Clusterverwaltung

ONTAP 9

NetApp
November 17, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/concept_administration_overview.html on November 17, 2026. Always check docs.netapp.com for the latest.

Inhalt

Clusterverwaltung . . . 1
Clusterverwaltung mit System Manager . . . 1
Informationen zur Clusterverwaltung mit ONTAP System Manager . . . 1
Mit System Manager auf einen ONTAP Cluster zugreifen . . . 2
Protokolle auf Ihrem ONTAP Cluster konfigurieren . . . 3
Neue Funktionen lassen sich durch das Hinzufügen von Lizenzschlüsseln mit ONTAP System Manager aktivieren. . . . 4
Eine Clusterkonfiguration mit ONTAP System Manager herunterladen . . . 4
Tags einem Cluster mit ONTAP System Manager zuweisen . . . 5
Supportfälle mit ONTAP System Manager anzeigen und einreichen . . . 6
Die maximale Kapazitätsgrenze einer Storage-VM im ONTAP System Manager verwalten . . . 7
Cluster-, Tier- und SVM-Kapazität im ONTAP System Manager überwachen . . . 8
Hardwareprobleme mit dem ONTAP System Manager beheben . . . 12
Knoten mit dem ONTAP System Manager verwalten . . . 16
Lizenzverwaltung . . . 18
ONTAP-Lizenzierungsübersicht . . . 18
Lizenzdateien (NLF) von NetApp von der NetApp Support Site herunterladen . . . 21
Installieren von NetApp-Lizenzen in ONTAP . . . 22
ONTAP Lizenzen verwalten . . . 23
Lizenzarten und Lizenzierungsverfahren . . . 25
Befehle zur Lizenzverwaltung in ONTAP . . . 26
Clusterverwaltung mit der CLI . . . 27
Informationen zur Clusterverwaltung mit der ONTAP CLI . . . 27
Cluster- und SVM-Administratoren . . . 27
Zugriff auf den Cluster über die CLI (nur für Cluster-Administratoren) . . . 29
Die ONTAP Befehlszeilenschnittstelle verwenden . . . 40
Eine ONTAP CLI Sitzung aufzeichnen und die aufgezeichneten Sitzungen verwalten . . . 53
Clusterverwaltung (nur für Clusteradministratoren) . . . 55
Knoten verwalten . . . 59
Das SP/BMC-Netzwerk konfigurieren . . . 84
Knoten aus der Ferne mit dem SP/BMC verwalten . . . 90
ONTAP Clusterzeit verwalten (nur für Clusteradministratoren) . . . 119
Banner und MOTD verwalten . . . 121
ONTAP Jobs und Jobpläne verwalten . . . 131
Sichern und Wiederherstellen von Cluster-Konfigurationen (nur für Clusteradministratoren) . . . 133
Knoten-Core-Dumps für einen ONTAP Cluster verwalten (nur für Cluster-Administratoren) . . . 143
Festplatten- und Tier-Management . . . 145
Festplatten und lokale ONTAP-Ebenen . . . 145
Lokale Ebenen verwalten . . . 146
Datenträger verwalten . . . 184
RAID Konfigurationen verwalten . . . 214
Flash Pool lokale Ebenen verwalten . . . 220
FabricPool Tier-Management . . . 235

Informationen zum Data Tiering mit ONTAP FabricPool . . . 235
Anforderungen für die Nutzung von ONTAP FabricPool . . . 235
ONTAP FabricPool Volume-Tiering-Richtlinien . . . 240
ONTAP FabricPool Konfigurations- und Verwaltungsworkflow . . . 245
Konfiguration von FabricPool . . . 245
Verwaltung von FabricPool . . . 263
Spiegel von FabricPool verwalten . . . 285
ONTAP-Befehle für die Verwaltung von FabricPool-Ressourcen . . . 293
SVM Datenmobilität . . . 295
Informationen zu ONTAP Datenmobilität . . . 295
Migration einer ONTAP SVM . . . 305
Überwachung der ONTAP Volume Migration . . . 307
ONTAP SVM Migration anhalten und fortsetzen . . . 307
Eine ONTAP SVM-Migration abbrechen . . . 308
Manuelle Umstellung der Clients nach einer ONTAP SVM Migration . . . 308
Die Quell-ONTAP SVM wird nach der Clientumstellung manuell entfernt. . . . 309
HA Pair Verwaltung . . . 309
Informationen zur Verwaltung von HA-Paaren in ONTAP Clustern . . . 309
Wie Hardware-unterstütztes Takeover in ONTAP funktioniert . . . 311
Wie automatisches Takeover und Giveback in ONTAP funktionieren . . . 312
ONTAP automatische Takeover-Befehle . . . 316
ONTAP automatische Rückgabebefehle . . . 317
ONTAP manuelle Takeover-Befehle . . . 319
ONTAP manuelle Rückgabebefehle . . . 322
Test von Takeover und Giveback in ONTAP . . . 325
ONTAP Befehle zur Überwachung eines HA-Paares . . . 327
ONTAP Befehle zum Aktivieren und Deaktivieren von Storage Failover . . . 331
ONTAP Knoten in Zwei-Node-Clustern anhalten oder neu starten, ohne eine Übernahme einzuleiten . . . 332
Verschlüsselung für ONTAP HA Datenverkehr konfigurieren . . . 336
REST API-Verwaltung mit System Manager . . . 337
REST API-Verwaltung mit ONTAP System Manager . . . 337
Zugriff auf das ONTAP REST API-Protokoll . . . 338

Clusterverwaltung

Clusterverwaltung mit System Manager

Informationen zur Clusterverwaltung mit ONTAP System Manager

System Manager ist eine auf HTML5 basierende grafische Managementoberfläche, die die Verwaltung von Speichersystemen und Speicherobjekten (wie Festplatten, Volumes und Speicherebenen) über einen Webbrowser sowie die Ausführung gängiger Verwaltungsaufgaben im Zusammenhang mit Speichersystemen ermöglicht.

- System Manager ist in der ONTAP-Software als Webdienst enthalten, standardmäßig aktiviert und über einen Browser zugänglich.
- Der Name von System Manager hat sich ab ONTAP 9.6 geändert. In ONTAP 9.5 und früher wurde er OnCommand System Manager genannt. Ab ONTAP 9.6 und später heißt er System Manager.
- Wenn der klassische System Manager verwendet wird (nur in ONTAP 9.7 und früher verfügbar), siehe "System Manager Classic (ONTAP 9.0 bis 9.7)"

Mithilfe des System Manager Dashboards werden auf einen Blick Informationen zu wichtigen Warnungen und Benachrichtigungen, zur Effizienz und Kapazität von Speicherebenen und Volumes, zu den in einem Cluster verfügbaren Knoten, zum Status der Knoten in einem HA-Paar, zu den aktivsten Anwendungen und Objekten sowie zu den Leistungskennzahlen eines Clusters oder eines Knotens angezeigt.

Mit dem System Manager in ONTAP 9.7 und späteren Versionen lassen sich viele gängige Aufgaben wie die folgenden durchführen:

- Ein Cluster wird erstellt, ein Netzwerk konfiguriert und Supportdetails für den Cluster eingerichtet.
- Speicherobjekte wie Festplatten, lokale Ebenen, Volumes, Qtrees und Kontingente können konfiguriert und verwaltet werden.
- Protokolle wie SMB und NFS konfigurieren und die Dateifreigabe bereitstellen.
- Protokolle wie FC, FCoE, NVMe und iSCSI für den Blockzugriff konfigurieren.
- Netzwerkkomponenten wie Subnetze, Broadcast-Domänen, Daten- und Managementoberflächen sowie Schnittstellengruppen erstellen und konfigurieren.
- Spiegelungs- und Vault-Beziehungen einrichten und verwalten.
- Cluster-Management, Speicherknoten-Management und Management von Storage Virtual Machines (Storage-VMs) werden durchgeführt.
- Speicher-VMs erstellen und konfigurieren, Speicherobjekte verwalten, die mit Speicher-VMs verknüpft sind, sowie Speicher-VM-Dienste verwalten.
- Hochverfügbarkeitskonfigurationen (HA) in einem Cluster überwachen und verwalten.
- Serviceprozessoren können so konfiguriert werden, dass sie sich unabhängig vom Zustand des Knotens remote anmelden, den Knoten verwalten, überwachen und administrieren.

System Manager-Terminologie

Der System Manager verwendet für einige wichtige ONTAP-Funktionen eine andere Terminologie als die CLI.

- **Lokale Ebene**: Eine Gruppe physischer Solid-State-Laufwerke oder Festplatten, auf denen Sie Ihre Daten speichern. Diese sind möglicherweise als Aggregate bekannt. Tatsächlich wird in der ONTAP-CLI weiterhin der Begriff *Aggregate* verwendet, um eine lokale Ebene darzustellen.
- **Cloud-Tier**: Speicher in der Cloud, der von ONTAP verwendet wird, wenn ein Teil Ihrer Daten aus verschiedenen Gründen außerhalb des eigenen Standorts gespeichert werden soll. Wer an den Cloud-Anteil einer FabricPool denkt, hat dies bereits erkannt. Und bei Verwendung eines StorageGRID Systems muss sich die Cloud möglicherweise gar nicht außerhalb des eigenen Standorts befinden. (Ein cloudähnliches Erlebnis am eigenen Standort wird als *private Cloud* bezeichnet.)
- **Storage-VM**: Eine virtuelle Maschine, die innerhalb von ONTAP Speicher- und Datendienste für Ihre Clients bereitstellt. Dies ist möglicherweise als *SVM* oder *vserver* bekannt.
- **Netzwerkschnittstelle**: Adresse und Eigenschaften, die einem physischen Netzwerkport zugewiesen sind. Dies ist möglicherweise als *logische Schnittstelle (LIF)* bekannt.
- **Pause**: Eine Aktion, die den Betrieb anhält. Vor ONTAP 9.8 wurde in anderen Versionen von System Manager möglicherweise *quiesce* genannt.

Mit System Manager auf einen ONTAP Cluster zugreifen

Wenn Sie für den Zugriff auf und die Verwaltung eines Clusters lieber eine grafische Benutzeroberfläche anstelle der Befehlszeilenschnittstelle (CLI) verwenden, ist dies mit System Manager möglich, das als Webdienst in ONTAP enthalten, standardmäßig aktiviert und über einen Browser zugänglich ist.

> Ab ONTAP 9.12.1 ist der System Manager vollständig in die NetApp Console integriert.
>
> Mit der Console ist die Verwaltung Ihrer hybriden Multicloud-Infrastruktur über eine einzige Steuerungsebene möglich, wobei das vertraute System Manager Dashboard erhalten bleibt.
>
> Siehe "System Manager Integration mit NetApp Console".

Über diese Aufgabe

Sie können eine Cluster-Management-Netzwerkschnittstelle (LIF) oder eine Node-Management-Netzwerkschnittstelle (LIF) verwenden, um auf System Manager zuzugreifen. Für unterbrechungsfreien Zugriff auf System Manager sollte eine Cluster-Management-Netzwerkschnittstelle (LIF) verwendet werden.

Bevor Sie beginnen

- Sie benötigen ein Cluster-Benutzerkonto, das mit der Rolle “admin” und den Anwendungstypen “http” und “console” konfiguriert ist.
- Cookies und Websitedaten müssen im Browser aktiviert sein.

Schritte

1. Der Webbrowser wird auf die IP-Adresse der Netzwerkschnittstelle für das Clustermanagement ausgerichtet:
   - Wenn Sie IPv4 verwenden: **`https://cluster-mgmt-LIF`**
   - Wenn Sie IPv6 verwenden: **`https://[cluster-mgmt-LIF]`**

     > Für den Browserzugriff auf System Manager wird ausschließlich HTTPS unterstützt.

   Wenn der Cluster ein selbstsigniertes digitales Zertifikat verwendet, zeigt der Browser möglicherweise eine

Warnung an, dass das Zertifikat nicht vertrauenswürdig ist. Es besteht die Möglichkeit, entweder das Risiko zu akzeptieren, um den Zugriff fortzusetzen, oder ein von einer Zertifizierungsstelle (CA) signiertes digitales Zertifikat auf dem Cluster für die Server-Authentifizierung zu installieren.

2. **Optional:** Wenn ein Zugriffsbanner über die CLI konfiguriert wurde, erscheint eine Meldung im **Warnungs** -Dialogfeld, und die gewünschte Option kann ausgewählt werden, um fortzufahren.

   Diese Option wird auf Systemen, auf denen die Security Assertion Markup Language (SAML) Authentifizierung aktiviert ist, nicht unterstützt.

   - Wenn Sie nicht fortfahren möchten, auf **Abbrechen** klicken und den Browser schließen.
   - Wenn Sie fortfahren möchten, klicken Sie auf **OK**, um zur System Manager-Anmeldeseite zu gelangen.

3. Melden Sie sich mit Ihren Cluster-Administrator-Anmeldeinformationen beim System Manager an.

   Ab ONTAP 9.11.1 kann beim Anmelden am System Manager das Gebietsschema festgelegt werden. Das Gebietsschema legt bestimmte Lokalisierungseinstellungen fest, wie Sprache, Währung, Zeit- und Datumsformat sowie ähnliche Einstellungen. Für ONTAP 9.10.1 und frühere Versionen wird das Gebietsschema für den System Manager vom Browser erkannt. Um das Gebietsschema für den System Manager zu ändern, muss das Gebietsschema des Browsers geändert werden.

4. **Optional**: Ab ONTAP 9.12.1 kann eine Präferenz für das Erscheinungsbild von System Manager angegeben werden:

   a. In der oberen rechten Ecke des System Manager auf klicken, um die Benutzeroptionen zu verwalten.

   b. Den Schalter für das **Systemdesign** entsprechend der eigenen Präferenz positionieren:

Position umschalten	Einstellung für das Erscheinungsbild
(links)	Helles Design (heller Hintergrund mit dunklem Text)
OS (Mitte)	Standardmäßig wird die Designeinstellung verwendet, die für die Anwendungen des Betriebssystems festgelegt wurde (in der Regel die Designeinstellung des Browsers, mit dem auf System Manager zugegriffen wird).
(Rechts)	Dunkles Design (dunkler Hintergrund mit hellem Text)

Verwandte Informationen

"Verwaltung des Zugriffs auf Webdienste"

"Zugriff auf die Log-, Core-Dump- und MIB-Dateien eines Knotens über einen Webbrowser"

Protokolle auf Ihrem ONTAP Cluster konfigurieren

Abhängig von den auf Ihrem Cluster aktivierten Lizenzen können die gewünschten Protokolle auf Ihrem Cluster aktiviert werden. Anschließend werden Netzwerkschnittstellen erstellt, über die auf den Speicher zugegriffen werden kann.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu folgen, um mithilfe des System Manager ein ONTAP Cluster einzurichten. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Schritt

1. **Dashboard** auswählen und anschließend auf **Protokolle konfigurieren** klicken.
   - Zur Aktivierung von NAS-Protokollen **NFS** oder **SMB** auswählen.
   - Zur Aktivierung von SAN-Protokollen **iSCSI** oder **FC** auswählen.
   - Zur Aktivierung von NVMe-Protokollen **NVMe** auswählen.

Neue Funktionen lassen sich durch das Hinzufügen von Lizenzschlüsseln mit ONTAP System Manager aktivieren.

In Versionen vor ONTAP 9.10.1 werden ONTAP-Funktionen mit Lizenzschlüsseln aktiviert, und Funktionen in ONTAP 9.10.1 und später werden mit einer NetApp Lizenzdatei aktiviert. Lizenzschlüssel und NetApp Lizenzdateien können mithilfe des System Manager hinzugefügt werden.

Ab ONTAP 9.10.1 wird der System Manager verwendet, um eine NetApp License File zu installieren und so mehrere lizenzierte Funktionen gleichzeitig zu aktivieren. Die Verwendung einer NetApp License File vereinfacht die Lizenzinstallation, da separate Lizenzschlüssel für einzelne Funktionen nicht mehr hinzugefügt werden müssen. Die NetApp License File wird von der NetApp Support Site heruntergeladen.

Wenn Sie bereits Lizenzschlüssel für bestimmte Funktionen besitzen und auf ONTAP 9.10.1 aktualisieren, können Sie diese Lizenzschlüssel weiterhin verwenden.

Schritte

1. **Cluster > Einstellungen** auswählen.
2. Unter **Lizenzen** → auswählen.
3. Wählen Sie **Durchsuchen**. Wählen Sie die heruntergeladene NetApp Lizenzdatei aus.
4. Wenn Lizenzschlüssel hinzugefügt werden sollen, **28-stellige Lizenzschlüssel verwenden** auswählen und die Schlüssel eingeben.

Eine Clusterkonfiguration mit ONTAP System Manager herunterladen

Ab ONTAP 9.11.1 kann mit dem System Manager eine Auswahl an Konfigurationsdetails zum Cluster und seinen Nodes heruntergeladen werden. Diese Informationen können für die Bestandsverwaltung, den Hardwareaustausch und Lebenszyklusaktivitäten genutzt werden. Diese Informationen sind besonders hilfreich für Standorte, die keine AutoSupport (ASUP) Daten senden.

Zu den Clusterkonfigurationsdetails gehören der Clustername, die Cluster ONTAP Version, die Cluster-Management-LIF, das Volume und die Anzahl der LIF.

Zu den Konfigurationsdetails des Knotens gehören der Node-Name, die Systemseriennummer, die System-ID, das Systemmodell, die ONTAP Version, MetroCluster-Informationen, SP/BMC-Netzwerkinformationen und Informationen zur Verschlüsselungskonfiguration.

Schritte

1. **Cluster > Übersicht** auswählen.
2. Klicken Sie auf 

, um das Dropdown-Menü anzuzeigen.
3. **Download configuration** auswählen.
4. Wählen Sie die HA Paare aus, dann auf **Herunterladen** klicken.

   Die Konfiguration wird als Excel-Tabelle heruntergeladen.

   - Das erste Blatt enthält Clusterdetails.
   - Die anderen Blätter enthalten Knotendetails.

Tags einem Cluster mit ONTAP System Manager zuweisen

Ab ONTAP 9.14.1 kann mit dem System Manager einem Cluster ein Tag zugewiesen werden, um Objekte als zu einer Kategorie wie Projekten oder Kostenstellen zugehörig zu kennzeichnen.

Über diese Aufgabe

Sie können einem Cluster ein Tag zuweisen. Zuerst muss das Tag definiert und hinzugefügt werden. Anschließend kann das Tag auch bearbeitet oder gelöscht werden.

Tags können beim Erstellen eines Clusters oder auch später hinzugefügt werden.

Ein Tag wird definiert, indem ein Schlüssel angegeben und ihm ein Wert im Format “key:value” zugeordnet wird. Beispielsweise “dept:engineering” oder “location:san-jose”.

Folgendes sollte beim Erstellen von Tags beachtet werden:

- Schlüssel müssen mindestens ein Zeichen lang sein und dürfen nicht null sein. Werte können null sein.
- Ein Schlüssel kann mit mehreren Werten verknüpft werden, indem die Werte durch ein Komma getrennt werden, zum Beispiel “location:san-jose,toronto”
- Tags können für mehrere Ressourcen verwendet werden.
- Die Schlüssel müssen mit einem Kleinbuchstaben beginnen.

Schritte

Zur Verwaltung von Tags sind die folgenden Schritte erforderlich:

1. Im System Manager auf **Cluster** klicken, um die Übersichtsseite anzuzeigen.

   Die Tags sind im Abschnitt **Tags** aufgelistet.

2. **Tags verwalten** ermöglicht das Ändern vorhandener Tags oder das Hinzufügen neuer Tags.

   Sie können die Tags hinzufügen, bearbeiten oder löschen.

Um diese Aktion durchzuführen…	Führen Sie diese Schritte aus…

Tag hinzufügen	a. **Tag hinzufügen** auswählen. b. Einen Schlüssel und dessen Wert oder Werte angeben (mehrere Werte durch Kommas trennen). c. Auf **Speichern** klicken.
Einen Tag bearbeiten	a. Den Inhalt in den Feldern **Schlüssel** und **Werte (optional)** anpassen. b. Auf **Speichern** klicken.
Tag löschen	a. Klicken Sie neben das Tag, das Sie löschen möchten.

Supportfälle mit ONTAP System Manager anzeigen und einreichen

Ab ONTAP 9.9.1 ist es möglich, Supportfälle aus Active IQ Digital Advisor (auch bekannt als Digital Advisor), die mit dem Cluster verknüpft sind, anzuzeigen. Es besteht außerdem die Möglichkeit, Clusterdetails zu kopieren, die für das Einreichen eines neuen Supportfalls auf der NetApp Support Site benötigt werden. Ab ONTAP 9.10.1 kann die Telemetrieprotokollierung aktiviert werden, wodurch das Supportpersonal bei der Problembehebung unterstützt wird.

Um Benachrichtigungen über Firmware-Updates zu erhalten, müssen Sie bei Active IQ Unified Manager registriert sein. Weitere Informationen unter "Active IQ Unified Manager Dokumentationsressourcen".

Schritte

1. Im System Manager **Support** auswählen.

   Eine Liste der offenen Supportfälle, die mit diesem Cluster verknüpft sind, wird angezeigt.

2. Klicken Sie auf die folgenden Links, um die Verfahren auszuführen:
   - **Fallnummer**: Details zum Fall.
   - **Zur NetApp Support-Website**: Auf der Seite **My AutoSupport** der NetApp Support-Website können Wissensdatenbankartikel angezeigt oder ein neuer Supportfall eingereicht werden.
   - **Meine Fälle anzeigen**: Zur Seite **Meine Fälle** auf der NetApp Support-Website navigieren.
   - **Clusterdetails anzeigen**: Informationen, die für die Einreichung eines neuen Falls benötigt werden, können hier angezeigt und kopiert werden.

Telemetrie-Protokollierung aktivieren

Ab ONTAP 9.10.1 kann die Telemetrieprotokollierung mit System Manager aktiviert werden. Wenn die Telemetrieprotokollierung erlaubt ist, erhalten die vom System Manager protokollierten Meldungen eine spezifische Telemetrie-Kennung, die den genauen Prozess angibt, der die Meldung ausgelöst hat. Alle Meldungen, die sich auf diesen Prozess beziehen, haben dieselbe Kennung, die aus dem Namen des operativen Workflows und einer Nummer besteht (zum Beispiel „add-volume-1941290“).

Bei Leistungsproblemen kann die Telemetrieprotokollierung aktiviert werden, wodurch Support-Personal den jeweiligen Prozess, für den eine Meldung ausgegeben wurde, leichter identifizieren kann. Wenn Telemetrie-Kennungen zu den Meldungen hinzugefügt werden, vergrößert sich die Protokolldatei nur geringfügig.

Schritte

1. Im System Manager **Cluster > Einstellungen** auswählen.
2. Im Abschnitt **UI Settings** das Kästchen für **Allow telemetry logging** aktivieren.

Die maximale Kapazitätsgrenze einer Storage-VM im ONTAP System Manager verwalten

Ab ONTAP 9.13.1 kann mit System Manager eine maximale Kapazitätsgrenze für eine Storage-VM aktiviert und ein Schwellenwert festgelegt werden, der Warnungen auslöst, wenn der belegte Speicher einen bestimmten Prozentsatz der maximalen Kapazität erreicht.

Eine maximale Kapazitätsgrenze für eine Storage-VM aktivieren

Ab ONTAP 9.13.1 können Sie die maximale Kapazität festlegen, die allen Volumes in einer Storage-VM zugewiesen werden kann. Die maximale Kapazität kann beim Hinzufügen einer Storage-VM oder beim Bearbeiten einer vorhandenen Storage-VM aktiviert werden.

Schritte

1. Wählen Sie **Storage** > **Storage VMs**.
2. Einer der folgenden Schritte kann durchgeführt werden:
   - Um eine Storage-VM hinzuzufügen, + Add auswählen.
   - Um eine Storage-VM zu bearbeiten, ⋮ neben dem Namen der Storage-VM auswählen und anschließend auf **Bearbeiten** klicken.
3. Geben Sie die Einstellungen für die Storage-VM ein oder ändern Sie diese und aktivieren Sie das Kästchen mit der Bezeichnung „Maximale Kapazitätsgrenze aktivieren“.
4. Geben Sie die maximale Kapazitätsgröße an.
5. Geben Sie den Prozentsatz der maximalen Kapazität an, den Sie als Schwellenwert für die Auslösung von Warnmeldungen verwenden möchten.
6. Auf **Speichern** klicken.

Die maximale Kapazitätsgrenze einer Storage-VM bearbeiten

Ab ONTAP 9.13.1 kann das maximale Kapazitätslimit einer bestehenden Storage-VM bearbeitet werden, wenn das Das maximale Kapazitätslimit wurde aktiviert. bereits besteht.

Schritte

1. Wählen Sie **Storage** > **Storage VMs**.
2. Klicken Sie ⋮ neben den Namen der Storage-VM und dann auf **Bearbeiten**.

   Das Kästchen mit der Bezeichnung „Maximale Kapazitätsgrenze aktivieren“ ist bereits aktiviert.
3. Einer der folgenden Schritte kann durchgeführt werden:

Aktion	Schritte
Maximale Kapazitätsbegrenzung deaktivieren	1. Deaktivieren Sie das Kästchen. 2. Auf **Speichern** klicken.

Die maximale Kapazitätsgrenze anpassen	1. Geben Sie die neue maximale Kapazitätsgröße an. (Es kann keine Größe angegeben werden, die kleiner ist als der bereits zugewiesene Speicherplatz in der Storage-VM.) 2. Geben Sie den neuen Prozentsatz der maximalen Kapazität an, den Sie als Schwellenwert zur Auslösung von Warnmeldungen verwenden möchten. 3. Auf **Speichern** klicken.

Verwandte Informationen

- "Maximale Kapazitätsgrenze einer Storage-VM anzeigen"
- "Kapazitätsmessungen im System Manager"
- "SVM Kapazitätsgrenzen verwalten"

Cluster-, Tier- und SVM-Kapazität im ONTAP System Manager überwachen

Mit System Manager kann überwacht werden, wie viel Speicherkapazität genutzt wurde und wie viel noch für einen Cluster, eine lokale Tier oder eine Storage-VM verfügbar ist.

Mit jeder Version von ONTAP stellt System Manager umfassendere Informationen zur Kapazitätsüberwachung bereit:

- Ab ONTAP 9.13.1 kann eine maximale Kapazitätsgrenze für eine Storage-VM aktiviert und ein Schwellenwert festgelegt werden, der Warnmeldungen auslöst, wenn der genutzte Speicher einen bestimmten Prozentsatz der maximalen Kapazität erreicht.
- Ab ONTAP 9.12.1 zeigt System Manager die für eine lokale Ebene zugesicherte Kapazität an.
- Ab ONTAP 9.10.1 ermöglicht System Manager die Anzeige historischer Daten zur Clusterkapazität sowie Prognosen dazu, wie viel Kapazität in Zukunft genutzt oder verfügbar sein wird. Außerdem kann die Kapazität lokaler Tiers und Volumes überwacht werden.

Die Anzeige der genutzten Kapazität variiert je nach ONTAP Version. Weitere Informationen in "Kapazitätsmessungen im System Manager".

Kapazität eines Clusters anzeigen

Kapazitätsmessungen für einen Cluster sind im System Manager auf dem Dashboard einsehbar.

Bevor Sie beginnen

Um Daten zur Kapazität in der Cloud anzuzeigen, ist ein Konto bei Digital Advisor erforderlich und eine Verbindung muss bestehen.

Schritte

1. Im System Manager auf **Dashboard** klicken.
2. Im Abschnitt **Kapazität** sind die folgenden Informationen verfügbar:
    - Gesamtkapazität des genutzten Speicherplatzes im Cluster
    - Gesamte verfügbare Kapazität des Clusters
    - Prozentsätze der genutzten und verfügbaren Kapazität.

- Verhältnis der Datenreduktion.
- In der Cloud genutzte Kapazität.
- Historie der Kapazitätsauslastung.
- Prognose der Kapazitätsauslastung

> Im System Manager berücksichtigen die Kapazitätsdarstellungen nicht die Kapazitäten der Root-Speicherebene (Aggregate).

3. Klicken Sie auf das Diagramm, um weitere Details zur Kapazität des Clusters anzuzeigen.

   Die Kapazitätsmessungen werden in zwei Balkendiagrammen dargestellt:

   - Das obere Diagramm zeigt die physische Kapazität: die Größe des genutzten, reservierten und verfügbaren physischen Speicherplatzes.
   - Das untere Diagramm zeigt die logische Kapazität: die Größe der Clientdaten, Snapshots und Klone sowie den gesamten logisch belegten Speicherplatz.

   Unterhalb der Balkendiagramme befinden sich Kennzahlen zur Datenreduktion:

   - Datenreduktionsverhältnis nur für die Kundendaten (Snapshots und Klone sind nicht enthalten).
   - Gesamtdatenreduktionsverhältnis.

Weitere Informationen finden sich unter "Kapazitätsmessungen im System Manager".

Kapazität einer lokalen Ebene anzeigen

Sie können Details zur Kapazität lokaler Tiers einsehen. Ab ONTAP 9.12.1 enthält die Ansicht **Kapazität** auch die zugesagte Kapazität für einen lokalen Tier, wodurch sich feststellen lässt, ob Kapazität zum lokalen Tier hinzugefügt werden muss, um die zugesagte Kapazität aufzunehmen und einen Mangel an freiem Speicherplatz zu vermeiden.

Schritte

1. **Speicher > Ebenen** auswählen.
2. Wählen Sie den Namen der lokalen Tier aus.
3. Auf der Seite **Übersicht** wird im Abschnitt **Kapazität** die Kapazität in einem Balkendiagramm mit drei Messwerten dargestellt:
   - Verwendete und reservierte Kapazität
   - Verfügbare Kapazität
   - Zugesicherte Kapazität (beginnend mit ONTAP 9.12.1)
4. Durch Klicken auf das Diagramm werden Details zur Kapazität der lokalen Ebene angezeigt.

   Die Kapazitätsmessungen werden in zwei Balkendiagrammen dargestellt:

   - Das obere Balkendiagramm zeigt die physische Kapazität: die Größe des genutzten, reservierten und verfügbaren physischen Speicherplatzes.
   - Das untere Balkendiagramm zeigt die logische Kapazität: die Größe der Clientdaten, Snapshots und Klone sowie die Gesamtsumme des logisch belegten Speicherplatzes.

   Unterhalb der Balkendiagramme befinden sich die Messverhältnisse zur Datenreduktion:

- Datenreduktionsverhältnis nur für die Kundendaten (Snapshots und Klone sind nicht enthalten).
- Gesamtdatenreduktionsverhältnis.

Weitere Informationen finden sich unter "Kapazitätsmessungen im System Manager".

Optionale Aktionen

- Wenn die zugesicherte Kapazität größer ist als die Kapazität der lokalen Ebene, kann es sinnvoll sein, die Kapazität der lokalen Ebene zu erhöhen, bevor der freie Speicherplatz erschöpft ist. Siehe "Kapazität zu einer lokalen Ebene hinzufügen (Festplatten zu einem Aggregat hinzufügen)".
- Sie können auch den Speicherplatz anzeigen, den bestimmte Volumes in der lokalen Ebene verwenden, indem die Registerkarte **Volumes** ausgewählt wird.

Anzeigen der Datenreduktionsrate

Die Datenreduktionsrate gibt an, um wie viel sich der von Ihren Daten belegte Storage nach der Anwendung von Speichereffizienzfunktionen wie Komprimierung, Verdichtung und Deduplizierung verringert.

Ab ONTAP 9.20.1 wird die Datenreduktionsrate (DRR) mit und ohne reduzierbare Daten angegeben. Reduzierbare Daten sind Daten, bei denen nach Anwendung von Storage-Effizienzfunktionen Speicherplatzeinsparungen erzielt werden. In ONTAP 9.19.1 und früheren Versionen umfasst die DRR sowohl reduzierbare als auch nicht reduzierbare Daten. Nicht reduzierbare Daten sind Daten, bei denen nach Anwendung von Storage-Effizienzfunktionen keine Speicherplatzeinsparungen erzielt werden, oder Daten, auf die Storage-Effizienzfunktionen nicht angewendet werden können. Die DDR ohne reduzierbare Daten bildet den durch ONTAP Storage-Effizienz eingesparten Speicherplatz genauer ab.

Schritte

Sie können die ONTAP CLI oder den System Manager verwenden, um Ihre DRR anzuzeigen.

System Manager

Ab ONTAP 9.13.1 berücksichtigt die im System Manager angezeigte Datenreduktionsrate die Ergebnisse der meisten Storage-Effizienzfunktionen; Snapshots und Thin Provisionierung werden jedoch nicht als Teil des Datenreduktionsverhältnisses gezählt. In ONTAP 9.12.1 und früheren Versionen kann diese Rate auch ohne die Berücksichtigung von Snapshots und Klonen angezeigt werden.

Zur Anzeige des DRR auf Aggregatebene:

1. In System Manager wählen Sie **Storage > Tiers** aus.
2. Die lokale Ebene (Aggregat), für die die DRR angezeigt werden soll, kann ausgewählt werden.

   DRR ist unter **Lokale Kapazitätsstufe** aufgeführt.

Anzeige der DRR auf Cluster-Ebene:

1. In System Manager erfolgt die Auswahl von **Dashboard**.

   Der DRR wird unter Kapazität angezeigt.

CLI

Die Anzeige Ihrer Datenreduktionsrate in der CLI hängt von Ihrer ONTAP Version ab.

> Sie sollten den `df -S` Befehl nicht verwenden, um Ihre Datenreduktionsrate anzuzeigen. Kommt der `df -S` Befehl in einem Automatisierungsprozess zum Einsatz, sollte stattdessen wie gezeigt der Befehl „volume show“ verwendet werden.

ONTAP Version	Um die DRR auf Clusterebene anzuzeigen	Anzeigen von DRR auf Aggregatebene	Anzeigen von DRR auf Volume-Ebene
9.20.1 und später	`cluster-show`	`storage aggregate show-cumulated-efficiency`	• `volume efficiency` • `volume show -volume <vol_name> -vserver <SVM> -fields used, sis-space-saved, dedupe-space-saved, compression-space-saved`
9.19.1 und früher	`cluster-show`	`cluster space show`	`volume show -volume <vol_name> -vserver <SVM> -fields used, sis-space-saved, dedupe-space-saved, compression-space-saved`

Kapazität der Volumes in einer Storage-VM anzeigen

Sie können einsehen, wie viel Speicherplatz von den Volumes einer Storage-VM belegt ist und wie viel Kapazität noch verfügbar ist. Die Gesamtmenge des belegten und verfügbaren Speicherplatzes wird als „Kapazität über alle Volumes“ bezeichnet.

Schritte

1. Wählen Sie **Storage** > **Storage VMs**.
2. Klicken Sie auf den Namen der Storage-VM.
3. Zum Abschnitt **Kapazität** scrollen, der ein Balkendiagramm mit den folgenden Messwerten zeigt:
    - **Physisch genutzt**: Summe des physisch genutzten Speicherplatzes über alle Volumes in dieser Storage-VM.
    - **Verfügbar**: Summe der verfügbaren Kapazität aller Volumes in dieser Storage-VM.
    - **Logisch verwendet**: Summe des logisch verwendeten Speicherplatzes über alle Volumes in dieser Storage-VM.

Weitere Details zu den Messungen sind unter "Kapazitätsmessungen im System Manager" zu finden.

Maximale Kapazitätsgrenze einer Storage-VM anzeigen

Ab ONTAP 9.13.1 ist die maximale Kapazitätsgrenze einer Storage-VM sichtbar.

Bevor Sie beginnen

Sie müssen "Das maximale Kapazitätslimit einer Storage-VM aktivieren" ausführen, bevor Sie es ansehen können.

Schritte

1. Wählen Sie **Storage** > **Storage VMs**.

Die maximalen Kapazitätsmesswerte lassen sich auf zwei Arten anzeigen:

- In der Zeile für die Storage-VM zeigt die Spalte **Maximale Kapazität** ein Balkendiagramm, das die belegte Kapazität, die verfügbare Kapazität und die maximale Kapazität darstellt.
- Klicken Sie auf den Namen der Storage-VM. Auf der Registerkarte **Übersicht** kann in der linken Spalte die maximale Kapazität, die zugewiesene Kapazität und der Kapazitätsalarmschwellenwert eingesehen werden.

Verwandte Informationen

- "Die maximale Kapazitätsgrenze einer Storage-VM bearbeiten"
- "Kapazitätsmessungen im System Manager"

Hardwareprobleme mit dem ONTAP System Manager beheben

Ab ONTAP 9.8 kann mit dem System Manager die Konfiguration der Hardware im Netzwerk angezeigt und der Zustand der Hardwaresysteme und Verkabelungskonfigurationen ermittelt werden.

