zu den wichtigsten Funktionen des SP gehören:

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

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

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

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

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

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

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

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

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

Verhalten bei Nachrichteninhalten werden von ONTAP übernommen.

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

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

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

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

  Das SEL enthält die folgenden Informationen:

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

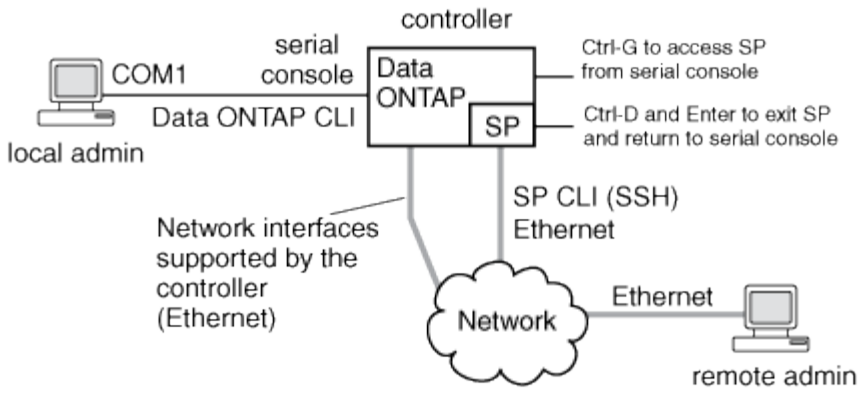
  Wenn Meldungen an die Konsole gesendet werden, speichert der SP sie im Konsole-Protokoll. Das Konsole-Protokoll bleibt gespeichert, solange der SP von einem der Netzteile des Node mit Strom versorgt wird. Da der SP mit Standby-Strom betrieben wird, bleibt er auch dann verfügbar, wenn der Node aus- und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

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

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

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

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



Was der Baseboard Management Controller tut

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

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

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

Es gibt einige Unterschiede zwischen SP und BMC:

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

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

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

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

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

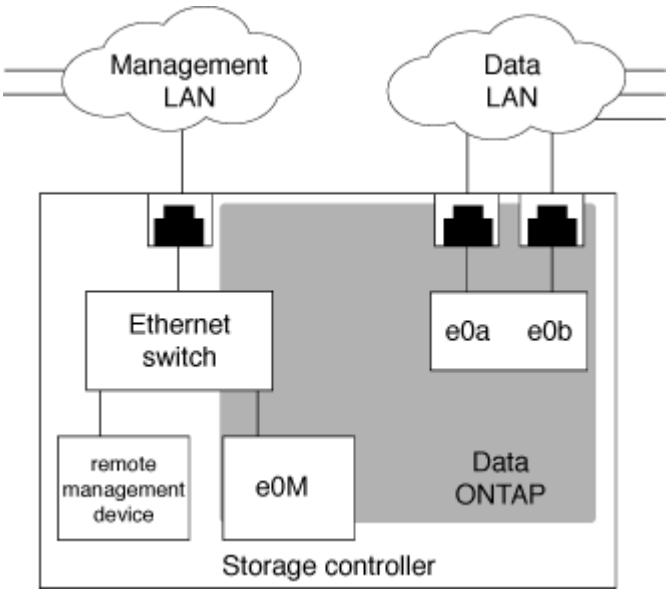
  Node-Vorgänge werden bei einem BMC-Neustart nicht beeinträchtigt.

Konfigurieren Sie das SP/BMC-Netzwerk

Isolierung des Managementnetzwerk-Traffic

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

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



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

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

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

Überlegungen zur SP/BMC-Netzwerkkonfiguration

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

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

Die automatische SP-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.
- Der `system service-processor network modify` Mit dem 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.

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

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

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

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

Aktivieren Sie die automatische Netzwerkkonfiguration für den 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` Mit dem Befehl werden Subnetzinformationen für das Cluster angezeigt.

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

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

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

Schritte

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

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

Konfigurieren Sie das SP/BMC-Netzwerk manuell

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

Was Sie benötigen

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

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

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

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

Schritte

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

     Sie können DHCP aktivieren (durch Einstellung `-dhcp` Bis `v4`) Nur, wenn Sie IPv4 verwenden. Sie können DHCP für IPv6-Konfigurationen nicht aktivieren.
   - Der `-ip-address` Der Parameter gibt die öffentliche IP-Adresse für den SP an.

     Wenn Sie versuchen, das SP-Netzwerk manuell mit Adressen zu konfigurieren, die einem Subnetz zugewiesen sind, wird eine Warnmeldung angezeigt. Wenn Sie die Warnung ignorieren und mit der manuellen Adresszuweisung fortfahren, kann dies zu einer doppelten Adresszuweisung führen.
   - Der `-netmask` Der Parameter gibt die Netmask für den SP an (wenn IPv4 verwendet wird).
   - Der `-prefix-length` Parameter gibt die Netzwerkpräfixlänge der Subnetzmaske für den SP an (bei Verwendung von IPv6).
   - Der `-gateway` Der Parameter gibt die Gateway-IP-Adresse für den SP an.
2. Konfigurieren Sie das SP-Netzwerk für die im Cluster verbliebenen Nodes, indem Sie den Schritt 1 wiederholen.
3. Zeigt die SP-Netzwerkkonfiguration an und überprüfen Sie den SP-Setup-Status mithilfe von `system service-processor network show` Befehl mit dem `-instance` Oder `-field setup-status` Parameter.

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

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

Beispiel für das Konfigurieren des SP-Netzwerks

Im folgenden Beispiel wird der SP eines Node zur Verwendung von IPv4 konfiguriert, der SP aktiviert und die SP-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 der Konfiguration des SP-API-Service

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

Situationen ändern.

Über diese Aufgabe

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

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

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

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

- Der SP-API-Service ist standardmäßig aktiviert.

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

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

Schritte

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

Ihr Ziel ist	Verwenden Sie den folgenden Befehl…
Ändern Sie den Port, der vom SP-API-Service verwendet wird	`system service-processor api-service modify` Mit dem `-port {49152..65535}`-Parameter
Erneuern der vom SP-API-Service verwendeten SSL- und SSH-Zertifikate für die interne Kommunikation	• Für die Verwendung mit ONTAP 9.5 oder höher `system service-processor api-service renew-internal-certificate` • Für ONTAP 9.4 und frühere Verwendung • `system service-processor api-service renew-certificates` Wenn kein Parameter angegeben wird, werden nur die Host-Zertifikate (einschließlich der Client- und Server-Zertifikate) erneuert. Wenn der `-renew-all true` Parameter wird angegeben, sowohl die Host-Zertifikate als auch das Root-CA-Zertifikat werden erneuert.

Ihr Ziel ist	Verwenden Sie den folgenden Befehl…
komm	
Deaktiviert bzw. reaktiviert den SP-API-Service	`system service-processor api-service modify` Mit dem `-is-enabled {true`

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

Methoden zum Verwalten von SP/BMC-Firmware-Updates

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

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

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

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

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

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

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

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

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

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

Sie können die folgenden Optionen angeben:

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

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

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

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

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

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

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

Verwandte Informationen

"NetApp Downloads: System-Firmware und -Diagnose"

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

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

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

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

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

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

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

Verwandte Informationen

"NetApp Downloads: System-Firmware und -Diagnose"

Zugriff auf den SP/BMC

Konten, die auf den SP zugreifen können

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

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

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

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

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

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

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

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

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

Was Sie benötigen

Folgende Bedingungen müssen erfüllt sein:

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

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

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

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

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

Schritte

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

   `ssh username@SP_IP_address`

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

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

Beispiele für SP-Zugriff von einem Administrationshost aus

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

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

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

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

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

Greifen Sie über die Systemkonsole auf den SP/BMC zu

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

```
cluster1::>
```

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

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

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

```
cluster1::>
```

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

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

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

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

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

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

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

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

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

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

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

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

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

auf SSH-Zugriff auf den SP aller Nodes im Cluster.

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Verwenden Sie die Online-Hilfe von SP/BMC CLI

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

Über diese Aufgabe

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

Schritte

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

Um auf die SP-Hilfe zuzugreifen…	Um auf die BMC-Hilfe zuzugreifen…
Typ `help` An der SP-Eingabeaufforderung.	Typ `system` An der BMC-Eingabeaufforderung.

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

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

Das folgende Beispiel zeigt die BMC CLI Online-Hilfe.

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

BMC>
```

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

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

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

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

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

BMC>
```

Befehle zum Remote-Management eines Node

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

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

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

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

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

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl…	Verwenden Sie diesen BMC-Befehl…	Oder dieser ONTAP Befehl …
`system power cycle`			Die Standby-Stromversorgung bleibt eingeschaltet, damit der SP unterbrechungsfrei betrieben wird. Während des Einschaltzyklus erfolgt eine kurze Pause, bevor der Strom wieder eingeschaltet wird. Wenn der Node mit diesen Befehlen aus- und wieder eingeschaltet wird, kann dies zu einem fehlerhaften Herunterfahren des Nodes führen (auch als „*dirty shutdown*“ bezeichnet) und kein Ersatz für ein ordnungsgemäßes Herunterfahren mithilfe der ONTAP `system node halt` Befehl.

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl…	Verwenden Sie diesen BMC-Befehl…	Oder dieser ONTAP Befehl …
Erstellen Sie einen Core Dump, und setzen Sie den Node zurück	`system core [-f]` Der `-f` Option erzwingt die Erstellung eines Core Dump und das Zurücksetzen des Node.		`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 Node aufgehängt ist oder nicht auf Befehle wie reagiert `system node shutdown`. Die generierten Core Dump-Dateien werden in der Ausgabe des angezeigt `system node coredump show` Befehl. 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	`system reset {primary.backup.current}`	

Ihr Ziel ist	Verwenden Sie diesen SP-Befehl…	Verwenden Sie diesen BMC-Befehl…	Oder dieser ONTAP Befehl …
`system node reset` Mit dem `-firmware {primary.backup.current}` Parameter(erweiterte Berechtigungsebene) `system node reset`	Dieser Vorgang bewirkt ein nicht ordnungsgemäßes Herunterfahren des Node. 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.	Zeigt den Status eines automatischen Updates der Akku-Firmware an oder aktiviert bzw. deaktiviert das automatische Update der Akku-Firmware beim nächsten Booten des SP	`system battery auto_update [status.enable.disable]` (Erweiterte Berechtigungsebene)
		Vergleicht das aktuelle Akku-Firmware-Image mit einem angegebenen Firmware-Image	`system battery verify [image_URL]` (Erweiterte Berechtigungsebene) Wenn `image_URL` Ist nicht angegeben, wird das Standard-Akku-Firmware-Image zum Vergleich verwendet.
		Aktualisieren Sie die Akku-Firmware vom Image am angegebenen Speicherort	`system battery flash image_URL` (Erweiterte Berechtigungsebene) Sie verwenden diesen Befehl, wenn das automatische Update der Akku-Firmware aus einem bestimmten Grund fehlgeschlagen ist.

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

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

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

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

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

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

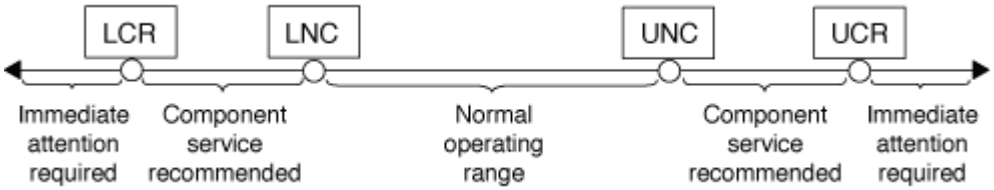
- Unterer kritischer Schwellenwert (LCR)
- Unterer nicht kritischer Schwellenwert (LNC)
- Oberer nicht kritischer Schwellenwert (UNC)
- Oberer kritischer Schwellenwert (UCR)

Ein Sensormesswert zwischen LNC und LCR bzw. zwischen UNC und UCR bedeutet, dass die Komponente

Anzeichen eines Problems aufweist und möglicherweise ein Systemausfall nicht ausgeschlossen werden kann. Daher sollten Sie eine baldige Komponentenwartung einplanen.

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

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



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

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

Beispiel der Befehlsausgabe des Befehls „System Sensors“

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

```
SP node1> system sensors

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

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

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

```
SP node1> system sensors get 5V

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

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

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

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

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

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

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

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

„System_FW_Status“

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

`AA` Kann einen der folgenden Werte aufweisen:

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

`BB` Kann einen der folgenden Werte aufweisen:

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

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

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

„System_Watchdog“

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

- **0x0080**

  Der Zustand dieses Sensors hat sich nicht geändert

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

Werte	Zustand des Sensors
0x0880	Aus- und wieder einschalten

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

PSU1_Input_Type und PSU2_Input_Type

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

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

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

Befehle zum Verwalten des SP über ONTAP

ONTAP bietet Befehle zum Verwalten des SP, einschließlich der SP-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…
Konfigurieren Sie das SP-Netzwerk für einen Node manuell, einschließlich folgender: • 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`
Zeigen Sie die SP-Netzwerkkonfiguration an, einschließlich der folgenden: • 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 erforderlich `-instance` Parameter.
Ändern Sie die SP-API-Service-Konfiguration, einschließlich folgender Komponenten: • 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	`system service-processor api-service show` (Erweiterte Berechtigungsebene)
Erneuern der vom SP-API-Service verwendeten SSL- und SSH-Zertifikate für die interne Kommunikation	• Für ONTAP 9.5 oder höher: `system service-processor api-service renew-internal-certificates` • Für ONTAP 9.4 oder früher: `system service-processor api-service renew-certificates` (Erweiterte Berechtigungsebene)

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: • 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	`system service-processor image show` Der `-is-current` Der Parameter gibt das Image (primär oder Backup) an, von dem der SP derzeit gebootet wird, nicht wenn die installierte Firmware-Version auf dem aktuellen Stand ist.
Aktiviert bzw. deaktiviert das automatische Firmware-Update des SP	`system service-processor image modify` 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.

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus…
Laden Sie manuell ein SP-Firmware-Image auf einem Node herunter	`system node image get` Bevor Sie den ausführen `system node image` Befehle. Sie müssen die Berechtigungsebene auf „erweitert“ setzen (`set -privilege advanced`Geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren. 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.
Zeigt den Status für das aktuelle, von ONTAP ausgelöste Firmware-Update an, einschließlich der folgenden Informationen: • Die Start- und Endzeit für das aktuelle SP-Firmware-Update • Ob ein Update ausgeführt wird und der Prozentsatz, der abgeschlossen ist	`system service-processor image update-progress show`

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	`system service-processor ssh add-allowed-addresses`
Blockieren Sie die angegebenen IP-Adressen vom Zugriff auf den SP	`system service-processor ssh remove-allowed-addresses`
Zeigt die IP-Adressen an, die auf den SP zugreifen können	`system service-processor ssh show`

Befehle für die allgemeine SP-Administration

Ihr Ziel ist	Führen Sie diesen ONTAP Befehl aus…
Zeigt allgemeine SP-Informationen an, einschließlich folgender: • 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	`system service-processor show` Zum Anzeigen vollständiger SP-Informationen muss das angezeigt werden `-instance` Parameter.
Bootet den SP auf einem Node neu	`system service-processor reboot-sp`
Generieren und senden Sie eine AutoSupport Meldung, die die SP-Protokolldateien, die von einem angegebenen Node erfasst wurden, enthält	`system node autosupport invoke-splog`
Zeigt die Zuordnungszuordnung der gesammelten SP-Protokolldateien im Cluster an, einschließlich der Sequenznummern für die SP-Protokolldateien, die sich in jedem Sammlungs-Node befinden	`system service-processor log show-allocations`

Verwandte Informationen

"ONTAP 9-Befehle"

ONTAP-Befehle für BMC Management

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

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

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

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

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

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

BMC-CLI-Befehle

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

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

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

Management der Audit-Protokollierung für Management-Aktivitäten

So implementiert ONTAP Audit-Protokollierung

Die im Audit-Protokoll aufgezeichneten Managementaktivitäten sind Teil der AutoSupport-Standardberichte und bestimmte Protokollierungsaktivitäten werden in EMS-Nachrichten erfasst. Sie können das Auditprotokoll auch an die von Ihnen angegebenen Ziele weiterleiten und Audit-Log-Dateien über die CLI oder einen Webbrowser anzeigen.

Ab ONTAP 9.11.1 können Sie den Inhalt des Revisionsprotokolls mithilfe von System Manager anzeigen.

Ab Version 9.12.1 sind Audit-Protokolle manipulationssicher. Das heißt, jede Protokolldatei, die eine Admin-Aktion aufzeichnet, kann selbst in Cluster-Administratorkonten nicht geändert oder gelöscht werden.

ONTAP protokolliert Managementaktivitäten, die auf dem Cluster ausgeführt werden, beispielsweise eine Anfrage, den Benutzer, der die Anforderung ausgelöst hat, die Zugriffsmethode des Benutzers und die Zeit der Anfrage.

Die Management-Aktivitäten können eine der folgenden Arten sein:

- LEGEN Sie Anforderungen FEST, die in der Regel für Befehle oder Vorgänge ohne Anzeige gelten
  - Diese Anfragen werden ausgegeben, wenn Sie ein ausführen `create`, `modify`, Oder `delete` Befehl zum Beispiel.
  - Festgelegte Anforderungen werden standardmäßig protokolliert.
- ABRUFEN von Anforderungen, die Informationen abrufen und in der Managementoberfläche anzeigen
  - Diese Anfragen werden ausgegeben, wenn Sie ein ausführen `show` Befehl zum Beispiel.
  - GET Requests werden nicht standardmäßig protokolliert, Sie können jedoch kontrollieren, ob GET Requests from the ONTAP CLI gesendet WERDEN (`-cliget`) Oder von den ONTAP APIs (`-ontapiget`) Sind in der Datei protokolliert.

ONTAP zeichnet die Managementaktivitäten in auf `/mroot/etc/log/mlog/audit.log` Datei eines Node. Befehle aus den drei Shells für CLI-Befehle - die clustershell, die nodeshell, und die nicht-interaktive Systemshell (interaktive Systemshell-Befehle werden nicht protokolliert)- sowie API-Befehle werden hier

protokolliert. In den Audit-Protokollen werden Zeitstempel verwendet, um anzuzeigen, ob alle Nodes in einem Cluster Zeit synchronisiert sind.

Der `audit.log` Die Datei wird vom AutoSupport-Tool an die angegebenen Empfänger gesendet. Sie können den Inhalt auch sicher an angegebene externe Ziele weiterleiten, z. B. an einen Splunk oder Syslog-Server.

Der `audit.log` Die Datei wird täglich gedreht. Die Rotation tritt auch auf, wenn sie 100 MB groß erreicht, und die vorherigen 48 Kopien erhalten bleiben (mit maximal 49 Dateien). Wenn die Audit-Datei ihre tägliche Rotation durchführt, wird keine EMS-Nachricht erzeugt. Wenn die Überwachungsdatei sich dreht, weil ihre Dateigröße überschritten wird, wird eine EMS-Nachricht generiert.

Änderungen an der Auditprotokollierung in ONTAP 9

Ab ONTAP 9 beginnt der `command-history.log` Datei wird durch ersetzt `audit.log`, Und das `mgwd.log` Die Datei enthält keine Audit-Informationen mehr. Wenn Sie ein Upgrade auf ONTAP 9 durchführen, sollten Sie alle Skripte oder Tools lesen, die sich auf die vorhandenen Dateien und deren Inhalte beziehen.

Nach dem Upgrade auf ONTAP 9 ist vorhanden `command-history.log` Dateien bleiben erhalten. Sie werden als neu ausgedreht (gelöscht) `audit.log` Dateien werden in gedreht (erstellt).

Tools und Skripte, die den prüfen `command-history.log` Die Datei wird möglicherweise weiterhin verwendet, da ein Soft-Link von verwendet wird `command-history.log` Bis `audit.log` Wird beim Upgrade erstellt. Jedoch Tools und Skripte, die prüfen, die `mgwd.log` Die Datei schlägt fehl, da diese Datei keine Audit-Informationen mehr enthält.

Darüber hinaus enthalten Audit-Protokolle in ONTAP 9 und höher nicht mehr die folgenden Einträge, da sie nicht als nützlich betrachtet werden und unnötige Protokollierungsaktivitäten verursachen:

- Interne Befehle, die von ONTAP ausgeführt werden (d. h., Benutzername=Root)
- Befehlsaliasen (getrennt vom Befehl, auf den sie verweisen)

Ab ONTAP 9 können Sie die Prüfprotokolle sicher mit den Protokollen TCP und TLS an externe Ziele übertragen.

Zeigt den Inhalt des Prüfprotokolls an

Sie können den Inhalt des Clusters anzeigen `/mroot/etc/log/mlog/audit.log` Dateien mithilfe der ONTAP-CLI, System Manager oder eines Webbrowsers.

Die Protokolldateieinträge des Clusters umfassen Folgendes:

Zeit
Zeitstempel der Protokolleingabe.

Applikation
Die Anwendung, die zum Herstellen einer Verbindung zum Cluster verwendet wird. Beispiele für mögliche Werte sind `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, Und `service-processor`.

Benutzer

Der Benutzername des Remote-Benutzers.

Bundesland

Der aktuelle Status des Audit-Antrags. Dies kann der Fall sein `success, pending,` Oder `error`.

Nachricht

Ein optionales Feld, das Fehler oder zusätzliche Informationen zum Status eines Befehls enthalten kann.

Sitzungs-ID

Die Sitzungs-ID, für die die Anforderung eingeht. Jeder SSH_Session_ wird eine Session-ID zugewiesen, während jedem HTTP, ONTAPI oder SNMP *Request* eine eindeutige Session-ID zugewiesen wird.

Storage VM

Der SVM, über die der Benutzer verbunden ist.

Umfang

Anzeigen `svm` Wenn sich die Anforderung auf einer Storage-VM befindet, wird anderenfalls angezeigt `cluster`.

Command ID

Die ID für jeden Befehl, der in einer CLI-Sitzung empfangen wurde. So können Sie Anfragen und Antworten korrelieren. ZAPI-, HTTP- und SNMP-Anforderungen verfügen nicht über Befehl-IDs.

Sie können die Protokolleinträge des Clusters aus der ONTAP CLI, aus einem Webbrowser und beginnend mit ONTAP 9.11.1, von System Manager anzeigen.

System Manager

- Um den Bestand anzuzeigen, wählen Sie **Events & Jobs > Audit Logs**. + jede Spalte verfügt über Steuerelemente zum Filtern, Sortieren, Suchen, Anzeigen und Inventar Kategorien. Die Bestandsdetails können als Excel-Arbeitsmappe heruntergeladen werden.
- Um Filter einzustellen, klicken Sie oben rechts auf die Schaltfläche **Filter** und wählen Sie dann die gewünschten Felder aus. + Sie können auch alle Befehle anzeigen, die in der Sitzung ausgeführt wurden, in der ein Fehler aufgetreten ist, indem Sie auf den Link Session-ID klicken.

CLI

Um die von mehreren Knoten im Cluster zusammengeführten Auditeinträge anzuzeigen, geben Sie: + ein `security audit log show` *`[parameters]`*

Sie können das verwenden `security audit log show` Befehl zum Anzeigen von Auditeinträgen für einzelne Nodes oder, die von mehreren Nodes im Cluster zusammengeführt wurden. Sie können auch den Inhalt des anzeigen `/mroot/etc/log/mlog` Verzeichnis auf einem einzelnen Knoten mit einem Webbrowser. Details finden Sie auf der man-Seite.

Webbrowser

Sie können den Inhalt des anzeigen `/mroot/etc/log/mlog` Verzeichnis auf einem einzelnen Knoten mit einem Webbrowser. "Erfahren Sie, wie Sie auf einen Knoten Protokoll zugreifen, Core Dump, und MIB-Dateien mit einem Web-Browser".

Verwalten DER Einstellungen für AUDITANFRAGE

Während FESTGELEGTE Anforderungen standardmäßig protokolliert werden, sind GET-Anforderungen nicht. Sie können jedoch kontrollieren, ob Anfragen von ONTAP HTML gesendet WERDEN (`-httpget`), die ONTAP CLI (`-cliget`) Oder von den ONTAP APIs (`-ontapiget`) Sind in der Datei protokolliert.

Sie können die Einstellungen für die Protokollierung von Audits über die ONTAP-CLI ändern, und beginnend mit ONTAP 9.11.1, in System Manager.

System Manager

1. Wählen Sie **Events & Jobs > Audit Logs** Aus.
2. Klicken Sie Auf ⚙ Wählen Sie in der rechten oberen Ecke die Anforderungen aus, die hinzugefügt oder entfernt werden sollen.

CLI

- Um festzulegen, dass GET-Anforderungen aus der ONTAP-CLI oder APIs im Audit-Protokoll (die Datei audit.log) aufgezeichnet werden sollen, geben Sie zusätzlich zu den Standard-Set-Anforderungen: + ein
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Um die aktuellen Einstellungen anzuzeigen, geben Sie: + ein
  `security audit show`

Weitere Informationen finden Sie auf den man-Pages.

Verwalten von Zielen für Überwachungsprotokolle

Sie können das Audit-Protokoll an maximal 10 Ziele weiterleiten. Sie können das Protokoll beispielsweise an einen Splunk oder Syslog-Server für Monitoring-, Analyse- und Backup-Zwecke weiterleiten.