Schritte

Um die Hardwarekonfigurationen anzuzeigen, sind die folgenden Schritte erforderlich:

1. Im System Manager **Cluster > Hardware** auswählen.
2. Fahren Sie mit der Maus über die Komponenten, um Status und weitere Details anzuzeigen.

   Verschiedene Arten von Informationen sind einsehbar:

   - Informationen zu Controllern
   - Informationen zu Festplattengehäusen
   - Informationen zu Speicherschaltern
3. Ab ONTAP 9.12.1 können Verkabelungsinformationen im System Manager angezeigt werden. Das Kästchen **Show Cables** kann aktiviert werden, um die Verkabelung anzuzeigen. Wenn der Mauszeiger über ein Kabel gehalten wird, werden die Verbindungsinformationen angezeigt.
   - Informationen zur Verkabelung

Informationen zu Controllern

Sie können Folgendes anzeigen:

Nodes

- Sie können die Vorder- und Rückansicht betrachten.
- Bei Modellen mit internem Festplattenfach ist die Festplattenanordnung auch in der Vorderansicht sichtbar.
- Die folgenden Plattformen sind sichtbar:

Plattform	Unterstützt im System Manager in ONTAP Version…										
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8 (nur Vorschaumodus)
AFF A20	Ja	Ja	Ja								
AFF A30	Ja	Ja	Ja								
AFF A50	Ja	Ja	Ja								
AFF A70	Ja	Ja	Ja	Ja							
AFF A90	Ja	Ja	Ja	Ja							
AFF A1K	Ja	Ja	Ja	Ja							
AFF A150				Ja	Ja	Ja					
AFF A220				Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AFF A250				Ja	Ja	Ja	Ja	Ja	Ja	Ja	
AFF A300				Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AFF A320				Ja	Ja	Ja	Ja	Ja	Ja	Ja	
AFF A400				Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AFF A700				Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AFF A700s				Ja	Ja	Ja	Ja	Ja	Ja	Ja	
AFF A800				Ja	Ja	Ja	Ja	Ja	Ja	Ja	
AFF A900	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja		
AFF C30	Ja	Ja	Ja								
AFF C60	Ja	Ja	Ja								
AFF C80	Ja	Ja	Ja								

AFF C190				Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
AFF C250				Ja	Ja	Ja	Ja *	Ja *	Ja *		
AFF C400				Ja	Ja	Ja	Ja *	Ja *	Ja *		
AFF C800	Ja	Ja	Ja	Ja	Ja	Ja	Ja *	Ja *	Ja *		
ASA A150				Ja	Ja	Ja					
ASA A250				Ja	Ja	Ja					
ASA A400				Ja	Ja	Ja					
ASA A800				Ja	Ja	Ja					
ASA A900				Ja	Ja	Ja					
ASA C250	Ja	Ja	Ja	Ja	Ja	Ja					
ASA C400	Ja	Ja	Ja	Ja	Ja	Ja					
ASA C800	Ja	Ja	Ja	Ja	Ja	Ja					
AFX 1X	Ja	Ja									
FAS50	Ja	Ja	Ja								
FAS70	Ja	Ja	Ja	Ja							
FAS90	Ja	Ja	Ja	Ja							
FAS500f				Ja	Ja	Ja	Ja	Ja	Ja	Ja	
FAS2750	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
FAS8300				Ja	Ja	Ja	Ja	Ja			
FAS8700				Ja	Ja	Ja	Ja	Ja			
FAS9000					Ja	Ja	Ja	Ja	Ja		
FAS9500					Ja	Ja	Ja	Ja	Ja		

Ports

- Ein Port wird rot hervorgehoben, wenn er nicht aktiv ist.

- Wenn Sie mit der Maus über den Port fahren, werden der Status des Ports und weitere Details angezeigt.
- Konsolenports können nicht angezeigt werden.

  Anmerkungen:

  - Ab ONTAP 9.11.1 werden SAS-Ports nur dann rot hervorgehoben, wenn sie sich in einem Fehlerzustand befinden oder wenn ein verkabelter Port, der verwendet wird, offline geht. Die Ports erscheinen weiß, wenn sie offline und nicht verkabelt sind.
  - Bei ONTAP 9.10.1 und älteren Versionen sind deaktivierte SAS-Ports rot hervorgehoben.

FRUs

Informationen zu FRUs erscheinen nur, wenn der Zustand einer FRU nicht optimal ist.

- Defekte Netzteile in Knoten oder Gehäusen.
- In den Knoten wurden hohe Temperaturen festgestellt.
- Defekte Lüfter an den Knoten oder am Gehäuse.

Adapterkarten

- Karten mit definierten Teilenummernfeldern werden in den Steckplätzen angezeigt, wenn externe Karten eingelegt wurden.
- Anschlüsse werden auf den Karten angezeigt.
- Für eine unterstützte Karte können Bilder dieser Karte angezeigt werden. Wenn sich die Karte nicht in der Liste der unterstützten Teilenummern befindet, erscheint eine allgemeine Grafik.

Informationen zu Festplattengehäusen

Sie können Folgendes anzeigen:

Festplattenregale

- Die Vorder- und Rückansicht kann angezeigt werden.
- Sie können die folgenden Festplattengehäusemodelle anzeigen:

Wenn Ihr System läuft…	Anschließend kann im System Manager angezeigt werden…
ONTAP 9.9.1 und höher	Alle Regale, die *nicht* als „end of service“ oder „end of availability“ gekennzeichnet sind
ONTAP 9.8	DS4243, DS4486, DS212C, DS2246, DS224C und NS224

Regalanschlüsse

- Sie können den Portstatus einsehen.
- Sie können Informationen zum Remote-Port anzeigen, wenn der Port verbunden ist.

Shelf-FRUs

- Informationen zu Netzteilfehlern werden angezeigt.

Informationen zu Speicherschaltern

Sie können Folgendes anzeigen:

Storage Switches

- Das Display zeigt Schalter, die als Speicherschalter verwendet werden, um Regale mit Knoten zu verbinden.
- Ab ONTAP 9.9.1 zeigt System Manager Informationen über einen Switch an, der sowohl als Storage Switch als auch als Cluster fungiert und auch zwischen Knoten eines HA-Paares gemeinsam genutzt werden kann.
- Die folgenden Informationen werden angezeigt:
  - Switch-Name
  - IP-Adresse
  - Seriennummer
  - SNMP Version
  - Systemversion
- Sie können die folgenden Storage-Switch-Modelle anzeigen:

Wenn Ihr System läuft…	Anschließend kann im System Manager angezeigt werden…
ONTAP 9.11.1 oder höher	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 NVIDIA SN2100
ONTAP 9.10.1 und 9.9.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
ONTAP 9.8	Cisco Nexus 3232C

Storage Switch Ports

- Die folgenden Informationen werden angezeigt:
  - Identitätsname
  - Identitätsindex
  - Status
  - Fernverbindung
  - Weitere Details

Informationen zur Verkabelung

Ab ONTAP 9.12.1 sind die folgenden Verkabelungsinformationen sichtbar:

- **Verkabelung** zwischen Controllern, Switches und Shelves, wenn keine Storage-Bridges verwendet werden
- **Konnektivität**, die die IDs und MAC-Adressen der Ports an beiden Enden des Kabels anzeigt

Knoten mit dem ONTAP System Manager verwalten

Mit dem System Manager können Sie Knoten zu einem Cluster hinzufügen und umbenennen. Sie können außerdem Knoten neu starten, übernehmen und wieder zurückgeben.

Knoten zu einem Cluster hinzufügen

Sie können die Größe und Leistungsfähigkeit Ihres Clusters durch Hinzufügen neuer Knoten erhöhen.

Bevor Sie beginnen

Die neuen Knoten sollten bereits mit dem Cluster verkabelt sein.

Über diese Aufgabe

Für die Arbeit mit System Manager in ONTAP 9.8 und höher oder ONTAP 9.7 existieren separate Prozesse.

ONTAP 9.8 und neuere Verfahren

Hinzufügen von Knoten zu einem Cluster mit System Manager (ONTAP 9.8 und höher)

Schritte

1. **Cluster > Übersicht** auswählen.

   Die neuen Controller werden als Knoten angezeigt, die mit dem Cluster-Netzwerk verbunden sind, aber nicht im Cluster sind.

2. Wählen Sie **Add**.
   - Die Knoten werden dem Cluster hinzugefügt.
   - Speicherplatz wird implizit zugewiesen.

ONTAP 9.7 Verfahren

Hinzufügen von Knoten zu einem Cluster mit System Manager (ONTAP 9.7)

Schritte

1. **(Zur klassischen Version zurückkehren)** auswählen.
2. **Konfigurationen > Clustererweiterung** auswählen.

   System Manager erkennt die neuen Knoten automatisch.

3. **Zur neuen Benutzeroberfläche wechseln** auswählen.
4. **Cluster > Übersicht** zeigt die neuen Nodes an.

Dienstprozessor herunterfahren, neu starten oder bearbeiten

Wenn ein Node neu gestartet oder heruntergefahren wird, führt der HA-Partner automatisch eine Übernahme durch.

> Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu befolgen, um einen Node herunterzufahren und neu zu starten. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Schritte

1. **Cluster > Übersicht** auswählen.
2. Unter **Knoten** ⋮ auswählen.

3. Den Node auswählen und dann **Herunterfahren**, **Neustart** oder **Service Processor bearbeiten** auswählen.

   Wenn ein Node neu gestartet wurde und auf die Rückgabe wartet, ist die Option **Giveback** ebenfalls verfügbar.

   Wenn Sie **Dienstprozessor bearbeiten** auswählen, können Sie **Manuell** wählen, um die IP-Adresse, Subnetzmaske und das Gateway einzugeben, oder Sie können **DHCP** für dynamische Hostkonfiguration wählen.

Knoten umbenennen

Ab ONTAP 9.14.1 kann ein Node-Name von der Cluster-Übersichtsseite aus umbenannt werden.

> Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu folgen, um einen Node umzubenennen. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Schritte

1. **Cluster** auswählen. Die Cluster Übersichtseite wird angezeigt.
2. Nach unten zum Abschnitt **Knoten** scrollen.
3. Neben dem Knoten, den Sie umbenennen möchten, ⋮ auswählen und anschließend **Umbenennen** wählen.
4. Den Node-Name ändern und anschließend **Umbenennen** auswählen.

Lizenzverwaltung

ONTAP-Lizenzierungsübersicht

Eine Lizenz ist ein Nachweis für eine oder mehrere Softwareberechtigungen. Ab ONTAP 9.10.1 werden alle Lizenzen als NetApp Lizenzdatei (NLF) bereitgestellt, bei der es sich um eine einzelne Datei handelt, die mehrere Funktionen aktiviert. Ab Mai 2023 werden alle AFF Systeme (sowohl A-Serie als auch C-Serie) und FAS Systeme entweder mit der ONTAP One Software Suite oder der ONTAP Base Software Suite verkauft, und ab Juni 2023 werden alle ASA Systeme mit ONTAP One für SAN verkauft. Jede Software Suite wird als einzelne NLF bereitgestellt und ersetzt die separaten NLF-Bundles, die erstmals in ONTAP 9.10.1 eingeführt wurden.

In ONTAP One enthaltene Lizenzen

ONTAP One umfasst alle verfügbaren lizenzierten Funktionen. Es enthält eine Kombination der Inhalte der ehemaligen Core Bundle, Data Protection Bundle, Security and Compliance Bundle, Hybrid Cloud Bundle und Encryption Bundle. Verschlüsselung ist in eingeschränkten Ländern nicht verfügbar.

ONTAP Schlüssel enthalten
FlexClone
SnapRestore

NFS, SMB, S3
FC, iSCSI
NVME-oF
Autonomous Ransomware Protection
MTKM
SnapLock
SnapMirror (asynchron, synchron, active sync)
SnapCenter
SnapMirror S3 für NetApp Ziele
SnapMirror Cloud
SnapMirror S3 für Nicht-NetApp-Ziele
NetApp Volume Encryption
Trusted Platform Module

Lizenzen, die nicht in ONTAP One enthalten sind

ONTAP One beinhaltet keine der von NetApp bereitgestellten Cloud-Services, einschließlich der folgenden:

- NetApp Cloud Tiering
- NetApp Backup and Recovery

ONTAP One für bestehende Systeme

Wenn Sie bestehende Systeme haben, die aktuell unter NetApp Support stehen, aber noch nicht auf ONTAP One aktualisiert wurden, bleiben die vorhandenen Lizenzen auf diesen Systemen gültig und funktionieren wie erwartet. Wenn zum Beispiel die SnapMirror Lizenz bereits auf bestehenden Systemen installiert ist, ist kein Upgrade auf ONTAP One erforderlich, um eine neue SnapMirror Lizenz zu erhalten. Wenn jedoch keine SnapMirror Lizenz auf einem bestehenden System installiert ist, kann diese Lizenz nur durch ein kostenpflichtiges Upgrade auf ONTAP One erworben werden.

Ab Juni 2023 können ONTAP-Systeme, die 28-stellige Lizenzschlüssel verwenden, auch "Upgrade auf das ONTAP One oder ONTAP Base Kompatibilitätspundle".

In ONTAP Base enthaltene Lizenzen

ONTAP Base ist eine optionale Software-Suite, die eine Alternative zu ONTAP One für ONTAP Systeme darstellt. Sie ist für spezielle Anwendungsfälle vorgesehen, in denen Datenschutztechnologien wie SnapMirror und SnapCenter sowie Sicherheitsfunktionen wie Autonomous Ransomware nicht erforderlich sind, beispielsweise bei Nicht-Produktionssystemen für dedizierte Test- oder Entwicklungsumgebungen. Zusätzliche Lizenzen können zu ONTAP Base nicht hinzugefügt werden. Wenn zusätzliche Lizenzen wie SnapMirror benötigt werden, ist ein Upgrade auf ONTAP One erforderlich.

ONTAP Schlüssel enthalten
FlexClone
SnapRestore

NFS, SMB, S3
FC, iSCSI
NVME-oF
NetApp Volume Encryption
Trusted Platform Module

Lizenzen, die in ONTAP One für SAN enthalten sind

ONTAP One für SAN ist für ASA A-Series und C-Series Systeme verfügbar. Dies ist die einzige Software Suite, die für SAN verfügbar ist. ONTAP One für SAN enthält die folgenden Lizenzen:

ONTAP Schlüssel enthalten
FlexClone
SnapRestore
FC, iSCSI
NVME-oF
MTKM
SnapLock
SnapMirror (asynchron, synchron, active sync)
SnapCenter
SnapMirror Cloud
NetApp Volume Encryption
Trusted Platform Module

Andere Methoden zur Lizenzbereitstellung

```
In ONTAP 9.0 through ONTAP 9.9.1, license keys are delivered as 28-
character strings, and there is one key per ONTAP feature. You use the
ONTAP CLI to install license keys in these releases.
```

ONTAP 9.10.1 unterstützt die Installation von 28-stelligen Lizenzschlüsseln mit System Manager oder der CLI. Wenn jedoch für eine Funktion eine NLF-Lizenz installiert ist, kann kein 28-stelliger Lizenzschlüssel über die NetApp Lizenzdatei für dieselbe Funktion installiert werden. Informationen zur Installation von NLFs oder Lizenzschlüsseln mit System Manager sind unter "ONTAP-Lizenzen installieren" zu finden.

Verwandte Informationen

"Wie eine ONTAP One Lizenz erhältlich ist, wenn das System bereits NLFs enthält"

"Überprüfung von ONTAP Software-Berechtigungen und zugehörigen Lizenzschlüsseln über die Support-Website"

"NetApp: ONTAP-Berechtigungsrisikostatus"

Lizenzdateien (NLF) von NetApp von der NetApp Support Site herunterladen

Wenn auf Ihrem System ONTAP 9.10.1 oder höher ausgeführt wird, können die Bundle-Lizenzdateien auf bestehenden Systemen durch Herunterladen der NLF für ONTAP One oder ONTAP Core von der NetApp Support Site aktualisiert werden.

Die SnapMirror Cloud- und SnapMirror S3-Lizenzen sind nicht im Lieferumfang von ONTAP One enthalten. Sie sind Teil des ONTAP One Compatibility Bundle, das kostenlos erhältlich ist, wenn ONTAP One und "separat anfordern" vorhanden sind.

Schritte

Sie können ONTAP One-Lizenzdateien für Systeme mit vorhandenen NetApp Lizenzdateipaketen und für Systeme mit 28-stelligen Lizenzschlüsseln herunterladen, die in NetApp Lizenzdateien auf Systemen mit ONTAP 9.10.1 und höher konvertiert wurden. Gegen Gebühr können Sie Systeme auch von ONTAP Base auf ONTAP One aktualisieren. Weitere Informationen zum Herunterladen von NetApp Lizenzdateien finden Sie im KB-Artikel "So laden Sie NLF-Lizenzen von der NetApp Support Site herunter".

Upgrade der bestehenden NLF

1. Wenden Sie sich an Ihr NetApp Vertriebsteam und fordern Sie das Lizenzdateipaket an, das für ein Upgrade oder eine Konvertierung gewünscht wird (zum Beispiel von ONTAP Base zu ONTAP One oder von Core Bundle und Data Protection Bundle zu ONTAP One).

   Wenn Ihre Anfrage bearbeitet wurde, erhalten Sie eine E-Mail von netappsw@netapp.com mit dem Betreff "NetApp Software Licensing Notification for SO# [SO Number]", und die E-Mail enthält einen PDF-Anhang, der Ihre Lizenzseriennummer enthält.

2. Melden Sie sich bei der "NetApp Support Site" an.
3. **Systeme > Softwarelizenzen** auswählen.
4. Im Menü **Seriennummer** auswählen, die erhaltene Seriennummer eingeben und auf **Neue Suche** klicken.
5. Das gewünschte Lizenzpaket zum Konvertieren ermitteln.
6. Für jedes Lizenzpaket auf **Get NetApp License File** klicken und die NLFs herunterladen, sobald sie verfügbar sind.
7. "Installieren"die ONTAP One Datei.

Upgrade NLF aus Lizenzschlüssel konvertiert

1. Melden Sie sich bei der "NetApp Support Site" an.
2. **Systeme > Softwarelizenzen** auswählen.
3. Im Menü **Seriennummer** auswählen, die Seriennummer des Systems eingeben und auf **Neue Suche** klicken.
4. Die gewünschte Lizenz zum Konvertieren in der Spalte **Berechtigung** suchen und dort auf **Prüfen** klicken.
5. Im Formular „Berechtigung prüfen“ die Option „Lizenzen für 9.10.x und höher generieren“ auswählen.
6. Das **Formular zur Überprüfung der Berechtigung** schließen.

Es ist mit einer Wartezeit von mindestens 2 Stunden zu rechnen, bis die Lizenzen generiert sind.

7. Schritte 1 bis 3 wiederholen.
8. Die ONTAP One Lizenz suchen, auf **Get NetApp License File** klicken und die Zustellungsmethode auswählen.
9. "Installieren"die ONTAP One Datei.

Installieren von NetApp-Lizenzen in ONTAP

Es besteht die Möglichkeit, NetApp Lizenzdateien (NLFs) und Lizenzschlüssel mithilfe von System Manager zu installieren, was die bevorzugte Methode für die Installation von NLFs ist, oder die ONTAP CLI zur Installation von Lizenzschlüsseln zu verwenden. In ONTAP 9.10.1 und höher werden Funktionen mit einer NetApp Lizenzdatei aktiviert, während in Versionen vor ONTAP 9.10.1 ONTAP Funktionen mit Lizenzschlüsseln aktiviert werden.

Schritte

Falls Sie bereits "heruntergeladene NetApp Lizenzdateien" oder Lizenzschlüssel besitzen, können Sie mithilfe des System Manager oder der ONTAP CLI NLFs und 28-stellige Lizenzschlüssel installieren.

System Manager – ONTAP 9.8 und höher

1. **Cluster > Einstellungen** auswählen.
2. Unter **Lizenzen** → auswählen.
3. Wählen Sie **Durchsuchen**. Wählen Sie die heruntergeladene NetApp Lizenzdatei aus.
4. Wenn Lizenzschlüssel hinzugefügt werden sollen, **28-stellige Lizenzschlüssel verwenden** auswählen und die Schlüssel eingeben.

System Manager – ONTAP 9.7 und früher

1. **Konfiguration > Cluster > Lizenzen** auswählen.
2. Unter **Lizenzen** → auswählen.
3. Im Fenster **Pakete** auf **Hinzufügen** klicken.
4. Im Dialogfeld **Lizenzpakete hinzufügen** auf **Dateien auswählen** klicken, um die heruntergeladene NetApp Lizenzdatei auszuwählen, und anschließend auf **Hinzufügen** klicken, um die Datei in den Cluster hochzuladen.

CLI

1. Einen oder mehrere Lizenzschlüssel hinzufügen:

   ```
   system license add
   ```

   Das folgende Beispiel installiert Lizenzen vom lokalen Knoten "/mroot/etc/lic_file", falls die Datei an diesem Speicherort existiert:

```
cluster1::> system license add -use-license-file true
```

Das folgende Beispiel fügt dem Cluster eine Liste von Lizenzen mit den Schlüsseln AAAAAAAAAAAAAAAAAAAAAAAAAAAA und BBBBBBBBBBBBBBBBBBBBBBBBBBBB hinzu:

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

Weitere Informationen zum Link:https://docs.netapp.com/us-en/ontap-cli/system-license-add.html[`system license add`^]-Befehl finden sich in der ONTAP-Befehlsreferenz.

ONTAP Lizenzen verwalten

Mit System Manager oder der ONTAP CLI lassen sich die auf Ihrem System installierten Lizenzen anzeigen und verwalten, einschließlich der Anzeige der Lizenz-Seriennummer, der Überprüfung des Lizenzstatus und der Entfernung einer Lizenz.

Details zu einer Lizenz

Schritte

Wie Details zu einer Lizenz angezeigt werden, hängt davon ab, welche Version von ONTAP verwendet wird und ob der System Manager oder die ONTAP CLI genutzt wird.

System Manager – ONTAP 9.8 und höher

1. Details zu einer bestimmten Funktionslizenz sind unter **Cluster > Einstellungen** einsehbar.
2. Unter **Lizenzen** → auswählen.
3. **Funktionen** auswählen.
4. Suchen Sie die lizenzierte Funktion, die angezeigt werden soll, und wählen Sie ⌄ aus, um die Lizenzdetails anzuzeigen.

System Manager – ONTAP 9.7 und früher

1. **Konfiguration > Cluster > Lizenzen** auswählen.
2. Im Fenster **Lizenzen** steht die entsprechende Aktion zur Auswahl:
3. Die Registerkarte **Details** auswählen.

CLI

1. Details zu einer installierten Lizenz:

```
system license show
```

Lizenz löschen

System Manager – ONTAP 9.8 und höher

1. Zum Löschen einer Lizenz **Cluster > Einstellungen** auswählen.
2. Unter **Lizenzen** → auswählen.
3. **Funktionen** auswählen.
4. Wählen Sie die lizenzierte Funktion aus, die Sie löschen möchten, und **Legacy-Schlüssel löschen**.

System Manager – ONTAP 9.7 und früher

1. **Konfiguration > Cluster > Lizenzen** auswählen.
2. Im Fenster **Lizenzen** steht die entsprechende Aktion zur Auswahl:

Wenn Sie möchten…	Folgendes ist zu tun…
Ein bestimmtes Lizenzpaket auf einem Knoten oder eine clusterweite Lizenz löschen	Die Registerkarte **Details** auswählen.
Ein bestimmtes Lizenzpaket auf allen Knoten im Cluster löschen	Auf die Registerkarte **Pakete** wechseln.

3. Wählen Sie das Softwarelizenzpaket aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

   Sie können jeweils nur ein Lizenzpaket löschen.

4. Das Bestätigungs Kästchen auswählen und anschließend auf **Löschen** klicken.

CLI

1. Lizenz löschen:

```
system license delete
```

   Das folgende Beispiel löscht eine Lizenz mit dem Namen CIFS und der Seriennummer 1-81-0000000000000000000123456 aus dem Cluster:

```
cluster1::> system license delete -serial-number 1-81-
0000000000000000000123456 -package CIFS
```

   Das folgende Beispiel löscht aus dem Cluster alle Lizenzen unter dem installierten Lizenzpaket Core Bundle für die Seriennummer 123456789:

```
cluster1::> system license delete { -serial-number 123456789
-installed-license "Core Bundle" }
```

Verwandte Informationen

"ONTAP CLI Befehle zur Lizenzverwaltung"

"ONTAP-Befehlsreferenz"

Lizenzarten und Lizenzierungsverfahren

Das Verständnis der Lizenztypen und der lizenzierten Methode hilft Ihnen bei der Verwaltung der Lizenzen in einem Cluster.

Lizenzarten

Ein Paket kann einen oder mehrere der folgenden Lizenztypen im Cluster installiert haben. Der `system license show` Befehl zeigt den oder die installierten Lizenztypen für ein Paket an.

- Standardlizenz (`license`)

  Eine Standardlizenz ist eine knotengebundene Lizenz. Sie wird für einen Knoten mit einer bestimmten Systemseriennummer (auch als *Controller-Seriennummer* bezeichnet) ausgestellt. Eine Standardlizenz ist nur für den Knoten gültig, der die entsprechende Seriennummer besitzt.

  Die Installation einer standardmäßigen, knotengebundenen Lizenz berechtigt einen Knoten zur Nutzung der lizenzierten Funktionalität. Damit der Cluster die lizenzierte Funktionalität nutzen kann, muss mindestens ein Knoten für die Funktionalität lizenziert sein. Es kann nicht konform sein, lizenzierte Funktionalität auf einem Knoten zu verwenden, der keine Berechtigung für die Funktionalität hat.

- Standortlizenz (`site`)

  Eine Standortlizenz ist nicht an eine bestimmte Systemseriennummer gebunden. Wenn eine Standortlizenz installiert ist, sind alle Knoten im Cluster zur lizenzierten Funktionalität berechtigt. Der `system license show` Befehl zeigt Standortlizenzen unter der Clusterseriennummer an.

  Wenn ein Cluster über eine Standortlizenz verfügt und ein Knoten aus dem Cluster entfernt wird, nimmt der Knoten die Standortlizenz nicht mit und ist nicht mehr berechtigt, die lizenzierte Funktionalität zu nutzen. Wird einem Cluster mit Standortlizenz ein Knoten hinzugefügt, ist dieser Knoten automatisch zur durch die Standortlizenz gewährten Funktionalität berechtigt.

- Evaluierungslizenz (`demo`)

  Eine Evaluierungslizenz ist eine temporäre Lizenz, die nach einem bestimmten Zeitraum abläuft (angegeben durch den `system license show` Befehl). Damit kann bestimmte Softwarefunktionalität ausprobiert werden, ohne eine Berechtigung erwerben zu müssen. Es handelt sich um eine clusterweite Lizenz, die nicht an eine bestimmte Seriennummer eines Knotens gebunden ist.

  Wenn Ihr Cluster über eine Evaluierungslizenz für ein Paket verfügt und Sie einen Knoten aus dem Cluster entfernen, nimmt der Knoten die Evaluierungslizenz nicht mit.

Lizenziertes Verfahren

Es ist möglich, sowohl eine clusterweite Lizenz (die `site` oder `demo`-Typ) als auch eine knotengebundene Lizenz (der `license`-Typ) für ein Paket zu installieren. Daher kann ein installiertes Paket mehrere Lizenztypen im Cluster haben. Für den Cluster gibt es jedoch nur eine *lizenzierte Methode* für ein Paket. Das `licensed method`-Feld des `system license status show`-Befehls zeigt die Berechtigung an, die für ein Paket verwendet wird. Die Lizenzierungsmethode wird durch den Befehl wie folgt bestimmt:

- Wenn für ein Paket nur ein Lizenztyp im Cluster installiert ist, ist der installierte Lizenztyp die lizenzierte Methode.
- Wenn für ein Paket keine Lizenzen im Cluster installiert sind, ist die lizenzierte Methode `none`.
- Wenn für ein 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 eine Standardlizenz und eine Evaluierungslizenz für ein Paket besitzen, ist die Lizenzierungsmethode für das Paket im Cluster `license`.
  - Wenn Sie nur eine Evaluierungslizenz für ein Paket besitzen, ist die Lizenzierungsmethode für das Paket im Cluster `demo`.

Befehle zur Lizenzverwaltung in ONTAP

Sie können die ONTAP CLI `system license`-Befehle verwenden, um Funktionslizenzen für den Cluster zu verwalten. Sie verwenden die `system feature-usage`-Befehle, um die Funktionsnutzung zu überwachen.

Weitere Informationen zu den in diesem Thema beschriebenen Befehlen finden Sie in der "ONTAP-Befehlsreferenz".

Die folgende Tabelle enthält einige der gängigen CLI-Befehle zur Lizenzverwaltung sowie Links zu den Manpages der Befehle für weitere Informationen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Alle Pakete, die Lizenzen benötigen, sowie deren aktuellen Lizenzstatus werden angezeigt, einschließlich der folgenden: • Der Paketname • Das lizenzierte Verfahren • Das Ablaufdatum, falls zutreffend	"system license show-status"
Abgelaufene oder ungenutzte Lizenzen anzeigen oder entfernen	"System License Clean-up"
Zusammenfassung der Funktionsnutzung im Cluster auf Knotenbasis anzeigen	"system feature-usage show-summary"
Anzeige des Nutzungsstatus von Funktionen im Cluster auf Knoten- und Wochenbasis	"system feature-usage show-history"

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Status des Lizenzberechtigungsrisikos für jedes Lizenzpaket anzeigen	"system license entitlement-risk show"

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "NetApp Knowledge Base: ONTAP 9.10.1 und spätere Versionen Lizenzübersicht"
- "Mit dem System Manager lässt sich eine NetApp Lizenzdatei installieren."
- "Systemfunktion"

Clusterverwaltung mit der CLI

Informationen zur Clusterverwaltung mit der ONTAP CLI

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

Diese Vorgehensweise sollte unter folgenden Umständen angewendet werden:

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

Verwandte Informationen

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

Cluster- und SVM-Administratoren

Informationen zu den Administratorrollen für ONTAP Cluster und SVM

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

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

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

Die ONTAP Befehlszeilenschnittstelle (CLI) verwendet weiterhin den Begriff *Vserver* in der

> Ausgabe, und `vserver` als Befehls- oder Parametername wurde nicht geändert.

Webbrowser-Zugriff auf ONTAP System Manager aktivieren oder deaktivieren

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

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

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

Informationen zum ONTAP Cluster Management Server

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

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

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

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

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

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

Arten von SVMs in einem ONTAP Cluster

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

Ein Cluster enthält die folgenden SVM-Typen:

- Admin-SVM

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

- Knoten-SVM

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

- System SVM (erweitert)

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

- Data SVM

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

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

> Sofern nicht anders angegeben, bezieht sich der Begriff SVM auf eine Data (datenservierende) SVM.
>
> In der CLI werden SVMs als Vservers angezeigt.

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

Zugriff auf ein ONTAP Cluster über den seriellen Port

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

Schritte

1. An der Konsole die Eingabetaste drücken.

   Das System antwortet mit der Anmeldeaufforderung.

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

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

   Das System antwortet mit der Aufforderung zur Passworteingabe.

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

Auf einen ONTAP Cluster mit SSH-Anfragen zugreifen

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

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

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

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

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

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

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

SSH Authentifizierungsoptionen

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

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

- Ab ONTAP 9.4 kann "SSH-Multifaktor-Authentifizierung aktivieren" für LDAP- und NIS-Remote-Benutzer verwendet werden.
- Ab ONTAP 9.13.1 können Sie optional die Zertifikatsvalidierung zum SSH-Authentifizierungsprozess hinzufügen, um die Anmeldesicherheit zu erhöhen. Dazu "Ein X.509-Zertifikat mit dem öffentlichen Schlüssel verknüpfen" das ein Konto verwendet, überprüfen. Wenn Sie sich per SSH mit sowohl einem öffentlichen SSH-Schlüssel als auch einem X.509-Zertifikat anmelden, prüft ONTAP die Gültigkeit des X.509-Zertifikats, bevor mit dem öffentlichen SSH-Schlüssel authentifiziert wird. Die SSH-Anmeldung wird verweigert, wenn dieses Zertifikat abgelaufen oder widerrufen ist, und der öffentliche SSH-Schlüssel wird automatisch deaktiviert.
- Ab ONTAP 9.14.1 können ONTAP-Administratoren "Cisco Duo Zwei-Faktor-Authentifizierung zum SSH-Authentifizierungsprozess hinzufügen" die Anmeldesicherheit erhöhen. Nach der Aktivierung der Cisco Duo Authentifizierung müssen Benutzer beim ersten Anmelden ein Gerät als Authentifikator für SSH-Sitzungen registrieren.
- Ab ONTAP 9.15.1 können Administratoren "Dynamische Autorisierung konfigurieren" zusätzliche adaptive Authentifizierung für SSH-Benutzer basierend auf dem Vertrauenswert des Benutzers bereitstellen.
- Ab ONTAP 9.19.1 können Administratoren den "security ssh publickey show -vserver -host-key-algorithm command" verwenden, um den Fingerabdruck des ONTAP-Hostschlüssels anzuzeigen. Dies ermöglicht Administratoren zu überprüfen, ob dieser Fingerabdruck mit dem in ONTAP gespeicherten übereinstimmt.

Schritte

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

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

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

command ist für SSH-interaktive Sitzungen nicht erforderlich.

Beispiele für SSH-Anfragen

Die folgenden Beispiele zeigen, wie das Benutzerkonto mit dem Namen “joe” eine SSH-Anfrage an einen Cluster stellen kann, dessen Cluster-Management-LIF 10.72.137.28 ist:

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

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

Die folgenden Beispiele zeigen, wie das Benutzerkonto mit dem Namen “john” aus der Domäne mit dem Namen “DOMAIN1” eine SSH-Anfrage an einen Cluster stellen kann, dessen Cluster-Management-LIF 10.72.137.28 ist:

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

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

Das folgende Beispiel zeigt, wie das Benutzerkonto mit dem Namen “joe” eine SSH-MFA-Anfrage stellen kann, um auf einen Cluster zuzugreifen, dessen Cluster-Management-LIF 10.72.137.32 ist:

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

Verwandte Informationen

"Administratorauthentifizierung und RBAC"

ONTAP SSH-Anmeldesicherheit

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

Sicherheitsrelevante Informationen werden angezeigt, wenn Sie sich erfolgreich als SSH-Administrator anmelden. Es erfolgt eine Benachrichtigung über die folgenden Bedingungen:

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

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

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

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

Einschränkungen und weitere Überlegungen zur Sicherheit bei der SSH-Anmeldung

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

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

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

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

Beispiele für SSH-Anmeldesicherheitsinformationen

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

- Diese Meldung wird nach jedem erfolgreichen Login angezeigt:

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

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

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

- Diese Meldungen werden angezeigt, wenn es fehlgeschlagene Anmeldeversuche gab und Ihre Berechtigungen seit der letzten erfolgreichen Anmeldung geändert wurden:

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

Telnet- oder RSH-Zugriff auf ein ONTAP Cluster ermöglichen

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

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

Über diese Aufgabe

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

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

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

- Für RSH Befehle sind erweiterte Berechtigungen erforderlich.

ONTAP 9.10.1 oder höher

Schritte

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

   ```
   security protocol show
   ```

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

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

Befehl aktiviert werden:

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

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

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

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

oder

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

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

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

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

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

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

ONTAP 9.9 oder früher

Über diese Aufgabe

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

Schritte

1. In den erweiterten Berechtigungsmodus wechseln:

```
set advanced
```

2. Ein Sicherheitsprotokoll (RSH oder Telnet) aktivieren:

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

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

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

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

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

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

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

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

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

Zugriff auf einen ONTAP Cluster mit Telnet-Anfragen

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

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

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

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

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

ONTAP 9.10.1 oder höher

Schritte

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

```
security protocol show
```

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

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

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

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

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

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

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

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

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

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

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

ONTAP 9.9 oder früher

Bevor Sie beginnen

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

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

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

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

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

Schritte

1. Auf einem Administrationsrechner ist folgender Befehl einzugeben:

```
telnet hostname_or_IP
```

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

Beispiel einer Telnet-Anfrage

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

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Auf einen ONTAP Cluster mit RSH-Anfragen zugreifen

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

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

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

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

- Für RSH Befehle sind erweiterte Berechtigungen erforderlich.

ONTAP 9.10.1 oder höher

Schritte

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

   `security protocol show`

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

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

      `security protocol modify -application rsh -enabled true`

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

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

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

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

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

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

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

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

ONTAP 9.9 oder früher

Bevor Sie beginnen

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

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

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

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

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

Schritte

1. Auf einem Administrationsrechner ist folgender Befehl einzugeben:

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

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

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

Beispiel einer RSH-Anfrage

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

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

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

admin_host$
```

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

Die ONTAP Befehlszeilenschnittstelle verwenden

Informationen zur ONTAP Befehlszeile

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

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

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

```
cluster_name::*>
```

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

Informationen zu den verschiedenen ONTAP Shells für CLI-Befehle

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

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

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

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

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

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

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

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

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

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

Zugriff auf Nodeshell-Befehle und Optionen in der Clustershell

Nodeshell-Befehle und Optionen sind über die Nodeshell zugänglich:

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

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

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

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

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

Verfügbare Nodeshell-Befehle

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

Schritte

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

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

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

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

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

   [*commandname*] help

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

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

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

Beispiel für die Anzeige der verfügbaren Nodeshell-Befehle

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

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

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

Navigation durch die ONTAP CLI-Befehlsverzeichnisse

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

Bei Verwendung der Befehlszeilenschnittstelle (CLI) kann auf ein Befehlsverzeichnis zugegriffen werden,

indem der Name des Verzeichnisses an der Eingabeaufforderung eingegeben und anschließend die Eingabetaste gedrückt wird. Der Verzeichnisname erscheint dann in der Eingabeaufforderung, um anzuzeigen, dass mit dem entsprechenden Befehlsverzeichnis interagiert wird. Um tiefer in die Befehlshierarchie zu gelangen, wird der Name eines Befehlsunterverzeichnisses eingegeben und anschließend die Eingabetaste gedrückt. Der Name des Unterverzeichnisses erscheint dann in der Eingabeaufforderung, und der Kontext wechselt zu diesem Unterverzeichnis.

Sie können durch mehrere Befehlsverzeichnisse navigieren, indem Sie den gesamten Befehl eingeben. Beispielsweise können Sie Informationen über Festplattenlaufwerke anzeigen, indem Sie den `storage disk show` Befehl an der Eingabeaufforderung eingeben. Der Befehl kann auch ausgeführt werden, indem jeweils durch ein Befehlsverzeichnis navigiert wird, wie im folgenden Beispiel dargestellt:

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

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

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

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

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

Verwandte Informationen

- "Spitze"
- "hoch"

Regeln zur Angabe von Werten in ONTAP CLI

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

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

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

- Die CLI interpretiert ein Fragezeichen (`?`) als Befehl zum Anzeigen von Hilfeinformationen für einen bestimmten Befehl.

- Bei einigen Texten, die Sie in der CLI eingeben, wie Befehlsnamen, Parameter und bestimmte Werte, wird nicht zwischen Groß- und Kleinschreibung unterschieden.

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

- Wenn der Wert eines Parameters gelöscht werden soll, der eine Text-String oder eine Liste erwartet, wird ein leeres Paar Anführungszeichen ("") oder ein Bindestrich ("-") angegeben.
- Das Hash-Zeichen (`#`, auch bekannt als Pfundzeichen, kennzeichnet einen Kommentar für eine Befehlszeileneingabe; falls es verwendet wird, sollte es nach dem letzten Parameter in einer Befehlszeile stehen.

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

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

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

Im folgenden Beispiel zeigt ein Befehlszeilenkommentar, der das `#` Zeichen verwendet, an, was der Befehl bewirkt.

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

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

ONTAP Befehlsverlauf anzeigen und jeden Befehl aus dem Verlauf erneut ausführen

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

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

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

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

  Wenn der einzige von Ihnen ausgeführte `volume` Befehl `volume show` war, kann der `redo volume`

Befehl verwendet werden, um den Befehl erneut auszuführen.

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

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

- Ein negativer Offset vom Ende der Verlaufsliste

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

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

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

Verwandte Informationen

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

ONTAP Tastenkombinationen zum Bearbeiten von CLI-Befehlen

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

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

Wenn Sie möchten…	Verwenden Sie eine dieser Tastenkombinationen…
Den Cursor um ein Zeichen zurückbewegen	• Strg+B • Zurück-Pfeil
Den Cursor um ein Zeichen vorwärts bewegen	• Strg-F • Vorwärtspfeil
Den Cursor um ein Wort zurück bewegen	Esc-B
Den Cursor um ein Wort vorwärts bewegen	Esc-F
Den Cursor an den Anfang der Zeile bewegen	Strg+A
Den Cursor an das Ende der Zeile bewegen.	Strg-E

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

Die Berechtigungsstufen für ONTAP CLI-Befehle

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

- **admin**

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

- **fortschrittlich**

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

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

- **Diagnostik**

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

Die Berechtigungsstufe in der ONTAP CLI festlegen

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

Schritte

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

Beispiel für die Festlegung der Berechtigungsstufe

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

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

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

Anzeigeeinstellungen für die ONTAP CLI festlegen

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

Über diese Aufgabe

Sie können die folgenden CLI-Anzeigeeinstellungen festlegen:

- Die Berechtigungsstufe der Befehlssitzung
- Ob Bestätigungen für potenziell unterbrechende Befehle erteilt werden
- Ob `show`Befehle alle Felder anzeigen
- Das oder die als Feldtrennzeichen zu verwendenden Zeichen
- Die Standardeinheit bei der Angabe von Datengrößen
- Die Anzahl der Zeilen, die der Bildschirm in der aktuellen CLI-Sitzung anzeigt, bevor die Schnittstelle die Ausgabe pausiert

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

Schritte

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

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

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

Beispiel für das Festlegen von Anzeigeeinstellungen in der Befehlszeile

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

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

Verwandte Informationen

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

Abfrageoperatoren in der ONTAP CLI verwenden

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

Die folgende Tabelle beschreibt die unterstützten Abfrageoperatoren:

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

Wenn Sie Abfragezeichen als Literale parsen möchten, müssen Sie die Zeichen in doppelte

Anführungszeichen setzen (zum Beispiel `"<10"`, `"0..100"`, `"*abc*"`, oder `"a|b"`), damit die korrekten Ergebnisse zurückgegeben werden.

Dateinamen müssen in doppelte Anführungszeichen gesetzt werden, um die Interpretation von Sonderzeichen zu verhindern. Dies gilt auch für Sonderzeichen, die von der clustershell verwendet werden.

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

Verwandte Informationen

"Tastenkombinationen zum Bearbeiten von CLI-Befehlen"

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

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

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

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

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

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

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

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

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

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

Wenn der `-instance` Parameter mit einem `show` Befehl zur Anzeige von Details verwendet wird, kann die Ausgabe sehr umfangreich sein und mehr Informationen

enthalten, als benötigt werden. Der `-fields` Parameter eines `show` Befehls ermöglicht die Anzeige nur der Informationen, die angegeben werden.

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

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

```
cluster1::> volume show -instance

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

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

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

Die Positionsparameter der ONTAP CLI in der Befehlseingabe verwenden

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

Was ein Positionsparameter ist

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



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

Einen Positionsparameter identifizieren

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

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

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

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

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

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

Beispiele für die Verwendung von Positionsparametern

Im folgenden Beispiel zeigt die ***volume create ?*** Ausgabe, dass drei Parameter für den Befehl positionell sind: `-volume`, `-aggregate` und `-size`.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
```

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

Im folgenden Beispiel wird der `volume create` Befehl angegeben, ohne die Funktionalität der Positionsparameter zu nutzen:

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

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

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

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

Zugriff auf die Manpages der ONTAP CLI

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

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

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

Eine ONTAP CLI Sitzung aufzeichnen und die aufgezeichneten Sitzungen verwalten

Sie können eine CLI-Sitzung in einer Datei mit einem festgelegten Namen und einer

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

Eine CLI-Sitzung aufzeichnen

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

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

Schritte

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

   ```
   system script start
   ```

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

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

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

   ```
   system script stop
   ```

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

   ONTAP beendet die Protokollierung Ihrer CLI-Sitzung.

Befehle zur Verwaltung von Protokollen von CLI-Sitzungen

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

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

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Befehle zur Verwaltung des automatischen Zeitüberschreitungszeitraums von CLI-Sitzungen

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

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

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

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

Verwandte Informationen

"ONTAP-Befehlsreferenz"

Clusterverwaltung (nur für Clusteradministratoren)

Details auf Knotenebene in einem ONTAP Cluster

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

Schritte

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

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

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

Beispiele für die Anzeige der Knoten in einem Cluster

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

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

```
node4                  true    true
```

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

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

cluster1::*> cluster show -node node1

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

ONTAP Cluster-Details auf Clusterebene anzeigen

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

Schritte

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

Beispiel für die Anzeige von Clusterattributen

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

```
cluster1::> cluster identity show

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

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

ONTAP Clusterattribute ändern

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

Über diese Aufgabe

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

Schritte

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

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

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

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

Beispiel für die Umbenennung eines Clusters

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

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

Den Replikationsstatus der ONTAP Clusterringe anzeigen

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

Schritte

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

Beispiel für die Anzeige des Cluster Ring-Replikationsstatus

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

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

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
```

```
        RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

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

ONTAP Cluster-Gesundheitsbewertungen mithilfe von Quorum und Epsilon

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

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

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

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



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

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

Im Allgemeinen gilt: Bei zuverlässiger Verbindung zwischen den Knoten des Clusters ist ein größerer Cluster stabiler als ein kleinerer. Die Quorumsanforderung einer einfachen Mehrheit (die Hälfte der Knoten plus

Epsilon) lässt sich in einem Cluster mit 24 Knoten leichter erfüllen als in einem Zwei-Node-Cluster.

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

Kapazitätsauslastung der Systemvolumes in einem ONTAP Cluster anzeigen

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

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

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

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

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

Knoten verwalten

Knoten zu einem ONTAP Cluster hinzufügen

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

Bevor Sie beginnen

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

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

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

- IP-Adresse
- Netzmaske
- Standardgateway

Über diese Aufgabe

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

Schritte

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

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

```
Welcome to node setup.

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

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

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

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

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

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

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

```
::> cluster setup

Welcome to the cluster setup wizard.

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

You can return to cluster setup at any time by typing "cluster setup".
```

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

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

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

Weitere Informationen zum Einrichten eines Clusters mithilfe der Setup-GUI finden Sie in der "Dokumentation zur Knotenverwaltung". Weitere Informationen zu `cluster setup` finden sich in der "ONTAP-Befehlsreferenz".

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

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

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

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

Nachdem Sie fertig sind

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

Verwandte Informationen

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

Knoten aus einem ONTAP Cluster entfernen

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

Bevor Sie beginnen

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

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

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

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

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

Über diese Aufgabe

- Wenn Sie einen Cluster mit gemischten Versionen betreiben, kann der letzte Node mit niedriger Version mithilfe eines der erweiterten Berechtigungsbefehle ab ONTAP 9.3 entfernt werden:
  - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9.4 und höher: `cluster remove-node -skip-last-low-version-node-check`
- Wenn Sie zwei Knoten aus einem vier-Knoten-Cluster entfernen, wird Cluster HA automatisch auf den beiden verbleibenden Knoten aktiviert.

Alle System- und Benutzerdaten von allen mit dem Knoten verbundenen Festplatten müssen für

die Benutzer unzugänglich gemacht werden, bevor ein Knoten aus dem Cluster entfernt wird.

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

Schritte

1. Ändern Sie die Berechtigungsstufe auf „advanced“:

```
set -privilege advanced
```

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

```
cluster show
```

Im folgenden Beispiel hält "node0" derzeit epsilon:

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

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

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

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

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

4. Aktueller primärer Knoten identifizieren:

```
cluster ring show
```

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

5. Falls der zu entfernende Knoten der aktuelle primäre Knoten ist, kann ein anderer Knoten im Cluster als primärer Knoten gewählt werden:

a. Den aktuellen primären Knoten für die Teilnahme am Cluster als nicht berechtigt markieren:

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

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

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

Wird der Partnerknoten als neuer primärer Knoten ausgewählt, muss vor seiner Deaktivierung überprüft werden, ob er Epsilon enthält. Wenn der Partnerknoten Epsilon enthält, muss Epsilon auf einen anderen, im Cluster verbleibenden Knoten verschoben werden, bevor er deaktiviert wird. Dies geschieht, wenn diese Schritte zum Entfernen des Partnerknotens wiederholt werden.

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

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

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

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

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

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

Das System informiert Sie über Folgendes:

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

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

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

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

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

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

    ```
    set -privilege admin
    ```

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

Verwandte Informationen

- "cluster remove-node"

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

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

Bevor Sie beginnen

- Der Cluster-Management-LIF muss aktiv sein.

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

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

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

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

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

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

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

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

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

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

Über diese Aufgabe

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

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

Schritte

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

     `cluster-mgmt-LIF` ist die IP-Adresse des Cluster-Management-LIF.

2. Wenn der Browser dazu auffordert, Benutzerkonto und Passwort eingeben.

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

Zugriff auf die Systemkonsole eines ONTAP Knotens

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

Verbindung zum SP oder zum Cluster zugänglich.

Über diese Aufgabe

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

Schritte

1. Zugriff auf die Systemkonsole eines Knotens:

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

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

Beispiele für den Zugriff auf die Systemkonsole

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

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

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

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

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

Das folgende Beispiel zeigt das Ergebnis der Eingabe des `system node run-console` Befehls aus ONTAP, um auf die Systemkonsole von node2 zuzugreifen, die an der Boot-Umgebungs-Eingabeaufforderung hängt. Der `boot_ontap` Befehl wird an der Konsole eingegeben, um node2 in ONTAP zu starten. Anschließend wird Strg+D gedrückt, um die Konsole zu verlassen und zu ONTAP zurückzukehren.

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

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

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

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

ONTAP Node-Root-Volumes und Root-Aggregate verwalten

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

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

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

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

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

ONTAP verhindert die Erstellung weiterer Volumes im Root-Aggregat.

"NetApp Hardware Universe"

Speicherplatz auf dem Root-Volume eines Knotens freigeben

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

Schritte

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

   `system node coredump show`

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

   `system node coredump delete`

3. Zugriff auf die Nodeshell:

   `system node run -node nodename`

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

4. Zur erweiterten Berechtigungsstufe der NodeShell wechseln:

   `priv set advanced`

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

      `ls /etc`

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

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

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

      `vol status`

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

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

```
node1*> vol status
```

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

a. Snapshots des Root-Volumes anzeigen:

```
snap list root_vol_name
```

b. Unerwünschte Root-Volume-Snapshots löschen:

```
snap delete root_vol_namesnapshot_name
```

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

```
exit
```

Root-Volumes auf neue Aggregate verschieben

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

Über diese Aufgabe

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

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

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

Schritte

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

```
set privilege advanced
```

2. Das Root-Aggregat verschieben:

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

   - **-Knoten**

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

   - **-disklist**

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

- **-RAID-Typ**

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

3. Den Fortschritt des Jobs überwachen:

   `job show -id jobid -instance`

Ergebnisse

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

Verwandte Informationen

- "storage failover modify"

Einen ONTAP Knoten für Wartungs- oder Fehlerbehebungszwecke starten oder stoppen

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

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

Einen Node an der Systemaufforderung neu starten

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

Schritte

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

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

      `set -privilege advanced`

   b. Ermitteln Sie, welcher Knoten Epsilon enthält:

      `cluster show`

      Das folgende Beispiel zeigt, dass “node1” epsilon enthält:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
```

```
node4                 true    true          false
4 entries were displayed.
```

a. Wenn der neu zu startende Knoten Epsilon enthält, ist Epsilon vom Knoten zu entfernen:

cluster modify -node *node_name* -epsilon false

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

cluster modify -node *node_name* -epsilon true

c. Zurück zur Administrator-Privilegstufe:

set -privilege admin

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

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

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

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

ONTAP an der Eingabeaufforderung der Startumgebung starten

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

Schritte

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

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

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

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

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

Einen Knoten herunterfahren

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

Schritte

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

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

      `set -privilege advanced`

   b. Ermitteln Sie, welcher Knoten Epsilon enthält:

      `cluster show`

      Das folgende Beispiel zeigt, dass “node1” epsilon enthält:

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

   a. Wenn der abzuschaltende Knoten Epsilon enthält, dann Epsilon aus dem Knoten entfernen:

      `cluster modify -node node_name -epsilon false`

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

      `cluster modify -node node_name -epsilon true`

   c. Zurück zur Administrator-Privilegstufe:

      `set -privilege admin`

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

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

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

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

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

Einen ONTAP-Knoten über das Bootmenü verwalten

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

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

Schritte

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

   Der Knoten startet den Neustartvorgang.

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

   Der Knoten zeigt die folgenden Optionen für das Bootmenü an:

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

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

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

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

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

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

Die Attribute der Knoten in einem ONTAP Cluster anzeigen

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

Schritte

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

Beispiel für die Anzeige von Informationen über einen Knoten

Das folgende Beispiel zeigt detaillierte Informationen zu node1:

```
cluster1::> system node show -node node1
                           Node: node1
                          Owner: Eng IT
                       Location: Lab 5
```

```
                          Model: model_number
                  Serial Number: 12345678
                      Asset Tag: -
                         Uptime: 23 days 04:42
                NVRAM System ID: 118051205
                      System ID: 0118051205
                         Vendor: NetApp
                         Health: true
                    Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
   All-Flash Select Optimized: false
SAS2/SAS3 Mixed Stack Support: none
```

Attribute eines ONTAP Knotens ändern

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

Über diese Aufgabe

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

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

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

Schritte

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

Beispiel für die Änderung von Knotenattributen

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

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

Verwandte Informationen

- "system node modify"
- "cluster modify"

Umbenennen eines ONTAP Knotens

Sie können den Namen eines Knotens nach Bedarf ändern.

Schritte

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

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

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

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

Beispiel für das Umbenennen eines Knotens

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

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

Verwaltung eines ONTAP Clusters mit einem einzelnen Knoten

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

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

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

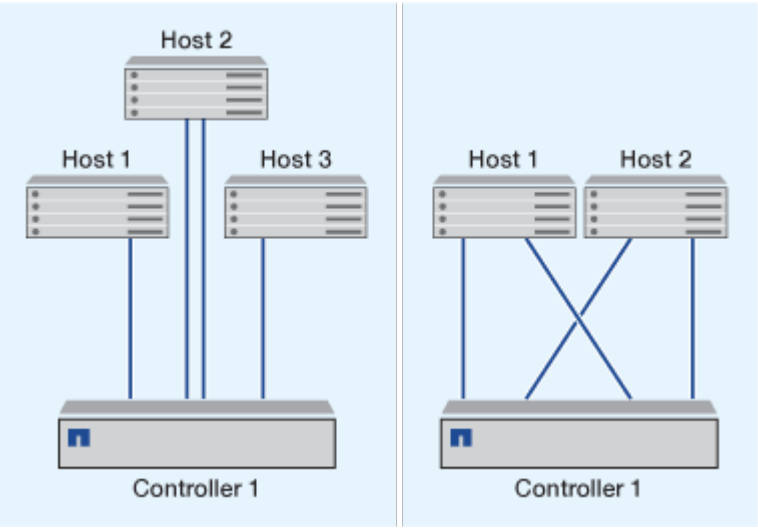
- Die Verschlüsselung des Root-Volumes wird auf Single-Node-Clustern nicht unterstützt.
- Wenn Sie Knoten entfernen, um einen Einzelknoten-Cluster zu erhalten, sollten die Cluster-Ports so modifiziert werden, dass sie den Datenverkehr bedienen, indem die Cluster-Ports in Daten-Ports umgewandelt und anschließend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

Möglichkeiten zur Konfiguration von iSCSI SAN Hosts mit einzelnen Knoten

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

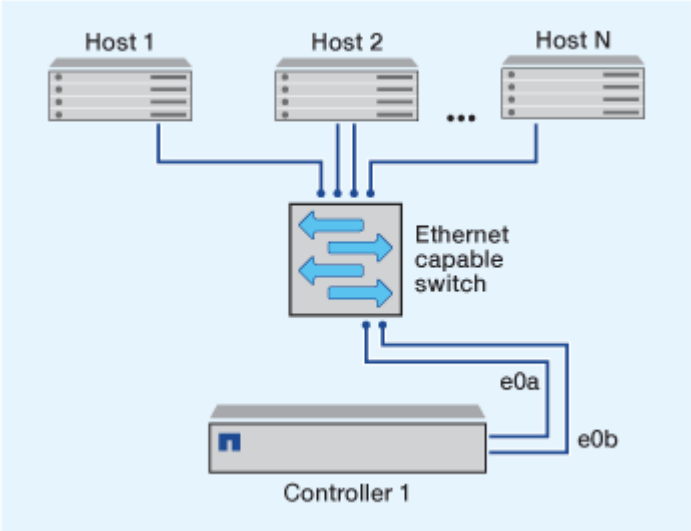
Direkt angeschlossene Single-Node Konfigurationen

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



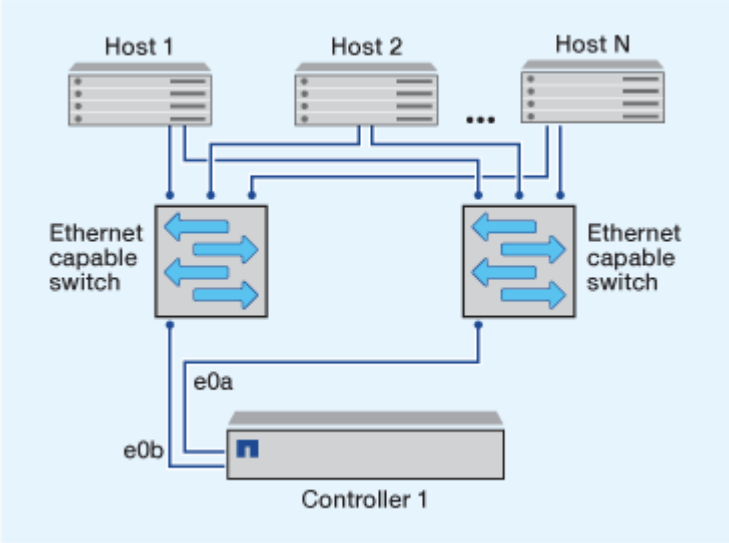
Single-network Single-Node-Konfigurationen

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



Multi-Network Single-Node-Konfigurationen

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



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

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

Single-fabric Single-Node-Konfigurationen

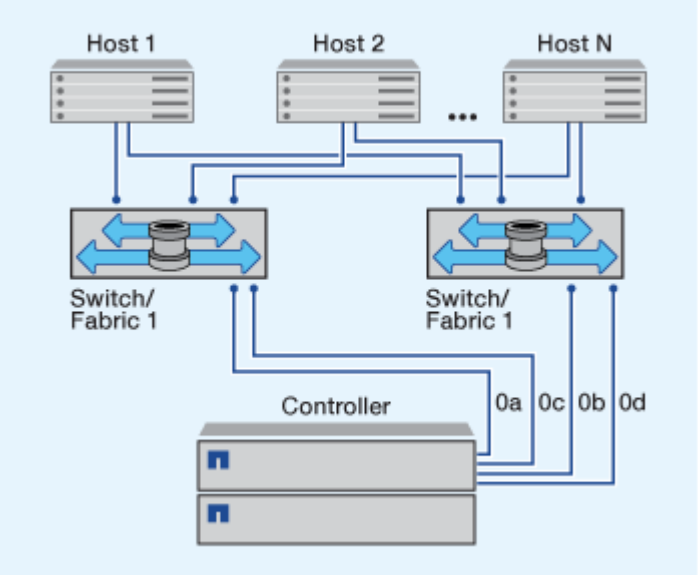
In Single Fabric Single Node Konfigurationen verbindet ein einzelner Switch einen Knoten mit einem oder mehreren Hosts. Da nur ein einziger Switch verwendet wird, ist diese Konfiguration nicht vollständig redundant.

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

Multifabric Einzelknoten-Konfigurationen

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

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



Verwandte Informationen

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

ONTAP Upgrade für Einzelknoten-Cluster

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

Bevor Sie beginnen

Das Upgrade-"Vorbereitung"Schritte müssen abgeschlossen werden.

Schritte

1. Das vorherige ONTAP Softwarepaket löschen:

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

2. Das gewünschte ONTAP Softwarepaket herunterladen:

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

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

Package download completed.
Package processing completed.
```

3. Es sollte sichergestellt sein, dass das Softwarepaket im Cluster-Paket-Repository verfügbar ist:

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

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

4. Es sollte überprüft werden, ob der Cluster für das Upgrade bereit ist:

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

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

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

5. Fortschritt der Validierung überwachen:

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

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

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

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

8. Das Software-Upgrade ausführen:

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



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

9. Fortschritt der Clusteraktualisierung anzeigen:

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

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

10. Benachrichtigung auslösen:

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

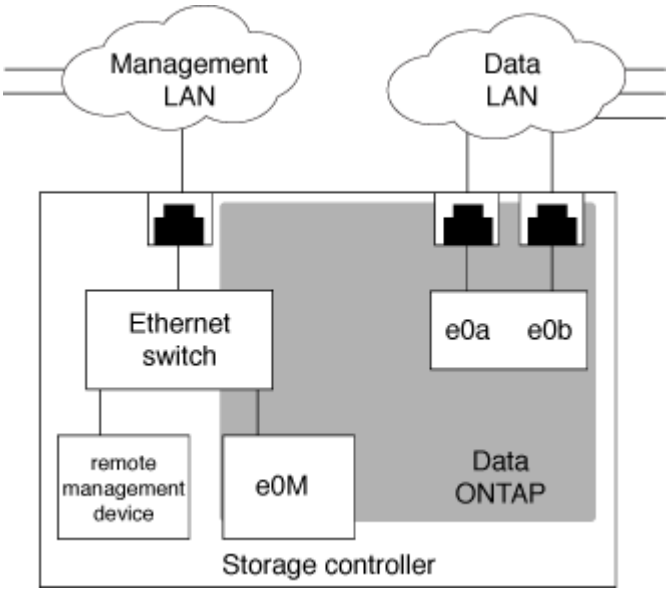
Wenn Ihr Cluster nicht für den Versand von Nachrichten konfiguriert ist, wird eine Kopie der Benachrichtigung lokal gespeichert.

Das SP/BMC-Netzwerk konfigurieren

ONTAP Verwaltungsdatenverkehr im Netzwerk isolieren

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

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



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

Wenn Sie den Management-Datenverkehr nicht isolieren können oder Ihr dediziertes Management-Netzwerk ungewöhnlich groß ist, sollte das Netzwerkverkehrsaufkommen so gering wie möglich gehalten werden.

Übermäßiger eingehender Broadcast- oder Multicast-Datenverkehr kann die Leistung von SP/BMC beeinträchtigen.

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

Informationen zur ONTAP SP/ BMC Netzwerkkonfiguration

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

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

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

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

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

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

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

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

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

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

Szenarien und Überlegungen:

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

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

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

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

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

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

Automatische Netzwerkkonfiguration für ONTAP SP/BMC aktivieren

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

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

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

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

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

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

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

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

Schritte

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

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

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

Das ONTAP SP/BMC Netzwerk manuell konfigurieren

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

Bevor Sie beginnen

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

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

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

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

Schritte

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

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

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

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

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

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

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

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

Beispiel für die Konfiguration des SP Netzwerks

Das folgende Beispiel konfiguriert den SP eines Knotens für die Verwendung von IPv4, aktiviert den SP und zeigt die SP Netzwerkkonfiguration an, um die Einstellungen zu überprüfen:

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

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

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
```

```
          Router Assigned IP Address: -
               Link Local IP Address: -
                  Gateway IP Address: 192.168.123.1
                   Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                         Subnet Name: -
Enable IPv6 Router Assigned Address: -
             SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

Die ONTAP Service Processor API-Konfiguration anpassen

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

Über diese Aufgabe

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

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

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

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

- Der SP API-Service ist standardmäßig aktiviert.

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

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

Schritte

1. Zur erweiterten Berechtigungsstufe wird mit dem `set -privilege advanced` Befehl gewechselt.
2. Die SP API-Service-Konfiguration anpassen:

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

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

Knoten aus der Ferne mit dem SP/BMC verwalten

Einen ONTAP Knoten remote mit dem SP/BMC verwalten

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

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

Remote-Knotenverwaltung mit dem ONTAP Service Processor

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

Zu den wichtigsten Funktionen des SP zählen die folgenden:

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

starten.

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

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

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

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

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

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

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

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

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

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

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

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

  Das SEL enthält die folgenden Informationen:

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

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

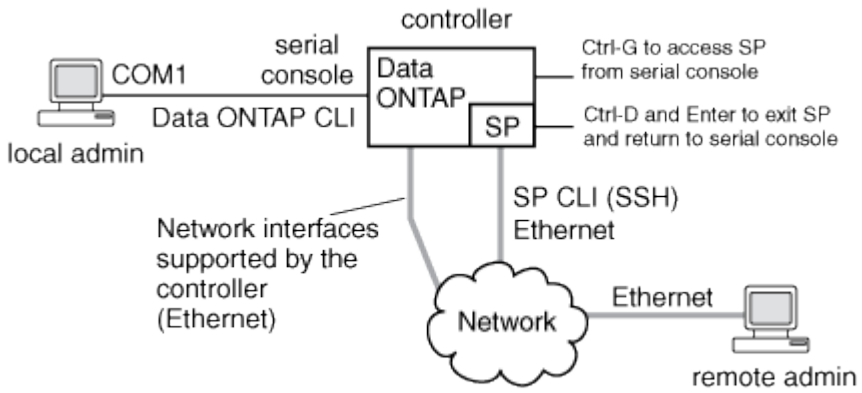
  Wenn Meldungen an die Konsole gesendet werden, speichert der SP diese im Konsole-Protokoll. Das Konsole-Protokoll bleibt so lange erhalten, wie der SP von einem der Knotennetzteile mit Strom versorgt wird. Da der SP mit Standby-Strom arbeitet, bleibt er auch dann verfügbar, wenn der Knoten neu gestartet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

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

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

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

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



Der ONTAP Baseboard Management Controller ermöglicht die Remoteverwaltung eines Knotens.

Auf bestimmten Hardwareplattformen wird die Software angepasst, um einen neuen Onboard-Controller im Baseboard Management Controller (BMC) zu unterstützen. Der BMC verfügt über Befehlszeilenbefehle (CLI), mit denen das Gerät remote verwaltet werden kann.

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

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

Es bestehen einige Unterschiede zwischen SP und BMC:

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

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

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

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

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

  Knotenoperationen werden während eines BMC Neustarts nicht beeinträchtigt.

ONTAP SP/BMC-Firmware-Updates verwalten

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

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

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

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

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

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

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

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

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

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

  Folgende Optionen können angegeben werden:

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

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

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

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

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

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

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

Verwandte Informationen

"NetApp Downloads: System Firmware und Diagnose"

ONTAP SP/BMC und Netzwerkschnittstelle für Firmware-Updates

Ein SP Firmware-Update, das von ONTAP ausgelöst wird und bei dem auf dem SP die Version 1.5, 2.5, 3.1 oder höher ausgeführt wird, unterstützt die Verwendung eines IP-basierten Dateiübertragungsmechanismus über die SP Netzwerkschnittstelle.

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

Ein SP-Firmware-Update über die Netzwerkschnittstelle ist schneller als ein Update über die serielle

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

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

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

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

Verwandte Informationen

"NetApp Downloads: System Firmware und Diagnose"

Zugriff auf den ONTAP Service Processor mit einem Cluster-Benutzerkonto

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

Benutzerkonten für den Zugriff auf den SP werden über ONTAP statt über die SP CLI verwaltet. Ein Cluster-Benutzerkonto kann auf den SP zugreifen, wenn es mit dem `-application` Parameter des `security login create` Befehls auf `service-processor` gesetzt und der `-authmethod` Parameter auf `password` gesetzt ist. Ab ONTAP 9.15.1 kann optional eine Zwei-Faktor-Authentifizierung für ein SP-Konto konfiguriert werden, indem das zweite Authentifizierungsverfahren auf `publickey` mit dem `security login modify` Befehl gesetzt und anschließend der öffentliche Schlüssel mit dem `security login publickey create` Befehl verknüpft wird.

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

- In ONTAP 9.9.1 und späteren Versionen muss `admin` für den `-role` Parameter angegeben werden, und jede Änderung an einem Konto erfordert die `admin` Rolle. Aus Sicherheitsgründen sind andere Rollen nicht mehr zulässig.
  - Wenn ein Upgrade auf ONTAP 9.9.1 oder eine spätere Version durchgeführt wird, siehe "Änderung der Benutzerkonten, die auf den Service Processor zugreifen können".
  - Wenn auf ONTAP 9.8 oder frühere Versionen zurückgegangen wird, siehe "Benutzerkonten, die auf den Serviceprozessor zugreifen können, überprüfen".

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

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

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

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

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

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

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

Bevor Sie beginnen

Folgende Bedingungen müssen erfüllt sein:

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

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

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

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

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

Schritte

1. Vom Administrationshost aus beim SP anmelden:

   `ssh username@SP_IP_address`

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

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

Beispiele für SP Zugriff von einem Administrationshost

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

auf den SP eingerichtet wurde.

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

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

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

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

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

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

```
cluster1::>
```

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

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

(Drücken Sie Strg+D und dann die Eingabetaste, um zur Systemkonsole zurückzukehren.)

```
cluster1::>
```

Wie die ONTAP SP CLI, SP Konsole und Systemkonsolensitzungen zusammenhängen

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

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

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

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

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

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

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

Eingabe der SP-CLI-Anmeldeinformationen.

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

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

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

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Die Hilfeinformationen in der ONTAP SP/BMC CLI anzeigen

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

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

BMC>
```

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

   Das folgende Beispiel zeigt die SP CLI Online-Hilfe für den SP `events`-Befehl.

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

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

```
BMC> system power help
```

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

BMC>
```

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

Verwandte Informationen

- "Ereignisse"
- "Systemstromversorgung"

ONTAP Befehle für die Remote-Knotenverwaltung

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

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

Beispiele

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

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

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

Wenn Sie möchten…	Dieser SP Befehl kann verwendet werden…	Dieser BMC Befehl kann verwendet werden…	Dieser ONTAP Befehl kann verwendet werden…
Verfügbare Befehle oder Unterbefehle eines bestimmten Befehls für SP/BMC/ONTAP	`help` [`command`]	`help` [`command`]	k. A.
Die aktuelle Berechtigungsstufe für die SP/BMC/ONTAP CLI anzeigen	`priv show`	`priv show`	k. A.

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

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

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

`system sensors` {`show`	`filter <sensor_string>` }	`system node environment sensors show`	Status und Details des angegebenen Sensors anzeigen
`system sensors get sensor_name` Sie können `sensor_name` mit dem `system sensors`- oder dem `system sensors show`-Befehl erhalten.	`system sensors` [`get`]	k. A.	Anzeige der SP/BMC/ONTAP-Firmware-Versionsinformationen
`version`	`version`	`system service-processor image show`	SP/BMC/ONTAP-Befehlsverlauf anzeigen

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

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

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

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

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

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

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

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

ONTAP Knotenzustandsüberwachung anhand schwellenwertbasierter SP Sensormesswerte und Status

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

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

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

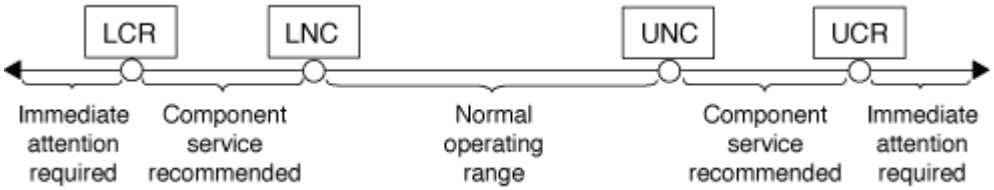
Schwellenwertbasierte Sensoren haben die folgenden Schwellenwerte, die in der Ausgabe des SP `system sensors`-Befehls angezeigt werden:

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

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

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

Das folgende Diagramm veranschaulicht die durch die Schwellenwerte festgelegten Schweregrade:



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

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

Beispiel für die Befehlsausgabe des system sensors-Kommandos

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

```
SP node1> system sensors

Sensor Name       | Current    | Unit        | Status| LCR        | LNC
| UNC        | UCR
------------------+------------+-------------+-------+------------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
CPU1_Temp_Margin | -56.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
In_Flow_Temp      | 32.000     | degrees C   | ok    | 0.000      | 10.000
| 42.000     | 52.000
Out_Flow_Temp     | 38.000     | degrees C   | ok    | 0.000      | 10.000
| 59.000     | 68.000
CPU1_Error        | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Therm_Trip   | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Hot          | 0x0        | discrete    | 0x0180| na         | na
| na         | na
IO_Mid1_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
```

```
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028     | 1.048
| 1.154     | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834     | 0.844
| 1.348     | 1.368
3.3V             | 3.323      | Volts      | ok    | 3.053     | 3.116
| 3.466     | 3.546
5V               | 5.002      | Volts      | ok    | 4.368     | 4.465
| 5.490     | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678     | 1.707
| 1.892     | 1.911
…
```

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

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

```
SP node1> system sensors get 5V

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

ONTAP SP Sensorstatuswerte in der Systemsensor-Befehlsausgabe

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

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

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

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

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

Obwohl der `system sensors get sensor_name` Befehl die Statusinformationen für die meisten diskreten Sensoren anzeigt, liefert er keine Statusinformationen für die diskreten Sensoren System_FW_Status, System_Watchdog, PSU1_Input_Type und PSU2_Input_Type. Die folgenden Informationen dienen zur Interpretation der Statuswerte dieser Sensoren.