Über diese Aufgabe

Für die Konfiguration der Weiterleitung müssen Sie die IP-Adresse des Syslog- oder Splunk-Hosts, seine Portnummer, ein Übertragungsprotokoll sowie die Syslog-Einrichtung für die weitergeleiteten Protokolle angeben. "Hier erfahren Sie mehr über Syslog-Funktionen".

Sie können einen der folgenden Übertragungswerte auswählen:

UDP unverschlüsselt
: User Datagram Protocol ohne Sicherheit (Standard)

TCP unverschlüsselt
: Übertragungsprotokoll ohne Sicherheit

TCP verschlüsselt
: Transmission Control Protocol mit Transport Layer Security (TLS) + A **Verify Server** Option ist verfügbar, wenn das TCP verschlüsselte Protokoll ausgewählt ist.

Sie können die Prüfprotokolle von der ONTAP CLI, und beginnend mit ONTAP 9.11.1, von System Manager weiterleiten.

System Manager

- Um die Ziele des Prüfprotokolls anzuzeigen, wählen Sie **Cluster >Einstellungen**. + die Anzahl der Protokollziele wird in der Kachel **Benachrichtigungsmanagement** angezeigt. Klicken Sie Auf ⋮ Um Details anzuzeigen.
- Um Ziele für das Auditprotokoll hinzuzufügen, zu ändern oder zu löschen, wählen Sie **Events & Jobs > Audit Logs** und klicken Sie dann rechts oben auf dem Bildschirm auf **Audit-Ziele verwalten**. + Klicken + Add , Oder klicken Sie auf ⋮ In der Spalte **Host Address** können Sie Einträge bearbeiten oder löschen.

CLI

1. Geben Sie für jedes Ziel, an das Sie das Prüfprotokoll weiterleiten möchten, die Ziel-IP-Adresse oder den Host-Namen und alle Sicherheitsoptionen an.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - Wenn der `cluster log-forwarding create` Der Befehl kann den Ziel-Host nicht pingen, um die Verbindung zu überprüfen. Der Befehl schlägt mit einem Fehler fehl. Obwohl nicht empfohlen, verwenden Sie die `-force` Parameter mit dem Befehl umgeht die Konnektivitätsprüfung.
   - Wenn Sie die einstellen `-verify-server` Parameter an `true`, Die Identität des Protokollweiterleitungsziels wird durch die Validierung seines Zertifikats überprüft. Sie können den Wert auf einstellen `true` Nur wenn Sie das auswählen `tcp-encrypted` Wert im `-protocol` Feld.

2. Überprüfen Sie, ob die Zieldatensätze korrekt sind, indem Sie die verwenden `cluster log-forwarding show` Befehl.

```
cluster1::> cluster log-forwarding show

                                             Verify Syslog
Destination Host          Port   Protocol    Server Facility
------------------------- ------ --------    ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

Weitere Informationen finden Sie auf den man-Pages.

Cluster-Zeit managen (nur Cluster-Administratoren)

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

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

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

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

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

  Wenn die angegebene NTP-Version für den NTP-Server nicht unterstützt wird, kann kein Zeitaustausch stattfinden.
    - Auf der erweiterten Berechtigungsebene können Sie einen externen NTP-Server angeben, der mit dem Cluster verbunden ist und als primäre Datenquelle für die Korrektur und Anpassung der Cluster-Zeit dient.
- Sie können die NTP-Server anzeigen, die mit dem Cluster verbunden sind (`cluster time-service ntp server show`).
- Sie können die NTP-Konfiguration des Clusters ändern (`cluster time-service ntp server modify`).
- Sie können die Verbindung des Clusters von einem externen NTP-Server beenden (`cluster time-service ntp server delete`).
- Sie können die Konfiguration auf der erweiterten Berechtigungsebene zurücksetzen, indem Sie die Zuordnung aller externen NTP-Server zum Cluster löschen (`cluster time-service ntp server reset`).

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

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

Befehle zum Verwalten der Cluster-Zeit

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

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

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

Ihr Ziel ist	Befehl
Verbinden Sie das Cluster ohne symmetrische Authentifizierung mit einem externen NTP-Server	`cluster time-service ntp server create -server server_name`
Verbinden Sie den Cluster mit einem externen NTP-Server mit symmetrischer AuthentifizierungVerfügbar in ONTAP 9.5 oder höher	`cluster time-service ntp server create -server server_ip_address -key-id key_id` Der `key_id` Beziehen Sie sich auf einen vorhandenen gemeinsamen Schlüssel, der mit ``Cluster Time-Service ntp key' konfiguriert ist.
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	`cluster time-service ntp server modify -server server_name -key-id key_id`
Deaktivieren Sie die symmetrische Authentifizierung	`cluster time-service ntp server modify -server server_name -authentication disabled`

Ihr Ziel ist	Befehl
Konfigurieren Sie einen freigegebenen NTP-Schlüssel	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Freigegebene Schlüssel werden durch eine ID bezeichnet. Die ID, der Typ und der Wert müssen auf dem Node und dem NTP-Server identisch sein
Zeigt Informationen zu den NTP-Servern an, die mit dem Cluster verbunden sind	`cluster time-service ntp server show`
Ändern Sie die Konfiguration eines externen NTP-Servers, der mit dem Cluster verbunden ist	`cluster time-service ntp server modify`
Distanzieren Sie einen NTP-Server vom Cluster	`cluster time-service ntp server delete`
Setzen Sie die Konfiguration zurück, indem Sie alle externen NTP-Server-Verknüpfungen mit dem Cluster löschen	`cluster time-service ntp server reset` Dieser Befehl erfordert die erweiterte Berechtigungsebene.

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

"ONTAP 9-Befehle"

Verwalten des Banners und der MOTD

Verwalten Sie die Übersicht über Banner und MOTD

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

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

Person anzeigen, die versucht, sich beim System anzumelden:

```
$ ssh admin@cluster1-01

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

Password:
```

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

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

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

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

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

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

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

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

  - Cluster-Name, Node-Name oder SVM-Name
  - Cluster-Datum und -Uhrzeit
  - Name des Benutzers, der sich anmeldet
  - Letzte Anmeldung für den Benutzer auf einem beliebigen Node im Cluster
  - Anmeldename oder IP-Adresse
  - Der Name des Betriebssystems
  - Softwareversion

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

Das Banner unterstützt keine dynamischen Inhalte.

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

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

    Wenn ein Banner auf Cluster-Ebene konfiguriert wurde, wird es durch das Banner auf SVM-Ebene für die angegebene SVM überschrieben.
- Folgende Fakten gelten für die MOTD:
  - Standardmäßig ist das für den Cluster konfigurierte MOTD auch für alle SVMs aktiviert.
  - Außerdem kann für jede SVM ein MOTD auf SVM-Ebene konfiguriert werden.

    Wenn sich Benutzer bei der SVM anmelden, werden in diesem Fall zwei MOTDs angezeigt, eine auf Cluster-Ebene definiert und die andere auf SVM-Ebene.
  - Die MOTD auf Cluster-Ebene kann vom Cluster-Administrator pro SVM aktiviert oder deaktiviert werden.

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

Erstellen Sie ein Banner

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

Schritte

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

Ihr Ziel ist	Dann…
Geben Sie eine Nachricht an, die eine einzelne Zeile ist	Verwenden Sie die `-message` „`text`" Parameter, um den Text anzugeben.
Fügen Sie neue Zeilen (auch als Zeilenende bezeichnet) in die Nachricht ein	Verwenden Sie den Befehl ohne das `-message` Oder `-uri` Parameter zum Starten des interaktiven Modus zum Bearbeiten des Banners.

Ihr Ziel ist	Dann…
Laden Sie Inhalte von einem Speicherort hoch, um für das Banner zu verwenden	Verwenden Sie die `-uri` Parameter zum Festlegen des FTP- oder HTTP-Speicherorts des Inhalts.

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

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

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

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

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

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

Beispiele für die Erstellung von Bannern

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

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

cluster1::>
```

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

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

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

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

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

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

2 entries were displayed.

cluster1::>
```

Verwandte Informationen

Verwalten des Banners

Verwalten des Banners

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

Wahlmöglichkeiten

- Managen Sie das Banner auf Cluster-Ebene:

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

- Banner auf SVM-Ebene managen:

  Angeben `-vserver *svm_name*` Ist im SVM-Kontext nicht erforderlich.

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

Erstellen Sie eine MOTD

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

Eingabeaufforderung.

Schritte

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

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

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

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

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

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

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

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

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

Beispiele für die Erstellung von MOTDs

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

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

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

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

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
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: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

Verwalten der MOTD

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

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	Legen Sie die MOTD auf Cluster-Ebene auf einen leeren String fest (`""`): **`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 aktivierter 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…
[-uri *ftp_or_http_addr*] }*` [NOTE] ==== 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. ====	Ein MOTD auf Cluster-Ebene steht optional allen SVMs zur Verfügung, soll aber nicht, dass der MOTD für Cluster-Anmeldungen angezeigt wird
Legen Sie eine MOTD auf Cluster-Ebene fest, deaktivieren Sie jedoch die Anzeige für das Cluster: `*security login motd modify -vserver *cluster_name* { [-message "*text*"]	[-uri *ftp_or_http_addr*] } -is-cluster-message-enabled false*`
Entfernen Sie alle MODs auf Cluster- und SVM-Ebene, wenn nur einige SVMs über MOTDs auf Cluster-Ebene und SVM-Ebene verfügen	Legen Sie den Cluster und alle SVMs so fest, dass für die MOTD ein leerer String verwendet wird: **`security login motd modify -vserver * -message ""`**
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	Verwenden Sie erweiterte Abfragen, um die MOTD selektiv zu ändern: `*security login motd modify { -vserver !"*cluster_name*" -message !"" } { [-message "*text*"]
[-uri *ftp_or_http_addr*] }*`	Alle MOTDs, die spezifischen Text enthalten (z. B. „`Januar`“ gefolgt von „`2015`“), können überall in einer einzelnen oder mehrzeiligen Nachricht angezeigt werden, auch wenn der Text über verschiedene Zeilen aufgeteilt wird
Verwenden Sie eine Abfrage, um MOTDs anzuzeigen: **`security login motd show -message *"January"*"2015"*`**	Erstellen Sie interaktiv ein MOTD, das mehrere und aufeinanderfolgende Zeilen enthält (auch als Zeilenende oder EOLs bezeichnet).

- Management von MOTD auf SVM-Ebene:

  Angeben `-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 Cluster-Administrator) **`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

Lizenzen managen (nur Cluster-Administratoren)

Übersicht über die Lizenzverwaltung (nur Cluster-Administratoren)

Eine Lizenz ist ein Datensatz mit einem oder mehreren Softwareberechtigungen. In ONTAP 8.2 bis ONTAP 9.9 werden Lizenzschlüssel als 28-stellige Zeichenfolgen ausgeliefert, und es gibt einen Schlüssel pro ONTAP-Funktion. In ONTAP 9.2 wurde nur für Cluster-weite Funktionen ein neues Lizenzschlüsselformat namens NetApp License File (NLF) eingeführt, beispielsweise FabricPool.

Ab ONTAP 9.10.1 werden alle Lizenzen als NLFs ausgeliefert. Bei NLF-Lizenzen können je nach Kauf eine oder mehrere ONTAP-Funktionen aktiviert werden. Sie können NLF-Lizenzen über die NetApp Support Site abrufen, indem Sie nach der Seriennummer des Systems (Controller) suchen.

Die Lizenzen für Ihre anfänglichen oder zusätzlichen Software-Bestellungen finden Sie auf der NetApp Support Site unter **Mein Support** > **Software-Lizenzen** (Anmeldung erforderlich). Weitere Informationen zum Austausch von Lizenzen finden Sie im Knowledge Base-Artikel "Lizenzierungsprozess für AFF/FAS Systeme nach dem Motherboard-Ersatzprozess".

ONTAP ermöglicht Ihnen die Verwaltung der Funktionslizenzen auf folgende Weise:

- Zeigt Informationen zu installierten Lizenzen an (`system license show`)
- Zeigen Sie die Pakete an, für die Lizenzen erforderlich sind, sowie den aktuellen Lizenzstatus auf dem Cluster an (`system license status show`)
- Löschen Sie eine Lizenz aus dem Cluster oder einem Node, dessen Seriennummer Sie angeben (`system license delete`)

- Abgelaufene oder nicht verwendete Lizenzen anzeigen oder entfernen (`system license clean-up`)

ONTAP bietet Ihnen folgende Möglichkeiten, das Risiko der Nutzung von Funktionen und Lizenzberechtigungen zu überwachen:

- Zeigen Sie eine Zusammenfassung der Funktionsnutzung im Cluster auf Node-Basis an (`system feature-usage show-summary`)

  Die Zusammenfassung enthält Zählerinformationen wie die Anzahl der Wochen, in denen eine Funktion verwendet wurde, sowie das letzte Datum und die letzte Uhrzeit, zu der die Funktion verwendet wurde.

- Anzeige des Funktionsnutzungsstatus im Cluster auf Node- und Wochenbasis (`system feature-usage show-history`)

  Der Funktionsnutzungsstatus kann sein `not-used`, `configured`, Oder `in-use`. Wenn die Nutzungsinformationen nicht verfügbar sind, wird der Status angezeigt `not-available`.

- Zeigen Sie den Status des Lizenzrisikos für jedes Lizenzpaket an (`system license entitlement-risk show`)

  Der Risikostatus kann sein `low`, `medium`, `high`, `unlicensed`, Oder `unknown`. Der Risikostatus ist auch in der AutoSupport Meldung enthalten. Das Lizenzberechtigungsrisiko gilt nicht für das Basilizenzpaket.

  Das Risiko für Lizenzberechtigungen wird anhand einer Reihe von Faktoren bewertet. Hierzu zählen unter anderem:

  - Der Lizenzstatus jedes Pakets
  - Die Art der einzelnen Lizenzen, ihr Ablaufdatum und die Einheitlichkeit der Lizenzen im gesamten Cluster
  - Verwendung für die Funktionen, die dem Lizenzpaket zugeordnet sind Wenn der Evaluierungsprozess feststellt, dass das Risiko eines Lizenzanspruchs besteht, schlägt die Befehlsausgabe eine Korrekturmaßnahme vor.

> Hinweis: ONTAP 9.10.1 unterstützt auch 28-stellige Lizenzschlüssel mit System Manager oder der CLI. Wenn jedoch eine NLF-Lizenz für eine Funktion installiert ist, können Sie keinen 28-stelligen Lizenzschlüssel für dieselbe Funktion über die NLF-Lizenz installieren. Informationen zum Installieren von NLFs oder Lizenzschlüssel mit System Manager finden Sie unter „Neue Funktionen aktivieren“.

Verwandte Informationen

"Was sind die Übersicht und Referenzen zu den Lizenzen für Data ONTAP 8.2 und 8.3?"

"Überprüfen von Data ONTAP-Softwareberechtigungen und zugehörigen Lizenzschlüssel mithilfe der Support-Website"

"FAQ: Lizenzierungs-Updates in Data ONTAP 9.2"

"NetApp: Data ONTAP-Berechtigungsrisiko"

Lizenztypen und lizenzierte Methode

Mit dem Verständnis der Lizenztypen und der lizenzierten Methode können Sie die

Lizenzen in einem Cluster verwalten.

Lizenztypen

Ein Paket kann einen oder mehrere der folgenden Lizenztypen enthalten, die im Cluster installiert sind. Der `system license show` Der Befehl zeigt den installierten Lizenztyp oder den Typ für ein Paket an.

- Standardlizenz (`license`)

  Bei einer Standardlizenz handelt es sich um eine Node-gesperrte Lizenz. Er wird für einen Node mit einer bestimmten System-Seriennummer ausgegeben (auch bekannt als *Controller-Seriennummer*). Eine Standardlizenz ist nur für den Node gültig, der über die entsprechende Seriennummer verfügt.

  Durch die Installation einer Node-gesperrten Standard-Lizenz ist ein Node auf die lizenzierte Funktionalität berechtigt. Damit der Cluster lizenzierte Funktionen nutzen kann, muss mindestens ein Node für die Funktionalität lizenziert sein. Die Verwendung der lizenzierten Funktionen auf einem Node, der nicht über einen Anspruch auf die Funktionalität verfügt, ist möglicherweise nicht konform.

- Standortlizenz (`site`)

  Eine Standortlizenz ist nicht an eine bestimmte Seriennummer des Systems gebunden. Wenn Sie eine Standortlizenz installieren, haben alle Knoten im Cluster Anspruch auf die lizenzierte Funktionalität. Der `system license show` Mit dem Befehl werden Standortlizenzen unter der Cluster-Seriennummer angezeigt.

  Wenn Ihr Cluster über eine Standortlizenz verfügt und Sie einen Node aus dem Cluster entfernen, enthält der Node nicht die Standortlizenz, und er ist nicht mehr berechtigt, die lizenzierte Funktionalität zu nutzen. Wenn Sie einem Cluster einen Node hinzufügen, der über eine Standortlizenz verfügt, hat der Node automatisch Anspruch auf die von der Standortlizenz gewährte Funktionalität.

- Evaluierungslizenz (`demo`)

  Eine Evaluierungslizenz ist eine temporäre Lizenz, die nach einer bestimmten Zeit (angegeben durch die) abläuft `system license show` Befehl). Es ermöglicht Ihnen, bestimmte Software-Funktionen ohne Erwerb einer Berechtigung zu testen. Der gesamte Cluster ist nicht an eine bestimmte Seriennummer des Nodes gebunden.

  Wenn Ihr Cluster über eine Evaluierungslizenz für ein Paket verfügt und Sie einen Node aus dem Cluster entfernen, enthält der Node nicht die Evaluierungslizenz.

Lizenzierte Methode

Es ist möglich, eine Cluster-weite Lizenz zu installieren (die `site` Oder `demo` Typ) und eine Node-gesperrte Lizenz (die `license` Typ) für ein Paket. Daher kann ein installiertes Paket mehrere Lizenztypen im Cluster umfassen. Für den Cluster gibt es jedoch nur eine *lizenzierte Methode* für ein Paket. Der `licensed method` Feld von `system license status show` Befehl zeigt die Berechtigung an, die für ein Paket verwendet wird. Der Befehl bestimmt die lizenzierte Methode wie folgt:

- Wenn in einem Paket nur ein Lizenztyp im Cluster installiert ist, ist der installierte Lizenztyp die lizenzierte Methode.
- Wenn in einem Paket keine Lizenzen im Cluster installiert sind, wird die lizenzierte Methode verwendet `none`.

- Wenn in einem Paket mehrere Lizenztypen im Cluster installiert sind, wird die lizenzierte Methode in der folgenden Prioritätsreihenfolge des Lizenztyps bestimmt:-`site`, `license`, und `demo`.

  Beispiel:

  - Wenn Sie über eine Standortlizenz, eine Standardlizenz und eine Evaluierungslizenz für ein Paket verfügen, ist die lizenzierte Methode für das Paket im Cluster `site`.
  - Wenn Sie über eine Standardlizenz und eine Evaluierungslizenz für ein Paket verfügen, wird für das Paket im Cluster die lizenzierte Methode verwendet `license`.
  - Wenn Sie nur über eine Evaluierungslizenz für ein Paket verfügen, lautet die lizenzierte Methode für das Paket im Cluster `demo`.

Befehle zum Verwalten von Lizenzen

Sie verwenden das `system license` Befehle zum Verwalten von Funktionslizenzen für den Cluster. Sie verwenden das `system feature-usage` Befehle für das Überwachen der Funktionsnutzung.

Ihr Ziel ist	Befehl
Fügen Sie eine oder mehrere Lizenzen hinzu	`system license add`
Informationen über installierte Lizenzen anzeigen, z. B.: • Name und Beschreibung des Lizenzpakets • Lizenztyp (`site`, `license`, Oder `demo`) • Ablaufdatum, falls zutreffend • Den Cluster oder Nodes, für die ein Paket lizenziert ist • Gibt an, ob die Lizenz vor Data ONTAP 8.2 installiert wurde (`legacy`) • Kunden-ID	`system license show` Einige Informationen werden nur angezeigt, wenn Sie das verwenden `-instance` Parameter.
Alle Pakete anzeigen, die Lizenzen und ihren aktuellen Lizenzstatus benötigen, einschließlich: • Der Paketname • Die lizenzierte Methode • Das Ablaufdatum, falls zutreffend	`system license status show`
Löschen Sie die Lizenz eines Pakets aus dem Cluster oder einem Node, dessen Seriennummer Sie angeben	`system license delete`

Ihr Ziel ist	Befehl
Abgelaufene oder nicht verwendete Lizenzen anzeigen oder entfernen	`system license clean-up`
Zusammenfassung der Funktionsnutzung im Cluster pro Node anzeigen	`system feature-usage show-summary`
Anzeige des Funktionsnutzungsstatus im Cluster auf Node- und Wochenbasis	`system feature-usage show-history`
Zeigen Sie den Status des Lizenzrisikos für jedes Lizenzpaket an	`system license entitlement-risk show` Einige Informationen werden nur angezeigt, wenn Sie das verwenden `-detail` Und `-instance` Parameter.

Verwandte Informationen

"ONTAP 9-Befehle"

Verwalten von Jobs und Zeitplänen

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

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.

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`
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)

Ihr Ziel ist	Befehl
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)

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

Verwandte Informationen

"ONTAP 9-Befehle"

Befehle zum Verwalten von Job-Zeitplänen

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

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

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

Ihr Ziel ist	Befehl
Informationen zu allen Zeitplänen anzeigen	`job schedule show`
Zeigt die Liste der Jobs nach Zeitplan an	`job schedule show-jobs`
Informationen zu cron-Zeitplänen anzeigen	`job schedule cron show`
Zeigt Informationen zu Intervallzeitplänen an	`job schedule interval show`
Erstellen Sie einen Cron-Zeitplan[1]	`job schedule cron create`
Erstellen eines Intervallplans	`job schedule interval create` Sie müssen mindestens einen der folgenden Parameter angeben: `-days`, `-hours`, `-minutes`, Oder `-seconds`.
Ändern Sie einen Cron-Zeitplan	`job schedule cron modify`
Ändern eines Intervallplans	`job schedule interval modify`
Löschen Sie einen Zeitplan	`job schedule delete`
Löschen Sie einen Cron-Zeitplan	`job schedule cron delete`
Einen Intervallzeitplan löschen	`job schedule interval delete`

[1]beginnt mit ONTAP 9.10.1, wenn Sie einen Job-Zeitplan mithilfe des erstellen `job schedule cron create` Sie können den Vserver für Ihren Job-Zeitplan angeben.

Verwandte Informationen

"ONTAP 9-Befehle"

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

Welche Backup-Dateien sind für die Konfiguration

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

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

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

Es gibt zwei Arten von Konfigurations-Backup-Dateien:

- **Knoten Konfiguration Backup-Datei**

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

- **Sicherungsdatei der Clusterkonfiguration**

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

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

Management von Konfigurations-Backups

Automatisierte Backups der Node- und Cluster-Konfigurationen

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

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

- Alle 8 Stunden
- Täglich
- Wöchentlich

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

Bei Single-Node-Clustern (einschließlich Data ONTAP Edge-Systemen) können Sie das Konfigurations-Backup-Ziel während des Software-Setups angeben. Nach dem Setup können diese Einstellungen mit ONTAP Befehlen geändert werden.

Befehle zum Management von Backup-Zeitplänen der Konfiguration

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

Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

Ihr Ziel ist	Befehl
Ändern Sie die Einstellungen für einen Konfigurations-Backup-Zeitplan: • Geben Sie eine Remote-URL an (HTTP, HTTPS, FTP, FTPS oder TFTP), bei der die Konfigurations-Backup-Dateien zusätzlich zu den Standardstandorten im Cluster hochgeladen werden • Geben Sie einen Benutzernamen an, der zur Anmeldung an der Remote-URL verwendet werden soll • Legen Sie die Anzahl der Backups fest, die für jeden Backup-Zeitplan der Konfiguration beibehalten werden sollen	`system configuration backup settings modify` Wenn Sie HTTPS in der Remote-URL verwenden, verwenden Sie das `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatvalidierung. Die Zertifikatvalidierung ist standardmäßig deaktiviert. 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.
Legen Sie das Kennwort fest, mit dem Sie sich bei der Remote-URL anmelden können	`system configuration backup settings set-password`
Zeigen Sie die Einstellungen für den Konfigurations-Backup-Zeitplan an	`system configuration backup settings show` Sie stellen die ein `-instance` Parameter zum Anzeigen des Benutzernamens und der Anzahl der Backups, die für jeden Zeitplan beibehalten werden sollen.

Befehle zum Management von Backup-Dateien der Konfiguration

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

Diese Befehle sind auf der erweiterten Berechtigungsebene verfügbar.

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

Ihr Ziel ist	Befehl
Hochladen einer Konfigurations-Backup-Datei von einem Knoten im Cluster auf eine Remote-URL (FTP, HTTP, HTTPS, TFTP oder FTPS)	`system configuration backup upload` Wenn Sie HTTPS in der Remote-URL verwenden, verwenden Sie das `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatvalidierung. Die Zertifikatvalidierung ist standardmäßig deaktiviert. Der Webserver, auf den Sie die Backup-Konfigurationsdatei hochladen, muss die für HTTP- und POST-Vorgänge aktivierten Vorgänge für HTTPS aktiviert haben. Einige Webserver erfordern möglicherweise die Installation eines zusätzlichen Moduls. Weitere Informationen finden Sie in der Dokumentation Ihres Webservers. Die unterstützten URL-Formate variieren je nach ONTAP-Version. Informationen zu Ihrer ONTAP Version finden Sie in der Hilfe zur Befehlszeile.
Laden Sie eine Sicherungsdatei der Konfiguration von einer Remote-URL auf einen Node im Cluster herunter, und validieren Sie, falls angegeben, das digitale Zertifikat	`system configuration backup download` Wenn Sie HTTPS in der Remote-URL verwenden, verwenden Sie das `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatvalidierung. Die Zertifikatvalidierung ist standardmäßig deaktiviert.
Benennen Sie eine Sicherungsdatei für die Konfiguration auf einem Node im Cluster um	`system configuration backup rename`
Zeigen Sie die Backup-Dateien für einen oder mehrere Nodes im Cluster an, die für eine oder mehrere Nodes konfiguriert sind	`system configuration backup show`
Löschen einer Backup-Konfigurationsdatei auf einem Knoten	`system configuration backup delete` 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.

Wiederherstellen einer Node-Konfiguration

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

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

Über diese Aufgabe

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

Schritt

1. Stellen Sie die Sicherungsdatei für die Konfiguration dem Knoten zur Verfügung, für den Sie die Konfiguration wiederherstellen müssen.

Wenn sich die Backup-Datei der Konfiguration befindet…	Dann…
Unter einer Remote-URL	Verwenden Sie die `system configuration backup download` Mit dem Befehl auf der erweiterten Berechtigungsebene können Sie ihn auf den wiederherzuenden Node herunterladen.
Auf einem Node im Cluster	a. Verwenden Sie die `system configuration backup show` Befehl auf der erweiterten Berechtigungsebene, um die Liste der Backup-Konfigurationsdateien anzuzeigen, die im Cluster verfügbar sind, die die Konfiguration des wiederherzuenden Node enthält. b. Wenn die von Ihnen identifizierte Konfigurations-Backup-Datei nicht auf dem wiederherzuenden Knoten vorhanden ist, verwenden Sie den `system configuration backup copy` Befehl zum Kopieren auf den Node zum Wiederherstellen.

Wenn Sie zuvor den Cluster neu erstellt haben, sollten Sie eine Konfigurations-Backup-Datei wählen, die nach der Cluster-Erholung erstellt wurde. Wenn Sie eine Backup-Datei der Konfiguration verwenden müssen, die vor der Cluster-Erholung erstellt wurde, dann müssen Sie nach der Wiederherstellung des Knotens den Cluster erneut erstellen.

Stellen Sie die Node-Konfiguration mithilfe einer Backup-Konfigurationsdatei wieder her

Sie stellen die Node-Konfiguration mithilfe der Backup-Datei der Konfiguration wieder her, die Sie für den Wiederherstellungsknoten identifiziert und bereitgestellt haben.

Über diese Aufgabe

Sie sollten diese Aufgabe nur durchführen, um nach einem Notfall, der zum Verlust der lokalen Konfigurationsdateien des Knotens führte, wiederherzustellen.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   `set -privilege advanced`

2. Wenn der Node sich in einem ordnungsgemäßen Zustand befindet, verwenden Sie auf der erweiterten Berechtigungsebene eines anderen Node die `cluster modify` Befehl mit dem `-node` Und `-eligibility` Parameter, die nicht unterstützt werden sollen, und um sie vom Cluster zu isolieren.

   Wenn der Knoten nicht ordnungsgemäß ist, sollten Sie diesen Schritt überspringen.

   In diesem Beispiel wird node2 so geändert, dass er nicht zur Teilnahme am Cluster berechtigt ist, damit seine Konfiguration wiederhergestellt werden kann:

   ```
   cluster1::*> cluster modify -node node2 -eligibility false
   ```

3. Verwenden Sie die `system configuration recovery node restore` Befehl auf der erweiterten Berechtigungsebene zum Wiederherstellen der Node-Konfiguration aus einer Backup-Konfigurationsdatei.

   Wenn der Knoten seine Identität verloren hat, einschließlich seines Namens, sollten Sie den verwenden `-nodename-in-backup` Parameter zum Angeben des Node-Namens in der Backup-Datei der Konfiguration.

   In diesem Beispiel wird die Konfiguration des Node mithilfe einer der auf dem Node gespeicherten Backup-Konfigurationsdateien wiederhergestellt:

   ```
   cluster1::*> system configuration recovery node restore -backup
   cluster1.8hour.2011-02-22.18_15_00.7z