System_FW_Status

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

`AA` kann einen der folgenden Werte annehmen:

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

`BB` kann einen der folgenden Werte annehmen:

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

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

System_Watchdog

Der System_Watchdog Sensor kann einen der folgenden Zustände aufweisen:

- **0x0080**

  Der Zustand dieses Sensors hat sich nicht geändert

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

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

auftritt und einen Systemneustart auslöst.

PSU1_Input_Type und PSU2_Input_Type

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

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

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

ONTAP Befehle für das Service Processor Management

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

Befehle zur Verwaltung der SP Netzwerkkonfiguration

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

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

Befehle zur Verwaltung des SP Firmware-Images

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

Befehle zur Verwaltung des SSH-Zugriffs auf den SP

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

Befehle für die allgemeine SP Verwaltung

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

Verwandte Informationen

"ONTAP-Befehlsreferenz"

ONTAP Befehle für BMC Management

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

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

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

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

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

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

Verwandte Informationen

- "System Service Processor"

Unterstützte CLI-Befehle für den ONTAP Baseboard Management Controller

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

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

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

ONTAP Clusterzeit verwalten (nur für Clusteradministratoren)

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

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

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

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

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

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

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

Neben der Verwendung von NTP ermöglicht ONTAP auch die manuelle Verwaltung der Clusterzeit. Diese Funktion ist hilfreich, wenn fehlerhafte Zeitangaben korrigiert werden müssen (zum Beispiel wenn die Zeit

eines Knotens nach einem Neustart erheblich falsch ist). In diesem Fall kann eine ungefähre Zeit für den Cluster angegeben werden, bis NTP mit einem externen Zeitserver synchronisieren kann. Die manuell festgelegte Zeit gilt für alle Knoten im Cluster.

Sie können die Clusterzeit auf folgende Weise manuell verwalten:

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

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

Befehle zur Verwaltung der Clusterzeit

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

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

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

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

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

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

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

Verwandte Informationen

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

Banner und MOTD verwalten

Informationen zum ONTAP Anmeldebanner und zum Text der Nachricht des Tages

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

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

```
$ ssh admin@cluster1-01

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

Password:
```

Eine MOTD (Meldung des Tages) wird in einer Konsolensitzung (nur für Clusterzugriff) oder einer SSH-Sitzung (für Cluster- oder SVM-Zugriff) angezeigt, nachdem ein Benutzer authentifiziert wurde, aber bevor die Clustershell-Eingabeaufforderung erscheint. Zum Beispiel kann die MOTD verwendet werden, um eine Willkommens- oder Informationsnachricht wie die folgende anzuzeigen, die nur authentifizierte Benutzer sehen:

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

Sie können den Inhalt des Banners oder der MOTD mit dem `security login banner modify` oder `security login motd modify` Befehl jeweils auf folgende Weise erstellen oder ändern:

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

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

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

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

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

  - Clustername, Node-Name oder SVM-Name
  - Datum und Uhrzeit des Clusters
  - Name des Benutzers, der sich anmeldet
  - Letzter Login des Benutzers auf einem beliebigen Node im Cluster
  - Anmeldegerätname oder IP-Adresse
  - Name des Betriebssystems
  - Software Release Version

- Effektive Clusterversion-Zeichenfolge

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

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

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

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

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

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

Ein ONTAP Anmeldebanner erstellen

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

Schritte

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

Wenn Sie möchten…	Dann…
Eine Nachricht angeben, die eine einzelne Zeile ist	Verwenden Sie den `-message „<text>“` Parameter, um den Text anzugeben.
Zeilenumbrüche (auch bekannt als Zeilenenden) in die Nachricht einbeziehen	Der Befehl kann ohne den `-message`- oder `-uri` -Parameter verwendet werden, um den interaktiven Modus zum Bearbeiten des Banners zu starten.
Inhalte von einem Speicherort hochladen, um sie für das Banner zu verwenden	Der `-uri`Parameter gibt den FTP- oder HTTP-Speicherort des Inhalts an.

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

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

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

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

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

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

Beispiele für die Erstellung von Bannern

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

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

cluster1::>
```

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

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

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

Das folgende Beispiel zeigt die erstellten Banner:

```
cluster1::> security login banner show
Vserver: cluster1
Message
```

```
------------------------------------------------------------------------
---
Authorized users only!

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

2 entries were displayed.

cluster1::>
```

Verwandte Informationen

- Verwalten des Banners
- "security login banner ändern"
- "Sicherheitsanmeldebanner anzeigen"

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

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

Auswahlmöglichkeiten

- Das Banner auf Clusterebene verwalten:

Wenn Sie möchten…	Dann…
Ein Banner für alle Anmeldesitzungen anzeigen lassen	Banner auf Clusterebene festlegen: `security login banner modify -vserver <cluster_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	Das Banner für alle (Cluster- und SVM-)Logins entfernen
Setzen Sie das Banner auf eine leere Zeichenkette (``): `security login banner modify -vserver * -message`	Ein von einem SVM-Administrator erstelltes Banner überschreiben
Die SVM-Bannernachricht ändern: `security login banner modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }`

- Das Banner auf SVM-Ebene verwalten:

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

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

Verwandte Informationen

- "security login banner ändern"

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

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

Schritte

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

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

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

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

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

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

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

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

   Weitere Informationen zu `security login motd modify` und Parametern, mit denen das MOTD dynamisch generierte Inhalte im "ONTAP-Befehlsreferenz" anzeigen kann.

Beispiele für das Erstellen von MOTDs

Das folgende Beispiel verwendet den nicht-interaktiven Modus, um eine MOTD für das `cluster1` Cluster zu erstellen:

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

Das folgende Beispiel verwendet den interaktiven Modus, um eine MOTD für die `svm1` SVM zu erstellen, die Escape-Sequenzen verwendet, um dynamisch generierte Inhalte anzuzeigen:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

Das folgende Beispiel zeigt die erstellten MOTDs:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
```

```
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

Weitere Informationen zu `security login motd show` finden sich in der "ONTAP-Befehlsreferenz".

Die Verwaltung des Message-of-the-Day-Textes, der auf ONTAP Cluster- und SVM-Ebene angezeigt wird

Sie können die Nachricht des Tages (MOTD) auf Cluster- oder SVM-Ebene verwalten. Standardmäßig ist die für den Cluster konfigurierte MOTD auch für alle SVMs aktiviert. Zusätzlich kann auf SVM-Ebene für jede SVM eine MOTD konfiguriert werden. Die MOTD auf Cluster-Ebene kann vom Clusteradministrator für jede SVM aktiviert oder deaktiviert werden.

Weitere Informationen zu den "Fluchtsequenzen"Funktionen, die zur dynamischen Generierung von Inhalten für die MOTD in der ONTAP-Befehlsreferenz verwendet werden können.

Auswahlmöglichkeiten

- Die MOTD auf Clusterebene verwalten:

Wenn Sie möchten…	Dann…
Eine MOTD für alle Anmeldungen erstellen, wenn noch keine MOTD vorhanden ist.	Eine MOTD auf Clusterebene festlegen: `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	Die MOTD für alle Anmeldungen wird geändert, wenn keine MOTDs auf SVM-Ebene konfiguriert sind.
Die MOTD auf Clusterebene ändern: `security login motd modify -vserver <cluster_name> { [-message "<text>"] }	[-uri <ftp_or_http_addr>] }`
Die MOTD für alle Anmeldungen wird entfernt, wenn keine MOTDs auf SVM-Ebene konfiguriert sind.	Setzen der MOTD auf Clusterebene auf eine leere Zeichenkette (`""`: `security login motd modify -vserver <cluster_name> -message ""`

Wenn Sie möchten…	Dann…
Jede SVM zeigt die MOTD auf Clusterebene an, anstatt die MOTD auf SVM-Ebene zu verwenden.	Eine MOTD auf Clusterebene festlegen und anschließend alle MOTDs auf SVM-Ebene auf eine leere Zeichenkette setzen, wobei die MOTD auf Clusterebene aktiviert ist: a. `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` .. `security login motd modify { -vserver !"<cluster_name>" } -message "" -is -cluster-message-enabled true`	Eine MOTD wird nur für ausgewählte SVMs angezeigt, ohne eine MOTD auf Clusterebene zu verwenden.
Die MOTD auf Clusterebene wird auf eine leere Zeichenkette gesetzt, anschließend werden die MOTDs auf SVM-Ebene für die ausgewählten SVMs festgelegt: a. `security login motd modify -vserver <cluster_name> -message ""` b. `security login motd modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }` + Diesen Schritt können Sie bei Bedarf für jede SVM wiederholen.
Die gleiche SVM-Ebene-MOTD wird für alle (Daten- und Verwaltungs-)SVMs verwendet.	Den Cluster und alle SVMs so einstellen, dass dasselbe MOTD verwendet wird: `security login motd modify -vserver * { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` [NOTE] ==== Im interaktiven Modus fordert die CLI dazu auf, die MOTD für den Cluster und jede SVM einzeln einzugeben. Die gleiche MOTD kann in jede Instanz eingefügt werden, wenn die entsprechende Aufforderung erscheint. ====	Eine MOTD auf Clusterebene soll optional für alle SVMs verfügbar sein, aber nicht bei Cluster-Logins angezeigt werden.
Eine MOTD auf Clusterebene festlegen, aber deren Anzeige für den Cluster deaktivieren: `security login motd modify -vserver <cluster_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] } -is-cluster-message -enabled false`
Entfernen aller MOTDs auf Cluster- und SVM-Ebene, wenn nur einige SVMs sowohl MOTDs auf Cluster- als auch auf SVM-Ebene haben	Für den Cluster und alle SVMs wird eine leere Zeichenkette als MOTD verwendet: `security login motd modify -vserver * -message ""`

Wenn Sie möchten…	Dann…
Die MOTD wird nur für die SVMs geändert, die eine nicht-leere Zeichenkette haben, wenn andere SVMs eine leere Zeichenkette verwenden und auf Clusterebene eine andere MOTD genutzt wird.	Erweiterte Abfragen ermöglichen eine gezielte Änderung der MOTD: `security login motd modify { -vserver !"<cluster_name>" -message !"" } { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	Alle MOTDs, die bestimmten Text enthalten (zum Beispiel „Januar“ gefolgt von „2015“), werden überall in einer ein- oder mehrzeiligen Nachricht angezeigt, selbst wenn der Text auf verschiedene Zeilen verteilt ist.
Eine Abfrage zeigt MOTDs an: `security login motd show -message *"January"*"2015"*`	Interaktiv eine MOTD erstellen, die mehrere und aufeinanderfolgende Zeilenumbrüche (auch bekannt als End-of-Line oder EOLs) enthält

- Das MOTD auf SVM-Ebene verwalten:

  Die Angabe von `-vserver <svm_name>` ist im SVM Kontext nicht erforderlich.

Wenn Sie möchten…	Dann…
Eine andere SVM-Level-MOTD verwenden, wenn die SVM bereits eine vorhandene SVM-Level-MOTD hat	Die MOTD auf SVM-Ebene ändern: `security login motd modify -vserver <svm_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	Nur die Cluster-Ebene MOTD für die SVM verwenden, wenn die SVM bereits eine SVM-Ebene MOTD hat.
Die MOTD auf SVM-Ebene wird auf eine leere Zeichenfolge gesetzt, danach kann der Clusteradministrator die MOTD auf Clusterebene für die SVM aktivieren: a. `security login motd modify -vserver <svm_name> -message ""` b. (Für den Cluster-Administrator) `security login motd modify -vserver <svm_name> -is-cluster-message -enabled true`	Keine MOTD für die SVM anzeigen, wenn sowohl die MOTD auf Cluster-Ebene als auch auf SVM-Ebene derzeit für die SVM angezeigt werden.

Verwandte Informationen

- "security login motd modify"
- "security login motd show"

ONTAP Jobs und Jobpläne verwalten

Aufträge werden in eine Auftragswarteschlange gestellt und im Hintergrund ausgeführt, sobald Ressourcen verfügbar sind. Wenn ein Auftrag zu viele Clusterressourcen verbraucht, kann er gestoppt oder pausiert werden, bis die Auslastung des Clusters sinkt. Auch die Überwachung und das erneute Starten von Aufträgen ist möglich.

Stellenkategorien

Es gibt drei Kategorien von Jobs, die Sie verwalten können: server-affiliierte, cluster-affiliierte und private Jobs.

Ein Job kann in eine der folgenden Kategorien fallen:

- **Serverbezogene Jobs**

  Diese Aufträge werden vom Management-Framework einem bestimmten Knoten zur Ausführung zugewiesen.

- **Cluster-zugeordnete Jobs**

  Diese Aufträge werden vom Management-Framework in eine Warteschlange gestellt, um auf einem beliebigen Knoten im Cluster ausgeführt zu werden.

- **Private Aufträge**

  Diese Jobs sind knotenspezifisch und nutzen weder die replizierte Datenbank (RDB) noch andere Clustermechanismen. Die Befehle zur Verwaltung privater Jobs erfordern die Berechtigungsstufe Advanced oder höher.

Befehle zur Verwaltung von Jobs

Wenn Sie einen Befehl eingeben, der einen Job startet, informiert der Befehl Sie normalerweise darüber, dass der Job in die Warteschlange gestellt wurde, und kehrt dann zur CLI-Befehlszeile zurück. Einige Befehle zeigen jedoch stattdessen den Fortschritt des Jobs an und kehren erst zur CLI-Befehlszeile zurück, wenn der Job abgeschlossen ist. In diesen Fällen kann mit Strg+C der Job in den Hintergrund verschoben werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu allen Jobs	`job show`
Informationen zu Jobs auf Knotenbasis anzeigen	`job show bynode`
Informationen zu clusterbezogenen Jobs	`job show-cluster`
Informationen zu abgeschlossenen Aufträgen anzeigen	`job show-completed`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zur Auftragsverlaufshistorie anzeigen	`job history show` Für jeden Knoten im Cluster werden bis zu 25.000 Auftragsdatensätze gespeichert. Daher kann die Anzeige des vollständigen Auftragsverlaufs längere Zeit in Anspruch nehmen. Um potenziell lange Wartezeiten zu vermeiden, empfiehlt es sich, die Aufträge nach Knoten, Storage Virtual Machine (SVM) oder Datensatz-ID anzuzeigen.
Die Liste der privaten Jobs anzeigen	`job private show` (Erweiterte Berechtigungsstufe)
Informationen zu abgeschlossenen privaten Aufträgen	`job private show-completed` (Erweiterte Berechtigungsstufe)
Informationen zum Initialisierungsstatus für Jobmanager	`job initstate show` (Erweiterte Berechtigungsstufe)
Den Fortschritt eines Auftrags überwachen	`job watch-progress`
Den Fortschritt eines privaten Jobs überwachen	`job private watch-progress` (Erweiterte Berechtigungsstufe)
Einen Job pausieren	`job pause`
Einen privaten Auftrag pausieren	`job private pause` (Erweiterte Berechtigungsstufe)
Einen pausierten Job wieder aufnehmen	`job resume`
Einen pausierten privaten Job wieder aufnehmen	`job private resume` (Erweiterte Berechtigungsstufe)
Einen Job stoppen	`job stop`
Einen privaten Job stoppen	`job private stop` (Erweiterte Berechtigungsstufe)
Einen Job löschen	`job delete`
Einen privaten Job löschen	`job private delete` (Erweiterte Berechtigungsstufe)
Einen einem Cluster zugeordneten Auftrag von einem nicht verfügbaren Knoten, dem er zugeordnet ist, trennen, sodass ein anderer Knoten die Zuständigkeit für diesen Auftrag übernehmen kann	`job unclaim` (Erweiterte Berechtigungsstufe)

Sie können den `event log show` Befehl verwenden, um das Ergebnis eines abgeschlossenen Auftrags zu bestimmen. Weitere Informationen zu `event log show` finden sich in der "ONTAP-Befehlsreferenz".

Befehle zur Verwaltung von Arbeitsplänen

Viele Aufgaben – beispielsweise Volume-Snapshots – können so konfiguriert werden, dass sie nach festgelegten Zeitplänen ausgeführt werden. Zeitpläne, die zu bestimmten Zeiten ausgeführt werden, werden als *Cron-Schedules* (ähnlich wie UNIX `cron`-Schedules) bezeichnet. Zeitpläne, die in Intervallen ausgeführt werden, werden als *Intervall-Schedules* bezeichnet. Sie verwenden die `job schedule` Befehle, um Job-

Schedules zu verwalten.

Jobpläne passen sich nicht an manuelle Änderungen von Datum und Uhrzeit des Clusters an. Diese Jobs werden basierend auf der aktuellen Clusterzeit geplant, die zum Zeitpunkt der Erstellung des Jobs oder der letzten Ausführung galt. Daher empfiehlt es sich, bei manuellen Änderungen von Datum oder Uhrzeit des Clusters die `job show` und `job history show` Befehle zu verwenden, um zu überprüfen, ob alle geplanten Jobs entsprechend Ihren Anforderungen in die Warteschlange gestellt und abgeschlossen wurden.

Wenn der Cluster Teil einer MetroCluster Konfiguration ist, müssen die Jobpläne auf beiden Clustern identisch sein. Daher ist bei Erstellung, Änderung oder Löschung eines Jobplans derselbe Vorgang auch auf dem Remote-Cluster durchzuführen.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu allen Zeitplänen anzeigen	`job schedule show`
Anzeige der Liste der Jobs nach Zeitplan	`job schedule show-jobs`
Informationen zu Cron-Schedules anzeigen	`job schedule cron show`
Informationen zu Intervallplänen	`job schedule interval show`
Einen Cron-Schedule erstellen	`job schedule cron create` Ab ONTAP 9.10.1 kann die SVM in den Jobplan aufgenommen werden.
Intervallplan erstellen	`job schedule interval create` Mindestens einer der folgenden Parameter muss angegeben werden: `-days`, `-hours`, `-minutes` oder `-seconds`.
Einen Cron-Schedule ändern	`job schedule cron modify`
Einen Intervallplan modifizieren	`job schedule interval modify`
Einen Zeitplan löschen	`job schedule delete`
Einen Cron-Schedule löschen	`job schedule cron delete`
Löschen eines Intervallplans	`job schedule interval delete`

Verwandte Informationen

- "Job"

Sichern und Wiederherstellen von Cluster-Konfigurationen (nur für Clusteradministratoren)

Informationen zu ONTAP Konfigurationssicherungsdateien

Konfigurationssicherungsdateien sind Archivdateien (.7z), die Informationen zu allen konfigurierbaren Optionen enthalten, die für den ordnungsgemäßen Betrieb des Clusters und der darin enthaltenen Nodes erforderlich sind.

Diese Dateien speichern die lokale Konfiguration jedes Knotens sowie die clusterweite replizierte Konfiguration. Konfigurationssicherungsdateien werden verwendet, um die Konfiguration des Clusters zu

sichern und wiederherzustellen.

Es gibt zwei Arten von Konfigurationssicherungsdateien:

- **Node-Konfigurationssicherungsdatei**

  Jeder fehlerfreie Knoten im Cluster verfügt über eine Sicherungsdatei der Knotenkonfiguration, die alle Konfigurationsinformationen und Metadaten enthält, die für den fehlerfreien Betrieb des Knotens im Cluster erforderlich sind.

- **Sicherungsdatei für die Cluster-Konfiguration**

  Diese Dateien enthalten ein Archiv aller Node-Konfigurationssicherungsdateien im Cluster sowie die replizierten Clusterkonfigurationsinformationen (die replizierte Datenbank oder RDB-Datei). Clusterkonfigurationssicherungsdateien ermöglichen die Wiederherstellung der Konfiguration des gesamten Clusters oder eines beliebigen Node im Cluster. Die Clusterkonfigurationssicherungspläne erstellen diese Dateien automatisch und speichern sie auf mehreren Nodes im Cluster.

> Konfigurationssicherungsdateien enthalten ausschließlich Konfigurationsinformationen. Sie enthalten keine Benutzerdaten. Informationen zur Wiederherstellung von Benutzerdaten sind unter "Datensicherung" zu finden.

Informationen zur Planung von Backups der ONTAP Cluster- und Knotenkonfigurationsdateien

Drei separate Zeitpläne erstellen automatisch Sicherungsdateien für die Cluster- und Knotenkonfiguration und replizieren sie zwischen den Knoten im Cluster.

Die Konfigurationssicherungsdateien werden automatisch nach folgenden Zeitplänen erstellt:

- Alle 8 Stunden
- Täglich
- Wöchentlich

Zu jedem dieser Zeitpunkte wird auf jedem fehlerfreien Knoten im Cluster eine Sicherungsdatei der Knotenkonfiguration erstellt. Alle diese Sicherungsdateien der Knotenkonfiguration werden anschließend zusammen mit der replizierten Clusterkonfiguration in einer einzigen Clusterkonfigurations-Sicherungsdatei zusammengefasst und auf einem oder mehreren Knoten im Cluster gespeichert.

ONTAP Befehle zur Verwaltung von Konfigurationssicherungszeitplänen

Sie können die `system configuration backup settings` Befehle verwenden, um Sicherungspläne für die Konfiguration zu verwalten.

Diese Befehle sind auf der Zugangsstufe „Erweitert“ verfügbar.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Die Einstellungen für einen Konfigurationssicherungsplan ändern: • Geben Sie eine Remote-URL (HTTP, HTTPS, FTP oder FTPS) an, unter der die Konfigurationssicherungsdateien zusätzlich zu den Standardspeicherorten im Cluster hochgeladen werden. • Ein Benutzername, der für die Anmeldung an der Remote-URL verwendet wird, ist anzugeben. • Die Anzahl der aufzubewahrenden Backups für jeden Konfigurations-Backup-Zeitplan festlegen	`system configuration backup settings modify` Wenn Sie HTTPS in der Remote-URL verwenden, kann die `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatsvalidierung verwendet werden. Die Zertifikatsvalidierung ist standardmäßig deaktiviert. Der Webserver, auf den Sie die Konfigurationssicherungsdatei hochladen, muss PUT-Operationen für HTTP und POST-Operationen für HTTPS aktiviert haben. Weitere Informationen enthält die Dokumentation Ihres Webservers.
Das Passwort festlegen, das für die Anmeldung an der Remote-URL verwendet wird.	`system configuration backup settings set-password`
Die Einstellungen für den Konfigurationssicherungsplan	`system configuration backup settings show` Sie legen den `-instance` Parameter fest, um den Benutzernamen und die Anzahl der aufzubewahrenden Backups für jeden Zeitplan anzuzeigen.

ONTAP Befehle zur Verwaltung von Sicherungsdateien für die Knotenkonfiguration

Sie verwenden die `system configuration backup` Befehle, um Sicherungsdateien für die Cluster- und Knotenkonfiguration zu verwalten.

Diese Befehle sind auf der Zugangsstufe „Erweitert“ verfügbar.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine neue Sicherungsdatei für die Knoten- oder Clusterkonfiguration erstellen	`system configuration backup create`
Kopieren einer Konfigurationssicherungsdatei von einem Knoten auf einen anderen Knoten im Cluster	`system configuration backup copy`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Konfigurationssicherungsdatei von einem Knoten im Cluster auf eine Remote-URL (FTP, HTTP, HTTPS oder FTPS) hochladen	`system configuration backup upload` Wenn Sie HTTPS in der Remote-URL verwenden, kann die `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatsvalidierung verwendet werden. Die Zertifikatsvalidierung ist standardmäßig deaktiviert. Der Webserver, auf den Sie die Konfigurationssicherungsdatei hochladen, muss PUT-Operationen für HTTP und POST-Operationen für HTTPS aktiviert haben. Auf manchen Webservern ist möglicherweise ein zusätzliches Modul erforderlich. Weitere Informationen enthält die Dokumentation Ihres Webservers. Die unterstützten URL-Formate variieren je nach ONTAP Version. Weitere Informationen zu Systemkonfigurationsbefehlen finden Sie im "ONTAP-Befehlsreferenz".
Eine Konfigurationssicherungsdatei kann von einer Remote-URL auf einen Knoten im Cluster heruntergeladen und, falls angegeben, das digitale Zertifikat validiert werden.	`system configuration backup download` Wenn Sie HTTPS in der Remote-URL verwenden, kann die `-validate-certification` Option zum Aktivieren oder Deaktivieren der digitalen Zertifikatsvalidierung verwendet werden. Die Zertifikatsvalidierung ist standardmäßig deaktiviert.
Eine Konfigurationssicherungsdatei auf einem Knoten im Cluster umbenennen	`system configuration backup rename`
Sicherungsdateien der Knoten- und Clusterkonfiguration für einen oder mehrere Knoten im Cluster anzeigen	`system configuration backup show`
Löschen einer Konfigurationssicherungsdatei auf einem Node	`system configuration backup delete` Dieser Befehl löscht die Konfigurationssicherungsdatei nur auf dem angegebenen Knoten. Wenn die Konfigurationssicherungsdatei auch auf anderen Knoten im Cluster vorhanden ist, bleibt sie auf diesen Knoten erhalten.

Verwandte Informationen

- "Sicherung der Systemkonfiguration"

Die ONTAP Knotenkonfigurationssicherungsdatei zum Wiederherstellen eines Knotens finden.

Eine Konfigurationssicherungsdatei, die sich an einer Remote-URL oder auf einem Knoten im Cluster befindet, wird verwendet, um eine Knotenkonfiguration wiederherzustellen.

Über diese Aufgabe

Sie können entweder eine Cluster- oder eine Knoten-Konfigurationssicherungsdatei verwenden, um eine Knoten-Konfiguration wiederherzustellen.

Schritt

1. Die Konfigurationssicherungsdatei muss dem Knoten zur Verfügung stehen, für den die Konfiguration wiederhergestellt werden soll.

Wenn sich die Konfigurationssicherungsdatei befindet…	Dann…
Unter einer entfernten URL	Der `system configuration backup download`-Befehl auf der erweiterten Berechtigungsebene kann verwendet werden, um ihn auf den wiederherzustellenden Node herunterzuladen.
Auf einem Knoten im Cluster	a. Mit dem `system configuration backup show` Befehl auf der Ebene erweiterter Berechtigungen lässt sich die Liste der im Cluster verfügbaren Konfigurationssicherungsdateien anzeigen, die die Konfiguration des wiederherzustellenden Knotens enthalten. b. Falls die von Ihnen angegebene Konfigurationssicherungsdatei auf dem wiederherzustellenden Knoten nicht vorhanden ist, kann der `system configuration backup copy` Befehl verwendet werden, um sie auf den wiederherzustellenden Knoten zu kopieren.

   Wenn Sie den Cluster zuvor neu erstellt haben, sollten Sie eine Konfigurationssicherungsdatei wählen, die nach der Neuerstellung des Clusters erstellt wurde. Falls Sie eine Konfigurationssicherungsdatei verwenden müssen, die vor der Neuerstellung des Clusters erstellt wurde, muss der Cluster nach der Wiederherstellung des Knotens erneut erstellt werden.

Verwandte Informationen

- "Sicherungskopie der Systemkonfiguration"

Einen Node mithilfe der ONTAP Node-Konfigurationssicherungsdatei wiederherstellen

Die Node-Konfiguration wird mithilfe der Konfigurationssicherungsdatei wiederhergestellt, die identifiziert und dem wiederherzustellenden Node zur Verfügung gestellt wurde.

Über diese Aufgabe

Diese Aufgabe sollte nur durchgeführt werden, um sich von einem Desaster zu erholen, das zum Verlust der

lokalen Konfigurationsdateien des Knotens geführt hat.

Schritte

1. Wechsel zur erweiterten Berechtigungsstufe:

   ```
   set -privilege advanced
   ```

2. Wenn der Knoten fehlerfrei ist, kann auf der erweiterten Berechtigungsstufe eines anderen Knotens der `cluster modify` Befehl mit den Parametern `-node` und `-eligibility` verwendet werden, um ihn als nicht berechtigt zu markieren und vom Cluster zu isolieren.

   Wenn der Node nicht in Ordnung ist, sollte dieser Schritt übersprungen werden.

   Dieses Beispiel ändert node2 so, dass es nicht mehr für die Teilnahme am Cluster infrage kommt, damit seine Konfiguration wiederhergestellt werden kann:

   ```
   cluster1::*> cluster modify -node node2 -eligibility false
   ```

   Weitere Informationen zu `cluster modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Der `system configuration recovery node restore` Befehl auf der erweiterten Berechtigungsebene stellt die Konfiguration des Node aus einer Konfigurationssicherungsdatei wieder her.

   Wenn der Knoten seine Identität, einschließlich seines Namens, verloren hat, sollte der `-nodename-in -backup` Parameter verwendet werden, um den Node-Name in der Konfigurationssicherungsdatei anzugeben.

   Dieses Beispiel stellt die Konfiguration des Knotens mithilfe einer der auf dem Knoten gespeicherten Konfigurationssicherungsdateien wieder her:

   ```
   cluster1::*> system configuration recovery node restore -backup
   cluster1.8hour.2011-02-22.18_15_00.7z

   Warning: This command overwrites local configuration files with
            files contained in the specified backup file. Use this
            command only to recover from a disaster that resulted
            in the loss of the local configuration files.
            The node will reboot after restoring the local configuration.
   Do you want to continue? {y|n}: y
   ```

   Die Konfiguration wird wiederhergestellt, und der Node wird neu gestartet.

4. Wenn der Node als nicht geeignet markiert wurde, kann der Node mit dem `system configuration recovery cluster sync` Befehl als geeignet markiert und mit dem Cluster synchronisiert werden.
5. In einer SAN-Umgebung kann der `system node reboot` Befehl verwendet werden, um den Node neu zu starten und das SAN-Quorum wiederherzustellen.

Nachdem Sie fertig sind

Wenn der Cluster zuvor neu erstellt wurde und die Node-Konfiguration mithilfe einer Konfigurationssicherungsdatei wiederhergestellt wird, die vor dieser Neuerstellung des Clusters erstellt wurde, muss der Cluster erneut erstellt werden.

Die Sicherungsdatei der ONTAP Clusterkonfiguration zum Wiederherstellen eines Clusters finden

Zur Wiederherstellung eines Clusters wird die Konfiguration entweder von einem Knoten im Cluster oder aus einer Clusterkonfigurationssicherungsdatei verwendet.

Schritte

1. Wählen Sie einen Konfigurationstyp aus, um den Cluster wiederherzustellen.

   - Ein Knoten im Cluster

     Besteht der Cluster aus mehr als einem Knoten und verfügt einer der Knoten über eine Clusterkonfiguration aus der Zeit, als sich der Cluster in der gewünschten Konfiguration befand, kann der Cluster mithilfe der auf diesem Knoten gespeicherten Konfiguration wiederhergestellt werden.

     In den meisten Fällen ist der Knoten mit dem Replikationsring mit der aktuellsten Transaktions-ID am besten für die Wiederherstellung der Cluster-Konfiguration geeignet. Der `cluster ring show` Befehl auf der erweiterten Berechtigungsstufe ermöglicht die Anzeige einer Liste der auf jedem Knoten im Cluster verfügbaren Replikationsringe.

   - Eine Clusterkonfiguration-Sicherungsdatei

     Wenn Sie keinen Knoten mit der korrekten Clusterkonfiguration identifizieren können oder wenn der Cluster nur aus einem einzigen Knoten besteht, kann eine Sicherungsdatei der Clusterkonfiguration zur Wiederherstellung des Clusters verwendet werden.

   Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, gehen alle seit der Sicherung vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Konfigurationssicherungsdatei und der aktuellen Konfiguration behoben werden. Siehe "NetApp Knowledge Base: ONTAP Konfigurationssicherungs-Resolution Guide" für Hinweise zur Fehlerbehebung.

2. Wenn Sie sich für die Verwendung einer Clusterkonfigurations-Sicherungsdatei entschieden haben, muss die Datei dem Knoten zur Verfügung stehen, den Sie zur Wiederherstellung des Clusters verwenden möchten.

Wenn sich die Konfigurationssicherungsdatei befindet…	**Dann…**
Unter einer entfernten URL	Der `system configuration backup download`-Befehl auf der erweiterten Berechtigungsebene kann verwendet werden, um ihn auf den wiederherzustellenden Node herunterzuladen.

Wenn sich die Konfigurationssicherungsdatei befindet…	Dann…
Auf einem Knoten im Cluster	a. Der `system configuration backup show` Befehl auf der Ebene mit erweiterten Berechtigungen ermöglicht das Auffinden einer Cluster-Konfigurationssicherungsdatei, die erstellt wurde, als sich der Cluster in der gewünschten Konfiguration befand. b. Falls sich die Sicherungsdatei der Clusterkonfiguration nicht auf dem Knoten befindet, den Sie für die Wiederherstellung des Clusters verwenden möchten, dann kann der `system configuration backup copy` Befehl verwendet werden, um sie auf den wiederherzustellenden Knoten zu kopieren.

Verwandte Informationen

- "cluster ring show"
- "Sicherungskopie der Systemkonfiguration"

Einen Cluster mithilfe der ONTAP Clusterkonfigurations-Sicherungsdatei wiederherstellen

Um nach einem Clusterausfall eine Clusterkonfiguration aus einer bestehenden Konfiguration wiederherzustellen, wird der Cluster mithilfe der ausgewählten und dem wiederherstellenden Node zur Verfügung gestellten Clusterkonfiguration neu erstellt, und anschließend wird jeder zusätzliche Node dem neuen Cluster wieder hinzugefügt.

Über diese Aufgabe

Diese Aufgabe sollte nur durchgeführt werden, um sich von einem Desaster zu erholen, das zum Verlust der Cluster-Konfiguration geführt hat.

> Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei neu erstellen, muss der technische Support kontaktiert werden, um etwaige Diskrepanzen zwischen der Konfigurationssicherungsdatei und der im Cluster vorhandenen Konfiguration zu klären.
>
> Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, gehen alle seit der Sicherung vorgenommenen Konfigurationsänderungen verloren. Nach der Wiederherstellung müssen alle Abweichungen zwischen der Konfigurationssicherungsdatei und der aktuellen Konfiguration behoben werden. Siehe "NetApp Knowledge Base: ONTAP Konfigurationssicherungs-Resolution Guide" für Hinweise zur Fehlerbehebung.

Schritte

1. Storage-Failover für jedes HA-Paar deaktivieren:

   `storage failover modify -node` *`node_name`* `-enabled false`

   Das Speicher-Failover muss nur einmal pro HA-Paar deaktiviert werden. Wenn das Speicher-Failover für einen Knoten deaktiviert wird, ist es auch auf dem Partnerknoten deaktiviert.

2. Jeden Knoten außer dem sich erholenden Knoten anhalten:

system node halt -node *node_name* -reason "text"

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   set -privilege advanced

4. Auf dem wiederherstellenden Knoten kann der Cluster mit dem **system configuration recovery cluster recreate** Befehl neu erstellt werden.

   Dieses Beispiel erstellt das Cluster mithilfe der auf dem wiederherstellenden Node gespeicherten Konfigurationsinformationen neu:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

   Auf dem wiederherstellenden Node wird ein neuer Cluster erstellt.

5. Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei wiederherstellen, überprüfen Sie, ob die Clusterwiederherstellung noch läuft:

   system configuration recovery cluster show

   Sie müssen den Wiederherstellungsstatus des Clusters nicht überprüfen, wenn Sie den Cluster von einem fehlerfreien Node aus neu erstellen.