   Warning: This command overwrites local configuration files with
            files contained in the specified backup file. Use this
            command only to recover from a disaster that resulted
            in the loss of the local configuration files.
            The node will reboot after restoring the local configuration.
   Do you want to continue? {y|n}: y
   ```

   Die Konfiguration wird wiederhergestellt und der Node wird neu gebootet.

4. Wenn Sie den nicht zugelassenen Knoten markiert haben, verwenden Sie den `system configuration recovery cluster sync` Befehl, um den Node als berechtigt zu markieren und mit dem Cluster zu synchronisieren.
5. Wenn Sie in einer SAN-Umgebung arbeiten, verwenden Sie das `system node reboot` Befehl zum Neustart des Knotens und Wiederherstellung des SAN Quorum.

Nachdem Sie fertig sind

Wenn Sie das Cluster zuvor neu erstellt haben und wenn Sie die Node-Konfiguration mithilfe einer Backup-Konfigurationsdatei wiederherstellen, die vor der erneuten Erstellung dieses Clusters erstellt wurde, müssen Sie das Cluster erneut erstellen.

Wiederherstellung einer Cluster-Konfiguration

Suchen Sie eine Konfiguration zum Wiederherstellen eines Clusters

Zur Wiederherstellung eines Clusters verwenden Sie die Konfiguration entweder für einen Node im Cluster oder für eine Backup-Datei einer Cluster-Konfiguration.

Schritte

1. Wählen Sie eine Art von Konfiguration, um das Cluster wiederherzustellen.

   - Ein Node im Cluster

     Wenn das Cluster mehr als einen Node enthält und einer der Nodes über eine Cluster-Konfiguration verfügt, als sich das Cluster in der gewünschten Konfiguration befand, können Sie das Cluster mithilfe der auf diesem Node gespeicherten Konfiguration wiederherstellen.

     In den meisten Fällen ist der Knoten, der den Replikationsring mit der letzten Transaktions-ID enthält, der für das Wiederherstellen der Cluster-Konfiguration am besten verwendet werden kann. Der `cluster ring show` Mit dem Befehl auf der erweiterten Berechtigungsebene können Sie eine Liste der replizierten Ringe anzeigen, die auf jedem Node im Cluster verfügbar sind.

   - Eine Backup-Datei für die Cluster-Konfiguration

     Wenn Sie keinen Node mit der korrekten Cluster-Konfiguration identifizieren können oder wenn das Cluster aus einem einzelnen Node besteht, können Sie eine Backup-Datei für die Cluster-Konfiguration verwenden, um das Cluster wiederherzustellen.

   Wenn Sie das Cluster von einer Backup-Datei der Konfiguration wiederherstellen, gehen alle seit dem Backup vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Backup-Datei der Konfiguration und der vorhandenen Konfiguration behoben werden. Siehe Knowledge Base-Artikel "ONTAP Konfigurations-Backup Resolution Guide" Zur Anleitung zur Fehlerbehebung.

2. Wenn Sie sich für eine Backup-Datei der Cluster-Konfiguration entscheiden, stellen Sie die Datei dem Knoten zur Verfügung, den Sie verwenden möchten, um das Cluster wiederherzustellen.

Wenn sich die Backup-Datei der Konfiguration befindet…	**Dann…**
Unter einer Remote-URL	Verwenden Sie die `system configuration backup download` Mit dem Befehl auf der erweiterten Berechtigungsebene können Sie ihn auf den wiederherzuenden Node herunterladen.

Wenn sich die Backup-Datei der Konfiguration befindet…	Dann…
Auf einem Node im Cluster	a. Verwenden Sie die `system configuration backup show` Befehl auf der erweiterten Berechtigungsebene zum Suchen einer Backup-Datei für die Cluster-Konfiguration, die erstellt wurde, als das Cluster in der gewünschten Konfiguration ausgeführt wurde. b. Wenn sich die Backup-Datei für die Cluster-Konfiguration nicht auf dem Node befindet, den Sie zur Wiederherstellung des Clusters verwenden möchten, verwenden Sie den `system configuration backup copy` Befehl zum Kopieren auf den Node zum Wiederherstellen.

Wiederherstellen einer Cluster-Konfiguration aus einer vorhandenen Konfiguration

Zum Wiederherstellen einer Cluster-Konfiguration aus einer vorhandenen Konfiguration nach einem Cluster-Ausfall erstellen Sie das Cluster erneut mit der von Ihnen gewählten Cluster-Konfiguration, die dem Wiederherstellungsknoten zur Verfügung gestellt wurde, und fügen Sie dann jeden zusätzlichen Node wieder zum neuen Cluster hinzu.

Über diese Aufgabe

Sie sollten diese Aufgabe nur ausführen, um nach einem Ausfall die Konfiguration des Clusters zu verlieren.

Wenn Sie das Cluster erneut aus einer Sicherungsdatei der Konfiguration erstellen, müssen Sie sich an den technischen Support wenden, um alle Abweichungen zwischen der Backup-Datei der Konfiguration und der im Cluster vorhandenen Konfiguration zu beheben.

Wenn Sie das Cluster von einer Backup-Datei der Konfiguration wiederherstellen, gehen alle seit dem Backup vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Backup-Datei der Konfiguration und der vorhandenen Konfiguration behoben werden. Weitere Informationen finden Sie im Knowledge Base-Artikel "ONTAP Leitfaden zur Lösung der Konfigurationssicherung enthält Hinweise zur Fehlerbehebung".

Schritte

1. Deaktivieren Sie Storage-Failover für jedes HA-Paar:

   `storage failover modify -node` *`node_name`* `-enabled false`

   Sie müssen den Storage-Failover nur einmal für jedes HA-Paar deaktivieren. Wenn Sie den Storage-Failover für einen Node deaktivieren, ist auch das Storage-Failover beim Partner des Nodes deaktiviert.

2. Anhalten jedes Knotens mit Ausnahme des wiederherenden Knotens:

   `system node halt -node` *`node_name`* `-reason "text"`

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Legen Sie die Berechtigungsebene auf erweitert fest:

   set -privilege advanced

4. Verwenden Sie auf dem Recovery-Node den **system configuration recovery cluster recreate** Befehl zum erneuten Erstellen des Clusters.

   In diesem Beispiel wird das Cluster mithilfe der Konfigurationsinformationen, die auf dem wiederherzuenden Node gespeichert sind, neu erstellt:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

   Auf dem wiederherstellenden Node wird ein neues Cluster erstellt.

5. Wenn Sie das Cluster aus einer Sicherungsdatei der Konfiguration neu erstellen, überprüfen Sie, ob die Cluster-Recovery noch läuft:

   system configuration recovery cluster show

   Sie müssen den Cluster-Recovery-Status nicht überprüfen, wenn Sie das Cluster von einem ordnungsgemäßen Node neu erstellen.