```
cluster1::*> system configuration recovery cluster show
 Recovery Status: in-progress
 Is Recovery Status Persisted: false
```

6. Jeder Node, der dem neu erstellten Cluster wieder beitreten muss, wird neu gestartet.

   Die Knoten müssen einzeln neu gestartet werden.

7. Für jeden Node, der dem neu erstellten Cluster hinzugefügt werden soll, ist Folgendes zu beachten:

   a. Von einem fehlerfreien Node im neu erstellten Cluster aus erfolgt der erneute Beitritt des Ziel-Node:

system configuration recovery cluster rejoin -node *node_name*

Dieses Beispiel fügt den Ziel-Node "node2" dem neu erstellten Cluster wieder hinzu:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
         cluster, potentially overwriting critical cluster
         configuration files. This command should only be used
         to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Der Zielknoten startet neu und tritt anschließend dem Cluster bei.

b. Es sollte sichergestellt werden, dass der Zielknoten fehlerfrei funktioniert und ein Quorum mit den übrigen Knoten im Cluster gebildet wurde:

cluster show -eligibility true

Der Zielknoten muss dem neu erstellten Cluster wieder beitreten, bevor Sie einen anderen Knoten wieder beitreten können.

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. Wenn Sie den Cluster aus einer Konfigurationssicherungsdatei neu erstellt haben, den Wiederherstellungsstatus auf „Abgeschlossen“ setzen:

system configuration recovery cluster modify -recovery-status complete

9. Zurück zur Administrator-Privilegstufe:

set -privilege admin

10. Besteht der Cluster nur aus zwei Knoten, kann der **cluster ha modify** Befehl zum erneuten Aktivieren von Cluster-HA verwendet werden.
11. Mit dem `**storage failover modify**`Befehl lässt sich das Storage-Failover für jedes HA-Paar wieder aktivieren.

Nachdem Sie fertig sind

Wenn der Cluster SnapMirror Peer-Beziehungen aufweist, müssen diese Beziehungen ebenfalls neu erstellt werden. Weitere Informationen finden sich unter "Datensicherung".

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "storage failover modify"

Einen Node mit dem ONTAP Cluster synchronisieren, damit das clusterweite Quorum gewährleistet ist.

Wenn ein clusterweites Quorum vorhanden ist, aber ein oder mehrere Knoten nicht mit dem Cluster synchron sind, muss der Knoten synchronisiert werden, um die replizierte Datenbank (RDB) auf dem Knoten wiederherzustellen und ihn in das Quorum zu bringen.

Schritt

1. Von einem fehlerfreien Knoten aus kann mit dem `system configuration recovery cluster sync` Befehl auf der Ebene mit erweiterten Berechtigungen der Knoten synchronisiert werden, der nicht mit der Clusterkonfiguration übereinstimmt.

   Dieses Beispiel synchronisiert einen Knoten (*node2*) mit dem Rest des Clusters:

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

Ergebnis

Die RDB wird auf den Knoten repliziert, und der Knoten ist somit berechtigt, am Cluster teilzunehmen.

Knoten-Core-Dumps für einen ONTAP Cluster verwalten (nur für Cluster-Administratoren)

Wenn ein Knoten abstürzt, tritt ein Core-Dump auf und das System erstellt eine Core-Dump-Datei, die der technische Support zur Fehlerbehebung verwenden kann. Es besteht die Möglichkeit, die Attribute des Core-Dumps zu konfigurieren oder anzuzeigen. Eine Core-Dump-Datei kann außerdem gespeichert, angezeigt, segmentiert, hochgeladen oder gelöscht werden.

Core Dumps können auf folgende Weise verwaltet werden:

- Konfiguration von Core Dumps und Anzeige der Konfigurationseinstellungen

- Anzeige von grundlegenden Informationen, dem Status und den Attributen von Core Dumps

  Core-Dump-Dateien und Berichte werden im `/mroot/etc/crash/` Verzeichnis eines Knotens gespeichert. Der Verzeichnisinhalt kann mit den `system node coredump` Befehlen oder einem Webbrowser angezeigt werden.

- Speichern des Core-Dump-Inhalts und Hochladen der gespeicherten Datei an einen bestimmten Speicherort oder an den technischen Support

  ONTAP verhindert das Initiieren des Speicherns einer Core-Dump-Datei während einer Übernahme, einer Aggregatverlagerung oder einer Rückgabe.

- Löschen nicht mehr benötigter Core Dump-Dateien

Befehle zur Verwaltung von Core Dumps

Sie verwenden die `system node coredump config` Befehle zur Verwaltung der Konfiguration von Core Dumps, die `system node coredump` Befehle zur Verwaltung der Core Dump-Dateien und die `system node coredump reports` Befehle zur Verwaltung von Application Core Reports.

Weitere Informationen zu den in diesem Thema beschriebenen Befehlen finden Sie in der "ONTAP-Befehlsreferenz".

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Core Dumps konfigurieren	`system node coredump config modify`
Konfigurationseinstellungen für Core Dumps anzeigen	`system node coredump config show`
Grundlegende Informationen zu Core Dumps	`system node coredump show`
Manuelles Auslösen eines Core Dumps beim Neustart eines Knotens	`system node reboot` mit sowohl dem `-dump` als auch dem `-skip-lif-migration-before -reboot` Parameter ⓘ Der Parameter `skip-lif-migration-before-reboot`link: gibt an, dass die LIF-Migration vor einem Neustart übersprungen wird.
Manuelles Auslösen eines Core Dump beim Herunterfahren eines Knotens	`system node halt` mit sowohl dem `-dump` als auch dem `-skip-lif-migration-before -shutdown` Parameter ⓘ Der Parameter `skip-lif-migration-before-shutdown` gibt an, dass die LIF-Migration vor einem Herunterfahren übersprungen wird.
Einen bestimmten Core Dump speichern	`system node coredump save`
Alle nicht gespeicherten Core-Dumps auf einem bestimmten Knoten speichern	`system node coredump save-all`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine AutoSupport-Nachricht mit einer von Ihnen angegebenen Core-Dump-Datei generieren und senden	`system node autosupport invoke-core-upload` Der `-uri`optionale Parameter gibt ein alternatives Ziel für die AutoSupport-Nachricht an.
Statusinformationen zu Core Dumps anzeigen	`system node coredump status`
Löschen eines bestimmten Core Dumps	`system node coredump delete`
Alle ungespeicherten Core-Dumps oder alle gespeicherten Core-Dateien auf einem Knoten löschen	`system node coredump delete-all`
Anwendungs-Core-Dump-Berichte anzeigen	`system node coredump reports show`
Löschen eines Application Core Dump-Berichts	`system node coredump reports delete`

Verwandte Informationen

"ONTAP-Befehlsreferenz"

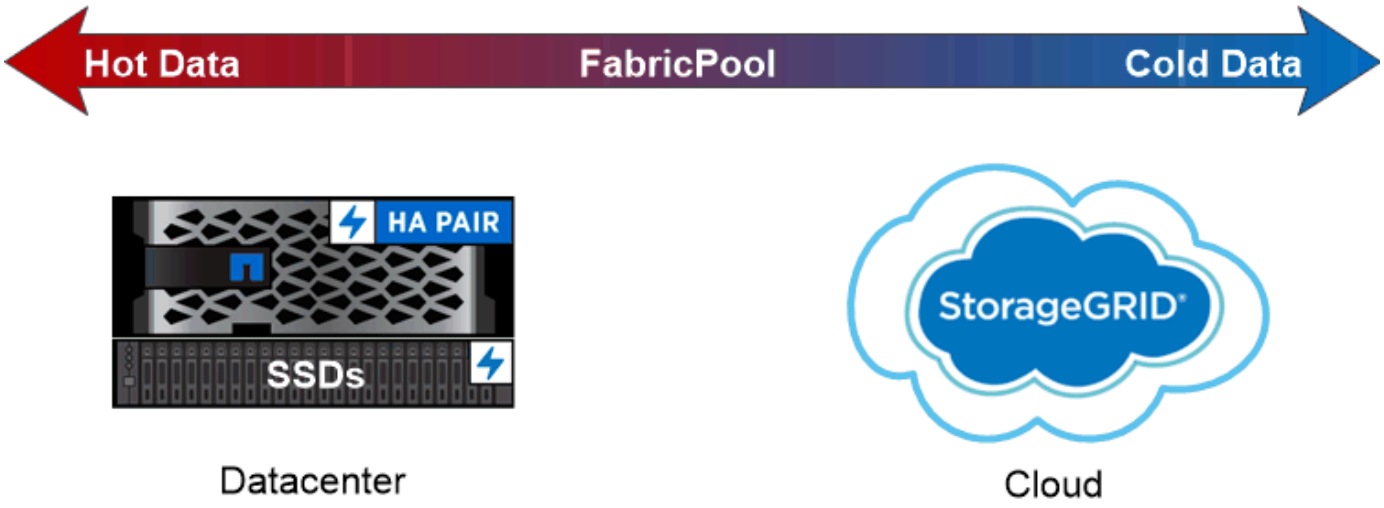
Festplatten- und Tier-Management

Festplatten und lokale ONTAP-Ebenen

Lokale Ebenen, auch *Aggregate* genannt, sind logische Container für die von einem Knoten verwalteten Festplatten. Lokale Ebenen ermöglichen die Isolierung von Workloads mit unterschiedlichen Leistungsanforderungen, das Tiering von Daten mit unterschiedlichen Zugriffsmustern oder die Trennung von Daten zu regulatorischen Zwecken.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*.

- Für geschäftskritische Anwendungen, die eine möglichst geringe Latenz und eine möglichst hohe Leistung erfordern, kann eine lokale Ebene erstellt werden, die ausschließlich aus SSDs besteht.
- Um Daten mit unterschiedlichen Zugriffsmustern zu schichten, kann eine *hybride lokale Tier* erstellt werden, wobei Flash als Hochleistungscache für einen Arbeitsdatensatz dient und kostengünstigere HDDs oder Objektspeicher für weniger häufig abgerufene Daten genutzt werden.
  - A "*Flash Pool*" besteht sowohl aus SSDs als auch aus HDDs.
  - A "*FabricPool*" besteht aus einer vollständig auf SSDs basierenden lokalen Schicht mit einem angeschlossenen Objektspeicher.
- Wenn aus regulatorischen Gründen archivierte Daten von aktiven Daten getrennt werden müssen, kann eine lokale Ebene verwendet werden, die aus Kapazitäts-HDDs oder einer Kombination aus Performance- und Kapazitäts-HDDs besteht.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

Arbeiten mit lokalen Ebenen in einer MetroCluster Konfiguration

Wenn Sie über eine MetroCluster Konfiguration verfügen, sind die in der "MetroCluster" Dokumentation beschriebenen Verfahren für die Erstkonfiguration sowie die Richtlinien für lokale Tiers und das Festplattenmanagement zu beachten.

Verwandte Informationen

- "Lokale Ebenen verwalten"
- "Datenträger verwalten"
- "RAID Konfigurationen verwalten"
- "Flash Pool Ebenen verwalten"
- "FabricPool Cloud-Tiers verwalten"

Lokale Ebenen verwalten

Informationen zum lokalen Tier-Management von ONTAP

Sie können den System Manager oder die ONTAP CLI verwenden, um lokale Ebenen hinzuzufügen, deren Nutzung zu verwalten und ihnen Kapazität (Festplatten) hinzuzufügen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Folgende Aufgaben sind möglich:

- "Eine lokale Ebene hinzufügen (erstellen)"

Um eine lokale Tier hinzuzufügen, wird einem bestimmten Workflow gefolgt. Die Anzahl der benötigten Festplatten oder Festplattenpartitionen für die lokale Tier wird ermittelt und es wird entschieden, welche Methode zur Erstellung der lokalen Tier verwendet wird. Lokale Tiers können automatisch hinzugefügt werden, indem ONTAP die Konfiguration zuweist, oder die Konfiguration kann manuell festgelegt werden.

- "Verwaltung der Nutzung lokaler Tiers"

  Für bestehende lokale Speicherebenen können Sie diese umbenennen, ihre Medienkosten festlegen oder ihre Laufwerks- und RAID-Gruppeninformationen bestimmen. Die RAID-Konfiguration einer lokalen Speicherebene kann geändert und lokalen Speicherebenen können Speicher-VMs (SVMs) zugewiesen werden. Die RAID-Konfiguration einer lokalen Speicherebene kann geändert und lokalen Speicherebenen können Speicher-VMs (SVMs) zugewiesen werden. Es kann festgestellt werden, welche Volumes sich auf einer lokalen Speicherebene befinden und wie viel Speicherplatz sie auf einer lokalen Speicherebene belegen. Es kann gesteuert werden, wie viel Speicherplatz Volumes belegen dürfen. Die Zuständigkeit für eine lokale Speicherebene kann mit einem HA-Paar verschoben werden. Eine lokale Speicherebene kann auch gelöscht werden.

- "Kapazität (Festplatten) zu einer lokalen Ebene hinzufügen"

  Mithilfe verschiedener Methoden wird ein bestimmter Workflow befolgt, um die Kapazität zu erweitern. Es können Festplatten zu einer lokalen Ebene und Laufwerke zu einem Knoten oder Shelf hinzugefügt werden. Falls erforderlich, lassen sich falsch ausgerichtete Ersatzpartitionen korrigieren.

Eine lokale Ebene hinzufügen (erstellen)

Workflow zur Erstellung der lokalen Ebene in ONTAP

Die Erstellung lokaler Tiers stellt Speicher für Volumes auf Ihrem System bereit.

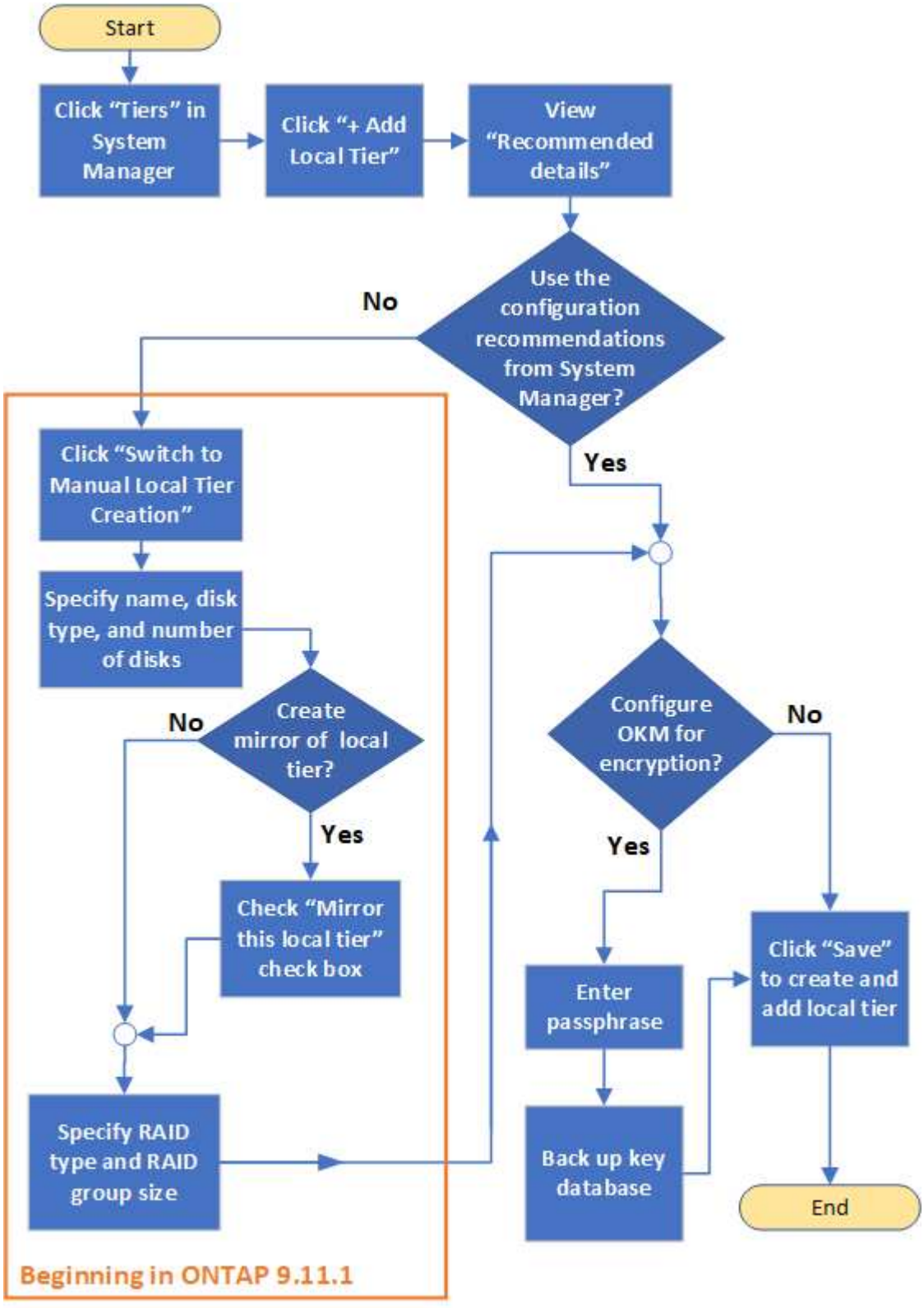
> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Der Workflow zum Erstellen lokaler Ebenen ist spezifisch für die verwendete Schnittstelle: System Manager oder die CLI.

System Manager

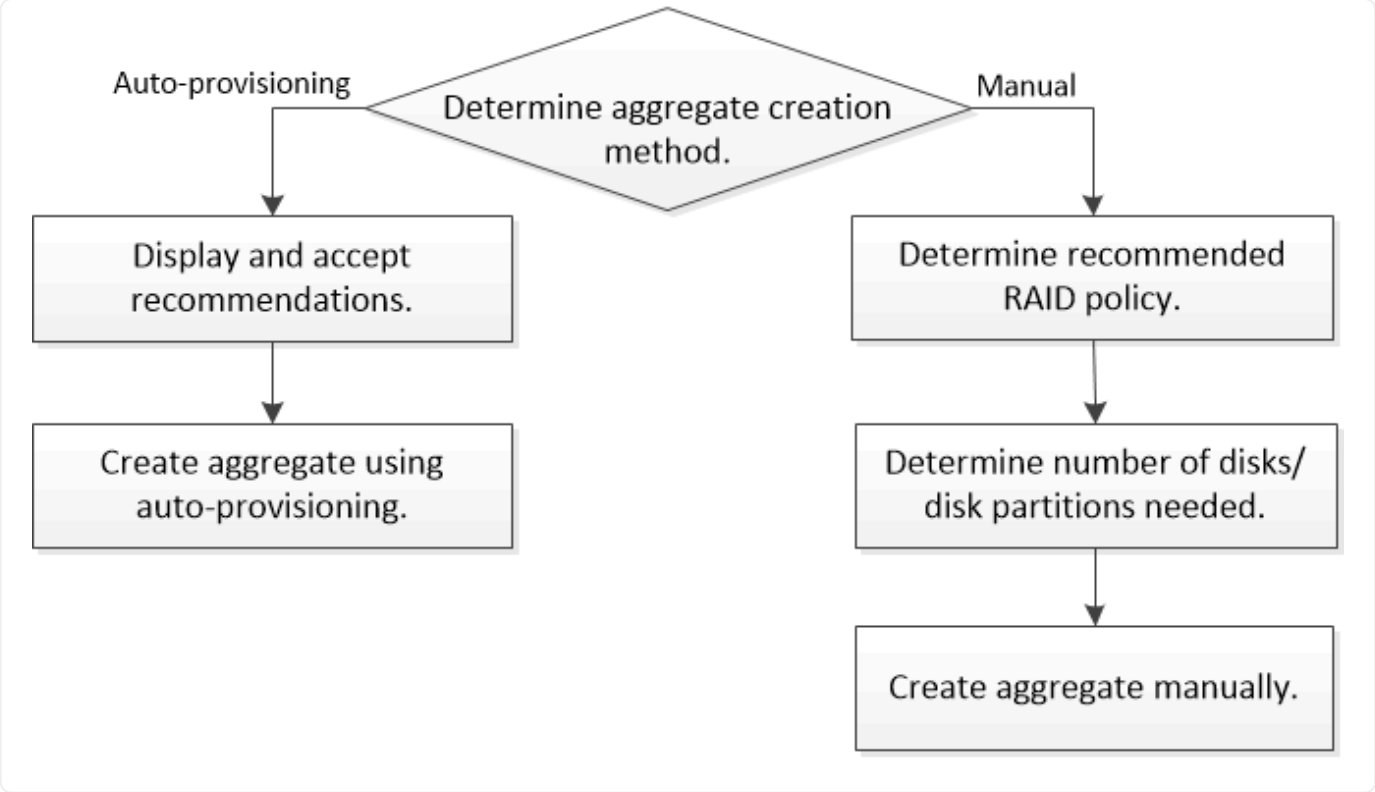
System Manager erstellt lokale Ebenen basierend auf empfohlenen Best Practices für die Konfiguration lokaler Ebenen.

Ab ONTAP 9.11.1 besteht die Möglichkeit, lokale Ebenen manuell zu konfigurieren, falls eine andere Konfiguration als die während des automatischen Prozesses zum Hinzufügen einer lokalen Ebene empfohlene gewünscht wird.



CLI

ONTAP kann beim Erstellen lokaler Tiers (Auto-Provisioning) empfohlene Konfigurationen bereitstellen. Wenn die empfohlenen Konfigurationen, basierend auf Best Practices, für Ihre Umgebung geeignet sind, können diese zur Erstellung des lokalen Tiers übernommen werden. Andernfalls ist es möglich, lokale Tiers manuell zu erstellen.



Festplatten- und Partitionsanforderungen für einen lokalen ONTAP Tier

Sie benötigen ausreichend Festplatten oder Festplattenpartitionen in Ihrer lokalen Speicherebene, um die System- und Geschäftsanforderungen zu erfüllen. Es wird außerdem empfohlen, die empfohlene Anzahl an Hot Spare Festplatten oder Hot Spare Festplattenpartitionen vorzuhalten, um das Risiko von Datenverlust zu minimieren.

Die Root-Datenpartitionierung ist in bestimmten Konfigurationen standardmäßig aktiviert. Systeme mit aktivierter Root-Datenpartitionierung verwenden Festplattenpartitionen zur Erstellung lokaler Tiers. Systeme ohne aktivierte Root-Datenpartitionierung verwenden unpartitionierte Festplatten.

Sie benötigen genügend Festplatten oder Festplattenpartitionen, um die für Ihre RAID-Richtlinie erforderliche Mindestanzahl sowie die Mindestkapazitätsanforderungen zu erfüllen.

Bei ONTAP ist der nutzbare Speicherplatz des Laufwerks geringer als dessen physische Kapazität. Der nutzbare Speicherplatz eines bestimmten Laufwerks sowie die Mindestanzahl der für jede RAID-Richtlinie erforderlichen Festplatten oder Festplattenpartitionen sind in der "Hardware Universe" zu finden.

Nutzbaren Speicherplatz einer bestimmten Festplatte ermitteln

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit dem System Manager lässt sich der nutzbare Speicherplatz der Festplatten bestimmen.

Führen Sie die folgenden Schritte aus, um die nutzbare Größe einer Festplatte anzuzeigen:

Schritte

1. Wechseln Sie zu **Storage > Tiers**
2. Klicken Sie ⋮ neben dem Namen der lokalen Ebene.
3. Die Registerkarte **Festplatteninformationen** auswählen.

CLI

Die Befehlszeilenschnittstelle (CLI) kann verwendet werden, um den nutzbaren Speicherplatz der Festplatten zu bestimmen.

Führen Sie den folgenden Schritt aus, um die nutzbare Größe einer Festplatte anzuzeigen:

Schritt

1. Informationen zur Ersatzfestplatte anzeigen:

```
storage aggregate show-spare-disks
```

Zusätzlich zu der Anzahl an Festplatten oder Festplattenpartitionen, die zum Erstellen Ihrer RAID-Gruppe und zur Erfüllung Ihrer Kapazitätsanforderungen erforderlich sind, sollte auch die empfohlene Mindestanzahl an Hot-Spare-Festplatten oder Hot-Spare-Festplattenpartitionen als Ersatzfestplatten für Ihre lokale Ebene vorhanden sein:

- Für alle lokalen Flash-Speicherebenen ist mindestens eine Hot-Ersatzfestplatte oder -Festplattenpartition erforderlich.

  ⓘ Der AFF C190 verfügt standardmäßig über keine Ersatzfestplatte. Diese Ausnahme ist vollständig unterstützt.

- Für homogene lokale Nicht-Flash-Speicherebenen sind mindestens zwei Ersatzfestplatten oder Festplattenpartitionen erforderlich.
- Für SSD-Speicherpools sollte mindestens eine Hot Spare-Ersatzfestplatte pro HA-Paar vorhanden sein.
- Für lokale Flash Pool Ebenen sollten mindestens zwei Ersatzfestplatten pro HA-Paar vorhanden sein. Weitere Informationen zu den unterstützten RAID-Richtlinien für Flash Pool lokale Ebenen finden sich in der "Hardware Universe".
- Um die Nutzung des Maintenance Center zu unterstützen und Probleme durch mehrere gleichzeitige Festplattenausfälle zu vermeiden, ist es empfehlenswert, mindestens vier Hot Spares in Multi-Disk-Carriern vorzuhalten.

Verwandte Informationen

- "NetApp Hardware Universe"
- "NetApp Technical Report 3838: Konfigurationsleitfaden für das Speichersubsystem"
- "storage aggregate show"

Methoden zur Erstellung lokaler Tiers in ONTAP

Obwohl ONTAP Best-Practice-Empfehlungen für das automatische Hinzufügen lokaler Ebenen bereitstellt, muss festgestellt werden, ob die empfohlenen Konfigurationen in Ihrer Umgebung unterstützt werden. Falls dies nicht der Fall ist, sind Entscheidungen bezüglich der RAID-Richtlinie und der Festplattenkonfiguration zu treffen und die lokalen

Ebenen anschließend manuell zu erstellen.

Wenn eine lokale Ebene automatisch erstellt wird, analysiert ONTAP die verfügbaren Ersatzfestplatten im Cluster und generiert eine Empfehlung, wie Ersatzfestplatten gemäß Best Practices zur Hinzufügung lokaler Ebenen verwendet werden sollten. ONTAP zeigt die empfohlenen Konfigurationen an. Es besteht die Möglichkeit, die Empfehlungen zu übernehmen oder die lokalen Ebenen manuell hinzuzufügen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie ONTAP Empfehlungen annehmen können

Wenn eine oder mehrere der folgenden Festplattenbedingungen vorliegen, müssen diese behoben werden, bevor die Empfehlungen von ONTAP übernommen werden:

- Fehlende Datenträger
- Schwankungen bei der Anzahl der Ersatzfestplatten
- Nicht zugewiesene Datenträger
- Nicht-Null-Ersatzfestplatten
- Festplatten, die Wartungstests unterzogen werden

Wann die manuelle Methode verwendet werden muss

In vielen Fällen ist das empfohlene Layout der lokalen Ebene optimal für Ihre Umgebung. Wenn Ihre Umgebung jedoch die folgenden Konfigurationen aufweist, muss die lokale Ebene mit der manuellen Methode erstellt werden.

> Ab ONTAP 9.11.1 ist es möglich, mit System Manager lokale Ebenen manuell hinzuzufügen.

- Lokale Ebenen mit Array-LUNs von Drittanbietern
- Virtuelle Festplatten mit Cloud Volumes ONTAP oder ONTAP Select
- MetroCluster System
- SyncMirror
- MSATA-Festplatten
- Flash Pool Tiers
- Mehrere Festplattentypen oder -größen sind mit dem Node verbunden.

Wählen Sie die Methode zum Erstellen lokaler Tiers aus.

Wählen Sie die Methode aus, die Sie verwenden möchten:

- "Lokale Ebenen automatisch hinzufügen (erstellen)"
- "Lokale Tiers manuell hinzufügen (erstellen)"

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

- "Automatische Bereitstellung von Speicheraggregaten"

ONTAP lokale Tiers automatisch hinzufügen

Wenn die von ONTAP empfohlene Best-Practice-Empfehlung zum automatischen Hinzufügen einer lokalen Tier in Ihrer Umgebung angemessen ist, kann die Empfehlung übernommen werden und ONTAP fügt die lokale Tier hinzu.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Festplatten müssen einem Node zugeordnet sein, bevor sie in einer lokalen Ebene verwendet werden können. Wenn Ihr Cluster nicht für die automatische Zuweisung des Festplattenbesitzes konfiguriert ist, muss "Besitzverhältnisse manuell zuweisen" erfolgen.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

System Manager

Schritte

1. Im System Manager auf **Speicher > Ebenen** klicken.
2. Auf der Seite **Tiers** + Add Local Tier einen neuen lokalen Tier erstellen:

   Auf der Seite **Lokale Ebene hinzufügen** wird die empfohlene Anzahl lokaler Ebenen angezeigt, die auf den Knoten erstellt werden können, sowie der verfügbare nutzbare Speicherplatz.

3. **Empfohlene Details** zeigt die von System Manager empfohlene Konfiguration an.

   Der System Manager zeigt ab ONTAP 9.8 folgende Informationen an:

   - **Lokaler Tiername** (der lokale Tiername kann ab ONTAP 9.10.1 bearbeitet werden)
   - **Node-Name**
   - **Nutzbare Größe**
   - **Speicherart**

     Ab ONTAP 9.10.1 werden zusätzliche Informationen angezeigt:

   - **Disks**: Anzeige der Anzahl, Größe und des Typs der Disks
   - **Layout**: Darstellung des RAID-Gruppenlayouts, einschließlich der Angabe, welche Festplatten Parität oder Daten sind und welche Steckplätze ungenutzt sind.
   - **Ersatzfestplatten**: Anzeige des Node-Name, der Anzahl und Größe der Ersatzfestplatten und des Speichertyps.
4. Einer der folgenden Schritte kann durchgeführt werden:

Wenn Sie Folgendes tun möchten…	Dann ist Folgendes zu tun…

Die Empfehlungen des System Manager werden übernommen.	Weiter zu Schritt zur Konfiguration des Onboard Key Manager für die Verschlüsselung.
Die lokalen Ebenen manuell konfigurieren und ***nicht*** die Empfehlungen des System Manager verwenden.	Weiter zu "Lokale Ebene manuell hinzufügen": • Für ONTAP 9.10.1 und frühere Versionen sind die folgenden Schritte zur Nutzung der CLI zu beachten. • Ab ONTAP 9.11.1 sind die folgenden Schritte zur Verwendung des System Manager zu beachten.

5. (Optional): Wenn der Onboard Key Manager installiert ist, kann er für die Verschlüsselung konfiguriert werden. Das Kästchen **Onboard Key Manager für Verschlüsselung konfigurieren** aktivieren.
   a. Geben Sie eine Passphrase ein.
   b. Geben Sie die Passphrase zur Bestätigung erneut ein.
   c. Bewahren Sie die Passphrase für die zukünftige Verwendung auf, falls das System wiederhergestellt werden muss.
   d. Die Schlüssel-Datenbank für die zukünftige Verwendung sichern.
6. **Speichern** erstellt die lokale Speicherebene und fügt sie der Speicherlösung hinzu.

CLI

Sie führen den `storage aggregate auto-provision` Befehl aus, um Empfehlungen für das lokale Tier-Layout zu generieren. Anschließend können lokale Tiers erstellt werden, nachdem ONTAP Empfehlungen geprüft und genehmigt wurden.

Über diese Aufgabe

Die mit dem `storage aggregate auto-provision` Befehl generierte Standardzusammenfassung listet die empfohlenen lokalen Tiers auf, einschließlich Namen und nutzbarer Größe. Die Liste kann eingesehen werden, um zu bestimmen, ob die empfohlenen lokalen Tiers bei entsprechender Aufforderung erstellt werden sollen.

Eine detaillierte Zusammenfassung kann auch mit der `-verbose` Option angezeigt werden, die die folgenden Berichte anzeigt:

- Zusammenfassung pro Node der neu zu erstellenden lokalen Tiers, der erkannten Ersatzfestplatten sowie der verbleibenden Ersatzfestplatten und Partitionen nach der Erstellung der lokalen Tiers
- Neue lokale Datenebenen, die mit der Anzahl der zu verwendenden Festplatten und Partitionen erstellt werden sollen
- RAID-Gruppenlayout, das zeigt, wie Ersatzfestplatten und Partitionen in den neuen lokalen Datenebenen verwendet werden.
- Details zu den nach der Erstellung der lokalen Tier verbleibenden Ersatzfestplatten und Partitionen

Wenn Sie mit der automatischen Bereitstellungsmethode vertraut sind und Ihre Umgebung korrekt vorbereitet ist, kann die `-skip-confirmation` Option verwendet werden, um die empfohlene lokale Tier ohne Anzeige und Bestätigung zu erstellen. Der `storage aggregate auto-provision` Befehl wird nicht von der CLI-Sitzung `-confirmations` Einstellung beeinflusst.

Weitere Informationen zu `storage aggregate auto-provision` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Den `storage aggregate auto-provision`Befehl mit den gewünschten Anzeigeoptionen ausführen.
   - Keine Optionen: Standardzusammenfassung
   - `-verbose`Option: Detaillierte Zusammenfassung anzeigen
   - `-skip-confirmation`Option: Empfohlene lokale Tiers ohne Anzeige oder Bestätigung erstellen
2. Einer der folgenden Schritte kann durchgeführt werden:

Wenn Sie Folgendes tun möchten…	Dann ist Folgendes zu tun…

Die Empfehlungen von ONTAP werden übernommen.	Die Anzeige der empfohlenen lokalen Tiers wird überprüft, anschließend erfolgt eine Reaktion auf die Aufforderung zur Erstellung der empfohlenen lokalen Tiers.
	
	`myA400-44556677::> storage aggregate auto-provision`
	`Node New Data Aggregate Usable Size`
	`---`
	`--- ---`
	`myA400-364 myA400_364_SSD_1 3.29TB`
	`myA400-363 myA400_363_SSD_1 1.46TB`
	`---`
	`--- ---`
	`Total: 2 new data aggregates 4.75TB`
	
	`Do you want to create recommended aggregates? {y`

n}: y Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress. myA400-44556677::> ----	Die lokalen Ebenen manuell konfigurieren und ***nicht*** die Empfehlungen von ONTAP verwenden.

Verwandte Informationen

- "ONTAP-Befehlsreferenz"

ONTAP lokale Tiers manuell hinzufügen

Wenn Sie keine lokale Ebene mithilfe der Best-Practice-Empfehlungen von ONTAP hinzufügen möchten, kann der Vorgang manuell durchgeführt werden.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Festplatten müssen einem Node zugeordnet sein, bevor sie in einer lokalen Ebene verwendet werden können. Wenn Ihr Cluster nicht für die automatische Zuweisung des Festplattenbesitzes konfiguriert ist, muss "Besitzverhältnisse manuell zuweisen" erfolgen.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

System Manager

Ab ONTAP 9.11.1 kann, falls nicht die vom System Manager empfohlene Konfiguration zum Erstellen einer lokalen Ebene verwendet werden soll, eine gewünschte Konfiguration angegeben werden.

Schritte

1. Im System Manager auf **Speicher > Ebenen** klicken.
2. Auf der Seite **Tiers** + Add Local Tier einen neuen lokalen Tier erstellen:

   Auf der Seite **Lokale Ebene hinzufügen** wird die empfohlene Anzahl lokaler Ebenen angezeigt, die auf den Knoten erstellt werden können, sowie der verfügbare nutzbare Speicherplatz.

3. Wenn der System Manager die Speicherempfehlung für die lokale Ebene anzeigt, im Abschnitt **Ersatzfestplatten** auf **Zur manuellen Erstellung der lokalen Ebene wechseln** klicken.

   Auf der Seite **Lokale Ebene hinzufügen** werden Felder angezeigt, die zur Konfiguration der lokalen Ebene verwendet werden.

4. Im ersten Abschnitt der Seite **Lokale Ebene hinzufügen** sind folgende Angaben zu machen:
   a. Geben Sie den Namen der lokalen Tier ein.
   b. (Optional): Aktivieren Sie das Kästchen **Mirror this local tier**, wenn die lokale Ebene gespiegelt werden soll.
   c. Wählen Sie einen Datenträgertyp aus.
   d. Wählen Sie die Anzahl der Festplatten.
5. Im Abschnitt **RAID Konfiguration** sind folgende Schritte auszuführen:
   a. Den RAID-Typ auswählen.
   b. Die Größe der RAID-Gruppe auswählen.
   c. Klicken Sie auf RAID-Zuordnung, um anzuzeigen, wie die Festplatten in der Gruppe zugewiesen sind.
6. (Optional): Falls der Onboard Key Manager installiert ist, kann er im Abschnitt **Verschlüsselung** der Seite für die Verschlüsselung konfiguriert werden. Das Kästchen **Onboard Key Manager für**

Verschlüsselung konfigurieren aktivieren.

a. Geben Sie eine Passphrase ein.

b. Geben Sie die Passphrase zur Bestätigung erneut ein.

c. Bewahren Sie die Passphrase für die zukünftige Verwendung auf, falls das System wiederhergestellt werden muss.

d. Die Schlüssel-Datenbank für die zukünftige Verwendung sichern.

7. **Speichern** erstellt die lokale Speicherebene und fügt sie der Speicherlösung hinzu.

CLI

Bevor Sie lokale Ebenen manuell erstellen, sollten Sie die Festplattenkonfigurationsoptionen überprüfen und die Erstellung simulieren.

Anschließend kann der `storage aggregate create` Befehl ausgeführt und die Ergebnisse überprüft werden.

Bevor Sie beginnen

Sie müssen die Anzahl der Festplatten und die Anzahl der benötigten Ersatzfestplatten in der lokalen Ebene ermittelt haben.

Über diese Aufgabe

Wenn die Root-Daten-Daten-Partitionierung aktiviert ist und Sie 24 oder weniger Solid-State-Drives (SSDs) in Ihrer Konfiguration haben, wird empfohlen, die Datenpartitionen verschiedenen Knoten zuzuweisen.

Die Vorgehensweise zum Erstellen lokaler Speicherebenen auf Systemen mit aktivierter Root-Daten-Partitionierung und Root-Daten-Daten-Partitionierung ist identisch mit der Vorgehensweise zum Erstellen lokaler Speicherebenen auf Systemen mit unpartitionierten Festplatten. Wenn die Root-Daten-Partitionierung auf Ihrem System aktiviert ist, sollte die Anzahl der Festplattenpartitionen für die `-diskcount` Option verwendet werden. Bei der Root-Daten-Daten-Partitionierung gibt die `-diskcount` Option die Anzahl der zu verwendenden Festplatten an.

Beim Erstellen mehrerer lokaler Ebenen zur Verwendung mit FlexGroup Volumes sollten die lokalen Ebenen möglichst einander in ihrer Größe angenähert sein.

Weitere Informationen zu `storage aggregate create` und zu den Optionen und Anforderungen für die Erstellung lokaler Tiers finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Die Liste der Ersatzfestplattenpartitionen zeigt, ob genügend Partitionen für die Erstellung Ihrer lokalen Ebene vorhanden sind:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Datenpartitionen werden unter `Local Data Usable` angezeigt. Eine Root-Partition kann nicht als Ersatzpartition verwendet werden.

2. Die Erstellung der lokalen Ebene simulieren:

   ```
   storage aggregate create -aggregate aggregate_name -node node_name
   -raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
   ```

3. Wenn bei der simulierten Befehlsausführung Warnungen angezeigt werden, sollte der Befehl angepasst und die Simulation wiederholt werden.
4. Lokale Ebene erstellen:

   ```
   storage aggregate create -aggregate aggr_name -node node_name -raidtype
   raid_dp -diskcount number_of_disks_or_partitions
   ```

5. Die lokale Ebene anzeigen, um zu überprüfen, ob sie erstellt wurde:

   ```
   storage aggregate show-status aggregate_name
   ```

Verwandte Informationen

- "storage aggregate show"

ONTAP lokale Tiers mit aktiviertem SyncMirror hinzufügen

Sie können SyncMirror aktivieren, wenn Sie manuell eine lokale Ebene erstellen, um die Daten der lokalen Ebene synchron zu spiegeln.

Weitere Informationen zu "gespiegelte und ungespiegelte lokale Tiers".

Bevor Sie beginnen

- Der Cluster muss ausschließlich mit internem Speicher initialisiert werden.
- Die Cluster-Einrichtung muss auf beiden Knoten abgeschlossen sein.

Über diese Aufgabe

Dieses Verfahren erstellt auf jedem Cluster-Node gespiegelte lokale Tiers gleicher Größe, und jedes lokale Tier verfügt über 44 Festplatten.

Schritte

1. Automatische Speicherzuweisung deaktivieren:

   ```
   storage disk option modify -node * -autoassign off
   ```

2. Bestätigen Sie, dass die automatische Zuweisung deaktiviert ist:

   ```
   storage disk option show
   ```

3. Das externe Shelf anschließen.
4. Weisen Sie jedem Node die externen Laufwerke zu, wobei Pool 1 angegeben wird:

   ```
   storage disk assign -disk <disk ID> -owner <node name> -pool 1
   ```

5. Die lokale Root-Ebene auf jedem Knoten spiegeln:

   ```
   storage aggregate mirror -aggregate <node1 root-aggr>