```
cluster1::*> system configuration recovery cluster show
 Recovery Status: in-progress
 Is Recovery Status Persisted: false
```

6. Booten aller Nodes, die neu mit dem neu erstellten Cluster verbunden werden müssen

   Sie müssen die Nodes nacheinander neu booten.

7. Gehen Sie für jeden Node, der mit dem neu erstellten Cluster verbunden werden muss, wie folgt vor:

   a. Fügen Sie auf dem neu erstellten Cluster von einem gesunden Node erneut dem Ziel-Node bei:

      system configuration recovery cluster rejoin -node *node_name*

In diesem Beispiel wird der Zielknoten „node2“ wieder dem neu erstellten Cluster hinzugefügt:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
         cluster, potentially overwriting critical cluster
         configuration files. This command should only be used
         to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Der Ziel-Node wird neu gebootet und Beitritt zum Cluster.

b. Vergewissern Sie sich, dass der Ziel-Node ordnungsgemäß ist und das Quorum mit den übrigen Nodes im Cluster gebildet wurde:

`cluster show -eligibility true`

Der Ziel-Node muss dem neu erstellten Cluster erneut beitreten, bevor Sie einem anderen Node erneut beitreten können.

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. Wenn Sie das Cluster aus einer Backup-Konfigurationsdatei neu erstellen, setzen Sie den Recovery-Status auf abgeschlossen:

`system configuration recovery cluster modify -recovery-status complete`

9. Zurück zur Administratorberechtigungsebene:

`set -privilege admin`

10. Wenn der Cluster nur aus zwei Nodes besteht, verwenden Sie den **`cluster ha modify`** Befehl zum Reaktivieren der Cluster HA
11. Verwenden Sie die **`storage failover modify`** Befehl zum Reaktivieren von Storage Failover für jedes HA-Paar.

Nachdem Sie fertig sind

Wenn der Cluster über SnapMirror Peer-Beziehungen verfügt, müssen Sie diese Beziehungen auch neu erstellen. Weitere Informationen finden Sie unter "Datensicherung".

Synchronisieren eines Node mit dem Cluster

Wenn ein oder mehrere Knoten nicht mit dem Cluster synchronisiert sind, müssen Sie den Knoten synchronisieren, um die replizierte Datenbank (RDB) auf dem Knoten wiederherzustellen und in das Quorum zu bringen.

Schritt

1. Verwenden Sie von einem gesunden Knoten die `system configuration recovery cluster sync` Befehl auf der erweiterten Berechtigungsebene zum Synchronisieren des Node, der nicht mit der Cluster-Konfiguration synchronisiert ist.

   Dieses Beispiel synchronisiert einen Knoten (*node2*) mit dem Rest des Clusters:

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

Ergebnis

Die RDB wird zum Node repliziert, und der Node kann am Cluster teilnehmen.

Management von Core Dumps (nur Cluster-Administratoren)

Wenn eine Panik eines Node auftritt, wird ein Core Dump angezeigt, und das System erstellt eine Core Dump-Datei, die vom technischen Support zum Beheben des Problems verwendet werden kann. Sie können Core Dump-Attribute konfigurieren oder anzeigen. Sie können auch eine Core Dump-Datei speichern, anzeigen, segmentieren, hochladen oder löschen.

Sie haben folgende Möglichkeiten, Core Dumps zu verwalten:

- Konfigurieren von Core Dumps und Anzeigen der Konfigurationseinstellungen
- Anzeigen von Basisinformationen, dem Status und den Attributen von Core Dumps

  Core Dump-Dateien und -Berichte werden in gespeichert `/mroot/etc/crash/` Verzeichnis eines Knotens. Sie können den Verzeichnisinhalt mithilfe der anzeigen `system node coredump` Befehle oder

einen Webbrowser.

- Speichern des Core Dump-Inhalts und Hochladen der gespeicherten Datei an einen bestimmten Speicherort oder technischen Support

  ONTAP verhindert, dass Sie das Speichern einer Core Dump-Datei während eines Takeover, einer Aggregatverschiebung oder einer Rückgabe initiieren.

- Löschen von Core Dump-Dateien, die nicht mehr benötigt werden

AFF A220, AFF A800, FAS2720, FAS2750 und höher speichern Core Dumps auf ihrem Boot-Gerät. Wenn auf diesen Systemen NetApp Volume Encryption (NVE) oder NetApp Storage Encryption (NSE) aktiviert ist, wird der Core Dump auch verschlüsselt.

Befehle zum Verwalten von Core Dumps

Sie verwenden das `system node coredump config` Befehle zum Verwalten der Konfiguration von Core Dumps, die `system node coredump` Befehle zum Verwalten der Core Dump-Dateien und des `system node coredump reports` Befehle zum Managen von Kernberichten für Anwendungen.

Ihr Ziel ist	Befehl
Konfigurieren von Core Dumps	`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 beiden `-dump` Und `-skip-lif-migration` Parameter
Lösen Sie beim Herunterfahren eines Node manuell einen Core Dump aus	`system node halt` Mit beiden `-dump` Und `-skip-lif-migration` Parameter
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` Der 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 9-Befehle"

Überwachen eines Speichersystems

Nutzen Sie AutoSupport und Active IQ Digital Advisor

Die AutoSupport-Komponente von ONTAP erfasst Telemetrie und sendet diese zur Analyse. Active IQ Digital Advisor analysiert die Daten von AutoSupport und bietet proaktive Betreuung und Optimierung. Mithilfe künstlicher Intelligenz erkennt Active IQ potenzielle Probleme und löst sie, bevor sie sich auf das Geschäft auswirken.

Mit Active IQ optimieren Kunden ihre Dateninfrastruktur in der gesamten globalen Hybrid Cloud. Dazu bieten sie konkrete prädiktive Analysen und proaktiven Support über ein Cloud-basiertes Portal und eine mobile App. NetApp Kunden mit aktivem SupportEdge-Vertrag profitieren von Daten-fokussierten Einblicken und Empfehlungen von Active IQ (Funktionen variieren je nach Produkt- und Support-Tier).

Folgende Möglichkeiten bietet Active IQ:

- Planung von Upgrades: Active IQ erkennt Probleme in Ihrer Umgebung, die durch ein Upgrade auf eine neuere Version von ONTAP behoben werden können, und die Upgrade Advisor Komponente unterstützt Sie bei der Planung eines erfolgreichen Upgrades.
- Sehen Sie sich das Wellness-System an. Ihr Active IQ Dashboard meldet alle Probleme im Zusammenhang mit dem Wellness-Bereich und hilft Ihnen, diese Probleme zu beheben. Überwachen Sie die Systemkapazität, um sicherzugehen, dass nie mehr Speicherplatz belegt wird. Zeigen Sie Support-Cases für Ihr System an.
- Performance-Management: Active IQ zeigt die System-Performance über einen längeren Zeitraum an, als Sie in System Manager sehen können. Identifizieren Sie Konfigurations- und Systemprobleme, die Ihre Performance beeinträchtigen.
- Maximale Effizienz Anzeige von Storage-Effizienz-Metriken und Identifizierung von Möglichkeiten, mehr Daten auf weniger Speicherplatz zu speichern
- Anzeige von Inventar und Konfiguration Active IQ zeigt vollständige Informationen zur Bestands- und Software- und Hardwarekonfiguration an. Prüfen Sie, wann die Serviceverträge ablaufen und verlängern Sie sie, um sicherzustellen, dass der Support weiterhin gewährleistet ist.

Verwandte Informationen

"NetApp Dokumentation: Active IQ Digital Advisor"

"Starten Sie Active IQ"

"SupportEdge Services"

Managen Sie AutoSupport-Einstellungen mit System Manager

Mit System Manager können Sie die Einstellungen für Ihr AutoSupport Konto anzeigen und bearbeiten.

Sie können folgende Aktionen durchführen:

- Zeigen Sie AutoSupport-Einstellungen an
- AutoSupport Daten generieren und senden
- Verbindung zu AutoSupport testen
- Aktivieren oder deaktivieren Sie AutoSupport
- Generierung von Support-Fällen unterdrücken
- Wiederaufnahme der Erstellung von Support-Cases
- AutoSupport-Einstellungen bearbeiten

Zeigen Sie AutoSupport-Einstellungen an

Mit System Manager können Sie die Einstellungen für Ihr AutoSupport Konto anzeigen.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.

   Im Abschnitt **AutoSupport** werden folgende Informationen angezeigt:

   - Status
   - Transportprotokoll
   - Proxy-Server
   - Von E-Mail-Adresse

2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Weitere Optionen**.

   Weitere Informationen zu den AutoSupport-Verbindungs- und E-Mail-Einstellungen werden angezeigt. Außerdem wird der Übertragungsverlauf von Nachrichten aufgelistet.

AutoSupport Daten generieren und senden

In System Manager können Sie die Generierung von AutoSupport Meldungen initiieren und aus welchem Cluster-Node oder welchen Nodes die Daten erfasst werden.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Erzeugen und Senden**.

3. Geben Sie einen Betreff ein.
4. Klicken Sie auf das Kontrollkästchen unter **Daten sammeln von**, um die Knoten anzugeben, aus denen die Daten erfasst werden sollen.

Verbindung zu AutoSupport testen

Von System Manager können Sie eine Testmeldung senden, um die Verbindung zu AutoSupport zu überprüfen.

Schritte

1. Klicken Sie in System Manager auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Konnektivität testen**.
3. Geben Sie einen Betreff für die Nachricht ein.

Aktivieren oder deaktivieren Sie AutoSupport

In System Manager können Sie die Fähigkeit von AutoSupport deaktivieren, den Zustand Ihres Storage-Systems zu überwachen und Ihnen Benachrichtigungsmeldungen zu senden. Sie können AutoSupport erneut aktivieren, nachdem sie deaktiviert wurde.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Deaktivieren**.
3. Wenn Sie AutoSupport erneut aktivieren möchten, klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Aktivieren**.

Generierung von Support-Fällen unterdrücken

Ab ONTAP 9.10.1 können Sie mit System Manager eine Anfrage an AutoSupport senden, um die Erstellung von Support-Fällen zu unterdrücken.

Über diese Aufgabe

Um die Generierung von Supportfällen zu unterdrücken, geben Sie die Knoten und die Anzahl der Stunden an, für die die Unterdrückung stattfinden soll.

Das Unterdrücken von Support-Cases ist besonders hilfreich, wenn AutoSupport während der Wartungsarbeiten an Ihren Systemen keine automatisierten Cases erstellt.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Support Case Generation unterdrücken**.
3. Geben Sie die Anzahl der Stunden ein, die die Unterdrückung stattfinden soll.
4. Wählen Sie die Knoten aus, für die die Unterdrückung stattfinden soll.

Wiederaufnahme der Erstellung von Support-Cases

Ab ONTAP 9.10.1 können Sie mit System Manager die Generierung von Support-Cases von AutoSupport fortsetzen, wenn diese unterdrückt wurde.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Support-Case-Erstellung fortsetzen**.
3. Wählen Sie die Knoten aus, für die die Erzeugung fortgesetzt werden soll.

AutoSupport-Einstellungen bearbeiten

Mit System Manager können Sie die Verbindungs- und E-Mail-Einstellungen für Ihr AutoSupport Konto ändern.

Schritte

1. Klicken Sie Auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **AutoSupport** auf ⋮ Klicken Sie dann auf **Weitere Optionen**.
3. Klicken Sie im Abschnitt **Connections** oder im Abschnitt **E-Mail** auf Edit So ändern Sie die Einstellung für einen der beiden Abschnitte.

Verwalten Sie AutoSupport mit der CLI

AutoSupport managen – Übersicht

AutoSupport ist ein Mechanismus, der proaktiv den Zustand Ihres Systems überwacht und automatisch Meldungen an den technischen Support von NetApp, Ihre interne Support-Abteilung und einen Support-Partner sendet. Obwohl AutoSupport Meldungen an den technischen Support standardmäßig aktiviert sind, müssen Sie die richtigen Optionen festlegen und einen gültigen Mail-Host besitzen, der Meldungen an Ihre interne Support-Abteilung gesendet hat.

Nur der Cluster-Administrator kann AutoSupport-Management durchführen. Der SVM-Administrator (Storage Virtual Machine) hat keinen Zugriff auf AutoSupport.

AutoSupport ist standardmäßig aktiviert, wenn Sie das Storage-System zum ersten Mal konfigurieren. AutoSupport beginnt 24 Stunden nach Aktivierung von AutoSupport mit dem Senden von Meldungen an den technischen Support. Sie können die Dauer von 24 Stunden verkürzen, indem Sie das System aktualisieren oder zurücksetzen, die AutoSupport Konfiguration ändern oder die Systemzeit auf eine andere als 24 Stunden verkürzen.

> ⓘ Sie können AutoSupport jederzeit deaktivieren, aber Sie sollten sie aktiviert lassen. Wenn auf dem Storage-System ein Problem auftritt, kann die Problembestimmung und -Behebung durch das Aktivieren von AutoSupport erheblich beschleunigt werden. Standardmäßig erfasst das System AutoSupport Informationen und speichert sie lokal, selbst wenn Sie AutoSupport deaktivieren.

Weitere Informationen zu AutoSupport finden Sie auf der NetApp Support Site.

Verwandte Informationen

- "NetApp Support"
- "Weitere Informationen zu den AutoSupport-Befehlen finden Sie in der ONTAP-CLI"

Wann und wo AutoSupport Meldungen gesendet werden

AutoSupport sendet je nach Nachrichtentyp Meldungen an verschiedene Empfänger. Wann und wo AutoSupport Nachrichten sendet, können Ihnen dabei helfen, Mitteilungen zu verstehen, die Sie per E-Mail oder auf der Active IQ-Website (ehemals My AutoSupport) erhalten.

Sofern nicht anders angegeben, handelt es sich bei den Einstellungen in den folgenden Tabellen um Parameter des `system node autosupport modify` Befehl.

Ereignisgesteuerte Meldungen

Wenn auf dem System Ereignisse auftreten, die Korrekturmaßnahmen erfordern, sendet AutoSupport automatisch eine Meldung, bei der ein Ereignis ausgelöst wurde.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
AutoSupport antwortet auf ein Trigger-Ereignis im EMS	Adressen angegeben in `-to` Und `-noteto`. (Es werden nur kritische Ereignisse gesendet, die sich auf den Service auswirken.) Adressen angegeben in `-partner-address` Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable`

Geplante Nachrichten

AutoSupport sendet automatisch mehrere Meldungen zu einem regelmäßigen Zeitplan.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Täglich (standardmäßig wird zwischen 12:00 Uhr gesendet Und 1:00 Uhr Als Protokollmeldung)	Adressen angegeben in `-partner-address` Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable`
Täglich (standardmäßig wird zwischen 12:00 Uhr gesendet Und 1:00 Uhr Als Leistungsmeldung), wenn der `-perf` Parameter ist auf festgelegt `true`	Adressen angegeben in -Partner-address`  Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable`
Wöchentlich (standardmäßig gesendet Sonntag zwischen 12:00 Uhr Und 1:00 Uhr)	Adressen angegeben in `-partner-address` Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable`

Manuell ausgelöste Nachrichten

Sie können eine AutoSupport Meldung manuell initiieren oder erneut senden.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Sie initiieren eine Meldung manuell über das `system node autosupport invoke` Befehl	Wenn ein URI mit angegeben wird `-uri` Parameter in `system node autosupport invoke` Befehl, die Meldung wird an diesen URI gesendet. Wenn `-uri` Wird nicht angegeben, wird die Meldung an die in angegebenen Adressen gesendet `-to` Und `-partner-address`. Die Meldung wird auch an den technischen Support gesendet, wenn `-support` Ist auf festgelegt `enable`.
Sie initiieren eine Meldung manuell über das `system node autosupport invoke-core-upload` Befehl	Wenn ein URI mit angegeben wird `-uri` Parameter in `system node autosupport invoke-core-upload` Befehl, die Meldung wird an diesen URI gesendet und die Core Dump-Datei wird auf den URI hochgeladen. Wenn `-uri` Wird im nicht angegeben `system node autosupport invoke-core-upload` Befehl, die Meldung wird an den technischen Support gesendet und die Core Dump-Datei wird auf die Website des technischen Supports hochgeladen. Beide Szenarien erfordern das `-support` Ist auf festgelegt `enable` Und `-transport` Ist auf festgelegt `https` Oder `http`. Aufgrund der großen Größe von Core Dump-Dateien wird die Meldung nicht an die Adressen gesendet, die in angegeben sind `-to` Und `-partner-addresses` Parameter.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Sie initiieren eine Meldung manuell über das `system node autosupport invoke-performance-archive` Befehl	Wenn ein URI mit angegeben wird `-uri` Parameter in `system node autosupport invoke-performance-archive` Befehl, die Meldung wird an diesen URI gesendet und die Performance-Archivdatei wird auf den URI hochgeladen. Wenn `-uri` Wird im nicht angegeben `system node autosupport invoke-performance-archive`, Die Nachricht wird an den technischen Support gesendet, und die Archiv-Datei für die Performance wird auf die Website des technischen Supports hochgeladen. Beide Szenarien erfordern das `-support` Ist auf festgelegt `enable` Und `-transport` Ist auf festgelegt `https` Oder `http`. Aufgrund der großen Größe von Performance-Archivdateien wird die Meldung nicht an die Adressen gesendet, die in angegeben sind `-to` Und `-partner-addresses` Parameter.
Sie senden eine frühere Nachricht manuell mit dem erneut `system node autosupport history retransmit` Befehl	Nur für den URI, den Sie im angeben `-uri` Parameter von `system node autosupport history retransmit` Befehl

Meldungen, die durch den technischen Support ausgelöst werden

Der technische Support kann Meldungen von AutoSupport über die AutoSupport OnDemand Funktion anfordern.

Wenn die Nachricht gesendet wird	Wo die Nachricht gesendet wird
Wenn das AutoSupport Lieferanweisungen erhält, um neue AutoSupport Meldungen zu generieren	Adressen angegeben in `-partner-address` Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable` Und `-transport` Ist auf festgelegt `https`
Wenn AutoSupport Lieferanweisungen erhält, um frühere AutoSupport Meldungen erneut zu senden	Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable` Und `-transport` Ist auf festgelegt `https`
Wenn AutoSupport Anweisungen zur Bereitstellung erhält, um neue AutoSupport Meldungen zu generieren, die Core Dump- oder Performance-Archivdateien hochladen	Technische Unterstützung, wenn `-support` Ist auf festgelegt `enable` Und `-transport` Ist auf festgelegt `https`. Die Core Dump- oder Performance-Archivdatei wird auf die technische Support-Website hochgeladen.

Wie AutoSupport ereignisgesteuerte Meldungen erstellt und sendet

AutoSupport erstellt ereignisgesteuerte AutoSupport-Meldungen, wenn das EMS ein Trigger-Ereignis verarbeitet. Eine ereignisgesteuerte AutoSupport-Meldung benachrichtigt Empfänger von Problemen, die Korrekturmaßnahmen erfordern und enthält nur für das Problem relevante Informationen. Sie können anpassen, welche Inhalte enthalten werden sollen und wer die Nachrichten erhält.

AutoSupport verwendet den folgenden Prozess, um ereignisgesteuerte AutoSupport-Meldungen zu erstellen und zu senden:

1. Wenn das EMS ein Triggerereignis verarbeitet, sendet EMS eine Anfrage an AutoSupport.

   Ein Auslöser ist ein EMS-Ereignis mit einem AutoSupport Ziel und einem Namen, der mit einem beginnt `callhome.` Präfix.

2. AutoSupport erstellt eine ereignisgesteuerte AutoSupport-Meldung.

   AutoSupport sammelt grundlegende und Fehlerbehebungsinformationen von Subsystemen, die mit dem Auslöser verbunden sind, um eine Meldung zu erstellen, die nur relevante Informationen für das Trigger-Ereignis enthalten.

   Jedem Trigger ist ein Standardsatz von Untersystemen zugeordnet. Sie können jedoch wählen, ob Sie zusätzliche Untersysteme mit einem Trigger verknüpfen möchten, indem Sie das verwenden `system node autosupport trigger modify` Befehl.

3. AutoSupport sendet die ereignisgesteuerte AutoSupport-Nachricht an die vom definierten Empfänger `system node autosupport modify` Befehl mit dem `-to`, `-noteto`, `-partner-address`, und `-support` Parameter.

   Sie können die Übermittlung von AutoSupport Meldungen für bestimmte Auslöser aktivieren und deaktivieren, indem Sie das verwenden `system node autosupport trigger modify` Befehl mit dem `-to` Und `-noteto` Parameter.

Beispiel für Daten, die für ein bestimmtes Ereignis gesendet werden

Der `storage shelf PSU failed` EMS-Ereignis löst eine Nachricht aus, die Basisdaten aus obligatorischen, Log-Dateien, Speicher, RAID, HA, enthält. Plattform- und Netzwerk-Subsysteme sowie Daten zur Fehlerbehebung von obligatorischen, Log-Dateien und Storage-Subsystemen.

Sie möchten künftig Daten zu NFS in alle AutoSupport-Meldungen aufnehmen, die als Antwort gesendet werden `storage shelf PSU failed` Ereignis: Sie geben den folgenden Befehl ein, um die Fehlerbehebung von Daten für NFS für die zu aktivieren `callhome.shlf.ps.fault` Ereignis:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Beachten Sie, dass die `callhome.` Das Präfix wird vom gelöscht `callhome.shlf.ps.fault` Ereignis, wenn Sie das verwenden `system node autosupport trigger` Befehle, oder bei Verwendung von AutoSupport- und EMS-Ereignissen in der CLI.

Arten von AutoSupport Nachrichten und deren Inhalt

AutoSupport-Meldungen enthalten Statusinformationen zu unterstützten Subsystemen. Erfahren Sie, welche AutoSupport-Nachrichten enthalten, können Sie dabei unterstützen, Nachrichten zu interpretieren oder auf sie zu reagieren, die Sie per E-Mail oder auf der Active IQ-Website (früher unter dem Namen „My AutoSupport“ bekannt) erhalten.

Nachrichtentyp	Typ der Daten, die die Nachricht enthält
Ereignis ausgelöst	Dateien, die kontextsensitive Daten über das spezifische Subsystem enthalten, in dem das Ereignis aufgetreten ist
Täglich	Log-Dateien
Leistung	Performance-Daten, die in den letzten 24 Stunden erfasst wurden
Wöchentlich	Konfigurations- und Statusdaten
Ausgelöst durch das `system node autosupport invoke` Befehl	Hängt von dem im angegebenen Wert ab `-type` Parameter: • `test` Sendet eine vom Benutzer ausgelöste Nachricht mit einigen Basisdaten. Bei dieser Meldung wird außerdem eine automatische E-Mail-Antwort vom technischen Support auf alle angegebenen E-Mail-Adressen über das ausgelöst `-to` Option, damit Sie bestätigen können, dass die AutoSupport Meldungen empfangen werden. • `performance` Sendet Performance-Daten. • `all` Sendet eine vom Benutzer ausgelöste Nachricht mit einem vollständigen Satz von Daten, die der wöchentlichen Nachricht ähnlich sind, einschließlich der Fehlerbehebungsdaten von jedem Subsystem. Technischer Support fordert diese Meldung in der Regel an.
Ausgelöst durch das `system node autosupport invoke-core-upload` Befehl	Core Dump-Dateien für einen Node
Ausgelöst durch das `system node autosupport invoke-performance-archive` Befehl	Performance-Archivdateien für einen bestimmten Zeitraum

Nachrichtentyp	Typ der Daten, die die Nachricht enthält
Wird von AutoSupport OnDemand ausgelöst	AutoSupport OnDemand kann neue Nachrichten oder frühere Nachrichten anfordern: • Je nach Typ der AutoSupport-Sammlung können neue Meldungen lauten `test`, `all`, Oder `performance`. • Frühere Nachrichten hängen von der Art der Nachricht ab, die neu gesendet wird. AutoSupport OnDemand kann neue Meldungen anfordern, die die folgenden Dateien auf die NetApp Support Site unter hochladen "mysupport.netapp.com": • Core Dump • Performance-Archivierung

Was sind AutoSupport-Subsysteme

Jedes Subsystem enthält grundlegende und Fehlerbehebungsinformationen, die AutoSupport für seine Meldungen verwendet. Jedes Subsystem wird auch mit Triggerereignissen verbunden, sodass AutoSupport nur Informationen aus Subsystemen sammeln können, die für das Triggerereignis relevant sind.

AutoSupport erfasst kontextabhängige Inhalte. Sie können Informationen zu Subsystemen und Ereignissen über das anzeigen `system node autosupport trigger show` Befehl.

Budgets für die Größe und Zeit von AutoSupport

AutoSupport sammelt Informationen, organisiert nach Subsystem und erzwingt ein Volumen- und Zeitbudget für die Inhalte jedes Subsystems. Bei wachsendem Storage-System bieten AutoSupport-Budgets die Kontrolle über die AutoSupport-Nutzlast, wodurch wiederum die skalierbare Bereitstellung von AutoSupport Daten ermöglicht wird.

AutoSupport erfasst Informationen nicht mehr und schneidet den AutoSupport-Inhalt ab, wenn der Subsysteminhalt seine Größe oder ihr Budget überschreitet. Wenn der Inhalt nicht leicht gekürzt werden kann (z. B. Binärdateien), macht AutoSupport den Inhalt aus.

Sie sollten die Standardgröße und -Zeit nur ändern, wenn Sie dazu vom NetApp Support aufgefordert werden. Sie können auch die Standardgröße und das Zeitbudget der Subsysteme überprüfen, indem Sie die verwenden `autosupport manifest show` Befehl.

In ereignisausgelösten AutoSupport Meldungen gesendete Dateien

Ereignisgesteuerte AutoSupport Meldungen enthalten nur grundlegende und Fehlerbehebungsinformationen aus Subsystemen, die mit dem Ereignis verknüpft sind, die zum Generieren der Meldung durch AutoSupport geführt haben. Diese Daten helfen NetApp Support und Support Partnern bei der Problemlösung.

AutoSupport verwendet die folgenden Kriterien, um Inhalte in ereignisausgelösten AutoSupport Meldungen zu kontrollieren:

- Welche Subsysteme sind im Lieferumfang enthalten

  Daten werden zu Subsystemen wie allgemeinen Subsystemen wie z. B. Log-Dateien und speziellen Subsystemen wie z. B. RAID gruppiert. Jedes Ereignis löst eine Meldung aus, die nur die Daten aus spezifischen Subsystemen enthält.

- Die Detailebene jedes enthaltenen Subsystems

  Die Daten für jedes enthaltene Subsystem werden auf Basis- oder Fehlerbehebungsebene bereitgestellt.

Sie können über das alle möglichen Ereignisse anzeigen und bestimmen, welche Subsysteme in Meldungen zu jedem Ereignis enthalten sind `system node autosupport trigger show` Befehl mit dem `-instance` Parameter.

Zusätzlich zu den standardmäßig für jedes Ereignis enthaltenen Subsystemen können Sie über das zusätzliche Subsysteme auf Basis- oder Fehlerbehebungsebene hinzufügen `system node autosupport trigger modify` Befehl.

In AutoSupport-Meldungen gesendete Protokolldateien

AutoSupport Meldungen können mehrere wichtige Protokolldateien enthalten, mit denen Mitarbeiter des technischen Supports die letzten Systemaktivitäten überprüfen können.

Alle Arten von AutoSupport-Meldungen können die folgenden Protokolldateien enthalten, wenn das Subsystem Log-Dateien aktiviert ist:

Protokolldatei	Menge der Daten aus der Datei enthalten
• Log-Dateien aus dem `/mroot/etc/log/mlog/` Verzeichnis • DIE MELDUNGSPROTOKOLLDATEI	Es werden nur neue Zeilen hinzugefügt, die den Protokollen seit der letzten AutoSupport Meldung bis zu einem angegebenen Maximum hinzugefügt wurden. Dadurch wird sichergestellt, dass AutoSupport-Nachrichten über eindeutige, relevante und nicht überlappende Daten verfügen. (Log-Dateien von Partnern sind ausgenommen, für Partner sind maximal zulässige Daten enthalten.)
• Log-Dateien aus dem `/mroot/etc/log/shelflog/` Verzeichnis • Log-Dateien aus dem `/mroot/etc/log/acp/` Verzeichnis • Ereignimanagementsystem (EMS) Protokolldaten	Die letzten Datenzeilen bis zu einem festgelegten Maximum.

Der Inhalt von AutoSupport-Meldungen kann zwischen Versionen von ONTAP ändern.

In wöchentlichen AutoSupport Meldungen gesendete Dateien

Wöchentliche AutoSupport-Meldungen enthalten zusätzliche Konfigurations- und Statusdaten, die dazu dienen, Änderungen im System im Laufe der Zeit nachzuverfolgen.

Die folgenden Informationen werden in wöchentlichen AutoSupport Meldungen gesendet:

- Grundlegende Informationen über jedes Subsystem
- Inhalt der ausgewählten `/mroot/etc` Verzeichnisdateien
- Log-Dateien
- Ausgabe von Befehlen zur Angabe von Systemdaten
- Weitere Informationen, darunter Informationen zu replizierten Datenbanken (RDB), Service-Statistiken und mehr

Wie AutoSupport OnDemand Anweisungen zur Bereitstellung durch den technischen Support erhält

AutoSupport OnDemand kommuniziert regelmäßig mit dem technischen Support, um Lieferanweisungen für das Senden, erneute Senden und Ablehnen von AutoSupport Meldungen zu erhalten sowie große Dateien auf die NetApp Support Website hochzuladen. AutoSupport OnDemand ermöglicht das bedarfsgerechte Senden von AutoSupport Meldungen anstatt auf die Ausführung des wöchentlichen AutoSupport Jobs zu warten.

AutoSupport OnDemand besteht aus den folgenden Komponenten:

- AutoSupport OnDemand-Client, der auf jedem Node ausgeführt wird
- AutoSupport OnDemand Service im technischen Support

Der AutoSupport OnDemand Client fragt regelmäßig den AutoSupport OnDemand Service ab, um Anweisungen zum technischen Support zu erhalten. Beispielsweise kann der technische Support den AutoSupport OnDemand Service verwenden, um eine neue AutoSupport Meldung zu erstellen. Wenn der AutoSupport OnDemand-Client den AutoSupport OnDemand-Service abfragt, erhält der Client die Lieferanweisungen und sendet die neue AutoSupport Meldung nach Bedarf.

AutoSupport OnDemand ist standardmäßig aktiviert. AutoSupport OnDemand verlässt sich jedoch auf einige AutoSupport-Einstellungen, um die Kommunikation mit dem technischen Support fortzusetzen. AutoSupport OnDemand kommuniziert automatisch mit dem technischen Support, wenn die folgenden Anforderungen erfüllt sind:

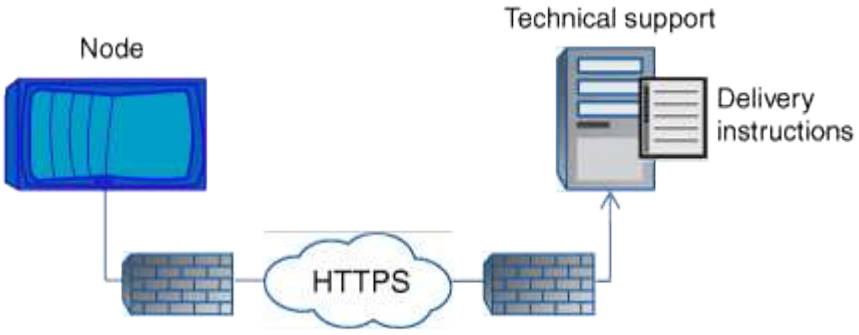
- AutoSupport ist aktiviert.
- AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
- AutoSupport ist für die Verwendung des HTTPS-Transportprotokolls konfiguriert.

Der AutoSupport OnDemand-Client sendet HTTPS-Anforderungen an denselben technischen Support-Standort, an den AutoSupport Meldungen gesendet werden. Der AutoSupport OnDemand-Client akzeptiert keine eingehenden Verbindungen.

> AutoSupport OnDemand kommuniziert über das „`AutoSupport`“ Benutzerkonto mit dem technischen Support. ONTAP verhindert, dass Sie dieses Konto löschen.

Wenn Sie AutoSupport OnDemand deaktivieren, aber AutoSupport aktiviert lassen möchten, verwenden Sie den Befehl: Link:https://docs.netapp.com/us-en/ontap-cli-95/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`].

Die folgende Abbildung zeigt, wie AutoSupport OnDemand HTTPS-Anfragen an den technischen Support sendet, um Lieferanweisungen zu erhalten.



Die Lieferanweisungen können auch Anfragen von AutoSupport zu folgenden Aufgaben enthalten:

- Generieren neuer AutoSupport Meldungen.

  Der technische Support fordert möglicherweise neue AutoSupport Meldungen zur Unterstützung der Problembehebung an.

- Generieren neuer AutoSupport Meldungen, die Core Dump-Dateien oder Performance-Archivdateien auf die NetApp Support Site hochladen.

  Der technische Support fordert möglicherweise Core Dump- oder Performance-Archivdateien an, um Probleme frühzeitig zu erkennen.

- Zuvor erzeugte AutoSupport Meldungen erneut übertragen.

  Diese Anforderung tritt automatisch ein, wenn aufgrund eines Lieferfehlers keine Meldung empfangen wurde.

- Deaktivieren der Bereitstellung von AutoSupport Meldungen für bestimmte Trigger-Ereignisse.

  Der technische Support deaktiviert möglicherweise die Bereitstellung von Daten, die nicht verwendet werden.

Struktur der per E-Mail gesendeten AutoSupport Nachrichten

Wenn eine AutoSupport-Nachricht per E-Mail gesendet wird, hat die Nachricht einen Standard-Betreff, einen kurzen Text und einen großen Anhang im 7z-Dateiformat, der die Daten enthält.

Wenn AutoSupport so konfiguriert ist, dass private Daten ausgeblendet werden, werden bestimmte Informationen, z. B. der Hostname, in der Kopfzeile, dem Betreff, dem Körper und den Anhängen weggelassen oder maskiert.

Betreff

Die vom AutoSupport-Mechanismus gesendete Betreffzeile von Nachrichten enthält eine Textzeichenfolge, die den Grund für die Benachrichtigung identifiziert. Das Format der Betreffzeile:

HA Group Notification from *System_Name* (*Message*) *Severity*

- *System_Name* ist je nach AutoSupport-Konfiguration entweder der Hostname oder die System-ID

Text

Der Text der AutoSupport-Meldung enthält die folgenden Informationen:

- Datum und Zeitstempel der Nachricht
- Die Version von ONTAP auf dem Node, der die Meldung generiert hat
- System-ID, Seriennummer und Hostname des Node, der die Meldung generiert hat
- AutoSupport-Sequenznummer
- Name und Standort des SNMP-Kontakts, falls angegeben
- System-ID und Hostname des HA Partner Node

Angehängte Dateien

Die Schlüsselinformationen in einer AutoSupport-Nachricht sind in Dateien enthalten, die in eine 7z-Datei mit dem Namen komprimiert werden `body.7z` Und an die Nachricht angehängt.

Die Dateien in dem Anhang sind spezifisch für den Typ der AutoSupport-Nachricht.

AutoSupport-Schweregrade

AutoSupport-Meldungen enthalten Typen von Schweregraden, mit denen Sie den Zweck jeder Meldung verstehen – beispielsweise das sofortige Aufzeichnen eines Notfallproblems oder nur das Bereitstellen von Informationen.

Die Nachrichten haben eine der folgenden Schweregrade:

- **Alarm**: Warnhinweise zeigen an, dass ein Ereignis der nächsten höheren Ebene auftreten kann, wenn Sie keine Aktion ergreifen.

  Sie müssen innerhalb von 24 Stunden eine Aktion für Warnmeldungen durchführen.

- **Notfall**: Notmeldungen werden angezeigt, wenn eine Störung aufgetreten ist.

  Sie müssen sofort Maßnahmen gegen Notmeldungen ergreifen.

- **Fehler**: Fehlerbedingungen geben an, was passieren könnte, wenn Sie ignorieren.
- **Hinweis**: Normaler, aber bedeutender Zustand.
- **Info**: Informationsmeldung enthält Details zum Problem, das Sie ignorieren können.
- **Debug**: Debug-Level-Meldungen enthalten Anweisungen, die Sie durchführen sollten.

Wenn Ihre interne Support-Abteilung AutoSupport-Meldungen über E-Mail erhält, wird der Schweregrad in der Betreffzeile der E-Mail-Nachricht angezeigt.

Anforderungen für die Verwendung von AutoSupport

Sie sollten HTTPS verwenden, um AutoSupport-Meldungen zu versenden, um die beste Sicherheit zu bieten und alle neuesten AutoSupport Funktionen zu unterstützen. Obwohl AutoSupport HTTP und SMTP für die Bereitstellung von AutoSupport-Meldungen unterstützt, wird HTTPS empfohlen.

Unterstützte Protokolle

Alle diese Protokolle werden auf IPv4 oder IPv6 ausgeführt, basierend auf der Adressfamilie, in die der Name auflöst.

Protokoll und Port	Beschreibung