   storage aggregate mirror -aggregate <node2 root-aggr>
   ```

   Die Laufwerke in Pool 1 werden automatisch so partitioniert, dass sie denen in Plex 0

entsprechen.

6. Auf Knoten 1 eine gespiegelte Daten lokale Datenebene mit einer Anzahl von 44 Festplatten erstellen. Dadurch werden 22 Partitionen aus Pool 0 und 22 Partitionen aus Pool 1 ausgewählt.

   ```
   storage aggregate create -node <node1 name> -aggregate <node1 aggr-name>
   -diskcount 44 -mirror true
   ```

7. Auf Knoten 2 eine gespiegelte Daten lokale Datenebene mit einer Anzahl von 44 Festplatten erstellen. Dadurch werden 22 Partitionen aus Pool 0 und 22 Partitionen aus Pool 1 ausgewählt.

   ```
   storage aggregate create -node <node2 name> -aggregate <node2 aggr-name>
   -diskcount 44 -mirror true
   ```

8. Es wird überprüft, ob lokale Ebenen gleicher Größe erfolgreich erstellt wurden:

   ```
   storage aggregate show
   ```

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Storage Disk Option ändern"
- "storage disk option show"

Verwaltung der Nutzung lokaler Tiers

Umbenennen einer lokalen ONTAP-Ebene

Sie können eine lokale Ebene umbenennen. Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

System Manager

System Manager zum Umbenennen einer lokalen Ebene verwenden

Ab ONTAP 9.10.1 kann der Name einer lokalen Ebene geändert werden.

Schritte

1. Im System Manager auf **Speicher > Ebenen** klicken.
2. Klicken Sie ⋮ neben dem Namen der lokalen Ebene.
3. **Umbenennen** auswählen.
4. Geben Sie einen neuen Namen für die lokale Tier an.

CLI

Die CLI kann verwendet werden, um eine lokale Ebene umzubenennen

Schritt

1. Die lokale Ebene kann mithilfe der Befehlszeile umbenannt werden:

   `storage aggregate rename -aggregate aggr-name -newname aggr-new-name`

   Im folgenden Beispiel wird ein Aggregat mit dem Namen “aggr5” in “sales-aggr” umbenannt:

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

Verwandte Informationen

- "storage aggregate rename"

Medienkosten einer lokalen ONTAP-Ebene festlegen

Ab ONTAP 9.11.1 ist es mit dem System Manager möglich, die Medienkosten einer lokalen Ebene festzulegen.

Schritte

1. Im System Manager auf **Speicher > Ebenen** klicken und dann in den gewünschten lokalen Ebenenkacheln auf **Medienkosten festlegen** klicken.
2. **Aktive und inaktive Stufen** auswählen, um den Vergleich zu ermöglichen.
3. Eine Währungsart und ein Betrag werden eingegeben.

Wenn Sie die Medienkosten eingeben oder ändern, wird die Änderung in allen Medientypen vorgenommen.

ONTAP Laufwerke manuell schnell auf null setzen

Bei Systemen, die neu mit ONTAP 9.4 oder höher installiert wurden, und Systemen, die mit ONTAP 9.4 oder höher neu initialisiert wurden, wird *fast zeroing* verwendet, um Laufwerke zu nullen.

Mit der *schnellen Nullsetzung* werden Laufwerke innerhalb von Sekunden genullt. Dies erfolgt automatisch vor der Bereitstellung und verkürzt die Zeit für die Initialisierung des Systems, das Erstellen lokaler Tiers oder das Erweitern lokaler Tiers beim Hinzufügen von Ersatzlaufwerken erheblich.

Fast zeroing wird sowohl auf SSDs als auch auf HDDs unterstützt.

> Die Schnellnullung wird auf Systemen, die von ONTAP 9.3 oder älter aktualisiert wurden, nicht unterstützt. ONTAP 9.4 oder höher muss neu installiert oder das System reinitialisiert werden. In ONTAP 9.3 und älter werden Laufwerke ebenfalls automatisch von ONTAP genullt, jedoch dauert der Vorgang länger.

Wenn Sie ein Laufwerk manuell nullen müssen, können Sie eine der folgenden Methoden verwenden. In ONTAP 9.4 und höher dauert das manuelle Nullen eines Laufwerks ebenfalls nur wenige Sekunden.

CLI Befehl

Einen CLI-Befehl verwenden, um Laufwerke schnell auf Null zu setzen

Über diese Aufgabe

Für die Ausführung dieses Befehls sind Administratorrechte erforderlich.

Schritte

1. Den CLI-Befehl eingeben:

```
storage disk zerospares
```

Optionen im Bootmenü

Im Bootmenü Optionen zum schnellen Nullsetzen von Laufwerken auswählen

Über diese Aufgabe

- Die Verbesserung der schnellen Nullstellung wird von Systemen, die von einer Version vor ONTAP 9.4 aktualisiert wurden, nicht unterstützt.

Schritte

1. Im Bootmenü steht eine der folgenden Optionen zur Auswahl:
   - (4) Konfiguration bereinigen und alle Festplatten initialisieren
   - (9a) Alle Festplatten entpartitionieren und deren Eigentümerinformationen entfernen
   - (9b) Konfiguration bereinigen und Knoten mit vollständigen Festplatten initialisieren

Verwandte Informationen

- "Storage Disk ZeroSpares"

ONTAP Festplattenbesitz manuell zuweisen

Festplatten müssen einem Node zugeordnet sein, bevor sie in einer lokalen Ebene verwendet werden können.

Über diese Aufgabe

- Wenn die Besitzverhältnisse in einem HA-Paar, das nicht initialisiert wird und nicht ausschließlich DS460C Shelves enthält, manuell zugewiesen werden, ist Option 1 zu verwenden.
- Wenn Sie ein HA-Paar initialisieren, das nur DS460C Shelves enthält, verwenden Sie Option 2, um die Eigentümerschaft für die Root-Laufwerke manuell zuzuweisen.

▼ Option 1: Die meisten HA Paare

Für ein HA-Paar, das nicht initialisiert wird und nicht ausschließlich DS460C Shelves enthält, kann dieses Verfahren zur manuellen Zuweisung des Eigentums verwendet werden.

Über diese Aufgabe

- Die Festplatten, denen Sie die Besitzrechte zuweisen, müssen sich in einem Shelf befinden, das physisch mit dem Node verbunden ist, dem Sie die Besitzrechte zuweisen.
- Wenn Sie Festplatten in einer lokalen Ebene (Aggregat) verwenden:
  - Festplatten müssen einem Knoten zugeordnet sein, bevor sie in einer lokalen Ebene (Aggregate) verwendet werden können.
  - Die Besitzverhältnisse einer Festplatte, die in einer lokalen Ebene (Aggregat) verwendet wird,

können nicht neu zugewiesen werden.

Schritte

1. Mit der Befehlszeilenschnittstelle (CLI) werden alle nicht zugeordneten Datenträger angezeigt:

   ```
   storage disk show -container-type unassigned
   ```

2. Jeder Festplatte Folgendes zuweisen:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   Sie können das Platzhalterzeichen verwenden, um mehr als einen Datenträger gleichzeitig zuzuweisen. Wenn Sie eine Ersatzffestplatte neu zuweisen, die bereits einem anderen Knoten gehört, muss die Option „-force“ verwendet werden.

▼ **Option 2: Ein HA-Paar mit ausschließlich DS460C Shelves**

Für ein HA-Paar, das initialisiert wird und nur DS460C Shelves enthält, kann mit diesem Verfahren die Eigentümerschaft für die Root-Laufwerke manuell zugewiesen werden.

Über diese Aufgabe

- Bei der Initialisierung eines HA-Paares, das ausschließlich DS460C Shelves enthält, müssen die Root-Laufwerke manuell so zugewiesen werden, dass sie der Half-Drawer-Richtlinie entsprechen.

  Nach der Initialisierung des HA-Paares (Bootvorgang) ist die automatische Zuweisung der Festplattenbesitzrechte aktiviert und verwendet die Half-Drawer-Richtlinie, um die Besitzrechte den verbleibenden Laufwerken (mit Ausnahme der Root-Laufwerke) und allen zukünftig hinzugefügten Laufwerken zuzuweisen, wie etwa beim Ersetzen ausgefallener Festplatten, beim Reagieren auf eine „low spares“-Meldung oder beim Hinzufügen von Kapazität.

  "Informationen zur Regelung zur halben Schublade".

- Für RAID sind mindestens 10 Laufwerke pro HA-Paar (5 pro Knoten) erforderlich, wenn NL-SAS-Laufwerke mit mehr als 8 TB in einem DS460C Shelf verwendet werden.

Schritte

1. Falls Ihre DS460C Shelves nicht vollständig bestückt sind, die folgenden Teilschritte ausführen; andernfalls zum nächsten Schritt wechseln.

   a. Zuerst werden die Laufwerke in der vorderen Reihe (Laufwerksschächte 0, 3, 6 und 9) jeder Schublade installiert.

      Die Installation der Laufwerke in der vordersten Reihe jeder Schublade ermöglicht eine ordnungsgemäße Luftzirkulation und verhindert eine Überhitzung.

   b. Die restlichen Laufwerke werden gleichmäßig auf die einzelnen Schubladen verteilt.

      Die Schubladenreihen werden von vorne nach hinten bestückt. Wenn nicht genügend Laufwerke vorhanden sind, um die Reihen zu füllen, werden sie paarweise installiert, sodass die Laufwerke die linke und rechte Seite einer Schublade gleichmäßig belegen.

      Die folgende Abbildung zeigt die Nummerierung und die Positionen der Laufwerksschächte in einer DS460C-Schublade.



2. Melden Sie sich über die node-management LIF oder die cluster-management LIF bei der clustershell an.
3. Die Stammlaufwerke in jedem Fach werden manuell gemäß der Halbfachrichtlinie zugewiesen, wobei die folgenden Teilschritte zu beachten sind:

   Bei der Half-Drawer-Richtlinie werden die Laufwerke der linken Hälfte eines Laufwerksschachts (Einschübe 0 bis 5) Knoten A und die Laufwerke der rechten Hälfte eines Laufwerksschachts (Einschübe 6 bis 11) Knoten B zugeordnet.

   a. Alle nicht zugeordneten Datenträger anzeigen:
   `storage disk show -container-type unassigned`

   b. Root-Disks zuweisen:
   `storage disk assign -disk disk_name -owner owner_name`

   Sie können das Platzhalterzeichen verwenden, um mehr als einen Datenträger gleichzeitig zuzuweisen.

Weitere Informationen zu `storage disk` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"

Laufwerks- und RAID-Gruppeninformationen für eine lokale ONTAP-Ebene ermitteln

Einige Aufgaben der lokalen Tier-Administration erfordern Kenntnisse darüber, aus welchen Laufwerkstypen die lokale Tier besteht, deren Größe, Prüfsumme und Status, ob sie mit anderen lokalen Tiers gemeinsam genutzt werden sowie über die Größe und Zusammensetzung der RAID-Gruppen.

Schritt

1. Die Laufwerke der lokalen Ebene nach RAID-Gruppe anzeigen:

`storage aggregate show-status` *aggr_name*

Die Laufwerke werden für jede RAID-Gruppe in der lokalen Ebene angezeigt.

Der RAID-Typ des Laufwerks (Daten, Parität, dParität) ist in der `Position` Spalte ersichtlich. Wenn in der `Position` Spalte `shared` angezeigt wird, ist das Laufwerk gemeinsam genutzt: Bei einer HDD handelt es sich um eine partitionierte Festplatte, bei einer SSD ist es Teil eines Speicherpools.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

Verwandte Informationen

- "storage aggregate show-status"

Zuweisung von ONTAP lokalen Tiers zu Storage VMs

Wenn Sie einer Storage Virtual Machine (Storage VM oder SVM, früher bekannt als Vserver) eine oder mehrere lokale Ebenen zuweisen, können nur diese lokalen Ebenen Volumes für diese Storage VM (SVM) enthalten.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff

aggregate. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Die Storage-VM und die lokalen Ebenen, die Sie dieser Storage-VM zuweisen möchten, müssen bereits existieren.

Über diese Aufgabe

Durch die Zuweisung lokaler Speicherebenen zu Ihren Storage-VMs bleiben die Storage-VMs voneinander isoliert, was insbesondere in einer Mandantenfähigkeit Umgebung wichtig ist.

Schritte

1. Die Liste der lokalen Ebenen, die dem SVM bereits zugewiesen sind, kann überprüft werden:

   ```
   vserver show -fields aggr-list
   ```

   Die dem SVM aktuell zugewiesenen lokalen Ebenen werden angezeigt. Falls keine lokalen Ebenen zugewiesen sind, `-`wird angezeigt.

2. Je nach Bedarf zugewiesene lokale Ebenen hinzufügen oder entfernen:

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Zusätzliche lokale Ebenen zuweisen	`vserver add-aggregates`
Lokale Ebenen aufheben	`vserver remove-aggregates`

   Die aufgelisteten lokalen Ebenen werden der SVM zugewiesen oder von ihr entfernt. Wenn die SVM bereits Volumes enthält, die ein Aggregat verwenden, das der SVM nicht zugewiesen ist, wird eine Warnmeldung angezeigt, aber der Befehl wird erfolgreich abgeschlossen. Alle lokalen Ebenen, die der SVM bereits zugewiesen waren und im Befehl nicht genannt wurden, bleiben unberührt.

Beispiel

Im folgenden Beispiel sind die lokalen Ebenen aggr1 und aggr2 der SVM svm1 zugewiesen:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

Ermitteln, welche Volumes sich auf einer lokalen ONTAP Ebene befinden.

Möglicherweise muss ermittelt werden, welche Volumes sich auf einer lokalen Ebene befinden, bevor Vorgänge wie das Verschieben oder das Offline-Schalten auf der lokalen Ebene durchgeführt werden.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Schritte

1. Die Volumes, die sich auf einer lokalen Ebene befinden, werden angezeigt, wenn folgender Befehl eingegeben wird:

```
volume show -aggregate aggregate_name
```

Alle Volumes, die sich auf der angegebenen lokalen Ebene befinden, werden angezeigt.

Speichernutzung eines Volumes in einer lokalen ONTAP-Ebene ermitteln und steuern

Sie können feststellen, welche FlexVol Volumes den meisten Speicherplatz in einer lokalen Ebene belegen und welche Features innerhalb des Volumes diesen Speicherplatz nutzen.

Der `volume show-footprint` Befehl liefert Informationen über den Footprint eines Volumes bzw. dessen Speicherplatznutzung innerhalb der übergeordneten lokalen Ebene.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Der `volume show-footprint` Befehl zeigt Details zur Speichernutzung jedes Volumes in einer lokalen Ebene an, einschließlich Offline-Volumes. Dieser Befehl schließt die Lücke zwischen den Ausgaben der `volume show-space` und `aggregate show-space` Befehle. Alle Prozentangaben werden als Prozentsatz der Größe der lokalen Ebene berechnet.

Das folgende Beispiel zeigt die `volume show-footprint` Befehlsausgabe für ein Volume namens testvol:

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                                     Used    Used%
      --------------------------------    ----------    -----
      Volume Data Footprint                    120.6MB       4%
      Volume Guarantee                          1.88GB      71%
      Flexible Volume Metadata                 11.38MB       0%
      Delayed Frees                             1.36MB       0%
      Total Footprint                           2.01GB      76%
```

Die folgende Tabelle erläutert einige der wichtigsten Zeilen der Ausgabe des `volume show-footprint` -Befehls und welche Möglichkeiten bestehen, den Speicherplatzverbrauch dieser Funktion zu verringern:

Zeilen-/Feature-Name	Beschreibung/Inhalt der Zeile	Einige Möglichkeiten zur Verringerung

`Volume Data Footprint`	Die Gesamtmenge an Speicherplatz, die im lokalen Speichermedium von den Daten eines Volumes im aktiven Dateisystem und dem von den Snapshots des Volumes belegten Speicherplatz verwendet wird. Diese Zeile enthält keinen reservierten Speicherplatz.	• Daten werden aus dem Volume gelöscht. • Snapshots aus dem Volume werden gelöscht.
`Volume Guarantee`	Der vom Volume im lokalen Speicherbereich für zukünftige Schreibvorgänge reservierte Speicherplatz. Die Menge des reservierten Speicherplatzes hängt vom Garantietyp des Volumes ab.	Änderung der Garantieart für das Volumen auf `none`.
`Flexible Volume Metadata`	Der gesamte Speicherplatz, der in der lokalen Tier von den Metadatendateien des Volumes belegt wird.	Keine direkte Methode zur Steuerung.
`Delayed Frees`	Blöcke, die ONTAP aus Performancegründen verwendet und die nicht sofort freigegeben werden können. Für SnapMirror-Ziele hat diese Zeile einen Wert von `0` und wird nicht angezeigt.	Keine direkte Methode zur Steuerung.
`File Operation Metadata`	Der gesamte reservierte Speicherplatz für Metadaten von Dateivorgängen.	Keine direkte Methode zur Steuerung.
`Total Footprint`	Der gesamte Speicherplatz, den das Volume in der lokalen Ebene belegt. Dies ist die Summe aller Zeilen.	Alle Methoden, die verwendet werden, um den von einem Volumen belegten Speicherplatz zu verringern.

Verwandte Informationen

"NetApp Technischer Bericht 3483: Thin Provisioning in einer NetApp SAN oder IP-SAN Unternehmensumgebung"

Speichernutzung in einer ONTAP lokalen Ebene

Sie können einsehen, wie viel Speicherplatz von allen Volumes in einer oder mehreren lokalen Ebenen belegt ist, sodass Maßnahmen zur Freigabe von Speicherplatz möglich sind.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

WAFL reserviert einen bestimmten Prozentsatz des gesamten Speicherplatzes für Metadaten und Leistung auf lokaler Tier-Ebene. Der für die Verwaltung der Volumes in der lokalen Tier verwendete Speicherplatz stammt

aus der WAFL Reserve und kann nicht geändert werden.

Bei lokalen Tiers unter 30 TB reserviert WAFL 10 % des gesamten Speicherplatzes für Metadaten und Leistung auf Tier-Ebene.

Ab ONTAP 9.12.1 wird in lokalen Speicherebenen ab 30 TB der für Metadaten und Leistungsdaten reservierte Speicherplatz reduziert, wodurch 5 % mehr nutzbarer Speicherplatz zur Verfügung steht. Die Verfügbarkeit dieser Speicherplatzersparnis variiert je nach Plattform und ONTAP-Version.

Von ONTAP in lokalen Ebenen reservierter Speicherplatz 30 TB oder mehr	Gilt für Plattformen	In ONTAP Versionen
5%	Alle AFF und FAS Plattformen	ONTAP 9.14.1 und höher
5%	AFF Plattformen und FAS500f Plattformen	ONTAP 9.12.1 und höher
10%	Alle Plattformen	ONTAP 9.11.1 und höher

Sie können die Speichernutzung aller Volumes in einer oder mehreren lokalen Ebenen mit dem `aggregate show-space` Befehl anzeigen. Dies hilft Ihnen zu erkennen, welche Volumes in ihren jeweiligen lokalen Ebenen den meisten Speicherplatz belegen, sodass entsprechende Maßnahmen zur Freigabe von mehr Speicherplatz ergriffen werden können.

Der belegte Speicherplatz in einer lokalen Ebene wird direkt vom belegten Speicherplatz in den darin enthaltenen FlexVol Volumes beeinflusst. Maßnahmen zur Erhöhung des Speicherplatzes in einem Volume wirken sich ebenfalls auf den Speicherplatz in der lokalen Ebene aus.

Ab ONTAP 9.15.1 stehen zwei neue Metadatenzähler zur Verfügung. Zusammen mit Änderungen an mehreren bestehenden Zählern ergibt sich ein klarerer Überblick über die Menge der zugewiesenen Benutzerdaten. Siehe "Speichernutzung in einem Volume oder einer lokalen Ebene ermitteln" für weitere Informationen.

Die folgenden Zeilen sind in der `aggregate show-space` Befehlsausgabe enthalten:

- **Volume Footprints**

  Die Gesamtgröße aller Volume-Footprints innerhalb der lokalen Ebene. Sie umfasst den gesamten Speicherplatz, der von allen Daten und Metadaten aller Volumes in der enthaltenen lokalen Ebene belegt oder reserviert wird.

- **Aggregate-Metadaten**

  Die gesamten Dateisystemmetadaten, die von der lokalen Ebene benötigt werden, wie Zuordnungsbitmaps und Inode-Dateien.

- **Snapshot-Reserve**

  Der für lokale Tier-Snapshots reservierte Speicherplatz basiert auf der Volume-Größe. Er gilt als belegter Speicherplatz und steht weder für Volume- noch für lokale Tier-Daten oder Metadaten zur Verfügung.

- **Snapshot Reserve nicht nutzbar**

Der ursprünglich für die lokale Tier-Snapshot-Reserve vorgesehene Speicherplatz, der für lokale Tier-Snapshots nicht verfügbar ist, weil er von Volumes verwendet wird, die der lokalen Tier zugeordnet sind. Dies kann nur bei lokalen Tiers mit einer von Null verschiedenen lokalen Tier-Snapshot-Reserve auftreten.

- **Gesamtverbrauch**

  Die Summe des gesamten Speicherplatzes, der in der lokalen Ebene von Volumes, Metadaten oder Snapshots belegt oder reserviert ist.

- **Gesamter physischer Verbrauch**

  Der aktuell für Daten genutzte Speicherplatz (statt für zukünftige Verwendung reserviert). Beinhaltet den von lokalen Tier-Snapshots belegten Speicherplatz.

Das folgende Beispiel zeigt die `aggregate show-space` Befehlsausgabe für eine lokale Tier, deren Snapshot-Reserve 5 % beträgt. Wenn die Snapshot-Reserve 0 wäre, würde die Zeile nicht angezeigt.

```
cluster1::> storage aggregate show-space

                      Aggregate : wqa_gx106_aggr1

      Feature                                  Used      Used%
      --------------------------------    ----------     ------
      Volume Footprints                      101.0MB         0%
      Aggregate Metadata                       300KB         0%
      Snapshot Reserve                        5.98GB         5%

      Total Used                              6.07GB         5%
      Total Physical Used                    34.82KB         0%
```

Verwandte Informationen

- "Knowledge Base Artikel: Platznutzung"
- "5 % des Speicherplatzes können durch ein Upgrade auf ONTAP 9.12.1 freigegeben werden"
- "storage aggregate show-space"

Zuständigkeit für eine ONTAP lokale Ebene innerhalb eines HA-Paares verlagern

Sie können die Zuständigkeit für lokale Ebenen zwischen den Knoten eines HA-Paares ändern, ohne den Dienst von den lokalen Ebenen zu unterbrechen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Beide Knoten eines HA-Paares sind physisch mit den Festplatten oder Array-LUNs des jeweils anderen Knotens verbunden. Jede Festplatte oder Array-LUN gehört einem der Knoten.

Bei einer Übernahme wechselt die Eigentümerschaft aller Festplatten oder Array-LUNs innerhalb einer lokalen

Ebene vorübergehend von einem Knoten zum anderen. Lokale Ebenenverschiebungsoperationen können die Eigentümerschaft jedoch auch dauerhaft ändern (zum Beispiel bei einer Lastverteilung). Die Eigentümerschaft ändert sich ohne Datenkopierprozesse oder physische Bewegung der Festplatten oder Array-LUNs.

Über diese Aufgabe

- Da Volume-Anzahl-Grenzwerte während der lokalen Tier-Umlagerungsvorgänge programmatisch überprüft werden, ist eine manuelle Überprüfung nicht erforderlich.

  Wenn die Volume-Anzahl das unterstützte Limit überschreitet, schlägt die lokale Tier-Verschiebung mit einer entsprechenden Fehlermeldung fehl.

- Eine lokale Tier-Verschiebung sollte nicht eingeleitet werden, wenn auf dem Quell- oder Zielknoten Systemoperationen ausgeführt werden; ebenso sollten diese Operationen nicht während der lokalen Tier-Verschiebung gestartet werden.

  Diese Vorgänge können Folgendes umfassen:

  - Übernahme
  - Giveback
  - Herunterfahren
  - Ein weiterer Vorgang zur lokalen Tier-Verlagerung
  - Änderungen des Festplattenbesitzes
  - Lokale Tier- oder Volume-Konfigurationsvorgänge
  - Speichercontroller Austausch
  - ONTAP Upgrade
  - ONTAP Revertierung
- Wenn Sie über eine MetroCluster Konfiguration verfügen, sollte keine lokale Tier-Verschiebung eingeleitet werden, während Notfallwiederherstellungsmaßnahmen (*switchover*, *healing* oder *switchback*) im Gange sind.
- Wenn Sie eine MetroCluster Konfiguration haben und eine lokale Tier-Verschiebung auf einem umgeschalteten lokalen Tier initiieren, kann der Vorgang fehlschlagen, weil die Volume-Anzahl des DR-Partners überschritten wird.
- Eine lokale Tier-Verschiebung sollte nicht auf lokalen Tiers durchgeführt werden, die beschädigt sind oder sich in der Wartung befinden.
- Vor Beginn der lokalen Tier Verschiebung sollten alle Core-Dumps auf den Quell- und Zielknoten gespeichert werden.

Schritte

1. Die lokalen Ebenen auf dem Knoten anzeigen, um zu bestätigen, welche lokalen Ebenen verschoben werden sollen, und sicherzustellen, dass sie online und in gutem Zustand sind:

   `storage aggregate show -node` *`source-node`*

   Der folgende Befehl zeigt sechs lokale Ebenen auf den vier Knoten im Cluster. Alle lokalen Ebenen sind online. Node1 und Node3 bilden ein HA-Paar und Node2 und Node4 bilden ein HA-Paar.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   ```

```
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. Den Befehl zum Starten der lokalen Tier-Verlagerung ausgeben:

   `storage aggregate relocation start -aggregate-list` *`aggregate-1`*`, `*`aggregate-2`*`… -node` *`source-node`* `-destination` *`destination-node`*

   Der folgende Befehl verschiebt die lokalen Tiers aggr_1 und aggr_2 von Node1 zu Node3. Node3 ist der HA-Partner von Node1. Die lokalen Tiers können nur innerhalb des HA-Paars verschoben werden.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. Der Fortschritt der lokalen Tier-Verschiebung kann mit dem `storage aggregate relocation show` Befehl überwacht werden:

   `storage aggregate relocation show -node` *`source-node`*

   Der folgende Befehl zeigt den Fortschritt der lokalen Ebenen, die zu Node3 verschoben werden:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

Wenn die Verlagerung abgeschlossen ist, zeigt die Ausgabe dieses Befehls für jede lokale Ebene den Verlagerungsstatus „Done“ an.

Verwandte Informationen

- "storage aggregate relocation show"
- "Start der Verlagerung des Storage Aggregats"
- "storage aggregate show"

Löschen einer ONTAP lokalen Ebene

Eine lokale Ebene kann gelöscht werden, wenn sich auf der lokalen Ebene keine Volumes befinden.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Der `storage aggregate delete` Befehl löscht eine lokale Speicherebene. Der Befehl schlägt fehl, wenn sich Volumes auf der lokalen Speicherebene befinden. Wenn der lokalen Speicherebene ein Objektspeicher zugeordnet ist, werden zusätzlich zur Löschung der lokalen Speicherebene auch die Objekte im Objektspeicher gelöscht. An der Objektspeicher Konfiguration werden durch diesen Befehl keine Änderungen vorgenommen.

Das folgende Beispiel löscht eine lokale Tier mit dem Namen “aggr1”:

```
> storage aggregate delete -aggregate aggr1
```

Verwandte Informationen

- "Speicheraggregate löschen"

ONTAP Befehle für die Verlagerung des lokalen Tiers

Es gibt spezielle ONTAP Befehle zum Verschieben der lokalen Tier-Zuständigkeit innerhalb eines HA-Paares.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Den lokalen Tier-Umstellungsprozess starten	`storage aggregate relocation start`
Den lokalen Tier-Umstellungsprozess überwachen	`storage aggregate relocation show`

Verwandte Informationen

- "storage aggregate relocation show"

- "Start der Verlagerung des Storage Aggregats"

ONTAP Befehle zur Verwaltung lokaler Ebenen

Sie verwenden den `storage aggregate` Befehl, um Ihre lokalen Tiers zu verwalten.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Die Größe des Caches für alle lokalen Flash Pool Ebenen anzeigen	`storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total >0`
Festplatteninformationen und Status für eine lokale Ebene anzeigen	`storage aggregate show-status`
Ersatzfestplatten nach Knoten anzeigen	`storage aggregate show-spare-disks`
Die lokalen Root-Tiers im Cluster anzeigen	`storage aggregate show -has-mroot true`
Grundlegende Informationen und Status für lokale Ebenen	`storage aggregate show`
Den in lokalen Tiers verwendeten Speichertyp anzeigen	`storage aggregate show -fields storage-type`
Eine lokale Stufe online bringen	`storage aggregate online`
Eine lokale Ebene löschen	`storage aggregate delete`
Eine lokale Ebene in den eingeschränkten Zustand versetzen	`storage aggregate restrict`
Eine lokale Ebene umbenennen	`storage aggregate rename`
Eine lokale Ebene offline nehmen	`storage aggregate offline`
Den RAID-Typ für eine lokale Ebene ändern	`storage aggregate modify -raidtype`

Verwandte Informationen

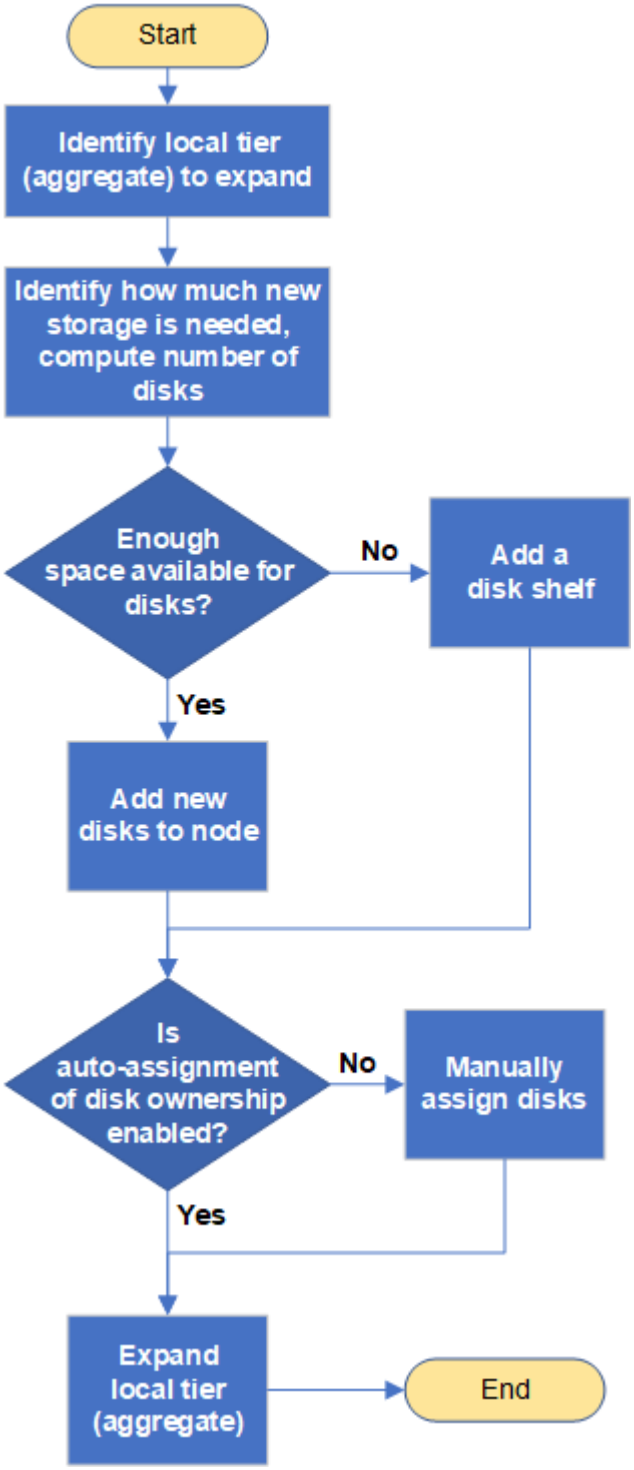
- "Speicheraggregate löschen"
- "storage aggregate ändern"
- "storage aggregate offline"
- "Storage Aggregate online"
- "storage aggregate rename"
- "storage aggregate restrict"
- "storage aggregate show"

Kapazität (Festplatten) zu einer lokalen Ebene hinzufügen

Workflow zur Erweiterung der Kapazität des ONTAP local tier

Um die Kapazität einer lokalen Ebene zu erhöhen, müssen zunächst die lokale Ebene identifiziert werden, zu der hinzugefügt werden soll, der benötigte neue Speicherplatz bestimmt, neue Festplatten installiert, die Festplattenzugehörigkeit zugewiesen und gegebenenfalls eine neue RAID-Gruppe erstellt werden.

Sie können entweder den System Manager oder die ONTAP CLI verwenden, um Kapazität hinzuzufügen.



Methoden zur Schaffung von Speicherplatz in einer ONTAP lokalen Ebene

Wenn der Speicherplatz auf einer lokalen Speicherebene erschöpft ist, können verschiedene Probleme auftreten, von Datenverlust bis hin zur Deaktivierung der Volume-Garantie. Es gibt mehrere Möglichkeiten, mehr Speicherplatz auf einer lokalen Speicherebene zu schaffen.

Alle Methoden haben unterschiedliche Konsequenzen. Vor der Durchführung von Maßnahmen empfiehlt sich das Lesen des entsprechenden Abschnitts in der Dokumentation.

Im Folgenden sind einige gängige Methoden zur Speicherplatzbeschaffung in der lokalen Speicherebene aufgeführt, in der Reihenfolge von den geringsten bis zu den größten Auswirkungen:

- Dem lokalen Tier werden Festplatten hinzugefügt.
- Einige Volumes auf eine andere lokale Ebene mit verfügbarem Speicherplatz verschieben.
- Die Größe der volumengarantierten Volumes in der lokalen Tier verkleinern.
- Nicht benötigte Volume-Snapshots löschen, wenn der Garantietyp des Volumes “none” ist.
- Nicht benötigte Volumes löschen.
- Speichersparende Funktionen wie Deduplizierung oder Komprimierung können genutzt werden.
- (Vorübergehend) Funktionen deaktivieren, die eine große Menge an Metadaten verwenden.

Kapazität zu einer lokalen ONTAP-Ebene hinzufügen

Sie können einer lokalen Tier Festplatten hinzufügen, damit sie den zugehörigen Volumes mehr Speicherplatz zur Verfügung stellt.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

System Manager (ONTAP 9.8 und höher)

Ab ONTAP 9.12.1 kann mit dem System Manager die zugesicherte Kapazität einer lokalen Tier angezeigt werden, um festzustellen, ob zusätzliche Kapazität für die lokale Tier erforderlich ist. Siehe "Kapazität im System Manager überwachen".

Schritte

1. **Speicher > Ebenen** auswählen.
2. Wählen Sie ⋮ neben dem Namen der lokalen Ebene aus, zu der Sie Kapazität hinzufügen möchten.
3. **Kapazität hinzufügen** auswählen.

   Wenn keine zusätzlichen Festplatten verfügbar sind, die hinzugefügt werden können, wird die Option **Kapazität hinzufügen** nicht angezeigt und die Kapazität der lokalen Ebene kann nicht erhöht werden.

4. Die folgenden Schritte sind abhängig von der installierten ONTAP-Version auszuführen:

Wenn diese Version von ONTAP installiert ist…	Führen Sie diese Schritte aus…
Ab ONTAP 9.11.1	a. Den Datenträgertyp und die Anzahl der Datenträger auswählen. b. Wenn Festplatten zu einer neuen RAID-Gruppe hinzugefügt werden sollen, ist das Kästchen zu aktivieren. Die RAID-Zuordnung wird angezeigt. c. **Speichern** auswählen.
ONTAP 9.10.1, 9.9 oder 9.8	a. Wenn der Knoten mehrere Speicherebenen enthält, kann die Anzahl der Festplatten ausgewählt werden, die der lokalen Ebene hinzugefügt werden sollen. Andernfalls, wenn der Knoten nur eine einzige Speicherebene enthält, wird die hinzugefügte Kapazität automatisch geschätzt. b. Wählen Sie **Add**.

5. (Optional) Der Vorgang benötigt einige Zeit, um abgeschlossen zu werden. Wenn der Vorgang im Hintergrund ausgeführt werden soll, **Im Hintergrund ausführen** auswählen.
6. Nach Abschluss des Vorgangs ist die erhöhte Kapazität in den lokalen Tier-Informationen unter **Speicher > Tiers** sichtbar.

System Manager (ONTAP 9.7 und früher)

Schritte

1. (Nur für ONTAP 9.7) **(Zurück zur klassischen Version)** auswählen.
2. **Hardware und Diagnose > Aggregate** auswählen.
3. Wählen Sie die lokale Tier aus, zu der Sie Kapazitätsdisks hinzufügen möchten, und wählen Sie dann **Aktionen > Kapazität hinzufügen**.

> Es empfiehlt sich, Festplatten hinzuzufügen, die die gleiche Größe wie die anderen Festplatten in der lokalen Ebene haben.

4. (Nur für ONTAP 9.7) **Zur neuen Benutzeroberfläche wechseln** auswählen.
5. **Storage > Tiers** auswählen, um die Größe des neuen lokalen Tiers zu überprüfen.

CLI

Bevor Sie beginnen

Die RAID-Gruppengröße der lokalen Speicherebene, zu der der Speicher hinzugefügt wird, muss bekannt sein.

Über diese Aufgabe

Das Verfahren zum Hinzufügen partitionierter Festplatten zu einer lokalen Ebene ist dem Verfahren zum Hinzufügen nicht partitionierter Festplatten ähnlich.

Beim Erweitern einer lokalen Ebene sollten Sie darauf achten, ob Sie partitionierte oder nicht partitionierte Festplatten zur lokalen Ebene hinzufügen. Wenn nicht partitionierte Festplatten zu einer bestehenden lokalen Ebene hinzugefügt werden, übernimmt die neue RAID-Gruppe die Größe der vorhandenen RAID-Gruppen, was die Anzahl der benötigten Paritätsfestplatten beeinflussen kann. Wenn eine nicht partitionierte Festplatte zu einer RAID-Gruppe mit partitionierten Festplatten hinzugefügt wird, wird die neue Festplatte partitioniert, wodurch eine ungenutzte Ersatzpartition entsteht.

Beim Bereitstellen von Partitionen muss sichergestellt werden, dass der Knoten nicht ohne ein Laufwerk mit beiden Partitionen als Reserve bleibt. Ist dies doch der Fall und es kommt zu einer Controller-Störung, könnten wertvolle Informationen zum Problem (die Core-Datei) für den technischen Support nicht verfügbar sein.

Schritte

1. Der verfügbare freie Speicherplatz auf dem System, dem die lokale Ebene zugeordnet ist, wird angezeigt:

   `storage aggregate show-spare-disks -original-owner` *`node_name`*

   Der `-is-disk-shared`Parameter kann verwendet werden, um nur partitionierte oder nur nicht partitionierte Laufwerke anzuzeigen.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                Local
Local
                                                                 Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                     BSAS    7200 block              0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. Die aktuellen RAID-Gruppen für die lokale Ebene anzeigen:

```
storage aggregate show-status <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. Das Hinzufügen des Speichers zum Aggregat simulieren:

```
storage aggregate add-disks -aggregate <aggr_name> -diskcount
<number_of_disks_or_partitions> -simulate true
```

Sie können das Ergebnis der Speichererweiterung sehen, ohne tatsächlich Speicher bereitzustellen. Wenn bei der simulierten Befehlsausführung Warnungen angezeigt werden, besteht die Möglichkeit, den Befehl anzupassen und die Simulation zu wiederholen.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
```

```
                                                             Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. Den Speicher dem Aggregat hinzufügen:

```
storage aggregate add-disks -aggregate <aggr_name> -raidgroup new
-diskcount <number_of_disks_or_partitions>
```

Beim Erstellen einer lokalen Flash Pool Ebene müssen Sie den `-checksumstyle` Parameter verwenden, wenn Festplatten mit einer anderen Prüfsumme als die der lokalen Ebene hinzugefügt werden oder wenn Festplatten zu einer lokalen Ebene mit gemischter Prüfsumme hinzugefügt werden.

Wenn Sie einem lokalen Flash Pool Tier Festplatten hinzufügen, müssen Sie den `-disktype` Parameter verwenden, um den Festplattentyp anzugeben.

Sie können den `-disksize`Parameter verwenden, um eine Größe der hinzuzufügenden Festplatten anzugeben. Es werden nur Festplatten mit ungefähr der angegebenen Größe für die lokale Tier ausgewählt.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Es wird überprüft, ob der Speicher erfolgreich hinzugefügt wurde:

```
storage aggregate show-status -aggregate <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                                    Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                        0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Es sollte überprüft werden, dass der Knoten weiterhin mindestens ein Laufwerk besitzt, bei dem sowohl die Stammpartition als auch die Datenpartition als Ersatzlaufwerk vorhanden sind:

```
storage aggregate show-spare-disks -original-owner <node_name>
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
```

```
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type      RPM Checksum          Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                      BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

Verwandte Informationen

- "storage aggregate add-disks"
- "storage aggregate show-spare-disks"
- "storage aggregate show-status"

Laufwerke zu einem ONTAP Node oder Shelf hinzufügen

Sie fügen einem Node oder Shelf Laufwerke hinzu, um die Anzahl der Hot Spares zu erhöhen oder um dem lokalen Tier zusätzlichen Speicherplatz hinzuzufügen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Das Laufwerk, das Sie hinzufügen möchten, muss von Ihrer Plattform unterstützt werden. Dies kann mit dem "NetApp Hardware Universe" bestätigt werden.

Die Mindestanzahl an HDDs, die Sie in einem einzigen Vorgang hinzufügen sollten, beträgt sechs. Die Mindestanzahl an SSDs, die Sie in einem einzigen Vorgang hinzufügen sollten, beträgt drei. Das Hinzufügen eines Einzellaufwerks kann die Leistung beeinträchtigen.

Schritte für das NetApp Hardware Universe

1. Im Dropdown-Menü **Produkte** die eigene Hardwarekonfiguration auswählen
2. Wählen Sie Ihre Plattform aus.
3. Die verwendete Version von ONTAP auswählen und anschließend **Ergebnisse anzeigen**.
4. Unterhalb der Grafik **Hier klicken, um alternative Ansichten anzuzeigen** auswählen. Die Ansicht auswählen, die der eigenen Konfiguration entspricht.



Schritte zur Installation der Laufwerke

1. Prüfen Sie das "NetApp Support Site" auf neuere Firmware-Dateien für Laufwerke und Gehäuse sowie Datenträgerqualifizierungspakete.

   Falls Ihr Node oder Ihr Shelf nicht über die neuesten Versionen verfügt, sollten diese vor der Installation des neuen Laufwerks aktualisiert werden.

   Bei neuen Laufwerken, die keine aktuelle Firmware-Version besitzen, wird die Laufwerksfirmware automatisch (unterbrechungsfrei) aktualisiert.

2. Sorgen Sie für eine ordnungsgemäße Erdung.
3. Die Blende wird vorsichtig von der Vorderseite der Plattform entfernt.
4. Der richtige Steckplatz für das neue Laufwerk ist zu identifizieren.

   Die korrekten Steckplätze für das Hinzufügen von Laufwerken variieren je nach Plattformmodell und ONTAP Version. In einigen Fällen ist es erforderlich, Laufwerke der Reihe nach in bestimmte Steckplätze einzusetzen. Beispielsweise werden beim AFF A800 die Laufwerke in bestimmten Abständen eingesetzt, sodass Gruppen leerer Steckplätze entstehen. Beim AFF A220 werden neue Laufwerke in die jeweils nächsten leeren Steckplätze eingesetzt, von außen zur Mitte des Shelfs.

   Die Schritte in **Bevor Sie beginnen** geben an, welche Steckplätze für Ihre Konfiguration in der "NetApp Hardware Universe" korrekt sind.

5. Das neue Laufwerk einsetzen:
   a. Bei geöffnetem Nockenhebel das neue Laufwerk mit beiden Händen einsetzen.
   b. Drücken, bis das Laufwerk stoppt.
   c. Den Nockenhebel so schließen, dass das Laufwerk vollständig in der Mittelebene sitzt und der Hebel hörbar einrastet. Darauf achten, den Nockenhebel langsam zu schließen, damit er korrekt mit der Vorderseite des Laufwerks abschließt.
6. Es sollte überprüft werden, ob die Aktivitäts-LED (grün) des Laufwerks leuchtet.

   Leuchtet die Aktivitäts-LED des Laufwerks dauerhaft, bedeutet dies, dass das Laufwerk mit Strom versorgt ist. Blinkt die Aktivitäts-LED des Laufwerks, bedeutet dies, dass das Laufwerk mit Strom versorgt ist und E/A-Vorgänge stattfinden. Wenn die Firmware des Laufwerks automatisch aktualisiert wird, blinkt die LED.

7. Um ein weiteres Laufwerk hinzuzufügen, wiederholen Sie die Schritte 4 bis 6.

   Die neuen Laufwerke werden erst erkannt, nachdem sie einem Knoten zugewiesen wurden. Die neuen Laufwerke können manuell zugewiesen werden, oder ONTAP weist die neuen Laufwerke automatisch zu, sofern Ihr Knoten die Regeln für die automatische Laufwerkszuweisung erfüllt.

8. Nachdem alle neuen Laufwerke erkannt wurden, sollte überprüft werden, ob sie hinzugefügt wurden und

die Eigentümerschaft korrekt angegeben ist.

Schritte zur Bestätigung der Installation

1. Die Liste der Datenträger wird angezeigt:

   ```
   storage aggregate show-spare-disks
   ```

   Die neuen Laufwerke, die dem richtigen Knoten zugeordnet sind, werden angezeigt.

2. **Optional (nur für ONTAP 9.3 und früher),** die neu hinzugefügten Laufwerke auf Null setzen:

   ```
   storage disk zerospares
   ```

   Laufwerke, die zuvor in einer ONTAP lokalen Tier verwendet wurden, müssen vor dem Hinzufügen zu einer anderen lokalen Tier genullt werden. In ONTAP 9.3 und früher kann das Nullsetzen je nach Größe der nicht genullten Laufwerke im Node mehrere Stunden dauern. Das Nullsetzen der Laufwerke kann Verzögerungen verhindern, falls die Größe einer lokalen Tier schnell erhöht werden muss. In ONTAP 9.4 oder später ist dies kein Problem, da die Laufwerke dort mit *Fast Zeroing* innerhalb von Sekunden genullt werden.

Ergebnisse

Die neuen Laufwerke sind einsatzbereit. Sie können sie einer lokalen Tier hinzufügen, sie auf die Liste der Hot Spares setzen oder sie beim Erstellen einer neuen lokalen Tier hinzufügen.

Verwandte Informationen

- "storage aggregate show-spare-disks"
- "Storage Disk ZeroSpares"

Falsch ausgerichtete ONTAP Ersatzpartitionen korrigieren

Beim Hinzufügen partitionierter Festplatten zu einer lokalen Ebene muss für jeden Node eine Festplatte mit sowohl der Root- als auch der Datenpartition als Ersatzfestplatte verfügbar sein. Wenn dies nicht der Fall ist und ein Node eine Störung aufweist, kann ONTAP den Core nicht auf die Ersatzdatenpartition schreiben.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Sowohl eine Ersatzdatenpartition als auch eine Ersatzstammpartition müssen sich auf demselben Festplattentyp befinden, der demselben Node gehört.

Schritte

1. Mit der CLI werden die Ersatzpartitionen für den Node angezeigt:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Notieren Sie, welche Festplatte eine Ersatzdatenpartition (spare_data) und welche Festplatte eine Ersatzrootpartition (spare_root) hat. Die Ersatzpartition zeigt einen Wert ungleich null in der `Local Data`

`Usable`- oder `Local Root Usable`-Spalte an.

2. Die Festplatte mit der Ersatzdatenpartition durch die Festplatte mit der Ersatz-Root-Partition ersetzen:

   `storage disk replace -disk spare_data -replacement spare_root -action start`

   Sie können die Daten in beide Richtungen kopieren; das Kopieren der Stammpartition benötigt jedoch weniger Zeit.

3. Den Fortschritt des Festplattenaustauschs überwachen:

   `storage aggregate show-status -aggregate aggr_name`

4. Nachdem der Austauschvorgang abgeschlossen ist, werden die Ersatzfestplatten erneut angezeigt, um zu bestätigen, dass eine vollständige Ersatzfestplatte vorhanden ist:

   `storage aggregate show-spare-disks -original-owner node_name`

   Eine Ersatzfestplatte mit nutzbarem Speicherplatz sollte sowohl unter „`Local Data Usable`“ als auch unter `Local Root Usable` angezeigt werden.

Beispiel

Sie zeigen Ihre Ersatzpartitionen für Node c1-01 an und sehen, dass Ihre Ersatzpartitionen nicht ausgerichtet sind:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                               Local    Local
                                Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- ------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block         0B 73.89GB  828.0GB
```

Der Festplattenaustausch wird gestartet:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

Während Sie auf den Abschluss des Austauschvorgangs warten, wird der Fortschritt des Vorgangs angezeigt:

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
```

```
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                      Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

Nach Abschluss des Austauschvorgangs sollte eine vollständige Ersatzfestplatte vorhanden sein:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                             Local    Local
                              Data     Root  Physical
 Disk    Type    RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

Verwandte Informationen

- "storage aggregate show"
- "Speicherfestplatte ersetzen"

Datenträger verwalten

Funktionsweise von ONTAP Hot Spare Festplatten

Eine Hot Spare-Ersatzfestplatte ist eine Festplatte, die einem Speichersystem zugewiesen ist und zur Verwendung bereitsteht, aber nicht von einer RAID-Gruppe verwendet wird und keine Daten enthält.

Tritt innerhalb einer RAID-Gruppe ein Festplattenausfall auf, wird die Ersatzfestplatte automatisch der RAID-Gruppe zugewiesen, um die ausgefallenen Festplatten zu ersetzen. Die Daten der ausgefallenen Festplatte werden im Hintergrund von der RAID-Paritätsfestplatte auf die Ersatzfestplatte rekonstruiert. Die Wiederherstellungsaktivität wird in der `/etc/message` Datei protokolliert und eine AutoSupport Meldung wird gesendet.

Wenn die verfügbare Hot Spare-Ersatzfestplatte nicht die gleiche Größe wie die ausgefallene Festplatte hat, wird eine Festplatte der nächstgrößeren Größe ausgewählt und anschließend verkleinert, um der Größe der zu

ersetzenden Festplatte zu entsprechen.

Ersatzfestplattenanforderungen für Multi-Disk Carrier Festplatten

Die Aufrechterhaltung der richtigen Anzahl von Ersatzfestplatten in Mehrfachfestplattenträgern ist entscheidend für die Optimierung der Speicherredundanz und die Minimierung der Zeit, die ONTAP für das Kopieren von Festplatten aufwenden muss, um ein optimales Festplattenlayout zu erreichen.

Es ist erforderlich, für Festplatten mit mehreren Datenträgern jederzeit mindestens zwei Hot-Spare-Festplatten vorzuhalten. Zur Unterstützung der Nutzung des Maintenance Center und zur Vermeidung von Problemen durch mehrere gleichzeitige Festplattenausfälle empfiehlt es sich, für den Dauerbetrieb mindestens vier Hot-Spare-Festplatten vorzuhalten und ausgefallene Festplatten zeitnah zu ersetzen.

Wenn zwei Festplatten gleichzeitig ausfallen und nur zwei Hot-Spare-Festplatten verfügbar sind, kann ONTAP möglicherweise die Inhalte sowohl der ausgefallenen Festplatte als auch ihrer Trägerfestplatte nicht auf die Ersatzfestplatten übertragen. Dieses Szenario wird als Pattsituation bezeichnet. In diesem Fall erfolgt eine Benachrichtigung über EMS-Meldungen und AutoSupport-Meldungen. Sobald die Ersatzträger verfügbar sind, sind die in den EMS-Meldungen bereitgestellten Anweisungen zu befolgen. Weitere Informationen finden sich unter "NetApp Knowledge Base: RAID-Layout kann nicht automatisch korrigiert werden - AutoSupport Meldung"

Wie Warnungen bei niedrigem Reservebestand in ONTAP funktionieren

Standardmäßig werden Warnungen in der Konsole und in den Protokollen ausgegeben, wenn weniger als eine Ersatzfestplatte vorhanden ist, die den Attributen jeder Festplatte in Ihrem Speichersystem entspricht.

Sie können den Schwellenwert für diese Warnmeldungen ändern, damit Ihr System den Best Practices entspricht.

Über diese Aufgabe

Die RAID-Option “min_spare_count” sollte auf “2” gesetzt werden, damit stets die empfohlene Mindestanzahl an Ersatzfestplatten vorhanden ist.

Schritt

1. Die Option auf “2” setzen:

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

Verwandte Informationen

- "storage raid-options modify"

Zusätzliche ONTAP Root Data Partitionierungsverwaltungsoptionen

Über das Bootmenü ist eine Option zur Root-Datenpartitionierung verfügbar, die zusätzliche Verwaltungsfunktionen für Festplatten bietet, die für die Root-Datenpartitionierung konfiguriert sind.

Die folgenden Verwaltungsfunktionen sind unter der Boot Menu Option 9 verfügbar.

- **Alle Festplatten entpartitionieren und deren Eigentümerinformationen entfernen**

  Diese Option ist nützlich, wenn Ihr System für die Root-Daten-Partitionierung konfiguriert ist und mit einer

anderen Konfiguration neu initialisiert werden muss.

- **Bereinigung der Konfiguration und Initialisierung des Knotens mit partitionierten Festplatten**

  Diese Option ist für Folgendes nützlich:

  - Ihr System ist nicht für die Root-Datenpartitionierung konfiguriert und es besteht der Wunsch, es für die Root-Datenpartitionierung zu konfigurieren.
  - Ihr System ist für die Root-Datenpartitionierung falsch konfiguriert und muss korrigiert werden
  - Sie besitzen eine AFF Plattform oder eine FAS Plattform mit ausschließlich SSDs, die für die vorherige Version der Root-Datenpartitionierung konfiguriert ist, und möchten diese auf die neuere Version der Root-Datenpartitionierung aktualisieren, um eine höhere Speichereffizienz zu erzielen.
- **Bereinigung der Konfiguration und Initialisierung des Knotens mit vollständigen Festplatten**

  Diese Option ist nützlich, wenn Sie Folgendes benötigen:

  - Vorhandene Partitionen entpartitionieren
  - Lokalen Festplattenbesitz entfernen
  - Das System mit vollständigen Festplatten unter Verwendung von RAID-DP neu initialisieren

Wann das ONTAP Disk Qualification Package aktualisiert werden sollte

Das Disk Qualification Package (DQP) bietet volle Unterstützung für neu qualifizierte Laufwerke. Bevor Sie die Firmware eines Laufwerks aktualisieren oder neue Laufwerkstypen oder -größen zu einem Cluster hinzufügen, muss das DQP aktualisiert werden. Eine bewährte Vorgehensweise ist es, das DQP regelmäßig zu aktualisieren, beispielsweise vierteljährlich oder halbjährlich.

Sie müssen das DQP in den folgenden Situationen herunterladen und installieren:

- Immer wenn ein neuer Laufwerkstyp oder eine neue Laufwerksgröße dem Knoten hinzugefügt wird

  Wenn Sie beispielsweise bereits 1-TB-Festplatten besitzen und 2-TB-Festplatten hinzufügen, müssen Sie auf das neueste DQP-Update prüfen.

- Immer wenn Sie die Festplatten-Firmware aktualisieren
- Sobald neuere Festplatten-Firmware oder DQP-Dateien verfügbar sind
- Immer wenn auf eine neue Version von ONTAP aktualisiert wird.

  Die DQP wird im Rahmen eines ONTAP Upgrades nicht aktualisiert.

Verwandte Informationen

"NetApp Downloads: Datenträgerqualifizierungspaket"

"NetApp Downloads: Festplatten-Firmware"

Festplatten- und Partitionsbesitz

Verwaltung der Datenträger- und Partitionseigentümerschaft in ONTAP

Sie können die Besitzverhältnisse von Festplatten und Partitionen verwalten.

Folgende Aufgaben sind möglich:

- **"Anzeige des Datenträger- und Partitionsbesitzes"**

  Sie können die Datenträgerbesitzverhältnisse einsehen, um festzustellen, welcher Knoten den Speicher kontrolliert. Sie können außerdem auf Systemen mit gemeinsam genutzten Datenträgern die Partitionsbesitzverhältnisse einsehen.

- **"Einstellungen für die automatische Zuweisung des Festplattenbesitzes ändern"**

  Sie können eine vom Standard abweichende Richtlinie für die automatische Zuweisung des Festplattenbesitzes auswählen oder die automatische Zuweisung des Festplattenbesitzes deaktivieren.

- **"Manuelle Zuweisung der Besitzrechte für nicht partitionierte Datenträger"**

  Wenn Ihr Cluster nicht für die automatische Zuweisung des Festplattenbesitzes konfiguriert ist, muss der Besitz manuell zugewiesen werden.

- **"Manuelle Zuweisung der Besitzrechte partitionierter Festplatten"**

  Sie können die Besitzverhältnisse der Container-Disk oder der Partitionen manuell oder mithilfe der automatischen Zuweisung festlegen, genau wie bei nicht partitionierten Disks.

- **"Entfernen einer defekten Festplatte"**

  Eine Festplatte, die vollständig ausgefallen ist, wird von ONTAP nicht mehr als verwendbare Festplatte betrachtet, und die Festplatte kann sofort vom Gehäuse getrennt werden.

- **"Besitzrechte von einer Festplatte entfernen"**

  ONTAP schreibt die Eigentümerinformationen auf die Festplatte. Vor dem Entfernen einer Ersatzfestplatte oder ihres Gehäuses aus einem Knoten empfiehlt es sich, die Eigentümerinformationen zu entfernen, damit sie ordnungsgemäß in einen anderen Knoten integriert werden kann.

Informationen zur automatischen Zuweisung des ONTAP Festplattenbesitzes

Die automatische Zuweisung nicht zugeordneter Datenträger ist standardmäßig aktiviert. Automatische Zuweisungen der Datenträgereigentümerschaft erfolgen 10 Minuten nach der Initialisierung des HA-Paars und anschließend alle fünf Minuten während des normalen Systembetriebs.

Wenn einem HA-Paar eine neue Festplatte hinzugefügt wird, beispielsweise beim Ersetzen einer ausgefallenen Festplatte, beim Reagieren auf eine Meldung über zu wenige Ersatzfestplatten oder beim Hinzufügen von Kapazität, weist die standardmäßige automatische Zuweisungsrichtlinie die Festplatte einem Knoten als Ersatzfestplatte zu.

Die standardmäßige Richtlinie für die automatische Zuweisung basiert auf plattformspezifischen Merkmalen oder auf dem DS460C Shelf, wenn Ihr HA-Paar nur über diese Shelves verfügt, und verwendet eine der folgenden Methoden (Richtlinien) zur Zuweisung des Festplattenbesitzes:

Zuweisungsmethode	Auswirkungen auf die Knotenzuordnungen	Plattformkonfigurationen, die standardmäßig der Zuweisungsmethode zugeordnet sind
Einschub	Die geraden Buchtennummern werden Knoten A und die ungeraden Buchtennummern Knoten B zugeordnet.	Einstiegssysteme in einer HA-Paar Konfiguration mit einem einzigen, gemeinsam genutzten Shelf.
Regal	Alle Festplatten im Gehäuse sind dem Knoten A zugeordnet.	Einstiegssysteme in einer HA-Paar Konfiguration mit einem Stack aus zwei oder mehr Shelves sowie MetroCluster Konfigurationen mit einem Stack pro Node, zwei oder mehr Shelves.
Split Shelf Diese Richtlinie fällt unter den Wert “default” für den `-autoassign-policy`Parameter des `storage disk option`Befehls für die entsprechenden Plattform- und Shelf-Konfigurationen.	Die Festplatten auf der linken Seite des Regals sind Node A und die auf der rechten Seite Node B zugeordnet. Teilregale auf HA-Paaren werden ab Werk mit Festplatten bestückt, die vom Rand des Regals zur Mitte hin angeordnet sind.	Die meisten AFF Plattformen und einige MetroCluster Konfigurationen.
Stapel	Alle Festplatten im Stapel sind dem Node A zugeordnet.	Stand-alone Einsteigersysteme und alle anderen Konfigurationen.
halbe Schublade Diese Richtlinie fällt unter den Wert “default” für den `-autoassign-policy`Parameter des `storage disk option`Befehls für die entsprechenden Plattform- und Shelf-Konfigurationen.	Alle Laufwerke in der linken Hälfte eines DS460C-Einschubs (Laufwerksschächte 0 bis 5) sind dem Knoten A zugeordnet, alle Laufwerke in der rechten Hälfte eines Einschubs (Laufwerksschächte 6 bis 11) sind dem Knoten B zugeordnet. Bei der Initialisierung eines HA-Paares mit ausschließlich DS460C Shelves wird die automatische Zuweisung des Festplattenbesitzes nicht unterstützt. Die Besitzrechte für Laufwerke, die Root-/Container-Laufwerke mit der Root-Partition enthalten, müssen manuell gemäß der Half-Drawer-Richtlinie zugewiesen werden.	HA-Paare mit nur DS460C Shelves, nach der Initialisierung des HA-Paares (Bootvorgang). Nach dem Hochfahren eines HA-Paares wird die automatische Zuweisung der Festplattenbesitzrechte aktiviert und verwendet die Half-Drawer-Richtlinie, um die Besitzrechte den verbleibenden Laufwerken (mit Ausnahme der Root-Laufwerke/Container-Laufwerke, die die Root-Partition enthalten) und allen zukünftig hinzugefügten Laufwerken zuzuweisen. Wenn Ihr HA-Paar neben anderen Shelf-Modellen auch DS460C Shelves enthält, wird die Half-Drawer Policy nicht verwendet. Die standardmäßig verwendete Policy wird durch plattformspezifische Eigenschaften bestimmt.

Einstellungen und Änderungen für die automatische Zuweisung:

- Die aktuellen Einstellungen für die automatische Zuweisung (ein/aus) lassen sich mit dem `storage disk option show` Befehl anzeigen.
- Die automatische Zuweisung kann mit dem `storage disk option modify` Befehl deaktiviert werden.
- Falls die standardmäßige automatische Zuweisungsrichtlinie in Ihrer Umgebung nicht erwünscht ist, kann die Zuweisungsmethode für Einschub, Regal oder Stapel mit dem `-autoassign-policy` Parameter im `storage disk option modify` Befehl angegeben (geändert) werden.

  Informationen dazu, wie "Einstellungen für die automatische Zuweisung des Festplattenbesitzes ändern".

> Die standardmäßigen automatischen Zuweisungsrichtlinien für halbe Schubladen und geteilte Regale sind insofern einzigartig, als sie nicht wie die Richtlinien für Fächer, Regale und Stapel von Benutzern festgelegt werden können.

In Advanced Drive Partitioning (ADP)-Systemen müssen die Laufwerke in den richtigen Shelf-Einschüben installiert werden, abhängig davon, welchen Shelf-Typ Sie haben, damit die automatische Zuweisung auf halb bestückten Shelves funktioniert:

- Wenn es sich bei Ihrem Shelf nicht um ein DS460C Shelf handelt, werden die Laufwerke gleichmäßig auf der äußersten linken und äußersten rechten Seite installiert und zur Mitte hin verteilt. Zum Beispiel sechs Laufwerke in den Einschüben 0-5 und sechs Laufwerke in den Einschüben 18-23 eines DS224C Shelf.
- Wenn Ihr Shelf ein DS460C Shelf ist, werden die Laufwerke in der vorderen Reihe (Laufwerksschächte 0, 3, 6 und 9) jeder Schublade installiert. Die verbleibenden Laufwerke werden gleichmäßig auf jede Schublade verteilt, indem die Schubladenreihen von vorne nach hinten befüllt werden. Wenn nicht genügend Laufwerke vorhanden sind, um die Reihen zu füllen, werden sie paarweise installiert, sodass die Laufwerke die linke und rechte Seite einer Schublade gleichmäßig belegen.

  Die Installation der Laufwerke in der vordersten Reihe jeder Schublade ermöglicht eine ordnungsgemäße Luftzirkulation und verhindert eine Überhitzung.

> Sind Laufwerke in halb bestückten Gehäusen nicht in den korrekten Einschüben installiert, weist ONTAP beim Ausfall und Austausch eines Containerlaufwerks die Besitzrechte nicht automatisch zu. In diesem Fall muss die Zuweisung des neuen Containerlaufwerks manuell erfolgen. Nach der Zuweisung der Besitzrechte für das Containerlaufwerk übernimmt ONTAP automatisch die erforderliche Laufwerkspartitionierung und Partitionszuweisung.

In manchen Situationen, in denen die automatische Zuweisung nicht funktioniert, ist die Festplattenzuweisung manuell mit dem `storage disk assign` Befehl vorzunehmen:

- Wenn die automatische Zuweisung deaktiviert ist, stehen neue Festplatten erst als Ersatzfestplatten zur Verfügung, nachdem sie manuell einem Knoten zugewiesen wurden.
- Wenn Sie möchten, dass Festplatten automatisch zugewiesen werden und Sie mehrere Stapel oder Regale haben, die unterschiedliche Eigentümer haben müssen, muss auf jedem Stapel oder Regal eine Festplatte manuell zugewiesen worden sein, damit die automatische Eigentümerzuweisung auf jedem Stapel oder Regal funktioniert.
- Wenn die automatische Zuordnung aktiviert ist und manuell ein Einzellaufwerk einem Knoten zugewiesen wird, der nicht in der aktiven Richtlinie angegeben ist, funktioniert die automatische Zuordnung nicht mehr und eine EMS-Meldung wird angezeigt.

Informationen dazu, wie "Manuelle Zuweisung des Festplattenbesitzes von nicht partitionierten Festplatten".

Informationen dazu, wie "Manuelle Zuweisung des Festplattenbesitzes partitionierter Festplatten".

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Storage Disk Option ändern"
- "storage disk option show"

Anzeige von ONTAP Festplatten- und Partitionszuordnungen

Sie können die Datenträgerbesitzverhältnisse einsehen, um festzustellen, welcher Knoten den Speicher kontrolliert. Sie können außerdem auf Systemen mit gemeinsam genutzten Datenträgern die Partitionsbesitzverhältnisse einsehen.

Schritte

1. Besitzverhältnisse der physischen Datenträger werden angezeigt:

   `storage disk show -ownership`

```
cluster::> storage disk show -ownership
Disk     Aggregate Home     Owner    DR Home  Home ID     Owner ID   DR
Home ID  Reserver    Pool
-------- --------- -------- -------- -------- ---------- -----------
----------- ----------- ------
1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
1.0.3    -         node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
```

2. Wenn ein System mit gemeinsam genutzten Festplatten verwendet wird, lässt sich die Partitionszugehörigkeit anzeigen:

   `storage disk show -partition-ownership`

```
cluster::> storage disk show -partition-ownership
                                Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
```

```
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

Verwandte Informationen

- "Speicherdatenträger anzeigen"

Einstellungen für die automatische Zuweisung der ONTAP Festplattenzugehörigkeit ändern

Sie können den `storage disk option modify`Befehl verwenden, um eine nicht standardmäßige Richtlinie für die automatische Zuweisung des Festplattenbesitzes auszuwählen oder die automatische Zuweisung des Festplattenbesitzes zu deaktivieren.

Informationen dazu "automatische Zuweisung des Festplattenbesitzes".

Über diese Aufgabe

Wenn ein HA-Paar ausschließlich aus DS460C Shelves besteht, ist die standardmäßige automatische Zuweisungsrichtlinie „half-drawer“. Ein Wechsel zu einer nicht standardmäßigen Richtlinie (bay, shelf, stack) ist nicht möglich.

Schritte

1. Automatische Datenträgerzuordnung ändern:
   a. Wenn Sie eine vom Standard abweichende Richtlinie auswählen möchten, geben Sie Folgendes ein:

      `storage disk option modify -autoassign-policy` *`autoassign_policy`* `-node` *`node_name`*

      - Verwenden Sie `stack` als *`autoassign_policy`* zur Konfiguration der automatischen Besitzverwaltung auf Stack- oder Schleifenebene.
      - Verwenden Sie `shelf` als *`autoassign_policy`* zur Konfiguration der automatischen Eigentümerschaft auf Shelf-Ebene.
      - Verwenden Sie `bay` als *`autoassign_policy`* zur Konfiguration der automatischen Eigentümerschaft auf Einschubebene.

   b. Wenn die automatische Zuweisung des Datenträgerbesitzes deaktiviert werden soll, ist folgender Befehl einzugeben:

      `storage disk option modify -autoassign off -node` *`node_name`*

2. Die Einstellungen für die automatische Datenträgerzuordnung überprüfen:

   `storage disk option show`

```
cluster1::> storage disk option show

Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                          Assign Policy
-------------  -------------  ------------  -------------  --------
```

```
cluster1-1     on              on              on              default
cluster1-2     on              on              on              default
```

Verwandte Informationen

- "Storage Disk Option ändern"
- "storage disk option show"

Manuelle Zuweisung von ONTAP Festplattenbesitzrechten für nicht partitionierte Festplatten

Wenn Ihr HA-Paar nicht für die automatische Zuweisung von Festplattenbesitz konfiguriert ist, muss der Besitz manuell zugewiesen werden. Wenn ein HA-Paar initialisiert wird, das ausschließlich DS460C Shelves enthält, muss der Besitz der Root-Laufwerke manuell zugewiesen werden.

Über diese Aufgabe

- Wenn die Besitzverhältnisse in einem HA-Paar, das nicht initialisiert wird und nicht ausschließlich DS460C Shelves enthält, manuell zugewiesen werden, ist Option 1 zu verwenden.
- Wenn Sie ein HA-Paar initialisieren, das nur DS460C Shelves enthält, verwenden Sie Option 2, um die Eigentümerschaft für die Root-Laufwerke manuell zuzuweisen.

▼ **Option 1: Die meisten HA Paare**

Für ein HA-Paar, das nicht initialisiert wird und nicht ausschließlich DS460C Shelves enthält, kann dieses Verfahren zur manuellen Zuweisung des Eigentums verwendet werden.