HTTPS an Port 443	Dies ist das Standardprotokoll. Sie sollten dies wann immer möglich verwenden. Dieses Protokoll unterstützt AutoSupport OnDemand und Uploads großer Dateien. Das Zertifikat des Remote-Servers wird mit dem Stammzertifikat validiert, es sei denn, Sie deaktivieren die Validierung. Bei der Lieferung wird eine HTTP PUT-Anforderung verwendet. Bei PUT wird die Anforderung bei der Übertragung neu gestartet, wo sie angehalten wurde. Wenn der Server, der die Anfrage empfängt, PUT nicht unterstützt, verwendet die Lieferung eine HTTP-POST-Anforderung.
HTTP an Port 80	Dieses Protokoll ist über SMTP bevorzugt. Dieses Protokoll unterstützt Uploads großer Dateien, jedoch nicht AutoSupport OnDemand. Bei der Lieferung wird eine HTTP PUT-Anforderung verwendet. Bei PUT wird die Anforderung bei der Übertragung neu gestartet, wo sie angehalten wurde. Wenn der Server, der die Anfrage empfängt, PUT nicht unterstützt, verwendet die Lieferung eine HTTP-POST-Anforderung.

Protokoll und Port	Beschreibung
SMTP an Port 25 oder an einem anderen Port	Dieses Protokoll sollte nur verwendet werden, wenn die Netzwerkverbindung HTTPS oder HTTP nicht zulässt. Der standardmäßige Port-Wert ist 25, Sie können jedoch AutoSupport für einen anderen Port konfigurieren. Beachten Sie bei der Verwendung von SMTP die folgenden Einschränkungen: • AutoSupport OnDemand und Uploads großer Dateien werden nicht unterstützt. • Die Daten sind nicht verschlüsselt. SMTP sendet Daten im Klartext, sodass Text in der AutoSupport-Nachricht einfach abgefangen und gelesen werden kann. • Einschränkungen hinsichtlich der Nachrichtenlänge und der Linienlänge können eingeführt werden.

Wenn Sie AutoSupport mit bestimmten E-Mail-Adressen für Ihre interne Support-Abteilung oder eine Support-Partnerorganisation konfigurieren, werden diese Meldungen immer über SMTP gesendet.

Wenn Sie beispielsweise das empfohlene Protokoll zum Senden von Meldungen an den technischen Support verwenden und auch Meldungen an Ihre interne Support-Organisation senden möchten, werden Ihre Nachrichten sowohl über HTTPS als auch SMTP übertragen.

AutoSupport begrenzt die maximale Dateigröße für jedes Protokoll. Die Standardeinstellung für HTTP- und HTTPS-Transfers ist 25 MB. Die Standardeinstellung für SMTP-Transfers ist 5 MB. Wenn die Größe der AutoSupport-Meldung das konfigurierte Limit übersteigt, liefert AutoSupport so viel wie möglich. Sie können die maximale Größe bearbeiten, indem Sie die AutoSupport-Konfiguration ändern. Siehe `system node autosupport modify` Man-Page für weitere Informationen.

AutoSupport überschreibt automatisch die maximale Dateigröße für die HTTPS- und HTTP-Protokolle, wenn Sie AutoSupport Meldungen generieren und senden, die Core Dump- oder Performance-Archivdateien auf die NetAp Support-Website oder einen angegebenen URI hochladen. Die automatische Überschreibung gilt nur, wenn Sie Dateien mit dem hochladen `system node autosupport invoke-core-upload` Oder im `system node autosupport invoke-performance-archive` Befehle.

Konfigurationsanforderungen

Je nach Netzwerkkonfiguration erfordert die Verwendung von HTTP- oder HTTPS-Protokollen möglicherweise eine zusätzliche Konfiguration einer Proxy-URL. Wenn Sie zum Senden von AutoSupport-Meldungen über HTTP oder HTTPS an den technischen Support verwenden und einen Proxy haben, müssen Sie die URL für diesen Proxy angeben. Wenn der Proxy einen anderen Port als den Standardport verwendet, der 3128 ist, können Sie den Port für diesen Proxy angeben. Sie können auch einen Benutzernamen und ein Kennwort für die Proxy-Authentifizierung angeben.

Wenn Sie SMTP zum Senden von AutoSupport-Meldungen an Ihre interne Supportorganisation oder an den technischen Support verwenden, müssen Sie einen externen E-Mail-Server konfigurieren. Das Speichersystem kann nicht als E-Mail-Server verwendet werden. Es ist ein externer Mail-Server an Ihrem Standort erforderlich, um E-Mails zu senden. Der Mail-Server muss ein Host sein, der den SMTP-Port (25) oder einen anderen Port abhört und für das Senden und Empfangen von 8-Bit-MIME-Kodierungen (MultiPurpose Internet Mail Extensions) konfiguriert sein muss. Zu den Beispiel-Mail-Hosts gehört ein UNIX-Host, auf dem ein SMTP-Server ausgeführt wird, z. B. das sendmail-Programm, und ein Windows-Server, auf dem der Microsoft Exchange-Server ausgeführt wird. Sie können einen oder mehrere E-Mail-Hosts haben.

AutoSupport einrichten

Sie haben die Möglichkeit, zu steuern, ob und wie AutoSupport Informationen an den technischen Support und Ihre interne Support-Abteilung gesendet werden, und können anschließend testen, ob die Konfiguration richtig ist.

Über diese Aufgabe

In ONTAP 9.5 und höher können Sie AutoSupport aktivieren und seine Konfiguration auf allen Nodes des Clusters gleichzeitig ändern. Wenn ein neuer Node dem Cluster hinzugefügt wird, übernimmt der Node die AutoSupport-Cluster-Konfiguration automatisch. Sie müssen die Konfiguration auf jedem Knoten nicht separat aktualisieren.

> Ab ONTAP 9.5 wird der Umfang von `system node autosupport modify` Befehl gilt für das gesamte Cluster. Die AutoSupport-Konfiguration wird auf allen Nodes im Cluster geändert, auch wenn der `-node` Option ist angegeben. Die Option wird ignoriert, wurde aber für die Rückwärtskompatibilität mit CLI beibehalten.
>
> In ONTAP 9.4 und älteren Versionen bezieht sich der Umfang des Befehls „System Node AutoSupport modify“ speziell auf den Node. Die AutoSupport-Konfiguration sollte auf jedem Node im Cluster geändert werden.

Standardmäßig ist AutoSupport auf jedem Node aktiviert, um Meldungen mithilfe des HTTPS-Transportprotokolls an den technischen Support zu senden.

Schritte

1. Vergewissern Sie sich, dass AutoSupport aktiviert ist:

   ```
   system node autosupport modify -state enable
   ```

2. Wenn Sie technischen Support AutoSupport Meldungen erhalten möchten, verwenden Sie den folgenden Befehl:

   ```
   system node autosupport modify -support enable
   ```

   Sie müssen diese Option aktivieren, wenn Sie AutoSupport aktivieren möchten, um mit AutoSupport OnDemand zu arbeiten, oder wenn Sie große Dateien wie Core Dump- und Performance-Archivdateien auf technischen Support oder eine angegebene URL hochladen möchten.

3. Wenn der technische Support für den Empfang von AutoSupport Meldungen aktiviert ist, geben Sie an, welches Transportprotokoll für die Meldungen verwendet werden soll.

Sie können aus folgenden Optionen wählen:

Ihr Ziel ist	Stellen Sie dann die folgenden Parameter des ein `system node autosupport modify` Befehl…
Verwenden Sie das HTTPS-Standardprotokoll	a. Einstellen `-transport` Bis `https`. b. Wenn Sie einen Proxy verwenden, legen Sie fest `-proxy-url` An die URL Ihres Proxy. Diese Konfiguration unterstützt die Kommunikation mit AutoSupport OnDemand und das Hochladen großer Dateien.
Verwenden Sie HTTP, das über SMTP bevorzugt wird	a. Einstellen `-transport` Bis `http`. b. Wenn Sie einen Proxy verwenden, legen Sie fest `-proxy-url` An die URL Ihres Proxy. Diese Konfiguration unterstützt Uploads großer Dateien, jedoch nicht AutoSupport OnDemand.
Verwenden Sie SMTP	Einstellen `-transport` Bis `smtp`. Diese Konfiguration unterstützt weder AutoSupport OnDemand noch Uploads großer Dateien.

4. Wenn Sie möchten, dass Ihre interne Support-Abteilung oder ein Support-Partner AutoSupport-Meldungen erhalten, führen Sie die folgenden Aktionen durch:
   a. Identifizieren Sie die Empfänger in Ihrem Unternehmen, indem Sie die folgenden Parameter des festlegen `system node autosupport modify` Befehl:

Diesen Parameter festlegen…	Künftige Situation
`-to`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die wichtige AutoSupport-Nachrichten empfangen
`-noteto`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer internen Support-Organisation, die eine verkürzte Version von wichtigen AutoSupport-Nachrichten erhalten, die für Mobiltelefone und andere mobile Geräte entwickelt wurden
`-partner-address`	Bis zu fünf kommagetrennte einzelne E-Mail-Adressen oder Verteilerlisten in Ihrer Support-Partnerorganisation, die alle AutoSupport Meldungen erhalten

   b. Überprüfen Sie, ob die Adressen richtig konfiguriert sind, indem Sie die Ziele mithilfe des auflisten `system node autosupport destinations show` Befehl.

5. Wenn Sie Meldungen an Ihre interne Support-Organisation senden oder SMTP-Transport für Meldungen an den technischen Support gewählt haben, konfigurieren Sie SMTP, indem Sie die folgenden Parameter des festlegen `system node autosupport modify` Befehl:

   ◦ Einstellen `-mail-hosts` An einen oder mehrere E-Mail-Hosts, getrennt durch Kommas.

     Sie können maximal fünf festlegen.

   Sie können einen Portwert für jeden Mail-Host konfigurieren, indem Sie einen Doppelpunkt und eine Portnummer nach dem Namen des Mail-Hosts angeben: Z. B. `mymailhost.example.com:5678`, Wo 5678 ist der Port für den Mail-Host.

   ◦ Einstellen `-from` An die E-Mail-Adresse, die die AutoSupport-Nachricht sendet.

6. Konfigurieren Sie DNS.
7. (Optional) Hinzufügen von Befehlsoptionen, wenn Sie bestimmte Einstellungen ändern möchten:

Wenn Sie das wollen…	Stellen Sie dann die folgenden Parameter des ein `system node autosupport modify` Befehl…
Verbergen Sie private Daten, indem Sie sensible Daten in den Nachrichten entfernen, maskieren oder kodieren	Einstellen `-remove-private-data` Bis `true`. Wenn Sie von wechseln `false` Bis `true`, Alle AutoSupport-Verlauf und alle zugehörigen Dateien werden gelöscht.
Beenden Sie das Senden von Performance-Daten in regelmäßigen AutoSupport Meldungen	Einstellen `-perf` Bis `false`.

8. Überprüfen Sie die Gesamtkonfiguration mithilfe von `system node autosupport show` Befehl mit dem `-node` Parameter.
9. Überprüfen Sie den AutoSupport-Vorgang mit `system node autosupport check show` Befehl.

   Wenn Probleme gemeldet werden, verwenden Sie das `system node autosupport check show-details` Befehl zum Anzeigen weiterer Informationen.

10. Testen, ob AutoSupport Meldungen gesendet und empfangen werden:

    a. Verwenden Sie die `system node autosupport invoke` Befehl mit dem `-type` Parameter auf gesetzt `test`.

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Bestätigen Sie, dass NetApp Ihre AutoSupport Mitteilungen erhält:

       AutoSupport-Verlauf des System-Node wird -Node lokal angezeigt

    Der Status der letzten ausgehenden AutoSupport-Meldung sollte schließlich in geändert werden `sent-successful` Für alle geeigneten Protokollziele.

    a. (Optional) Bestätigen Sie, dass die AutoSupport-Nachricht an Ihre interne Support-Organisation oder

an Ihren Support-Partner gesendet wird, indem Sie die E-Mail mit einer beliebigen Adresse überprüfen, die Sie für konfiguriert haben `-to`, `-noteto`, Oder `-partner-address` Parameter des `system node autosupport modify` Befehl.

Laden Sie Core Dump-Dateien hoch

Wenn eine Core Dump-Datei gespeichert wird, wird eine Ereignismeldung generiert. Wenn der AutoSupport Service aktiviert und konfiguriert ist, um Meldungen an den NetApp Support zu senden, wird eine AutoSupport-Meldung übertragen und eine automatische E-Mail-Bestätigung an Sie gesendet.

Was Sie benötigen

- Sie müssen AutoSupport mit den folgenden Einstellungen einrichten:
  - AutoSupport ist auf dem Node aktiviert.
  - AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
  - AutoSupport ist für die Verwendung des HTTP- oder HTTPS-Transportprotokolls konfiguriert.

    Das SMTP-Transportprotokoll wird nicht unterstützt, wenn Meldungen mit großen Dateien, wie z. B. Core Dump-Dateien, gesendet werden.

Über diese Aufgabe

Sie können die Core Dump-Datei auch über den AutoSupport-Service über HTTPS hochladen, indem Sie die verwenden `system node autosupport invoke-core-upload` Befehl, falls durch den NetApp Support angefordert.

"Wie zum Hochladen einer Datei auf NetApp"

Schritte

1. Zeigen Sie die Core Dump-Dateien für einen Node an, indem Sie den verwenden `system node coredump show` Befehl.

   Im folgenden Beispiel werden Core Dump-Dateien für den lokalen Node angezeigt:

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------ -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. Generieren Sie eine AutoSupport Meldung und laden Sie mithilfe der eine Core Dump-Datei hoch `system node autosupport invoke-core-upload` Befehl.

   Im folgenden Beispiel wird eine AutoSupport Meldung generiert und an den Standardspeicherort gesendet, d. h. technischen Support. Und die Core Dump-Datei wird an den Standardspeicherort hochgeladen, der die NetApp Support Site ist:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Im folgenden Beispiel wird eine AutoSupport Meldung generiert und an den in der URI angegebenen Speicherort gesendet, und die Core Dump-Datei wird auf den URI hochgeladen:

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Archivdateien für die Performance werden hochgeladen

Sie können eine AutoSupport Nachricht generieren und senden, die ein Performance-Archiv enthält. Standardmäßig erhält der technische Support von NetApp die Meldung „AutoSupport“, und das Performance-Archiv wird auf die NetApp Support Site hochgeladen. Sie können ein anderes Ziel für die Nachricht angeben und hochladen.

Was Sie benötigen

- Sie müssen AutoSupport mit den folgenden Einstellungen einrichten:
  - AutoSupport ist auf dem Node aktiviert.
  - AutoSupport wurde konfiguriert, um Meldungen an den technischen Support zu senden.
  - AutoSupport ist für die Verwendung des HTTP- oder HTTPS-Transportprotokolls konfiguriert.

    Das SMTP-Transportprotokoll wird nicht unterstützt, wenn Meldungen mit großen Dateien, z. B. Performance-Archivdateien, gesendet werden.

Über diese Aufgabe

Sie müssen ein Startdatum für die Performance-Archivdaten angeben, die Sie hochladen möchten. Bei den meisten Storage-Systemen werden Performance-Archive für zwei Wochen aufbewahrt, wodurch Sie ein Startdatum bis vor zwei Wochen angeben können. Wenn beispielsweise heute Januar 15 ist, können Sie ein Startdatum vom 2. Januar angeben.

Schritt

1. Generieren Sie eine AutoSupport-Meldung, und laden Sie die Performance-Archivdatei mithilfe des hoch `system node autosupport invoke-performance-archive` Befehl.

   Im folgenden Beispiel werden einer AutoSupport Meldung 4 Stunden an Performance-Archivdateien vom 12. Januar 2015 hinzugefügt und an den Standardspeicherort hochgeladen, die sich auf der NetApp Support Site befindet:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   Im folgenden Beispiel werden 4 Stunden Performance-Archivdateien vom 12. Januar 2015 einer

AutoSupport-Nachricht hinzugefügt und an den von der URI angegebenen Speicherort hochgeladen:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

Informieren Sie sich über die Beschreibungen von AutoSupport Meldungen

Die Beschreibungen der AutoSupport Meldungen, die Sie erhalten, sind über den ONTAP Syslog Translator verfügbar.

Schritte

1. Wechseln Sie zum "Syslog Translator".
2. Geben Sie im Feld **Release** die Version von ONTAP ein, die Sie verwenden. Geben Sie im Feld **Suche Zeichenfolge** „Callhome“ ein. Wählen Sie **Übersetzen**.
3. Der Syslog Translator führt in alphabetischer Reihenfolge alle Ereignisse auf, die mit der eingegebenen Meldungszeichenfolge übereinstimmen.

Befehle zum Verwalten von AutoSupport

Sie verwenden das `system node autosupport` Befehle zum Ändern oder Anzeigen der AutoSupport Konfiguration, zum Anzeigen von Informationen über frühere AutoSupport Meldungen und zum Senden, Neusenden oder Abbrechen einer AutoSupport Meldung.

Konfigurieren Sie AutoSupport

Ihr Ziel ist	Befehl
Steuern, ob AutoSupport Meldungen gesendet werden	`system node autosupport modify` Mit dem `-state` Parameter
Steuern, ob AutoSupport Meldungen an den technischen Support gesendet werden	`system node autosupport modify` Mit dem `-support` Parameter
Richten Sie AutoSupport ein, oder ändern Sie die Konfiguration von AutoSupport	`system node autosupport modify`
Aktivieren und deaktivieren Sie AutoSupport Meldungen für einzelne Triggerereignisse an Ihre interne Support-Abteilung und legen Sie zusätzliche Subsystemberichte fest, die als Antwort auf einzelne Trigger-Ereignisse gesendete Meldungen enthalten	`system node autosupport trigger modify`

Zeigt Informationen zur AutoSupport-Konfiguration an

Ihr Ziel ist	Befehl
Zeigt die AutoSupport-Konfiguration an	`system node autosupport show` Mit dem `-node` Parameter
Zeigen Sie eine Zusammenfassung aller Adressen und URLs an, die AutoSupport Meldungen erhalten	`system node autosupport destinations show`
Anzeige der AutoSupport Meldungen, die an Ihre interne Support-Abteilung gesendet werden, für einzelne Auslöser	`system node autosupport trigger show`
Anzeige des Status der AutoSupport-Konfiguration sowie der Lieferung an verschiedene Ziele	`system node autosupport check show`
Anzeige des detaillierten Status der AutoSupport-Konfiguration sowie Lieferung an verschiedene Ziele	`system node autosupport check show-details`

Zeigt Informationen zu früheren AutoSupport Meldungen an

Ihr Ziel ist	Befehl
Zeigt Informationen zu mindestens einer der 50 neuesten AutoSupport Meldungen an	`system node autosupport history show`
Informationen über kürzlich generierte AutoSupport-Meldungen anzeigen, um Core Dump- oder Performance-Archivdateien auf die technische Support-Website oder einen angegebenen URI hochzuladen	`system node autosupport history show-upload-details`
Anzeigen der Informationen in den AutoSupport Meldungen, einschließlich Name und Größe der einzelnen für die Nachricht gesammelten Dateien sowie etwaiger Fehler	`system node autosupport manifest show`

Senden, erneutes Senden oder Abbrechen von AutoSupport Meldungen

Ihr Ziel ist	Befehl
Übertragen Sie eine lokal gespeicherte AutoSupport-Nachricht, die durch die AutoSupport-Sequenznummer gekennzeichnet ist, erneut Wenn Sie eine AutoSupport-Meldung erneut senden und die Unterstützung diese Meldung bereits erhalten hat, erstellt das Support-System keinen doppelten Fall. Wenn andererseits der Support diese Meldung nicht erhalten hat, analysiert das AutoSupport System die Meldung und erstellt bei Bedarf einen Case.	`system node autosupport history retransmit`
Generieren und senden Sie eine AutoSupport Message – zum Beispiel zu Testzwecken	`system node autosupport invoke` Verwenden Sie die `-force` Parameter zum Senden einer Meldung, selbst wenn AutoSupport deaktiviert ist. Verwenden Sie die `-uri` Parameter, um die Meldung an das Ziel zu senden, das Sie anstelle des konfigurierten Ziels angeben.
Abbrechen einer AutoSupport Nachricht	`system node autosupport history cancel`

Verwandte Informationen

"ONTAP 9-Befehle"

Informationen, die im AutoSupport-Manifest enthalten sind

Das AutoSupport Manifest bietet Ihnen eine detaillierte Ansicht der Dateien, die für jede AutoSupport Nachricht gesammelt wurden. Das AutoSupport-Manifest enthält auch Informationen über Erfassungsfehler, wenn AutoSupport die benötigten Dateien nicht sammeln kann.

Das AutoSupport-Manifest enthält folgende Informationen:

- Sequenznummer der AutoSupport-Meldung
- Welche Dateien AutoSupport in der AutoSupport Nachricht enthalten
- Größe jeder Datei in Byte
- Der Status der AutoSupport Manifest-Sammlung
- Fehlerbeschreibung, falls AutoSupport eine oder mehrere Dateien nicht sammeln konnte

Sie können das AutoSupport-Manifest mit dem anzeigen `system node autosupport manifest show` Befehl.

Das AutoSupport-Manifest ist in jeder AutoSupport-Nachricht enthalten und im XML-Format dargestellt, was bedeutet, dass Sie entweder einen generischen XML-Viewer zum Lesen verwenden oder es mit dem Active IQ-Portal (früher bekannt als My AutoSupport) anzeigen können.

Unterdrückung von AutoSupport-Cases während geplanter Wartungszeiten

Durch die AutoSupport-Fallunterdrückung können Sie verhindern, dass unnötige Fälle durch AutoSupport Meldungen erstellt werden, die während eines geplanten Wartungsfensters ausgelöst werden.

Um AutoSupport-Fälle zu unterdrücken, müssen Sie eine AutoSupport-Nachricht manuell mit einer speziell formatierten Textzeichenfolge aufrufen: `MAINT=xh`. `x` Ist die Dauer des Wartungsfensters in Stundeneinheiten.

Verwandte Informationen

"Wie kann die automatische Case-Erstellung während geplanter Wartungszeiträume unterdrückt werden"

Fehler bei AutoSupport

Beheben Sie AutoSupport, wenn keine Meldungen empfangen werden

Wenn das System die AutoSupport Meldung nicht sendet, können Sie bestimmen, ob das der Fall ist, weil AutoSupport die Meldung nicht generieren kann oder die Meldung nicht liefern kann.

Schritte

1. Überprüfen Sie den Zustellungsstatus der Meldungen mithilfe der `system node autosupport history show` Befehl.
2. Lesen Sie den Status.

Diesem Status	Bedeutet
Initialisierung	Der Erfassungsprozess wird gestartet. Wenn dieser Zustand vorübergehend ist, ist alles gut. Wenn dieser Status jedoch weiterhin besteht, gibt es ein Problem.
Sammlung fehlgeschlagen	AutoSupport kann den AutoSupport-Inhalt im Spool-Verzeichnis nicht erstellen. Sie können anzeigen, was AutoSupport zu erfassen versucht, indem Sie die eingeben `system node autosupport history show -detail` Befehl.
Inkassovorgang läuft	AutoSupport sammelt AutoSupport-Inhalte. Sie können anzeigen, was AutoSupport erfasst, indem Sie die eingeben `system node autosupport manifest show` Befehl.
Warteschlange	AutoSupport Nachrichten werden für die Lieferung in die Warteschlange eingereiht, aber noch nicht geliefert.
Übertragung	AutoSupport stellt derzeit Meldungen aus.

Diesem Status	Bedeutet
Gesendet-erfolgreich	AutoSupport hat die Meldung erfolgreich übermittelt. Finden Sie heraus, an welchen Stellen AutoSupport die Nachricht geliefert hat, indem Sie den eingeben `system node autosupport history show -delivery` Befehl.
Ignorieren	AutoSupport verfügt über keine Ziele für die Meldung. Sie können die Lieferdetails anzeigen, indem Sie die eingeben `system node autosupport history show -delivery` Befehl.
Erneut in Warteschlange gestellt	AutoSupport hat versucht, Nachrichten zu senden, aber der Versuch ist fehlgeschlagen. Infolgedessen wurden die Nachrichten von AutoSupport wieder in die Ausgabewarteschlange für einen anderen Versuch platziert. Sie können den Fehler anzeigen, indem Sie die eingeben `system node autosupport history show` Befehl.
Übertragung fehlgeschlagen	AutoSupport konnte die Nachricht nicht mit der angegebenen Anzahl von Zeiten senden und hörte nicht auf, die Nachricht zu liefern. Sie können den Fehler anzeigen, indem Sie die eingeben `system node autosupport history show` Befehl.
ondemand-Ignorieren	Die AutoSupport Meldung wurde erfolgreich verarbeitet, aber der AutoSupport OnDemand Dienst wählte, um sie zu ignorieren.

3. Führen Sie eine der folgenden Aktionen aus:

Für diesen Status	Tun Sie das
Initialisierung oder Sammlung fehlgeschlagen	Wenden Sie sich an den NetApp Support, da AutoSupport die Nachricht nicht generieren kann. Erwähnen Sie den folgenden Knowledge Base-Artikel: "AutoSupport kann nicht liefern: Der Status befindet sich in Initialisierung"
Ignorieren, erneute Warteschlange oder Übertragung fehlgeschlagen	Überprüfen Sie, ob die Ziele für SMTP, HTTP oder HTTPS richtig konfiguriert sind, da AutoSupport die Meldung nicht senden kann.

Fehlerbehebung bei der Bereitstellung von AutoSupport Meldungen über HTTP oder HTTPS

Wenn das System die erwartete AutoSupport-Meldung nicht sendet und Sie HTTP oder HTTPS verwenden oder die Funktion zum automatischen Aktualisieren nicht funktioniert, können Sie eine Reihe von Einstellungen überprüfen, um das Problem zu beheben.

Was Sie benötigen

Sie sollten die grundlegende Netzwerkverbindung und das DNS-Lookup bestätigt haben:

- Die Node-Management-LIF muss den Status „Betriebs“ und „Administration“ aufweisen.
- Sie müssen in der Lage sein, einen funktionierenden Host in demselben Subnetz von der Cluster-Management-LIF zu pingen (keine LIF auf keinem der Nodes).
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF zu pingen.
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF mit dem Namen des Hosts (nicht die IP-Adresse) anzupingen.

Über diese Aufgabe

Diese Schritte sind für Fälle, in denen Sie festgestellt haben, dass AutoSupport die Meldung generieren kann, die Meldung jedoch nicht über HTTP oder HTTPS übermitteln kann.

Wenn bei diesem Vorgang Fehler auftreten oder ein Schritt nicht ausgeführt werden kann, ermitteln und beheben Sie das Problem, bevor Sie mit dem nächsten Schritt fortfahren.

Schritte

1. Anzeigen des detaillierten Status des AutoSupport-Subsystems:

   ```
   system node autosupport check show-details
   ```

   Dazu gehört auch die Überprüfung der Verbindung zu AutoSupport Zielen durch Senden von Testmeldungen und Bereitstellen einer Liste möglicher Fehler in Ihren AutoSupport Konfigurationseinstellungen.

2. Überprüfen Sie den Status der Node-Management-LIF:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   Der `status-oper` Und `status-admin` Felder sollten „`up`“ zurückgeben.

3. Notieren Sie den SVM-Namen, den LIF-Namen und die LIF-IP-Adresse für die spätere Verwendung.
4. Stellen Sie sicher, dass DNS richtig aktiviert und konfiguriert ist:

   ```
   vserver services name-service dns show
   ```

5. Beheben Sie alle Fehler, die von der AutoSupport Meldung zurückgegeben werden:

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   Informationen zur Fehlerbehebung bei zurückgegebenen Fehlern finden Sie im "ONTAP AutoSupport (Transport HTTPS und HTTP) Auflösungsleitfaden".

6. Vergewissern Sie sich, dass das Cluster sowohl auf die Server zugreifen kann, die es benötigt, als auch auf das Internet:

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

Die Adresse `support.netapp.com` Selbst reagiert nicht auf Ping/Traceroute, aber die Informationen pro Hop sind wertvoll.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

Wenn eine dieser Routen nicht funktioniert, versuchen Sie die gleiche Route von einem funktionierenden Host im selben Subnetz wie das Cluster, indem Sie das Dienstprogramm „`traceroute`“ oder „`tracert`“ verwenden, das auf den meisten Netzwerk-Clients von Drittanbietern gefunden wurde. Dadurch können Sie herausfinden, ob das Problem in Ihrer Netzwerkkonfiguration oder der Cluster-Konfiguration vorliegt.

7. Wenn Sie HTTPS für Ihr AutoSupport-Transportprotokoll verwenden, stellen Sie sicher, dass HTTPS-Datenverkehr das Netzwerk beenden kann:

   a. Konfigurieren Sie einen Web-Client im gleichen Subnetz wie die Cluster-Management-LIF.

      Stellen Sie sicher, dass alle Konfigurationsparameter dieselben Werte wie für die AutoSupport-Konfiguration sind, einschließlich der Verwendung desselben Proxy-Servers, Benutzernamens, Passworts und Ports.

   b. Datenzugriff `https://support.netapp.com` Mit dem Web-Client.

      Der Zugriff sollte erfolgreich sein. Wenn nicht, stellen Sie sicher, dass alle Firewalls richtig konfiguriert sind, um HTTPS- und DNS-Datenverkehr zu ermöglichen, und dass der Proxy-Server korrekt konfiguriert ist. Weitere Informationen zum Konfigurieren der statischen Namensauflösung für support.netapp.com finden Sie im Knowledge Base-Artikel "Wie würde ein HOST-Eintrag in ONTAP für support.netapp.com? hinzugefügt werden"

8. Wenn Sie mit ONTAP 9.10.1 die Funktion Automatische Aktualisierung aktiviert haben, stellen Sie sicher, dass Sie über eine HTTPS-Verbindung zu den folgenden zusätzlichen URLs verfügen:
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

Fehlerbehebung bei der AutoSupport Nachrichtenübermittlung über SMTP

Wenn das System keine AutoSupport Meldungen über SMTP liefern kann, können Sie eine Reihe von Einstellungen überprüfen, um das Problem zu lösen.

Was Sie benötigen

Sie sollten die grundlegende Netzwerkverbindung und das DNS-Lookup bestätigt haben:

- Die Node-Management-LIF muss den Status „Betriebs“ und „Administration“ aufweisen.
- Sie müssen in der Lage sein, einen funktionierenden Host in demselben Subnetz von der Cluster-Management-LIF zu pingen (keine LIF auf keinem der Nodes).
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF zu pingen.
- Sie müssen in der Lage sein, einen funktionierenden Host außerhalb des Subnetzes von der Cluster-Management-LIF mit dem Namen des Hosts (nicht die IP-Adresse) anzupingen.

Über diese Aufgabe

Diese Schritte sind für Fälle, in denen Sie festgestellt haben, dass AutoSupport die Meldung generieren kann, die Meldung jedoch nicht über SMTP liefern kann.

Wenn bei diesem Vorgang Fehler auftreten oder ein Schritt nicht ausgeführt werden kann, ermitteln und beheben Sie das Problem, bevor Sie mit dem nächsten Schritt fortfahren.

Sofern nicht anders angegeben, werden alle Befehle über die ONTAP-Befehlszeilenschnittstelle eingegeben.

Schritte

1. Überprüfen Sie den Status der Node-Management-LIF:

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   Der `status-oper` Und `status-admin` Die Felder sollten zurückgegeben werden `up`.

2. Notieren Sie den SVM-Namen, den LIF-Namen und die LIF-IP-Adresse für die spätere Verwendung.
3. Stellen Sie sicher, dass DNS richtig aktiviert und konfiguriert ist:

   vserver services name-service dns show

4. Alle Server anzeigen, die für die Verwendung durch AutoSupport konfiguriert sind:

   system node autosupport show -fields mail-hosts

   Notieren Sie alle angezeigten Servernamen.

5. Für jeden Server, der im vorherigen Schritt angezeigt wird, und `support.netapp.com`, Stellen Sie sicher, dass der Server oder die URL durch den Knoten erreicht werden kann:

   network traceroute -node local -destination *server_name*

   Wenn eine dieser Routen nicht funktioniert, versuchen Sie die gleiche Route von einem funktionierenden Host im selben Subnetz wie das Cluster, indem Sie das Dienstprogramm „`traceroute`“ oder „`tracert`“ verwenden, das auf den meisten Netzwerk-Clients von Drittanbietern gefunden wurde. Dadurch können Sie herausfinden, ob das Problem in Ihrer Netzwerkkonfiguration oder der Cluster-Konfiguration vorliegt.

6. Melden Sie sich beim Host an, der als E-Mail-Host bezeichnet wird, und stellen Sie sicher, dass er SMTP-Anforderungen bereitstellen kann:

   netstat -aAn|grep 25

   `25` Ist die SMTP-Port-Nummer des Listeners.

   Es wird eine Meldung wie der folgende Text angezeigt:

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. Öffnen Sie von einem anderen Host eine Telnet-Sitzung mit dem SMTP-Port des Mail-Hosts:

   telnet *mailhost* 25

Es wird eine Meldung wie der folgende Text angezeigt:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. Stellen Sie an der Eingabeaufforderung Telnet sicher, dass eine Nachricht von Ihrem Mail-Host weitergeleitet werden kann:

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` Ist der Domain-Name Ihres Netzwerks.

   Wenn ein Fehler zurückgegeben wird, der besagt, dass das Relying verweigert wird, ist das Relying auf dem Mail-Host nicht aktiviert. Wenden Sie sich an Ihren Systemadministrator.

9. Senden Sie an der Eingabeaufforderung Telnet eine Testmeldung:

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   Stellen Sie sicher, dass Sie den letzten Zeitraum (.) in einer Zeile selbst eingeben. Der Zeitraum gibt dem Mail-Host an, dass die Nachricht abgeschlossen ist.

   Wenn ein Fehler zurückgegeben wird, ist Ihr Mail-Host nicht richtig konfiguriert. Wenden Sie sich an Ihren Systemadministrator.

10. Senden Sie über die ONTAP Befehlszeilenschnittstelle eine AutoSupport-Testmeldung an eine vertrauenswürdige E-Mail-Adresse, auf die Sie Zugriff haben:

    system node autosupport invoke -node local -type test

11. Suchen Sie die Sequenznummer des Versuchs:

    system node autosupport history show -node local -destination smtp

    Suchen Sie die Sequenznummer Ihres Versuchs basierend auf dem Zeitstempel. Es ist wahrscheinlich der jüngste Versuch.

12. Zeigen Sie den Fehler für den Versuch der Testmeldung an:

    system node autosupport history show -node local -seq-num seq_num -fields error

    Wenn der Fehler angezeigt wird `Login denied`, Ihr SMTP-Server akzeptiert keine Anfragen von der

Cluster-Management-LIF. Wenn Sie als Transportprotokoll nicht zu HTTPS wechseln möchten, wenden Sie sich an den Standortnetzwerkadministrator, um die SMTP-Gateways zu konfigurieren, um dieses Problem zu beheben.

Wenn dieser Test erfolgreich ist, aber dieselbe Nachricht an mailto:autosupport@netapp.com nicht gesendet wird, stellen Sie sicher, dass SMTP-Relais auf allen Ihren SMTP-Mail-Hosts aktiviert ist, oder verwenden Sie HTTPS als Transportprotokoll.

Wenn auch die Meldung an das lokal verwaltete E-Mail-Konto nicht erfolgreich ist, bestätigen Sie, dass Ihre SMTP-Server so konfiguriert sind, dass Anlagen mit beiden folgenden Eigenschaften weitergeleitet werden:

- Das Suffix „`7z`“
- Der Typ „`Application/x-7x-compressed`“ MIME.

Fehler beim AutoSupport-Subsystem

Der `system node check show` Mit diesen Befehlen können Probleme hinsichtlich der AutoSupport-Konfiguration und -Bereitstellung überprüft und behoben werden.

Schritt

1. Zeigen Sie mit den folgenden Befehlen den Status des AutoSupport-Subsystems an.

Befehl	Hier…
`system node autosupport check show`	Zeigt den Gesamtstatus des AutoSupport-Subsystems an, z. B. den Status von AutoSupport HTTP- oder HTTPS-Ziel, AutoSupport SMTP-Ziele, AutoSupport OnDemand Server und AutoSupport-Konfiguration
`system node autosupport check show-details`	Anzeige des detaillierten Status des AutoSupport-Subsystems, z. B. detaillierte Beschreibungen der Fehler und der Korrekturmaßnahmen

Überwachen Sie den Systemzustand Ihres Systems

Überwachen Sie den Systemzustand Ihrer Systemübersicht

Zustandsüberwachung überwachen proaktiv bestimmte kritische Bedingungen in Ihrem Cluster und Warnmeldungen, wenn ein Fehler oder Risiko erkannt wird, aus. Wenn aktive Meldungen vorliegen, wird der Systemzustand den Status des Systems für das Cluster mit einem Status „beeinträchtigt“ angezeigt. Die Meldungen enthalten die Informationen, die Sie benötigen, um auf den beeinträchtigten Systemzustand zu reagieren.

Wenn der Status „beeinträchtigt“ lautet, können Sie Details zum Problem anzeigen, einschließlich der wahrscheinlichen Ursache und der empfohlenen Wiederherstellungsmaßnahmen. Nachdem Sie das Problem behoben haben, kehrt der Systemzustand automatisch zu OK zurück.

Der Systemzustand gibt mehrere separate Integritätsmonitore wieder. Ein Status „beeinträchtigt“ in einer

einzelnen Systemzustandsüberwachung bewirkt einen Status „beeinträchtigt“ für den gesamten Systemzustand.

Details dazu, wie ONTAP Cluster Switches für die Überwachung des Systemzustands im Cluster unterstützt, finden Sie unter *Hardware Universe*.

"Unterstützte Switches im Hardware Universe"

Einzelheiten zu den Ursachen von AutoSupport-Meldungen (Cluster Switch Health Monitor, CSHM) und den zur Behebung dieser Warnmeldungen erforderlichen Maßnahmen finden Sie im Knowledgebase Artikel.

"AutoSupport Meldung: Health Monitor Prozess CSHM"

Funktionsweise der Statusüberwachung

Individuelle Systemzustandsüberwachung verfügen über eine Reihe von Richtlinien, die Warnungen auslösen, wenn bestimmte Bedingungen auftreten. Wenn Sie verstehen, wie das Statusüberwachung funktioniert, können Sie auf Probleme reagieren und zukünftige Warnmeldungen steuern.

Die Statusüberwachung besteht aus den folgenden Komponenten:

- Individuelle Gesundheitsmonitore für bestimmte Subsysteme, von denen jeder seinen eigenen Gesundheitszustand hat

  Beispielsweise verfügt das Storage-Subsystem über eine Systemzustandsüberwachung für die Node-Konnektivität.

- Eine allgemeine Systemzustandsüberwachung, die den Systemzustand der einzelnen Systemzustandsüberwachung konsolidiert

  Ein Status „beeinträchtigt“ in einem einzelnen Subsystem führt zu einem Status „beeinträchtigt“ für das gesamte System. Wenn keine Subsysteme Warnmeldungen enthalten, ist der gesamte Systemstatus OK.

Jede Systemzustandsüberwachung setzt sich aus den folgenden wichtigen Elementen zurück:

- Meldungen, die von der Systemzustandsüberwachung potenziell angehoben werden können

  Jede Meldung hat eine Definition, die Details wie den Schweregrad der Warnmeldung und die wahrscheinliche Ursache enthält.

- Integritätsrichtlinien, die festlegen, wann jede Meldung ausgelöst wird

  Jede Systemzustandsüberwachung verfügt über einen Regelausdruck. Dies ist die genaue Bedingung oder Änderung, durch die die Meldung ausgelöst wird.

Eine Systemzustandsüberwachung überwacht kontinuierlich die Ressourcen in ihrem Subsystem auf ihre Zustandsänderungen. Wenn eine Änderung einer Bedingung oder eines Status mit einem Regelausdruck in einer Systemzustandsüberwachung übereinstimmt, erhöht die Systemzustandsüberwachung eine Meldung. Eine Meldung bewirkt, dass der Systemzustand des Subsystems und der gesamte Systemzustand beeinträchtigt werden.

Möglichkeiten zur Reaktion auf Systemzustandsmeldungen

Wenn eine Systemzustandsmeldung auftritt, können Sie sie bestätigen, mehr darüber erfahren, den zugrunde liegenden Zustand reparieren und verhindern, dass er erneut auftritt.

Wenn eine Systemzustandsüberwachung eine Meldung aufwirft, können Sie auf folgende Arten reagieren:

- Informieren Sie sich über die Meldung, zu der die betroffene Ressource, der Schweregrad der Warnmeldung, die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen gehören.
- Detaillierte Informationen über die Warnmeldung, z. B. den Zeitpunkt, zu dem die Warnmeldung ausgegeben wurde und ob jemand anderer die Warnmeldung bereits bestätigt hat.
- Abrufen von Systemzustandsinformationen zum Status der betroffenen Ressource oder Subsysteme, z. B. ein bestimmtes Shelf oder eine bestimmte Festplatte
- Bestätigen Sie den Alarm, um anzuzeigen, dass jemand an dem Problem arbeitet und identifizieren Sie sich als „`Danker`“.
- Beheben Sie das Problem, indem Sie die in der Warnmeldung angegebenen Korrekturmaßnahmen ergreifen, z. B. Kabelbefestigung zur Behebung eines Verbindungsproblems.
- Löschen Sie die Meldung, wenn sie vom System nicht automatisch gelöscht wurde.
- Unterdrücken einer Meldung, um zu verhindern, dass sie den Integritätsstatus eines Subsystems beeinflusst.

  Das Unterdrücken ist nützlich, wenn Sie ein Problem verstehen. Nachdem Sie eine Meldung unterdrückt haben, kann sie weiterhin auftreten, der Systemzustand des Subsystems wird jedoch als „`ok-with-unterdrückung`“ angezeigt, wenn die unterdrückte Meldung auftritt.

Anpassung der Systemzustandsmeldung

Sie können steuern, welche Meldungen eine Systemzustandsüberwachung generiert, indem Sie die Systemintegritätsrichtlinien aktivieren und deaktivieren, die definieren, wann Meldungen ausgelöst werden. So können Sie das System zur Statusüberwachung für Ihre spezifische Umgebung anpassen.

Sie können den Namen einer Richtlinie erlernen, indem Sie ausführliche Informationen über eine generierte Meldung anzeigen oder Richtliniendefinitionen für eine bestimmte Systemzustandsüberwachung, Node oder Alarm-ID anzeigen.

Das Deaktivieren von Integritätsrichtlinien unterscheidet sich vom Unterdrücken von Meldungen. Wenn Sie eine Meldung unterdrücken, hat dies keine Auswirkung auf den Systemzustand des Subsystems, aber die Meldung kann immer noch auftreten.

Wenn Sie eine Richtlinie deaktivieren, löst die im Richtlinienausdruck definierte Bedingung oder der Status keine Meldung mehr aus.

Beispiel für eine Meldung, die Sie deaktivieren möchten

Angenommen, eine Meldung tritt auf, die für Sie nicht hilfreich ist. Sie verwenden das `system health alert show –instance` Befehl zum Abrufen der Richtlinien-ID für die Meldung. Sie verwenden die Richtlinien-ID im `system health policy definition show` Befehl zum Anzeigen von Informationen zur Richtlinie. Nachdem Sie den Regelausdruck und andere Informationen über die Richtlinie geprüft haben,

entscheiden Sie, die Richtlinie zu deaktivieren. Sie verwenden das `system health policy definition modify` Befehl zum Deaktivieren der Richtlinie

Wie Systemzustandsmeldungen AutoSupport Meldungen und Ereignisse auslösen

Systemzustandsmeldungen lösen AutoSupport-Meldungen und Ereignisse im Event Management System (EMS) aus, so dass Sie den Systemzustand mithilfe von AutoSupport-Meldungen und dem EMS sowie die direkte Verwendung des Integritätsüberwachungssystems überwachen können.

Das System sendet eine AutoSupport Meldung innerhalb von fünf Minuten nach einer Meldung. Die AutoSupport Meldung enthält alle seit der letzten AutoSupport Meldung generierten Warnmeldungen, mit Ausnahme von Warnungen, die eine Meldung für dieselbe Ressource und wahrscheinliche Ursache innerhalb der vorherigen Woche duplizieren.

Einige Meldungen lösen keine AutoSupport-Meldungen aus. Eine Meldung löst keine AutoSupport Meldung aus, wenn ihre Integritätsrichtlinie das Senden von AutoSupport Meldungen deaktiviert. Beispielsweise kann eine Systemzustandsüberwachung standardmäßig AutoSupport Meldungen deaktivieren, da AutoSupport bereits eine Meldung generiert, wenn das Problem auftritt. Sie können Richtlinien so konfigurieren, dass AutoSupport-Meldungen nicht mit dem ausgelöst werden `system health policy definition modify` Befehl.

Sie können eine Liste aller AutoSupport Meldungen, die in der vorherigen Woche über die gesendet wurden, anzeigen `system health autosupport trigger history show` Befehl.

Warnmeldungen auslösen außerdem die Generierung von Ereignissen an das EMS. Jedes Mal, wenn eine Meldung erstellt wird, wird ein Ereignis generiert, wenn eine Meldung gelöscht wird.

Verfügbare Cluster-Zustandsmonitore

Verschiedene Systemzustandsüberwachung überwachen verschiedene Teile eines Clusters. Die Zustandsüberwachung unterstützen Sie bei der Wiederherstellung nach Fehlern in ONTAP Systemen. Dazu werden Ereignisse erkannt, Warnmeldungen an Sie gesendet und Ereignisse gelöscht, sobald sie gelöscht werden.

Name der Systemzustandsüberwachung (Kennung)	Subsystemname (Kennung)	Zweck
Cluster-Switch (Cluster-Switch)	Switch (Switch-Health)	Überwacht Cluster-Netzwerk-Switches und Management-Netzwerk-Switches auf Temperatur, Auslastung, Schnittstellenkonfiguration, Redundanz (nur Cluster-Netzwerk-Switches) sowie Lüfter- und Netzteilbetrieb. Die Cluster-Switch-Systemzustandsüberwachung kommuniziert mit Switches über SNMP. SNMPv2c ist die Standardeinstellung. Ab ONTAP 9.2 kann dieser Monitor erkennen und melden, wenn ein Cluster-Switch seit der letzten Abrufzeit neu gestartet wurde.
MetroCluster Fabric	Switch	Überwacht die Back-End-Fabric-Topologie der MetroCluster Konfiguration und erkennt Fehlkonfigurationen wie falsche Verkabelung und Zoning oder ISL-Ausfälle.
Systemzustand von MetroCluster	Interconnect, RAID und Storage	Überwacht FC-VI-Adapter, FC Initiator-Adapter, Aggregate und Festplatten im Hintergrund sowie Cluster-Ports
Node-Konnektivität (Node-Connect)	Unterbrechungsfreier CIFS-Betrieb (CIFS-NDO)	Überwachung von SMB-Verbindungen für unterbrechungsfreien Betrieb von Hyper-V Applikationen
Storage (SAS-Connect)	Überwacht Shelfs, Festplatten und Adapter auf Node-Ebene für entsprechende Pfade und Verbindungen.	System
Keine Angabe	Fasst Informationen aus anderen Zustandsmonitoren zusammen.	Systemkonnektivität (System-connect)

Automatisches Empfangen von SystemSystemzustandsmeldungen

Sie können Systemzustandsmeldungen manuell mit der anzeigen `system health alert show` Befehl. Sie sollten jedoch bestimmte EMS-Meldungen (Event Management System) abonnieren, um Benachrichtigungen automatisch zu erhalten, wenn eine Systemzustandsüberwachung eine Meldung generiert.

Über diese Aufgabe

Das folgende Verfahren zeigt Ihnen, wie Sie Benachrichtigungen für alle hm.alert.alert.hopped Nachrichten und alle hm.alert.cleaned Nachrichten einrichten.

Alle hm.alert.alered Nachrichten und alle hm.alert.cleaned Nachrichten enthalten einen SNMP-Trap. Die Namen der SNMP-Traps sind `HealthMonitorAlertRaised` Und `HealthMonitorAlertCleared`. Informationen zu SNMP-Traps finden Sie im *Network Management Guide*.

Schritte

1. Verwenden Sie die `event destination create` Befehl zum Festlegen des Ziels, an das Sie die EMS-Nachrichten senden möchten.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Verwenden Sie die `event route add-destinations` Befehl zum Umleiten des `hm.alert.raised` Botschaft und der `hm.alert.cleared` Nachricht an ein Ziel senden.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Verwandte Informationen

"Netzwerkmanagement"

Reagieren Sie auf den eingeschränkten Systemzustand

Wenn der Systemzustand des Systems beeinträchtigt ist, können Sie Meldungen anzeigen, die wahrscheinliche Ursache und die möglichen Korrekturmaßnahmen lesen, Informationen zum beeinträchtigten Subsystem anzeigen und das Problem lösen. Unterdrückte Warnungen werden ebenfalls angezeigt, damit Sie sie ändern und sehen können, ob sie bestätigt wurden.

Über diese Aufgabe

Sie können feststellen, dass eine Meldung durch die Anzeige einer AutoSupport Meldung, eines EMS-Ereignisses oder mithilfe des generiert wurde `system health` Befehle.

Schritte

1. Verwenden Sie die `system health alert show` Befehl zum Anzeigen der Meldungen, die den Systemzustand beeinträchtigen.

2. Lesen Sie die wahrscheinliche Ursache, die mögliche Auswirkung und die Korrekturmaßnahmen der Meldung, um zu ermitteln, ob Sie das Problem beheben oder weitere Informationen benötigen.
3. Wenn Sie weitere Informationen benötigen, verwenden Sie das `system health alert show -instance` Befehl zum Anzeigen weiterer Informationen, die für die Meldung verfügbar sind.
4. Verwenden Sie die `system health alert modify` Befehl mit dem `-acknowledge` Parameter, um anzugeben, dass Sie an einer bestimmten Warnmeldung arbeiten.
5. Führen Sie Korrekturmaßnahmen durch, um das Problem zu lösen, wie im beschrieben `Corrective Actions` Feld in der Meldung.

   Die Korrekturmaßnahmen können ein Neubooten des Systems umfassen.

   Nach Behebung des Problems wird die Meldung automatisch behoben. Wenn das Subsystem keine weiteren Warnmeldungen aufweist, ändert sich der Systemzustand des Subsystems in `OK`. Wenn der Systemzustand aller Subsysteme in Ordnung ist, ändert sich der Gesamtzustand des Systems in `OK`.

6. Verwenden Sie die `system health status show` Befehl zur Bestätigung, dass der Systemzustand lautet `OK`.

   Wenn der Systemstatus nicht lautet `OK`, Wiederholen Sie dieses Verfahren.

Beispiel der Reaktion auf den eingeschränkten Systemzustand

Durch Überprüfung eines bestimmten Beispiels des beeinträchtigten Systemzustands, der durch ein Shelf verursacht wurde, in dem zwei Pfade zu einem Node fehlen, werden Sie sehen, was die CLI zeigt, wenn Sie auf eine Meldung antworten.

Nach dem Starten von ONTAP überprüfen Sie den Systemzustand, und Sie stellen fest, dass der Status „beeinträchtigt“ lautet:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Sie zeigen die Meldungen an, um herauszufinden, wo das Problem ist, und sehen, dass Shelf 2 keine zwei Pfade zu node1 hat:

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

Sie zeigen Details über die Meldung an, um weitere Informationen zu erhalten, einschließlich der Warn-ID:

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

Sie bestätigen die Meldung, dass Sie daran arbeiten.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Sie reparieren die Verkabelung zwischen Shelf 2 und node1 und booten das System dann neu. Anschließend überprüfen Sie den Systemzustand wieder und sehen, dass der Status lautet `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Konfigurieren der Erkennung von Cluster- und Management-Netzwerk-Switches

Die Cluster-Switch-Systemzustandsüberwachung versucht automatisch, die Cluster- und Management-Netzwerk-Switches mithilfe des Cisco Discovery Protocol (CDP) zu erkennen. Sie müssen die Systemzustandsüberwachung konfigurieren, wenn ein Switch nicht automatisch erkannt werden kann oder wenn Sie nicht für die automatische Erkennung CDP verwenden möchten.

Über diese Aufgabe

Der `system cluster-switch show` Mit dem Befehl werden die Switches aufgeführt, die die Systemzustandsüberwachung erkannt hat. Wenn für Sie keinen Schalter in der Liste angezeigt wird, kann die Systemzustandsüberwachung ihn nicht automatisch erkennen.

Schritte

1. Wenn Sie CDP für die automatische Erkennung verwenden möchten, gehen Sie wie folgt vor:

   a. Stellen Sie sicher, dass das Cisco Discovery Protocol (CDP) auf Ihren Switches aktiviert ist.

      Anweisungen hierzu finden Sie in der Switch-Dokumentation.

   b. Führen Sie für jeden Knoten im Cluster den folgenden Befehl aus, um zu überprüfen, ob CDP aktiviert oder deaktiviert ist:

      `run -node *node_name* -command options cdpd.enable`

      Wenn CDP aktiviert ist, fahren Sie mit Schritt d. fort Wenn CDP deaktiviert ist, mit Schritt c fortfahren

   c. Führen Sie den folgenden Befehl aus, um CDP zu aktivieren:

      `run -node *node_name* -command options cdpd.enable on`

   Warten Sie fünf Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

   a. Verwenden Sie die `system cluster-switch show` Befehl zum Überprüfen, ob ONTAP die Switches jetzt automatisch erkennen kann.

2. Wenn die Systemzustandsüberwachung keinen Switch automatisch erkennt, verwenden Sie den `system cluster-switch create` Befehl zum Konfigurieren der Erkennung des Switches:

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Warten Sie fünf Minuten, bevor Sie mit dem nächsten Schritt fortfahren.

3. Verwenden Sie die `system cluster-switch show` Befehl um zu überprüfen, ob ONTAP den Switch erkennen kann, für den Sie Informationen hinzugefügt haben.

Nachdem Sie fertig sind

Überprüfen Sie, ob die Systemzustandsüberwachung Ihre Switches überwachen kann.

Überprüfen Sie die Überwachung von Cluster- und Managementnetzwerk-Switches

Die Cluster-Switch-Systemzustandsüberwachung versucht automatisch, die Switches zu überwachen, die sie erkannt haben. Die Überwachung erfolgt jedoch möglicherweise nicht automatisch, wenn die Switches nicht richtig konfiguriert sind. Sie sollten überprüfen, ob die Systemzustandsüberwachung ordnungsgemäß für das Monitoring Ihrer Switches konfiguriert ist.

Schritte

1. Geben Sie den folgenden Befehl ein, um die Switches zu identifizieren, die die Systemzustandsüberwachung des Cluster-Switch erkannt haben:

   ONTAP 9.8 und höher

   ```
   system switch ethernet show
   ```

   ONTAP 9.7 und früher

   ```
   system cluster-switch show
   ```

   Wenn der `Model` Spalte zeigt den Wert an `OTHER`, Dann kann ONTAP den Schalter nicht überwachen. ONTAP setzt den Wert auf `OTHER` Wenn ein automatisch erkannte Switch nicht für das Monitoring des Systemzustands unterstützt wird.

   ⓘ Wenn in der Befehlsausgabe des Befehls kein Switch angezeigt wird, müssen Sie die Erkennung des Switches konfigurieren.

2. Führen Sie ein Upgrade auf die neueste unterstützte Switch-Software durch, und verwenden Sie die Konfigurationsdatei (RCF) von der NetApp Support Site.

   "NetApp Support Downloads Seite"

   Die Community-Zeichenfolge in der RCF des Switches muss mit der Community-Zeichenfolge übereinstimmen, die die Systemzustandsüberwachung konfiguriert ist. Standardmäßig verwendet die Systemzustandsüberwachung die Community-Zeichenfolge `cshm1!`.

   ⓘ Derzeit unterstützt die Systemzustandsüberwachung nur SNMPv2.

   Wenn Sie Informationen über einen Switch ändern müssen, der vom Cluster überwacht wird, können Sie den Community-String, den die Systemzustandsüberwachung mit dem folgenden Befehl verwendet, ändern:

ONTAP 9.8 und höher

`system switch ethernet modify`

ONTAP 9.7 und früher

`system cluster-switch modify`

3. Vergewissern Sie sich, dass der Managementport des Switch mit dem Managementnetzwerk verbunden ist.

   Diese Verbindung ist erforderlich, um SNMP-Abfragen durchzuführen.

Befehle für das Monitoring des Systemzustands Ihres Systems

Sie können das verwenden `system health` Befehle zum Anzeigen von Informationen über den Systemzustand der Systemressourcen, zum Reagieren auf Meldungen und zum Konfigurieren zukünftiger Warnmeldungen. Mithilfe der CLI-Befehle können Sie detaillierte Informationen über das Konfigurieren des Systemzustands anzeigen. Die man-Pages für die Befehle enthalten weitere Informationen.

Zeigt den Status des Systemzustands an

Ihr Ziel ist	Befehl
Anzeigen des Integritätsstatus des Systems, der den Gesamtstatus einzelner Integritätsmonitore wiedergibt	`system health status show`
Anzeigen des Funktionszustands von Subsystemen, für die ein Zustandsüberwachung verfügbar ist	`system health subsystem show`

Zeigt den Status der Node-Konnektivität an

Ihr Ziel ist	Befehl
Zeigt Details zur Konnektivität vom Node zum Storage Shelf an, einschließlich Portinformationen, HBA-Port-Geschwindigkeit, I/O-Durchsatz und der Geschwindigkeit von I/O-Vorgängen pro Sekunde	`storage shelf show -connectivity` Verwenden Sie die `-instance` Parameter zum Anzeigen detaillierter Informationen zu jedem Shelf.
Anzeigen von Informationen zu Laufwerken und Array-LUNs, einschließlich des nutzbaren Speicherplatzes, Shelf- und Einschubnummern sowie des eigenen Node-Namens	`storage disk show` Verwenden Sie die `-instance` Parameter zum Anzeigen detaillierter Informationen zu jedem Laufwerk.

Ihr Ziel ist	Befehl
Zeigt detaillierte Informationen über Storage-Shelf-Ports an, einschließlich Porttyp, Geschwindigkeit und Status	`storage port show` Verwenden Sie die `-instance` Parameter zum Anzeigen detaillierter Informationen zu den einzelnen Adaptern.

Managen Sie die Erkennung von Cluster-, Storage- und Management-Netzwerk-Switches

Ihr Ziel ist	Verwenden Sie diesen Befehl.. (ONTAP 9.8 und höher)	Verwenden Sie diesen Befehl.. (ONTAP 9.7 und früher)
Zeigen Sie die Switches an, die das Cluster überwacht	`system switch ethernet show`	`system cluster-switch show`
Zeigen Sie die Switches an, die das Cluster derzeit überwacht, einschließlich der von Ihnen gelöschten Switches (siehe Spalte „Grund“ der Befehlsausgabe), und Konfigurationsinformationen, die Sie für den Netzwerkzugriff auf das Cluster und auf die Management-Netzwerk-Switches benötigen. Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.	`system switch ethernet show-all`	`system cluster-switch show-all`
Konfigurieren Sie die Erkennung eines nicht erkannten Switches	`system switch ethernet create`	`system cluster-switch create`
Ändern von Informationen über einen vom Cluster überwachen Switch (z. B. Gerätename, IP-Adresse, SNMP-Version und Community String)	`system switch ethernet modify`	`system cluster-switch modify`
Deaktivieren Sie die Überwachung eines Switches	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Deaktivieren Sie die Erkennung und Überwachung eines Switch und löschen Sie die Switch-Konfigurationsinformationen	`system switch ethernet delete`	`system cluster-switch delete`

Ihr Ziel ist	Verwenden Sie diesen Befehl.. (ONTAP 9.8 und höher)	Verwenden Sie diesen Befehl.. (ONTAP 9.7 und früher)
Entfernen Sie die in der Datenbank gespeicherten Switch-Konfigurationsinformationen dauerhaft (wodurch die automatische Erkennung des Switch wieder möglich ist).	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Aktivieren Sie die automatische Protokollierung zum Senden mit AutoSupport-Nachrichten.	`system switch ethernet log`	`system cluster-switch log`

Reagieren Sie auf generierte Warnmeldungen

Ihr Ziel ist	Befehl
Anzeige von Informationen zu generierten Meldungen, z. B. Ressource und Node, auf dem die Meldung ausgelöst wurde, sowie des Schweregrads und der wahrscheinlichen Ursache der Meldung	`system health alert show`
Zeigt Informationen zu jeder generierten Meldung an	`system health alert show -instance`
Geben Sie an, dass jemand an einer Warnung arbeitet	`system health alert modify`
Bestätigen Sie eine Meldung	`system health alert modify -acknowledge`
Unterdrücken Sie eine nachfolgende Meldung, damit sie den Integritätsstatus eines Subsystems nicht beeinflusst	`system health alert modify -suppress`
Löschen Sie eine Meldung, die nicht automatisch gelöscht wurde	`system health alert delete`
Informationen zu den AutoSupport Meldungen, die innerhalb der letzten Woche ausgelöst wurden, anzeigen, um z. B. zu bestimmen, ob eine Meldung eine AutoSupport Meldung ausgelöst hat	`system health autosupport trigger history show`

Konfigurieren Sie zukünftige Warnmeldungen

Ihr Ziel ist	Befehl
Aktivieren oder deaktivieren Sie die Richtlinie, die steuert, ob ein bestimmter Ressourcenzustand eine bestimmte Warnmeldung ausgibt	`system health policy definition modify`

Zeigt Informationen zur Konfiguration der Systemzustandsüberwachung an

Ihr Ziel ist	Befehl
Anzeigen von Informationen über Systemzustandsüberwachung, z. B. ihre Nodes, Namen, Subsysteme und Status	`system health config show`  Verwenden Sie die `-instance` Parameter zum Anzeigen detaillierter Informationen zu jeder Systemzustandsüberwachung.
Zeigen Sie Informationen zu den Meldungen an, die eine Systemzustandsüberwachung möglicherweise generiert werden kann	`system health alert definition show`  Verwenden Sie die `-instance` Parameter zum Anzeigen detaillierter Informationen zu jeder Meldungsdefinition.
Anzeigen von Informationen über Richtlinien der Systemzustandsüberwachung, die bestimmen, wann Meldungen ausgegeben werden	`system health policy definition show`  Verwenden Sie die `-instance` Parameter zum Anzeigen detaillierter Informationen zu jeder Richtlinie Verwenden Sie andere Parameter, um die Meldungsliste zu filtern, z. B. nach Richtlinienstatus (aktiviert oder nicht), Systemzustandsüberwachung, Meldung usw.

Zeigt Umgebungsinformationen an

Sensoren helfen Ihnen dabei, die Umgebungskomponenten Ihres Systems zu überwachen. Die Informationen, die Sie zu Umgebungssensoren anzeigen können, umfassen ihren Typ, ihren Namen, den Zustand, ihren Wert und ihre Schwellenwerte.

Schritt

1. Verwenden Sie das, um Informationen zu Umgebungssensoren anzuzeigen `system node environment sensors show` Befehl.

Management des Zugriffs auf Webservices

Verwaltung des Zugriffs auf Webservices – Übersicht

Ein Webservice ist eine Anwendung, auf die Benutzer über HTTP oder HTTPS zugreifen können. Der Clusteradministrator kann die Web-Protokoll-Engine einrichten, SSL konfigurieren, einen Webdienst aktivieren und Benutzern einer Rolle den Zugriff auf einen Webdienst ermöglichen.

Ab ONTAP 9.6 werden die folgenden Webservices unterstützt:

- Service Processor Infrastructure (`spi`)

  Dieser Service stellt Protokoll, Core Dump und MIB-Dateien für HTTP- oder HTTPS-Zugriff über die Cluster-Management-LIF oder Node-Management-LIF bereit. Die Standardeinstellung ist `enabled`.

  Bei einer Anforderung für den Zugriff auf die Log-Dateien eines Node oder auf Core Dump-Dateien liefert das `spi` Web Service erstellt automatisch einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Nodes, auf dem sich die Dateien befinden. Sie müssen den Bereitstellungspunkt nicht manuell erstellen. `

- ONTAP APIs (`ontapi`)

  Mit diesem Service können Sie ONTAP APIs ausführen und administrative Funktionen mit einem Remote-Programm ausführen. Die Standardeinstellung ist `enabled`.

  Dieser Service ist möglicherweise für einige externe Verwaltungstools erforderlich. Wenn Sie beispielsweise System Manager verwenden, sollten Sie diesen Service aktiviert lassen.

- Data ONTAP Discovery (`disco`)

  Dieser Service ermöglicht Off-Box-Managementapplikationen, den Cluster im Netzwerk zu erkennen. Die Standardeinstellung ist `enabled`.

- Support-Diagnose (`supdiag`)

  Dieser Service steuert den Zugriff auf eine privilegierte Umgebung des Systems, um die Problemanalyse und -Behebung zu unterstützen. Die Standardeinstellung ist `disabled`. Sie sollten diesen Service nur aktivieren, wenn Sie sich unter Anleitung durch den technischen Support richten.

- System Manager (`sysmgr`)

  Dieser Service steuert die Verfügbarkeit von System Manager, der in ONTAP enthalten ist. Die Standardeinstellung ist `enabled`. Dieser Service wird nur auf dem Cluster unterstützt.

- Aktualisierung des Firmware BaseBoard Management Controller (BMC) (`FW_BMC`)

  Mit diesem Service können Sie BMC-Firmware-Dateien herunterladen. Die Standardeinstellung ist `enabled`.

- ONTAP-Dokumentation (`docs`)

  Dieser Service bietet Zugriff auf die ONTAP-Dokumentation. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful APIs (`docs_api`)

  Dieser Service bietet Zugriff auf die Dokumentation der ONTAP RESTful API. Die Standardeinstellung ist `enabled`.

- Datei hochladen und herunterladen (`fud`)

  Dieser Service bietet Datei-Upload und Download. Die Standardeinstellung ist `enabled`.

- ONTAP Messaging (`ontapmsg`)

  Dieser Service unterstützt eine Schnittstelle für Veröffentlichung und Abonnements, über die Sie Ereignisse abonnieren können. Die Standardeinstellung ist `enabled`.

- ONTAP Portal (`portal`)

  Dieser Service implementiert das Gateway auf einem virtuellen Server. Die Standardeinstellung ist `enabled`.

- ONTAP RESTful Schnittstelle (`rest`)

  Dieser Service unterstützt eine RESTful Schnittstelle, über die alle Elemente der Cluster-Infrastruktur per Remote-Zugriff gemanagt werden. Die Standardeinstellung ist `enabled`.

- Security Assertion Markup Language (SAML) Service Provider-Unterstützung (`saml`)

  Dieser Service bietet Ressourcen zur Unterstützung des SAML-Service-Providers. Die Standardeinstellung ist `enabled`.

- SAML-Service-Provider (`saml-sp`)

  Dieser Service bietet Services wie SP-Metadaten und den Assertion Consumer Service an den Service Provider. Die Standardeinstellung ist `enabled`.

Ab ONTAP 9.7 werden die folgenden zusätzlichen Services unterstützt:

- Backup-Dateien Für Die Konfiguration (`backups`)

  Dieser Service ermöglicht Ihnen das Herunterladen von Backup-Konfigurationsdateien. Die Standardeinstellung ist `enabled`.

- ONTAP Sicherheit (`security`)

  Dieser Service unterstützt das CSRF-Token-Management für eine erweiterte Authentifizierung. Die Standardeinstellung ist `enabled`.

Verwalten der Web Protocol Engine

Sie können die Web Protocol Engine auf dem Cluster so konfigurieren, dass festgelegt wird, ob Webzugriff zulässig ist und welche SSL-Versionen verwendet werden können. Sie können auch die Konfigurationseinstellungen für die Web-Protokoll-Engine anzeigen.

Sie haben folgende Möglichkeiten, die Web-Protokoll-Engine auf Cluster-Ebene zu verwalten:

- Sie können festlegen, ob Remote-Clients HTTP oder HTTPS für den Zugriff auf Web-Service-Inhalte verwenden können, indem Sie die verwenden `system services web modify` Befehl mit dem `-external` Parameter.
- Sie können angeben, ob SSLv3 für sicheren Webzugriff verwendet werden soll, indem Sie die verwenden `security config modify` Befehl mit dem `-supported-protocol` Parameter. SSLv3 ist standardmäßig deaktiviert. Transport Layer Security 1.0 (TLSv1.0) ist aktiviert und kann bei Bedarf

deaktiviert werden.

- Sie können den Compliance-Modus des Federal Information Processing Standard (FIPS) 140-2 für Cluster-weite Webservice-Schnittstellen auf Kontrollebene aktivieren.

  Der FIPS 140-2-2-Compliance-Modus ist standardmäßig deaktiviert.

  - **Wenn der FIPS 140-2-Compliance-Modus deaktiviert ist** können Sie den FIPS 140-2-Compliance-Modus aktivieren, indem Sie den einstellen `is-fips-enabled` Parameter an `true` Für das `security config modify` Befehl und dann mit `security config show` Befehl zum Bestätigen des Online-Status.
  - **Wenn der FIPS 140-2-Konformitätsmodus aktiviert ist**
    - Ab ONTAP 9.11.1 sind TLSv1, TLSv1.1 und SSLv3 deaktiviert, und nur TSLv1.2 und TSLv1.3 bleiben aktiviert. Sie wirkt sich auf andere interne und externe Systeme und Kommunikation mit ONTAP 9 aus. Wenn Sie den FIPS 140-2 Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1, TLSv1.1 und SSLv3 deaktiviert. Je nach der vorherigen Konfiguration bleiben entweder TLSV.1 oder TLSv1.3 aktiviert.
    - Für Versionen von ONTAP vor 9.11.1 sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn der Compliance-Modus nach FIPS 140-2 aktiviert ist. Wenn Sie den FIPS 140-2-Compliance-Modus aktivieren und anschließend deaktivieren, bleiben TLSv1 und SSLv3 deaktiviert, jedoch sind je nach vorheriger Konfiguration entweder TLSv1.2 oder TLSv1.1 und TLSv1.2 aktiviert.
- Sie können die Konfiguration der Cluster-weiten Sicherheit mit anzeigen `system security config show` Befehl.

Wenn die Firewall aktiviert ist, muss die Firewallrichtlinie für die logische Schnittstelle (LIF) eingerichtet werden, die für Webservices verwendet werden soll, damit HTTP- oder HTTPS-Zugriff möglich ist.

Wenn Sie HTTPS für den Webservice-Zugriff verwenden, muss auch die SSL für das Cluster oder die Storage Virtual Machine (SVM) mit dem Web-Service aktiviert sein. Des Weiteren müssen Sie ein digitales Zertifikat für das Cluster oder die SVM angeben.

In MetroCluster Konfigurationen werden die von Ihnen vorgenommenen Änderungen an der Web Protocol Engine eines Clusters nicht im Partner-Cluster repliziert.

Befehle zum Verwalten der Web Protocol Engine

Sie verwenden das `system services web` Befehle zum Verwalten der Web Protocol Engine. Sie verwenden das `system services firewall policy create` Und `network interface modify` Befehle, mit denen Webzugriffsanfragen durch die Firewall gehen können.

Ihr Ziel ist	Befehl
Konfigurieren Sie die Web Protocol Engine auf Cluster-Ebene: • Aktiviert oder deaktiviert die Web Protocol Engine für das Cluster • Aktivieren oder deaktivieren Sie SSLv3 für das Cluster • Aktivieren oder Deaktivieren der Compliance nach FIPS 140-2 für sichere Web-Services (HTTPS)	`system services web modify`
Anzeige der Konfiguration der Web Protocol Engine auf Cluster-Ebene, Ermittlung der Funktionsfähigkeit der Webprotokolle im gesamten Cluster und Anzeige der online-aktivierten FIPS 140-2-Compliance-Funktionen	`system services web show`
Zeigt die Konfiguration der Web-Protokoll-Engine auf Node-Ebene und die Aktivitäten der Webservice-Handhabung für die Knoten im Cluster an	`system services web node show`
Erstellen Sie eine Firewallrichtlinie oder fügen Sie einem vorhandenen Firewallrichtlinie HTTP- oder HTTPS-Protokollservice hinzu, um Webzugriffsanfragen durch die Firewall zu durchlaufen	`system services firewall policy create` Einstellen des `-service` Parameter an `http` Oder `https` Ermöglicht das Durchgehen von Webzugriffsanfragen durch die Firewall.
Zuordnen einer Firewallrichtlinie zu einer logischen Schnittstelle	`network interface modify` Sie können das verwenden `-firewall-policy` Parameter zum Ändern der Firewall-Richtlinie einer LIF.

Konfiguration der SAML-Authentifizierung für Webservices

Konfigurieren Sie die SAML-Authentifizierung

Ab ONTAP 9.3 können Sie die SAML-Authentifizierung (Security Assertion Markup Language) für Webservices konfigurieren. Wenn die SAML-Authentifizierung konfiguriert und aktiviert ist, werden Benutzer von einem externen Identitäts-Provider (IdP) anstelle von Verzeichnisdienstanbietern wie Active Directory und LDAP authentifiziert.

Was Sie benötigen

- Sie müssen das IdP für SAML-Authentifizierung konfiguriert haben.
- Sie müssen über die IdP-URI verfügen.

Über diese Aufgabe

- SAML-Authentifizierung gilt nur für das `http` Und `ontapi` Applikationen unterstützt.

  Der `http` Und `ontapi` Applikationen werden von folgenden Web-Services verwendet: Service Processor Infrastructure, ONTAP APIs oder System Manager.

- SAML-Authentifizierung ist nur für den Zugriff auf die Administrator-SVM anwendbar.

Schritte

1. SAML-Konfiguration für den Zugriff von ONTAP auf die IdP-Metadaten erstellen:

   security saml-sp create -idp-uri *idp_uri* -sp-host *ontap_host_name*

   `idp_uri` Ist die FTP- oder HTTP-Adresse des IdP-Hosts, von dem die IdP-Metadaten heruntergeladen werden können.

   `ontap_host_name` Ist der Hostname oder die IP-Adresse des Host des SAML-Service-Providers, was in diesem Fall das ONTAP-System ist. Standardmäßig wird die IP-Adresse der Cluster-Management-LIF verwendet.

   Optional können Sie die Zertifikatsinformationen für den ONTAP-Server angeben. Standardmäßig werden die Zertifikatinformationen des ONTAP-Webservers verwendet.

   ```
   cluster_12::> security saml-sp create -idp-uri
   https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
   -metadata-server false

   Warning: This restarts the web server. Any HTTP/S connections that are
   active
            will be disrupted.
   Do you want to continue? {y|n}: y
   [Job 179] Job succeeded: Access the SAML SP metadata using the URL:
   https://10.63.56.150/saml-sp/Metadata

   Configure the IdP and Data ONTAP users for the same directory server
   domain to ensure that users are the same for different authentication
   methods. See the "security login show" command for the Data ONTAP user
   configuration.
   ```

   Die URL für den Zugriff auf die ONTAP-Hostmetadaten wird angezeigt.

2. Konfigurieren Sie vom IdP-Host aus das IdP mit den ONTAP-Host-Metadaten.

   Weitere Informationen zum Konfigurieren des IdP finden Sie in der IdP-Dokumentation.

3. SAML-Konfiguration aktivieren:

   security saml-sp modify -is-enabled true

   Alle bestehenden Benutzer, die auf das zugreifen `http` Oder `ontapi` Die Applikation wird automatisch für die SAML-Authentifizierung konfiguriert.

4. Wenn Sie Benutzer für das erstellen möchten `http` Oder `ontapi` Anwendung, nachdem SAML konfiguriert wurde, geben Sie SAML als Authentifizierungsmethode für die neuen Benutzer an.

   a. Erstellen Sie eine Anmeldemethode für neue Benutzer mit SAML-Authentifizierung:
   `security login create -user-or-group-name user_name -application [http | ontapi] -authentication-method saml -vserver svm_name`

   ```
   cluster_12::> security login create -user-or-group-name admin1
   -application http -authentication-method saml -vserver  cluster_12
   ```

   b. Vergewissern Sie sich, dass der Benutzereintrag erstellt wurde:

   `security login show`

```
cluster_12::> security login show

Vserver: cluster_12
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no     none
admin          http        password      admin            no     none
admin          http        saml          admin            -      none
admin          ontapi      password      admin            no     none
admin          ontapi      saml          admin            -      none
admin          service-processor
                           password      admin            no     none
admin          ssh         password      admin            no     none
admin1         http        password      backup           no     none
**admin1         http        saml          backup           -
none**
```

Verwandte Informationen

"ONTAP 9-Befehle"

Deaktivieren Sie die SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Webbenutzern mithilfe eines externen Identitätsanbieters (IdP) beenden möchten. Wenn die SAML-Authentifizierung deaktiviert ist, werden die konfigurierten Verzeichnisdienstanbieter wie Active Directory und LDAP zur Authentifizierung verwendet.

Was Sie benötigen

Sie müssen über die Konsole angemeldet sein.

Schritte

1. SAML-Authentifizierung deaktivieren:

   ```
   security saml-sp modify -is-enabled false
   ```

2. Wenn Sie die SAML-Authentifizierung nicht mehr verwenden möchten oder wenn Sie die IdP ändern möchten, löschen Sie die SAML-Konfiguration:

   ```
   security saml-sp delete
   ```

Fehlerbehebung bei der SAML-Konfiguration

Wenn die Konfiguration der SAML-Authentifizierung (Security Assertion Markup Language) fehlschlägt, können Sie jeden Knoten, auf dem die SAML-Konfiguration fehlgeschlagen ist, manuell reparieren und nach dem Fehler wiederherstellen. Während der Reparatur wird der Webserver neu gestartet und alle aktiven HTTP-Verbindungen oder HTTPS-Verbindungen werden unterbrochen.

Über diese Aufgabe

Bei der Konfiguration der SAML-Authentifizierung wendet ONTAP pro Node die SAML-Konfiguration an. Wenn Sie die SAML-Authentifizierung aktivieren, versucht ONTAP automatisch, jeden Node bei Konfigurationsproblemen zu reparieren. Wenn Probleme mit der SAML-Konfiguration auf einem beliebigen Node auftreten, können Sie die SAML-Authentifizierung deaktivieren und dann die SAML-Authentifizierung erneut aktivieren. Es kann Situationen geben, in denen die SAML-Konfiguration auf einem oder mehreren Nodes nicht angewendet werden kann, selbst wenn Sie die SAML-Authentifizierung reaktivieren. Sie können den Node identifizieren, auf dem die SAML-Konfiguration ausgefallen ist, und diesen Node manuell reparieren.

Schritte

1. Melden Sie sich bei der erweiterten Berechtigungsebene an:

   ```
   set -privilege advanced
   ```

2. Ermitteln des Knotens, auf dem die SAML-Konfiguration fehlgeschlagen ist:

   ```
   security saml-sp status show -instance
   ```

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

3. Reparieren Sie die SAML-Konfiguration auf dem ausgefallenen Node:

   security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Der Webserver wird neu gestartet und alle aktiven HTTP-Verbindungen oder HTTPS-Verbindungen werden unterbrochen.

4. Vergewissern Sie sich, dass SAML auf allen Knoten erfolgreich konfiguriert wurde:

   security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: **config-success**
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Verwalten von Webservices

Web Services-Übersicht verwalten

Sie können einen Webdienst für das Cluster oder eine Storage Virtual Machine (SVM) aktivieren bzw. deaktivieren, die Einstellungen für Webservices anzeigen und festlegen, ob Benutzer einer Rolle auf einen Webservice zugreifen können.

Es gibt folgende Möglichkeiten, Web-Services für das Cluster oder eine SVM zu managen:

- Aktivieren oder Deaktivieren eines bestimmten Webservice
- Festlegen, ob der Zugriff auf einen Webdienst nur auf verschlüsseltes HTTP (SSL) beschränkt ist
- Anzeigen der Verfügbarkeit von Webservices
- Benutzern einer Rolle den Zugriff auf einen Webservice zu ermöglichen oder zu verdrängen
- Anzeigen der Rollen, die auf einen Webdienst zugreifen dürfen

Damit ein Benutzer auf einen Webdienst zugreifen kann, müssen alle folgenden Bedingungen erfüllt sein:

- Der Benutzer muss authentifiziert sein.

  Beispielsweise kann ein Webdienst einen Benutzernamen und ein Kennwort anfordern. Die Antwort des Benutzers muss mit einem gültigen Konto übereinstimmen.

- Der Benutzer muss mit der richtigen Zugriffsmethode eingerichtet sein.

  Authentifizierung ist nur für Benutzer mit der richtigen Zugriffsmethode für den angegebenen Webdienst erfolgreich. Für den Webservice der ONTAP API `ontapi`), Benutzer müssen die haben `ontapi` Zugriffsmethode. Für alle anderen Web-Dienste müssen die Benutzer über die verfügen `http`

Zugriffsmethode.

> Sie verwenden das `security login` Befehle zum Verwalten von Zugriffsmethoden und Authentifizierungsmethoden für Benutzer`.

- Der Webdienst muss so konfiguriert sein, dass die Zugriffskontrollrolle des Benutzers zugelassen wird.

> Sie verwenden das `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Wenn eine Firewall aktiviert ist, muss die Firewallrichtlinie für die Nutzung von LIF für Web-Services so eingerichtet sein, dass HTTP oder HTTPS möglich sind.

Wenn Sie HTTPS für den Webservice-Zugriff verwenden, muss auch die SSL für das Cluster oder die SVM mit dem Webservice aktiviert sein. Des Weiteren müssen Sie ein digitales Zertifikat für das Cluster oder die SVM vorlegen.

Befehle zum Verwalten von Webservices

Sie verwenden das `vserver services web` Befehle zum Managen der Verfügbarkeit von Web-Services für das Cluster oder einer Storage Virtual Machine (SVM) Sie verwenden das `vserver services web access` Befehle, um den Zugriff einer Rolle auf einen Webdienst zu steuern.

Ihr Ziel ist	Befehl
Konfigurieren eines Webservice für das Cluster oder anSVM: • Aktivieren oder Deaktivieren eines Webservice • Geben Sie an, ob nur HTTPS für den Zugriff auf einen Webdienst verwendet werden kann	`vserver services web modify`
Anzeigen der Konfiguration und Verfügbarkeit von Webservices für das Cluster oder eine anSVM	`vserver services web show`
Autorisieren eine Rolle für den Zugriff auf einen Web-Service auf dem Cluster oder einer anSVM	`vserver services web access create`
Zeigen Sie die Rollen an, die für den Zugriff auf Webservices im Cluster oder auf anSVM autorisiert sind	`vserver services web access show`
Verhindern Sie, dass eine Rolle auf einen Webservice auf dem Cluster oder einer anSVM zugreift	`vserver services web access delete`

Verwandte Informationen

"ONTAP 9-Befehle"

Befehle zum Verwalten von Mount-Punkten auf den Nodes

Der `spi` Webservice erstellt bei Anforderung einen Mount-Punkt automatisch von einem Node zum Root-Volume eines anderen Nodes, um auf die Log-Dateien oder Kerndateien des Node zuzugreifen. Obwohl Sie Mount-Punkte nicht manuell verwalten müssen, können Sie dies mit dem tun `system node root-mount` Befehle.

Ihr Ziel ist	Befehl
Erstellen Sie manuell einen Mount-Punkt von einem Node zum Root-Volume eines anderen Nodes	`system node root-mount create` Nur ein einzelner Mount-Punkt kann von einem Node zum anderen vorhanden sein.
Zeigen Sie vorhandene Mount-Punkte auf den Nodes im Cluster an, einschließlich der Zeit, die ein Mount-Punkt erstellt wurde, und des aktuellen Status	`system node root-mount show`
Löschen Sie einen Bereitstellungspunkt von einem Node zum Root-Volume eines anderen Node, und erzwingen Sie die Verbindungen zum Mount-Punkt zum Schließen	`system node root-mount delete`

Verwandte Informationen

"ONTAP 9-Befehle"

SSL verwalten

Das SSL-Protokoll verbessert die Sicherheit des Webzugriffs, indem ein digitales Zertifikat verwendet wird, um eine verschlüsselte Verbindung zwischen einem Webserver und einem Browser herzustellen.

Sie haben folgende Möglichkeiten, SSL für das Cluster oder eine Storage Virtual Machine (SVM) zu verwalten:

- Aktivieren von SSL
- Generieren und Installieren eines digitalen Zertifikats und Verknüpfen eines Zertifikats mit dem Cluster oder der SVM
- Anzeigen der SSL-Konfiguration zur Bestätigung, ob SSL aktiviert wurde, und, falls verfügbar, der Name des SSL-Zertifikats
- Einrichtung von Firewallrichtlinien für das Cluster oder SVM, um Webzugriffsanfragen durchzuführen
- Definieren, welche SSL-Versionen verwendet werden können
- Beschränkung des Zugriffs auf nur HTTPS-Anforderungen für einen Webdienst

Befehle zum Verwalten von SSL

Sie verwenden das `security ssl` Befehle zum Managen des SSL-Protokolls für das Cluster ora Storage Virtual Machine (SVM).

Ihr Ziel ist	Befehl
Aktivieren Sie SSL für den Cluster oranSVM und verknüpfen Sie ein digitales Zertifikat mit ihm	`security ssl modify`
Zeigt den SSL-Konfigurations- und Zertifikatnamen für die Cluster-oranSVM an	`security ssl show`

Konfigurieren Sie den Zugriff auf Webservices

Durch die Konfiguration des Zugriffs auf Webservices können autorisierte Benutzer HTTP oder HTTPS verwenden, um auf den Service-Inhalt des Clusters oder eine Storage Virtual Machine (SVM) zuzugreifen.

Schritte

1. Wenn eine Firewall aktiviert ist, stellen Sie sicher, dass in der Firewallrichtlinie für die LIF HTTP- oder HTTPS-Zugriffe eingerichtet sind, die für Web-Services verwendet werden:

   Sie können überprüfen, ob eine Firewall über die aktiviert ist `system services firewall show` Befehl.

   a. Um zu überprüfen, ob HTTP oder HTTPS in der Firewallrichtlinie eingerichtet sind, verwenden Sie das `system services firewall policy show` Befehl.

      Sie stellen die ein `-service` Parameter von `system services firewall policy create` Befehl an `http` Oder `https` Aktivieren der Richtlinie zur Unterstützung des Webzugriffs

   b. Um zu überprüfen, ob die Firewallrichtlinie, die HTTP oder HTTPS unterstützt, der logischen Schnittstelle zugeordnet ist, die Webservices bereitstellt, verwenden Sie die `network interface show` Befehl mit dem `-firewall-policy` Parameter.

      Sie verwenden das `network interface modify` Befehl mit dem `-firewall-policy` Parameter, um die Firewall-Richtlinie für ein LIF zu nutzen

2. Verwenden Sie zum Konfigurieren der Webprotokoll-Engine auf Cluster-Ebene und für den Zugriff auf Webservice-Inhalte das `system services web modify` Befehl.
3. Wenn Sie Secure Web Services (HTTPS) verwenden möchten, aktivieren Sie SSL und stellen mithilfe von digitale Zertifikatinformationen für den Cluster oder die SVM zur Verfügung `security ssl modify` Befehl.
4. Um einen Webservice für das Cluster oder die SVM zu aktivieren, verwenden Sie den `vserver services web modify` Befehl.

   Sie müssen diesen Schritt für jeden Service wiederholen, den Sie für das Cluster oder die SVM aktivieren möchten.

5. Um eine Rolle für den Zugriff auf Web-Services auf dem Cluster oder der SVM zu autorisieren, verwenden Sie den `vserver services web access create` Befehl.

   Die Rolle, die Sie Zugriff gewähren, muss bereits vorhanden sein. Sie können vorhandene Rollen mit dem anzeigen `security login role show` Führen Sie den Befehl aus, oder erstellen Sie neue Rollen mit

`security login role create` Befehl.

6. Stellen Sie für eine Rolle, die für den Zugriff auf einen Webdienst autorisiert wurde, sicher, dass die Benutzer auch mit der richtigen Zugriffsmethode konfiguriert sind, indem Sie die Ausgabe des überprüfen `security login show` Befehl.

   Um auf den Webdienst der ONTAP API zuzugreifen `ontapi`) Muss ein Benutzer mit dem konfiguriert werden `ontapi` Zugriffsmethode. Für den Zugriff auf alle anderen Webservices muss ein Benutzer mit dem konfiguriert werden `http` Zugriffsmethode.

   Sie verwenden das `security login create` Befehl zum Hinzufügen einer Zugriffsmethode für einen Benutzer.

Fehlerbehebung bei Problemen mit dem Webservice-Zugriff

Konfigurationsfehler führen zu Problemen mit dem Webservice-Zugriff. Sie können die Fehler beheben, indem Sie sicherstellen, dass LIF, Firewall-Richtlinie, Web-Protokoll-Engine, Web-Services, digitale Zertifikate, Und die Benutzerzugriffsautorisierung sind alle richtig konfiguriert.

Die folgende Tabelle hilft Ihnen bei der Identifizierung und Behebung von Fehlern bei der Webservice-Konfiguration:

Dieses Zugriffsproblem…	**Tritt wegen dieses Konfigurationsfehlers auf…**	**So beheben Sie den Fehler:**
Ihr Webbrowser gibt einen zurück `unable to connect` Oder `failure to establish a connection` Fehler beim Zugriff auf einen Webdienst.	Ihr LIF ist möglicherweise falsch konfiguriert.	Stellen Sie sicher, dass Sie die LIF anpingen können, die den Webservice bereitstellt. Sie verwenden das `network ping` Befehl zum Ping eines LIF. Informationen zur Netzwerkkonfiguration finden Sie im *Network Management Guide*.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Ihre Firewall ist möglicherweise falsch konfiguriert. Stellen Sie sicher, dass die Web Protocol Engine aktiviert ist, damit Webservices verfügbar sind. Sie verwenden das `system services web` Befehle zum Verwalten der Web Protocol Engine für den Cluster. Stellen Sie sicher, dass jeder Webdienst, auf den Sie Zugriff zulassen möchten, individuell aktiviert ist. Sie verwenden das `vserver services web modify` Befehl zum Aktivieren eines Webservices für den Zugriff.	Vergewissern Sie sich, dass eine Firewallrichtlinie eingerichtet ist, um HTTP oder HTTPS zu unterstützen und die Richtlinie der logischen Schnittstelle, die den Webservice bereitstellt, zugewiesen ist. Sie verwenden das `system services firewall policy` Befehle zum Management von Firewallrichtlinien Sie verwenden das `network interface modify` Befehl mit dem `-firewall -policy` Parameter zum Zuordnen einer Richtlinie zu einer LIF. Ihr Webbrowser gibt einen zurück `not found` Fehler beim Zugriff auf einen Webdienst. Der Webbrowser meldet sich nicht bei einem Webdienst mit dem Kontonamen und Passwort eines Benutzers an.	Ihre Web-Protokoll-Engine ist möglicherweise deaktiviert. Der Webdienst ist möglicherweise deaktiviert. Der Benutzer kann nicht authentifiziert werden, die Zugriffsmethode ist nicht korrekt oder der Benutzer ist nicht berechtigt, auf den Webdienst zuzugreifen.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Stellen Sie sicher, dass das Benutzerkonto vorhanden ist und mit der richtigen Zugriffsmethode und Authentifizierungsmethode konfiguriert ist. Stellen Sie außerdem sicher, dass die Rolle des Benutzers für den Zugriff auf den Webdienst autorisiert ist. Sie verwenden das `security login` Befehle zum Verwalten von Benutzerkonten und deren Zugriffsmethoden und Authentifizierungsmethoden. Für den Zugriff auf den Webdienst der ONTAP API ist das erforderlich `ontapi` Zugriffsmethode. Für den Zugriff auf alle anderen Webservices ist das erforderlich `http` Zugriffsmethode. Sie verwenden das `vserver services web access` Befehle zum Verwalten des Zugriffs einer Rolle auf einen Webdienst.	Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung unterbrochen wird.	Möglicherweise ist SSL nicht auf dem Cluster oder der Storage Virtual Machine (SVM) aktiviert, die den Webservice bereitstellt.

Dieses Zugriffsproblem…	Tritt wegen dieses Konfigurationsfehlers auf…	So beheben Sie den Fehler:
Vergewissern Sie sich, dass für den Cluster oder die SVM SSL aktiviert ist und das digitale Zertifikat gültig ist. Sie verwenden das `security ssl` Befehle zum Verwalten der SSL-Konfiguration für HTTP-Server und der `security certificate show` Befehl zum Anzeigen von digitalen Zertifikatinformationen.	Sie stellen eine Verbindung zu Ihrem Webdienst über HTTPS her, und Ihr Webbrowser zeigt an, dass die Verbindung nicht vertrauenswürdig ist.	Möglicherweise verwenden Sie ein selbstsigniertes digitales Zertifikat.

Überprüfen Sie die Identität der Remoteserver mit Zertifikaten

Überprüfen Sie die Identität von Remote-Servern mithilfe der Zertifikatübersicht

ONTAP unterstützt die Funktionen für Sicherheitszertifikate zur Überprüfung der Identität von Remote-Servern.

Die ONTAP Software ermöglicht sichere Verbindungen unter Verwendung dieser digitalen Zertifikatfunktionen und -Protokolle:

- Online Certificate Status Protocol (OCSP) validiert den Status von digitalen Zertifikatsanforderungen von ONTAP-Diensten mithilfe von SSL- und TLS-Verbindungen (Transport Layer Security). Diese Funktion ist standardmäßig deaktiviert.
- Die ONTAP-Software enthält standardmäßig vertrauenswürdige Stammzertifikate.
- KMIP-Zertifikate (Key Management Interoperability Protocol) ermöglichen die gegenseitige Authentifizierung eines Clusters und eines KMIP-Servers.

Überprüfen Sie, ob digitale Zertifikate mit OCSP gültig sind

Ab ONTAP 9.2 ermöglicht OCSP (Online Certificate Status Protocol) ONTAP-Anwendungen, die TLS-Kommunikation (Transport Layer Security) nutzen, den digitalen Zertifikatsstatus zu erhalten, wenn OCSP aktiviert ist. Sie können OCSP-Zertifikatsprüfungen für bestimmte Anwendungen jederzeit aktivieren oder deaktivieren. Standardmäßig ist die Überprüfung des OCSP-Zertifikatsstatus deaktiviert.

Was Sie benötigen

Diese Befehle müssen auf der erweiterten Berechtigungsebene ausgeführt werden.

Über diese Aufgabe

OCSP unterstützt folgende Anwendungen:

- AutoSupport
- Event Management System (EMS)
- LDAP über TLS
- Key Management Interoperability Protocol (KMIP)
- Audit-Protokollierung
- FabricPool

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`.
2. Um OCSP-Zertifikatsprüfungen für bestimmte ONTAP-Anwendungen zu aktivieren oder zu deaktivieren, verwenden Sie den entsprechenden Befehl.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für einige Anwendungen…	Verwenden Sie den Befehl…
Aktiviert	`security config ocsp enable -app app name`
Deaktiviert	`security config ocsp disable -app app name`

   Mit dem folgenden Befehl wird OCSP-Unterstützung für AutoSupport und EMS aktiviert.

```
cluster::*> security config ocsp enable -app asup,ems
```

   Wenn OCSP aktiviert ist, erhält die Anwendung eine der folgenden Antworten:

   - Gut - das Zertifikat ist gültig und die Kommunikation wird fortgesetzt.
   - Widerrufen: Das Zertifikat wird von der ausstellenden Zertifizierungsstelle dauerhaft als nicht vertrauenswürdig eingestuft und die Kommunikation kann nicht fortgesetzt werden.
   - Unbekannt – der Server verfügt über keine Statusinformationen zum Zertifikat und die Kommunikation kann nicht fortgesetzt werden.
   - OCSP-Serverinformationen fehlen im Zertifikat - der Server fungiert als deaktiviert und fährt mit der TLS-Kommunikation fort, aber es erfolgt keine Statusüberprüfung.
   - Keine Antwort vom OCSP-Server - die Anwendung schlägt fehl.
3. Verwenden Sie den entsprechenden Befehl, um OCSP-Zertifikatsprüfungen für alle Anwendungen mithilfe von TLS-Kommunikation zu aktivieren oder zu deaktivieren.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für alle Anwendungen durchgeführt werden…	Verwenden Sie den Befehl…
Aktiviert	`security config ocsp enable -app all`
Deaktiviert	`security config ocsp disable -app all`

Wenn alle Applikationen aktiviert sind, wird eine signierte Antwort empfangen, die angibt, dass das angegebene Zertifikat in Ordnung, annulliert oder unbekannt ist. Im Fall eines annulliert Zertifikats kann die Anwendung nicht fortgesetzt werden. Wenn die Anwendung keine Antwort vom OCSP-Server erhält oder der Server nicht erreichbar ist, wird die Anwendung nicht fortgesetzt.

4. Verwenden Sie die `security config ocsp show` Befehl zur Anzeige aller Applikationen, die OCSP unterstützen, und ihres Supportstatus.

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true

         7 entries were displayed.
```

Anzeigen von Standardzertifikaten für TLS-basierte Anwendungen

Ab ONTAP 9.2 bietet ONTAP einen Standardsatz an vertrauenswürdigen Root-Zertifikaten für ONTAP-Anwendungen mithilfe von Transport Layer Security (TLS).

Was Sie benötigen

Die Standardzertifikate werden während der Erstellung oder beim Upgrade auf ONTAP 9.2 nur auf der Administrator-SVM installiert.

Über diese Aufgabe

Die aktuellen Applikationen, die als Client fungieren und eine Zertifikatvalidierung erfordern, sind AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Und KMIP.

Wenn Zertifikate ablaufen, wird eine EMS-Nachricht aufgerufen, die den Benutzer zum Löschen der Zertifikate

auffordert. Die Standardzertifikate können nur auf der erweiterten Berechtigungsebene gelöscht werden.

Das Löschen der Standardzertifikate kann dazu führen, dass einige ONTAP-Anwendungen nicht wie erwartet funktionieren (z. B. AutoSupport- und Audit-Protokollierung).

Schritt

1. Sie können die Standardzertifikate, die auf der Admin-SVM installiert sind, anzeigen. Verwenden Sie dazu den Befehl „Security Certificate show“:

   security certificate show -vserver –type server-ca

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                              Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

Beide Seiten authentifizieren das Cluster und einen KMIP-Server

Die Authentifizierung des Clusters und eine Übersicht über KMIP-Server wurden gegenseitig überprüft

Durch die gegenseitige Authentifizierung des Clusters und eines externen Schlüsselmanagers wie einem KMIP-Server (Key Management Interoperability Protocol) kann der Schlüsselmanager mithilfe von KMIP über SSL mit dem Cluster kommunizieren. Sie tun dies, wenn eine Applikation oder eine bestimmte Funktion (z. B. die Storage-Verschlüsselung) sicheren Datenzugriff mit sicheren Schlüsseln erfordert.

Generieren Sie eine Anforderung zum Signieren eines Zertifikats für das Cluster

Sie können das Sicherheitszertifikat verwenden `generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR). Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Was Sie benötigen

Um diese Aufgabe auszuführen, müssen Sie ein Cluster-Administrator oder SVM-Administrator sein.

Schritte

1. CSR erstellen:

   security certificate generate-csr -common-name *FQDN_or_common_name* -size 512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash

-function SHA1|SHA256|MD5

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Der folgende Befehl erzeugt einen CSR mit einem 2,048-bit privaten Schlüssel, der von der SHA256 Hashing-Funktion erzeugt wird, zur Verwendung durch die Software-Gruppe in der IT-Abteilung eines Unternehmens mit individuellem gemeinsamen Namen server1.companyname.com, mit Sitz in Sunnyvale, Kalifornien, USA. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet web@example.com. Das System zeigt den CSR und den privaten Schlüssel in der Ausgabe an.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Kopieren Sie die Zertifikatanforderung aus der CSR-Ausgabe, und senden Sie sie dann in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat. Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten digitalen Zertifikats aufbewahren.

Installieren Sie ein von einer Zertifizierungsstelle signiertes Serverzertifikat für das Cluster

Damit ein SSL-Server die Authentifizierung des Clusters oder der Storage Virtual Machine (SVM) als SSL-Client aktiviert, installieren Sie ein digitales Zertifikat mit dem

Clienttyp auf dem Cluster oder der SVM. Anschließend stellen Sie dem SSL-Serveradministrator das Client-Ca-Zertifikat zur Installation auf dem Server zur Verfügung.

Was Sie benötigen

Sie müssen bereits das Stammzertifikat des SSL-Servers auf dem Cluster oder SVM mit dem installiert haben `server-ca` Zertifikatstyp.

Schritte

1. Um ein selbstsigniertes digitales Zertifikat für die Clientauthentifizierung zu verwenden, verwenden Sie das `security certificate create` Befehl mit dem `type client` Parameter.
2. Gehen Sie wie folgt vor, um ein von einer Zertifizierungsstelle signiertes digitales Zertifikat für die Clientauthentifizierung zu verwenden:

   a. Generieren Sie mithilfe des Sicherheitszertifikats eine digitale Zertifikatsignierungsanforderung (CSR) `generate-csr` Befehl.

      ONTAP zeigt die CSR-Ausgabe an, die eine Zertifikatanforderung und einen privaten Schlüssel enthält, und erinnert Sie daran, die Ausgabe in eine Datei zu kopieren, um sie später verwenden zu können.

   b. Senden Sie die Zertifikatsanforderung von der CSR-Ausgabe in einem elektronischen Formular (z. B. E-Mail) an eine vertrauenswürdige CA zum Signieren.

      Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten Zertifikats für zukünftige Referenz aufbewahren.

   Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat.

   a. Installieren Sie das CA-signierte Zertifikat mithilfe der `security certificate install` Befehl mit dem `-type client` Parameter.
   b. Geben Sie das Zertifikat und den privaten Schlüssel ein, wenn Sie dazu aufgefordert werden, und drücken Sie dann **Enter**.
   c. Geben Sie bei der Aufforderung zusätzliche Root- oder Zwischenzertifikate ein, und drücken Sie dann **Enter**.

      Sie installieren ein Zwischenzertifikat auf dem Cluster oder der SVM, wenn eine Zertifikatkette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt und mit dem Ihnen ausgestellten SSL-Zertifikat endet, die Zwischenzertifikate fehlen. Ein Zwischenzertifikat ist ein vom vertrauenswürdigen Stammverzeichnis herausgegebenem untergeordneten Zertifikat, das speziell für die Ausgabe von Serverzertifikaten der Endeinheit ausgegeben wird. Das Ergebnis ist eine Zertifikatskette, die an der vertrauenswürdigen Stammzertifizierungsstelle beginnt, durch das Zwischenzertifikat geht und mit dem Ihnen ausgestellten SSL-Zertifikat endet.

3. Versorgen `client-ca` Zertifikat des Clusters oder der SVM an den Administrator des SSL-Servers zur Installation auf dem Server.

   Der Befehl zum Anzeigen des Sicherheitszertifikats mit dem `-instance` Und `-type client-ca` Parameter zeigt das an `client-ca` Zertifikatsinformationen

Installieren Sie ein CA-signiertes Client-Zertifikat für den KMIP-Server

Der Zertifikatsubtyp des Key Management Interoperability Protocol (KMIP) (der Parameter -subtype kmip-cert) legt gemeinsam mit den Client- und Server-Ca-Typen fest, dass das Zertifikat für die wechselseitige Authentifizierung des Clusters und einen externen Schlüsselmanager, z. B. einen KMIP-Server, verwendet wird.

Über diese Aufgabe

Installieren Sie ein KMIP-Zertifikat, um einen KMIP-Server als SSL-Server für das Cluster zu authentifizieren.

Schritte

1. Verwenden Sie die `security certificate install` Befehl mit dem `-type server-ca` Und `-subtype kmip-cert` Parameter zur Installation eines KMIP-Zertifikats für den KMIP-Server.
2. Wenn Sie aufgefordert werden, geben Sie das Zertifikat ein, und drücken Sie anschließend die Eingabetaste.

   ONTAP erinnert Sie daran, dass Sie eine Kopie des Zertifikats zur späteren Verwendung aufbewahren.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```