Über diese Aufgabe

- Die Festplatten, denen Sie die Besitzrechte zuweisen, müssen sich in einem Shelf befinden, das physisch mit dem Node verbunden ist, dem Sie die Besitzrechte zuweisen.
- Wenn Sie Festplatten in einer lokalen Ebene (Aggregat) verwenden:
  - Festplatten müssen einem Knoten zugeordnet sein, bevor sie in einer lokalen Ebene (Aggregate) verwendet werden können.
  - Die Besitzverhältnisse einer Festplatte, die in einer lokalen Ebene (Aggregat) verwendet wird, können nicht neu zugewiesen werden.

Schritte

1. Mit der Befehlszeilenschnittstelle (CLI) werden alle nicht zugeordneten Datenträger angezeigt:

   ```
   storage disk show -container-type unassigned
   ```

2. Jeder Festplatte Folgendes zuweisen:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   Sie können das Platzhalterzeichen verwenden, um mehr als einen Datenträger gleichzeitig zuzuweisen. Wenn Sie eine Ersatzfestplatte neu zuweisen, die bereits einem anderen Knoten gehört, muss die Option „-force“ verwendet werden.

▼ **Option 2: Ein HA-Paar mit ausschließlich DS460C Shelves**

Für ein HA-Paar, das initialisiert wird und nur DS460C Shelves enthält, kann mit diesem Verfahren die Eigentümerschaft für die Root-Laufwerke manuell zugewiesen werden.

Über diese Aufgabe

- Bei der Initialisierung eines HA-Paares, das ausschließlich DS460C Shelves enthält, müssen die Root-Laufwerke manuell so zugewiesen werden, dass sie der Half-Drawer-Richtlinie entsprechen.

  Nach der Initialisierung des HA-Paares (Bootvorgang) ist die automatische Zuweisung der Festplattenbesitzrechte aktiviert und verwendet die Half-Drawer-Richtlinie, um die Besitzrechte den verbleibenden Laufwerken (mit Ausnahme der Root-Laufwerke) und allen zukünftig hinzugefügten Laufwerken zuzuweisen, wie etwa beim Ersetzen ausgefallener Festplatten, beim Reagieren auf eine „low spares“-Meldung oder beim Hinzufügen von Kapazität.

  "Informationen zur Regelung zur halben Schublade".

- Für RAID sind mindestens 10 Laufwerke pro HA-Paar (5 pro Knoten) erforderlich, wenn NL-SAS-Laufwerke mit mehr als 8 TB in einem DS460C Shelf verwendet werden.

Schritte

1. Falls Ihre DS460C Shelves nicht vollständig bestückt sind, die folgenden Teilschritte ausführen; andernfalls zum nächsten Schritt wechseln.

   a. Zuerst werden die Laufwerke in der vorderen Reihe (Laufwerksschächte 0, 3, 6 und 9) jeder Schublade installiert.

      Die Installation der Laufwerke in der vordersten Reihe jeder Schublade ermöglicht eine ordnungsgemäße Luftzirkulation und verhindert eine Überhitzung.

   b. Die restlichen Laufwerke werden gleichmäßig auf die einzelnen Schubladen verteilt.

      Die Schubladenreihen werden von vorne nach hinten bestückt. Wenn nicht genügend Laufwerke vorhanden sind, um die Reihen zu füllen, werden sie paarweise installiert, sodass die Laufwerke die linke und rechte Seite einer Schublade gleichmäßig belegen.

      Die folgende Abbildung zeigt die Nummerierung und die Positionen der Laufwerksschächte in einer DS460C-Schublade.



2. Melden Sie sich über die node-management LIF oder die cluster-management LIF bei der clustershell an.

3. Die Stammlaufwerke in jedem Fach werden manuell gemäß der Halbfachrichtlinie zugewiesen, wobei die folgenden Teilschritte zu beachten sind:

   Bei der Half-Drawer-Richtlinie werden die Laufwerke der linken Hälfte eines Laufwerksschachts (Einschübe 0 bis 5) Knoten A und die Laufwerke der rechten Hälfte eines Laufwerksschachts (Einschübe 6 bis 11) Knoten B zugeordnet.

   a. Alle nicht zugeordneten Datenträger anzeigen:
      `storage disk show -container-type unassigned`

   b. Root-Disks zuweisen:
      `storage disk assign -disk disk_name -owner owner_name`

      Sie können das Platzhalterzeichen verwenden, um mehr als einen Datenträger gleichzeitig zuzuweisen.

Weitere Informationen zu `storage disk` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"

Manuelle Zuweisung der Besitzrechte von ONTAP partitionierten Festplatten

Sie können die Besitzrechte der Containerfestplatte oder der Partitionen auf Advanced Drive Partitioning (ADP) Systemen manuell zuweisen. Wenn ein HA-Paar initialisiert wird, das ausschließlich DS460C Shelves enthält, muss die Besitzrechte für die Containerfestplatten, die Root-Partitionen enthalten werden, manuell zugewiesen werden.

Über diese Aufgabe

- Die Art des verwendeten Speichersystems bestimmt, welche Methode von ADP unterstützt wird, root-data (RD) oder root-data-data (RD2).

  FAS Speichersysteme verwenden RD und AFF Speichersysteme verwenden RD2.

- Wenn die Besitzverhältnisse in einem HA-Paar, das nicht initialisiert wird und nicht ausschließlich DS460C Shelves enthält, manuell zugewiesen werden, kann Option 1 zur manuellen Zuweisung von Festplatten mit Root-Data-Partitionierung (RD) oder Option 2 zur manuellen Zuweisung von Festplatten mit Root-Data-Data-Partitionierung (RD2) verwendet werden.
- Wenn Sie ein HA-Paar initialisieren, das nur DS460C Shelves enthält, verwenden Sie Option 3, um die Eigentümerschaft für die Container-Laufwerke, die die Root-Partition enthalten, manuell zuzuweisen.

▼ Option 1: Manuelle Zuweisung von Festplatten mit Root-Data-Partitionierung (RD)

Bei der Root-Datenpartitionierung gibt es drei zugehörige Entitäten (die Container-Festplatte und die beiden Partitionen), die gemeinsam dem HA Pair gehören.

Über diese Aufgabe

- Die Container-Festplatte und die beiden Partitionen müssen nicht alle demselben Knoten im HA-Paar gehören, solange sie alle einem der Knoten im HA-Paar zugeordnet sind. Wenn jedoch eine Partition in einer lokalen Ebene verwendet wird, muss sie demselben Knoten gehören, dem auch die lokale Ebene gehört.

- Wenn eine Container-Festplatte in einem nur halb bestückten Shelf ausfällt und ersetzt wird, kann es erforderlich sein, die Festplattenzugehörigkeit manuell zuzuweisen, da ONTAP in diesem Fall die Eigentumszuweisung nicht immer automatisch vornimmt.
- Nach der Zuweisung der Container-Festplatte übernimmt die ONTAP Software automatisch alle erforderlichen Partitionierungen und Partitionszuweisungen.

Schritte

1. Die CLI zeigt den aktuellen Eigentümer der partitionierten Festplatte an:

   `storage disk show -disk` *`disk_name`* `-partition-ownership`

2. Die CLI-Berechtigungsstufe auf „Erweitert“ setzen:

   `set -privilege advanced`

3. Geben Sie den entsprechenden Befehl ein, abhängig davon, für welche Eigentümereinheit die Eigentümerschaft zugewiesen werden soll:

   Falls eine der Eigentümergesellschaften bereits in Besitz ist, muss die Option `-force` eingeschlossen werden.

Wenn Sie die Eigentumsrechte für die… zuweisen möchten	Verwenden Sie diesen Befehl…
Container-Festplatte	`storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`*
Datenpartition	`storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`* `-data true`
Root-Partition	`storage disk assign -disk` *`disk_name`* `-owner` *`owner_name`* `-root true`

▼ **Option 2: Manuelle Zuweisung von Festplatten mit Root-Data-Data (RD2) Partitionierung**

Bei der Root-Daten-Daten-Partitionierung gehören vier Entitäten (die Container-Festplatte und die drei Partitionen) gemeinsam dem HA-Paar. Die Root-Daten-Daten-Partitionierung erstellt eine kleine Partition als Root-Partition und zwei größere, gleich große Partitionen für Daten.

Über diese Aufgabe

- Parameter müssen mit dem `disk assign` Befehl verwendet werden, um die richtige Partition einer root-data-data-partitionierten Festplatte zuzuweisen. Diese Parameter können nicht für Festplatten verwendet werden, die Teil eines Speicherpools sind. Der Standardwert ist `false`.
  - Der `-data1 true`Parameter weist die `data1`Partition einer root-data1-data2 partitionierten Festplatte zu.
  - Der `-data2 true`Parameter weist die `data2`Partition einer root-data1-data2 partitionierten Festplatte zu.
- Wenn eine Container-Festplatte in einem nur halb bestückten Shelf ausfällt und ersetzt wird, kann es erforderlich sein, die Festplattenzugehörigkeit manuell zuzuweisen, da ONTAP in diesem Fall die Eigentumszuweisung nicht immer automatisch vornimmt.
- Nach der Zuweisung der Container-Festplatte übernimmt die ONTAP Software automatisch alle erforderlichen Partitionierungen und Partitionszuweisungen.

Schritte

1. Die CLI zeigt den aktuellen Eigentümer der partitionierten Festplatte an:

   `storage disk show -disk disk_name -partition-ownership`

2. Die CLI-Berechtigungsstufe auf „Erweitert“ setzen:

   `set -privilege advanced`

3. Geben Sie den entsprechenden Befehl ein, abhängig davon, für welche Eigentümereinheit die Eigentümerschaft zugewiesen werden soll:

   Falls eine der Eigentümergesellschaften bereits in Besitz ist, muss die Option `-force` eingeschlossen werden.

Wenn Sie die Eigentumsrechte für die… zuweisen möchten	Verwenden Sie diesen Befehl…
Container-Festplatte	`storage disk assign -disk disk_name -owner owner_name`
Data1 Partition	`storage disk assign -disk disk_name -owner owner_name -data1 true`
Data2 Partition	`storage disk assign -disk disk_name -owner owner_name -data2 true`
Root-Partition	`storage disk assign -disk disk_name -owner owner_name -root true`

▼ **Option 3: Manuelle Zuweisung von DS460C Containerlaufwerken mit der Root-Partition**

Wenn Sie ein HA-Paar initialisieren, das nur DS460C Shelves enthält, müssen Sie die Besitzrechte für die Container-Laufwerke, die die Root-Partition enthalten, manuell zuweisen, indem Sie die Half-Drawer-Richtlinie einhalten.

Über diese Aufgabe

- Bei der Initialisierung eines HA-Paares, das ausschließlich DS460C Shelves enthält, unterstützen die ADP Bootmenüoptionen 9a und 9b keine automatische Laufwerkszuweisung. Die Containerlaufwerke mit der Root-Partition müssen gemäß der Half-Drawer-Richtlinie manuell zugewiesen werden.

  Nach der Initialisierung des HA-Paares (Bootvorgang) ist die automatische Zuweisung der Festplattenbesitzrechte automatisch aktiviert und verwendet die Half-Drawer-Richtlinie, um die Besitzrechte den verbleibenden Laufwerken (außer den Container-Laufwerken, die die Root-Partition enthalten) und allen zukünftig hinzugefügten Laufwerken zuzuweisen, wie etwa beim Ersetzen ausgefallener Laufwerke, beim Reagieren auf eine „Low Spares“-Meldung oder beim Hinzufügen von Kapazität.

- "Informationen zur Regelung zur halben Schublade".

Schritte

1. Falls Ihre DS460C Shelves nicht vollständig bestückt sind, die folgenden Teilschritte ausführen; andernfalls zum nächsten Schritt wechseln.

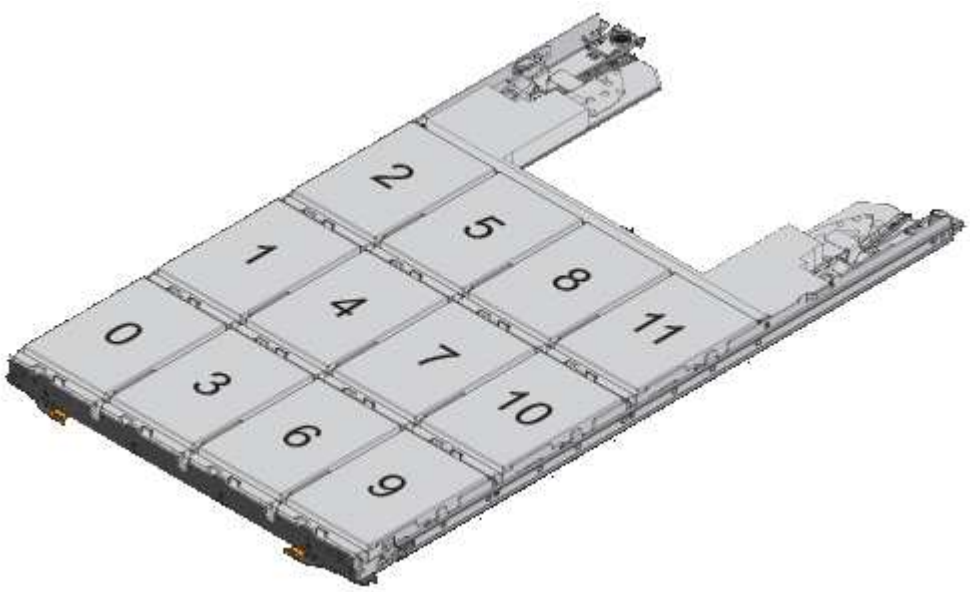
   a. Zuerst werden die Laufwerke in der vorderen Reihe (Laufwerksschächte 0, 3, 6 und 9) jeder Schublade installiert.

Die Installation der Laufwerke in der vordersten Reihe jeder Schublade ermöglicht eine ordnungsgemäße Luftzirkulation und verhindert eine Überhitzung.

b. Die restlichen Laufwerke werden gleichmäßig auf die einzelnen Schubladen verteilt.

   Die Schubladenreihen werden von vorne nach hinten bestückt. Wenn nicht genügend Laufwerke vorhanden sind, um alle Reihen zu füllen, sollten sie paarweise so eingesetzt werden, dass die linke und rechte Seite einer Schublade gleichmäßig belegt sind.

   Die folgende Abbildung zeigt die Nummerierung und die Positionen der Laufwerksschächte in einer DS460C-Schublade.



2. Melden Sie sich über die node-management LIF oder die cluster-management LIF bei der clustershell an.
3. Für jede Schublade werden die Containerlaufwerke, die die Stammpartition enthalten, manuell zugewiesen, indem die Richtlinie für halbe Schubladen unter Verwendung der folgenden Teilschritte eingehalten wird:

   Bei der Half-Drawer-Richtlinie werden die Laufwerke der linken Hälfte eines Drawers (Einschübe 0 bis 5) Node A und die Laufwerke der rechten Hälfte eines Drawers (Einschübe 6 bis 11) Node B zugewiesen.

   a. Alle nicht zugeordneten Datenträger anzeigen:
      `storage disk show -container-type unassigned`

   b. Weisen Sie die Containerlaufwerke zu, die die Root-Partition enthalten:
      `storage disk assign -disk disk_name -owner owner_name`

      Sie können das Platzhalterzeichen verwenden, um mehr als ein Laufwerk gleichzeitig zuzuweisen.

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"

Wenn ein HA-Paar werkseitig für die Verwendung der Root-Datenpartitionierung konfiguriert ist, wird die Eigentümerschaft der Datenpartitionen zwischen beiden Knoten des Paares für die Nutzung in einer Aktiv/Aktiv-Konfiguration aufgeteilt. Soll das HA-Paar in einer Aktiv/Passiv-Konfiguration verwendet werden, ist die Partitionseigentümerschaft vor der Erstellung der lokalen Datenebene zu aktualisieren.

Bevor Sie beginnen

- Es sollte festgelegt sein, welcher Knoten der aktive und welcher der passive Knoten ist.
- Die Speicherausfallsicherung muss auf dem HA Pair konfiguriert werden.

Über diese Aufgabe

Diese Aufgabe wird auf zwei Knoten ausgeführt: Knoten A und Knoten B.

Dieses Verfahren ist für Knoten vorgesehen, für die kein Datenaggregat aus den partitionierten Festplatten erstellt wurde.

Informationen dazu "Erweiterte Festplattenpartitionierung".

Schritte

Alle Befehle werden in der Cluster-Shell eingegeben.

1. Die aktuelle Eigentümerstruktur der Datenpartitionen wird angezeigt:

   ```
   storage aggregate show-spare-disks
   ```

   Die Ausgabe zeigt, dass die Hälfte der Datenpartitionen einem Knoten und die andere Hälfte dem anderen Knoten zugeordnet ist. Alle Datenpartitionen sollten Reservepartitionen sein.

   ```
   cluster1::> storage aggregate show-spare-disks

   Original Owner: cluster1-01
    Pool0
     Partitioned Spares
                                                                  Local
   Local
                                                                   Data
   Root Physical
    Disk                       Type     RPM Checksum         Usable
   Usable     Size
    -------------------------- ----- ------ -------------- --------
   -------- --------
    1.0.0                      BSAS    7200 block           753.8GB
   0B  828.0GB
    1.0.1                      BSAS    7200 block           753.8GB
   73.89GB  828.0GB
    1.0.5                      BSAS    7200 block           753.8GB
   0B  828.0GB
   ```

```
 1.0.6                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                     BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                     BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                        Local
Local
                                                         Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                      BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. Die erweiterte Berechtigungsstufe eingeben:

   ```
   set advanced
   ```

3. Für jede Datenpartition, die dem Knoten gehört, der der passive Knoten sein wird, wird sie dem aktiven Knoten zugewiesen:

   ```
   storage disk assign -force -data true -owner active_node_name -disk disk_name
   ```

   Sie müssen die Partition nicht als Teil des Datenträgernamens angeben.

   Für jede Datenpartition, die Sie neu zuweisen müssen, wäre ein Befehl ähnlich dem folgenden Beispiel einzugeben:

   ```
   storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
   ```

4. Bestätigen Sie, dass alle Partitionen dem aktiven Knoten zugewiesen sind.

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                     BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                     BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
```

```
Root Physical
 Disk                        Type      RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Beachten Sie, dass cluster1-02 weiterhin eine freie Root-Partition besitzt.

5. Zurück zu als Administrator angemeldet:

   `set admin`

6. Erstellen Sie Ihre lokale Datenebene und lassen Sie mindestens eine Datenpartition als Reserve:

   `storage aggregate create` *`new_aggr_name`* `-diskcount` *`number_of_partitions`* `-node` *`active_node_name`*

   Die lokale Datenebene wird erstellt und gehört dem aktiven Knoten.

Verwandte Informationen

- "Speicheraggregat erstellen"
- "storage aggregate show"
- "Speicherdatenträger zuweisen"

Einrichtung von Aktiv/Passiv ONTAP Knoten mit Root-Data-Data-Partitionierung

Wenn ein HA-Paar werkseitig für die Verwendung der Root-Daten-Daten-Partitionierung konfiguriert ist, wird die Eigentümerschaft der Datenpartitionen zwischen beiden Knoten des Paares für die Verwendung in einer Aktiv/Aktiv-Konfiguration aufgeteilt. Soll das HA-Paar in einer Aktiv/Passiv-Konfiguration verwendet werden, ist die Partitionseigentümerschaft vor der Erstellung der lokalen Datenebene zu aktualisieren.

Bevor Sie beginnen

- Es sollte festgelegt sein, welcher Knoten der aktive und welcher der passive Knoten ist.
- Die Speicherausfallsicherung muss auf dem HA Pair konfiguriert werden.

Über diese Aufgabe

Diese Aufgabe wird auf zwei Knoten ausgeführt: Knoten A und Knoten B.

Dieses Verfahren ist für Knoten vorgesehen, für die kein Datenaggregat aus den partitionierten Festplatten erstellt wurde.

Informationen dazu "Erweiterte Festplattenpartitionierung".

Schritte

Alle Befehle werden in der Cluster-Shell eingegeben.

1. Die aktuelle Eigentümerstruktur der Datenpartitionen wird angezeigt:

   `storage aggregate show-spare-disks -original-owner passive_node_name -fields local-usable-data1-size, local-usable-data2-size`

   Die Ausgabe zeigt, dass die Hälfte der Datenpartitionen einem Knoten und die andere Hälfte dem anderen Knoten zugeordnet ist. Alle Datenpartitionen sollten Reservepartitionen sein.

2. Die erweiterte Berechtigungsstufe eingeben:

   `set advanced`

3. Jede data1-Partition, die dem Knoten gehört, der der passive Knoten sein wird, dem aktiven Knoten zuweisen:

   `storage disk assign -force -data1 -owner active_node_name -disk disk_name`

   Sie müssen die Partition nicht als Teil des Datenträgernamens angeben.

4. Jede data2-Partition, die dem Knoten gehört, der der passive Knoten sein wird, dem aktiven Knoten zuweisen:

   `storage disk assign -force -data2 -owner active_node_name -disk disk_name`

   Sie müssen die Partition nicht als Teil des Datenträgernamens angeben.

5. Bestätigt wird, dass alle Partitionen dem aktiven Knoten zugewiesen sind:

   `storage aggregate show-spare-disks`

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                      BSAS    7200 block           753.8GB
```

```
0B  828.0GB
 1.0.4                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                       BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Beachten Sie, dass cluster1-02 weiterhin eine freie Root-Partition besitzt.

6. Zurück zu als Administrator angemeldet:

   ```
   set admin
   ```

7. Das Datenaggregat wird erstellt, wobei mindestens eine Datenpartition als Reserve verbleibt:

   ```
   storage aggregate create new_aggr_name -diskcount number_of_partitions -node
   active_node_name
   ```

   Das Datenaggregat wird erstellt und befindet sich im Besitz des aktiven Knotens.

8. Alternativ lässt sich das von ONTAP empfohlene lokale Tier-Layout nutzen, das Best Practices für das RAID-Gruppenlayout und die Anzahl der Ersatzfestplatten umfasst:

```
storage aggregate auto-provision
```

Verwandte Informationen

- "Automatische Bereitstellung von Speicheraggregaten"
- "Speicheraggregat erstellen"
- "storage aggregate show"
- "Speicherdatenträger zuweisen"

ONTAP Besitzrechte von einer Festplatte entfernen

ONTAP schreibt die Eigentümerinformationen auf die Festplatte. Vor dem Entfernen einer Ersatzfestplatte oder ihres Gehäuses aus einem Knoten empfiehlt es sich, die Eigentümerinformationen zu entfernen, damit sie ordnungsgemäß in einen anderen Knoten integriert werden kann.

> Wenn die Festplatte für die Root-Datenpartitionierung partitioniert ist und ONTAP 9.10.1 oder höher verwendet wird, ist der NetApp Technical Support für Unterstützung beim Entfernen der Besitzrechte zu kontaktieren. Weitere Informationen finden sich im "Knowledge Base Artikel: Fehler beim Entfernen des Festplattenbesitzers".

Bevor Sie beginnen

Die Festplatte, von der Sie die Besitzverhältnisse entfernen möchten, muss die folgenden Anforderungen erfüllen:

- Es muss sich um eine Ersatzfestplatte handeln.

  Sie können die Besitzrechte an einer Festplatte, die in einer lokalen Tier verwendet wird, nicht entfernen.

- Es kann sich nicht im Wartungszentrum befinden.
- Es darf sich nicht in der Bereinigung befinden.
- Es kann nicht fehlgeschlagen sein.

  Es ist nicht notwendig, die Besitzrechte einer ausgefallenen Festplatte zu entfernen.

Über diese Aufgabe

Wenn die automatische Festplattenzuweisung aktiviert ist, kann ONTAP die Besitzverhältnisse automatisch neu zuweisen, bevor die Festplatte aus dem Knoten entfernt wird. Aus diesem Grund wird die automatische Besitzzuweisung deaktiviert, bis die Festplatte entfernt ist, und anschließend wieder aktiviert.

Schritte

1. Wenn die automatische Zuweisung der Festplattenbesitzrechte aktiviert ist, kann sie über die Befehlszeile deaktiviert werden:

   ```
   storage disk option modify -node node_name -autoassign off
   ```

2. Falls erforderlich kann der vorherige Schritt für den HA-Partner des Knotens wiederholt werden.
3. Die Software-Eigentümerinformationen werden von der Festplatte entfernt:

   ```
   storage disk removeowner disk_name
   ```

Um Besitzinformationen von mehreren Datenträgern zu entfernen, ist eine durch Kommas getrennte Liste zu verwenden.

Beispiel:

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. Wenn die Festplatte für die Root-Datenpartitionierung partitioniert ist und ONTAP 9.9.1 oder eine frühere Version verwendet wird, sind die Besitzrechte der Partitionen zu entfernen:

   `storage disk removeowner -disk disk_name -root true`

   `storage disk removeowner -disk disk_name -data true`

   Beide Partitionen gehören keinem Knoten mehr.

5. Wenn Sie die automatische Zuweisung des Datenträgerbesitzes zuvor deaktiviert hatten, sollte sie nach dem Entfernen oder der Neuzuweisung des Datenträgers wieder aktiviert werden:

   `storage disk option modify -node node_name -autoassign on`

6. Falls erforderlich kann der vorherige Schritt für den HA-Partner des Knotens wiederholt werden.

Verwandte Informationen

- "Storage Disk Option ändern"
- "storage disk removeowner"

Entfernen einer ausgefallenen ONTAP Festplatte

Eine vollständig ausgefallene Festplatte wird von ONTAP nicht mehr als nutzbare Festplatte gezählt und kann sofort vom Festplattengehäuse getrennt werden. Eine teilweise ausgefallene Festplatte sollte jedoch so lange angeschlossen bleiben, bis der Rapid RAID Recovery-Prozess abgeschlossen ist.

Über diese Aufgabe

Wenn Sie eine Festplatte entfernen, weil sie defekt ist oder übermäßig viele Fehlermeldungen ausgibt, sollte die Festplatte weder in diesem noch in einem anderen Speichersystem wiederverwendet werden.

Schritte

1. Verwenden Sie die Befehlszeilenschnittstelle (CLI), um die Festplatten-ID der ausgefallenen Festplatte zu ermitteln:

   `storage disk show -broken`

   Wenn die Festplatte nicht in der Liste der ausgefallenen Festplatten erscheint, ist sie möglicherweise teilweise ausgefallen, und eine Rapid RAID Recovery ist im Gange. In diesem Fall wird empfohlen, zu warten, bis die Festplatte in der Liste der ausgefallenen Festplatten aufgeführt ist (was bedeutet, dass der Rapid RAID Recovery Prozess abgeschlossen ist), bevor die Festplatte entfernt wird.

   Ermitteln Sie die Modellnummer aus der letzten Spalte der Ausgabe.

2. Den physischen Standort der Festplatte bestimmen, die entfernt werden soll:

   `storage disk set-led -action on -disk disk_name 2`

   Die Fehler-LED auf der Vorderseite der Festplatte leuchtet.

3. Die Festplatte ist gemäß den Anweisungen im Hardwarehandbuch für das jeweilige Festplattengehäusemodell aus dem Festplattengehäuse zu entfernen.

Verwandte Informationen

- "Storage Disk Set-LED"
- "Speicherdatenträger anzeigen"

Datenträgerbereinigung

Informationen zur ONTAP Festplattenbereinigung

Festplattenbereinigung ist der Prozess der physischen Vernichtung von Daten durch Überschreiben von Festplatten oder SSDs mit festgelegten Byte-Mustern oder Zufallsdaten, sodass eine Wiederherstellung der Originaldaten unmöglich wird. Durch den Bereinigungsprozess wird sichergestellt, dass niemand die Daten auf den Festplatten wiederherstellen kann.

Diese Funktionalität ist in allen ONTAP 9 Versionen über die nodeshell verfügbar und ab ONTAP 9.6 auch im Wartungsmodus.

Der Festplattenbereinigungsprozess verwendet drei aufeinanderfolgende, standardmäßige oder benutzerdefinierte Byte-Überschreibungsmuster für bis zu sieben Zyklen pro Vorgang. Das zufällige Überschreibungsmuster wird für jeden Zyklus wiederholt.

Je nach Festplattenkapazität, Mustern und Anzahl der Zyklen kann der Vorgang mehrere Stunden dauern. Die Festplattenbereinigung läuft im Hintergrund. Der Status des Festplattenbereinigungsprozesses kann angezeigt werden, außerdem kann der Prozess gestartet und gestoppt werden. Der Festplattenbereinigungsprozess besteht aus zwei Phasen: der „Formatierungsphase“ und der „Musterüberschreibungsphase“.

Formatierungsphase

Die für die Formatierungsphase durchgeführte Operation hängt von der Klasse des zu bereinigenden Datenträgers ab, wie in der folgenden Tabelle dargestellt:

Datenträgerklasse	Formatierungsphasenoperation
Kapazitäts-HDDs	Übersprungen
Performance-HDDs	SCSI-Formatvorgang
SSDs	SCSI-Sanitize-Operation

Musterüberschreibungsphase

Die festgelegten Überschreibungsmuster werden für die angegebene Anzahl von Zyklen wiederholt.

Nach Abschluss des Bereinigungsprozesses befinden sich die angegebenen Festplatten im bereinigten Zustand. Sie werden nicht automatisch wieder in den Ersatzstatus zurückversetzt. Die bereinigten Festplatten müssen dem Ersatzpool hinzugefügt werden, bevor die neu bereinigten Festplatten einer anderen lokalen

Ebene hinzugefügt werden können.

Nicht unterstützte Szenarien für ONTAP Festplattenbereinigung

Unter diesen Umständen kann keine Festplattenbereinigung durchgeführt werden.

- Im Übernahmemodus für Systeme in einem HA-Paar wird dies nicht unterstützt.
- Dies kann nicht auf Festplatten durchgeführt werden, die aufgrund von Lese- oder Schreibproblemen ausgefallen sind.
- Wenn Sie das Zufallsmuster verwenden, kann es nicht auf mehr als 100 Datenträger gleichzeitig durchgeführt werden.
- Es wird auf Array LUNs nicht unterstützt.

Wie ONTAP mit unterbrochener Festplattenbereinigung umgeht

Wird die Festplattenbereinigung durch Benutzereingriffe oder ein unerwartetes Ereignis wie einen Stromausfall unterbrochen, ergreift ONTAP Maßnahmen, um die Datenträger, die bereinigt wurden, in einen bekannten Zustand zurückzuversetzen. Es sind jedoch auch Ihrerseits Maßnahmen erforderlich, bevor der Bereinigungsprozess abgeschlossen werden kann.

Die Festplattenbereinigung ist ein langwieriger Vorgang. Wird der Bereinigungsprozess durch Stromausfall, Systemabsturz oder manuelle Eingriffe unterbrochen, muss der Bereinigungsprozess von Anfang an wiederholt werden. Die Festplatte wird nicht als bereinigt ausgewiesen.

Wird die Formatierungsphase der Festplattenbereinigung unterbrochen, muss ONTAP alle durch die Unterbrechung beschädigten Datenträger wiederherstellen. Nach einem Systemneustart und anschließend einmal pro Stunde prüft ONTAP, ob ein Bereinigungsziel-Datenträger vorhanden ist, dessen Formatierungsphase nicht abgeschlossen wurde. Werden solche Datenträger gefunden, stellt ONTAP sie wieder her. Die Wiederherstellungsmethode hängt vom Typ des Datenträgers ab. Nach der Wiederherstellung eines Datenträgers kann der Bereinigungsprozess für diesen Datenträger erneut ausgeführt werden; bei HDDs kann die `-s` Option verwendet werden, um festzulegen, dass die Formatierungsphase nicht erneut durchgeführt wird.

Tipps zur Datenbereinigung in ONTAP lokalen Tiers

Wenn Sie lokale Speicherebenen erstellen oder sichern, die Daten enthalten, die möglicherweise bereinigt werden müssen, verkürzt die Befolgung einiger einfacher Richtlinien die Zeit, die für die Festplattenbereinigung benötigt wird.

- Stellen Sie sicher, dass Ihre lokalen Tiers, die sensible Daten enthalten, nicht größer sind als nötig.

  Sind sie größer als nötig, erfordert die Bereinigung mehr Zeit, Festplattenspeicher und Bandbreite.

- Beim Sichern lokaler Speicherebenen, die sensible Daten enthalten, sollte vermieden werden, diese auf einer lokalen Speicherebene zu sichern, die auch große Mengen an nicht sensiblen Daten enthält.

  Dadurch verringert sich der Ressourcenaufwand für die Verschiebung nicht sensibler Daten vor der Bereinigung sensibler Daten.

Durch das Bereinigen einer Festplatte können Daten von einer Festplatte oder einem Satz von Festplatten auf außer Betrieb genommenen oder nicht funktionsfähigen Systemen so entfernt werden, dass die Daten niemals wiederhergestellt werden können.

Zwei Methoden stehen zur Verfügung, um Festplatten mithilfe der CLI zu bereinigen:

▼ Eine Festplatte mit Befehlen im „maintenance mode“ bereinigen

Ab ONTAP 9.6 ist Festplattenbereinigung im Wartungsmodus möglich.

Bevor Sie beginnen

- Die Datenträger dürfen keine selbstverschlüsselnden Datenträger (SED) sein.

  Sie müssen den `storage encryption disk sanitize` Befehl verwenden, um eine SED zu bereinigen.

  "Verschlüsselung von Daten im Ruhezustand"

  Weitere Informationen zu `storage encryption disk sanitize` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Im Wartungsmodus starten.
   a. Die aktuelle Shell wird durch Eingabe von `halt` beendet.

      Die LOADER-Eingabeaufforderung wird angezeigt.

   b. In den Wartungsmodus wechseln durch Eingabe von `boot_ontap maint`.

      Nach der Anzeige einiger Informationen wird die Eingabeaufforderung für den Wartungsmodus angezeigt.

2. Wenn die zu bereinigenden Festplatten partitioniert sind, jede Festplatte entpartitionieren:

   > Der Befehl zum Aufheben der Partitionierung einer Festplatte ist nur auf der Diagnoseebene verfügbar und sollte nur unter Aufsicht des NetApp Supports durchgeführt werden. Es wird dringend empfohlen, vorab den NetApp Support zu kontaktieren. Weitere Informationen finden sich in der "NetApp Knowledge Base: Wie eine Ersatzfestplatte in ONTAP entpartitioniert wird"

   ```
   disk unpartition <disk_name>
   ```

3. Die angegebenen Festplatten bereinigen:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-r]]]
   [-c <cycle_count>] <disk_list>
   ```

   > Schalten Sie den Knoten während der Festplattenbereinigung nicht aus, unterbrechen Sie nicht die Speicherverbindung und entfernen Sie keine Zielfestplatten. Wird die Festplattenbereinigung während der Formatierungsphase unterbrochen, muss die Formatierungsphase neu gestartet und abgeschlossen werden, bevor die Festplatten

bereinigt und dem Ersatzspeicherpool wieder zugeführt werden können. Falls der Bereinigungsprozess abgebrochen werden muss, ist dies mit dem `disk sanitize abort` Befehl möglich. Befinden sich die angegebenen Festplatten in der Formatierungsphase der Festplattenbereinigung, erfolgt der Abbruch erst nach Abschluss dieser Phase.

```
`-p` `<pattern1>` `-p` `<pattern2>` `-p` `<pattern3>` Gibt einen
Zyklus von ein bis drei benutzerdefinierten Hex-Byte-
Überschreibungsmustern an, die nacheinander auf die zu bereinigenden
Festplatten angewendet werden können. Das Standardmuster besteht aus
drei Durchgängen: 0x55 für den ersten Durchgang, 0xaa für den zweiten
Durchgang und 0x3c für den dritten Durchgang.
```

`-r`Ersetzt ein strukturiertes Überschreiben durch ein zufälliges Überschreiben für einen oder alle Durchläufe.

`-c` `<cycle_count>`Gibt die Anzahl der Male an, wie oft die angegebenen Überschreibungsmuster angewendet werden. Der Standardwert ist ein Zyklus. Der Maximalwert beträgt sieben Zyklen.

`<disk_list>`gibt eine durch Leerzeichen getrennte Liste der IDs der zu bereinigenden Ersatzfestplatten an.

4. Bei Bedarf kann der Status des Festplattenbereinigungsprozesses überprüft werden:

   ```
   disk sanitize status [<disk_list>]
   ```

5. Nach Abschluss des Bereinigungsprozesses werden die Festplatten wieder in den Ersatzdatenträgerstatus versetzt:

   ```
   disk sanitize release <disk_name>
   ```

6. Wartungsmodus beenden.

▼ **Bereinigen einer Festplatte mit “nodeshell” Befehlen (alle ONTAP 9 Versionen)**

Nachdem die Festplattenbereinigung mithilfe von nodeshell-Befehlen auf einem Knoten aktiviert wurde, kann sie nicht mehr deaktiviert werden.

Bevor Sie beginnen

- Bei den Festplatten muss es sich um Ersatzfestplatten handeln; sie müssen einem Knoten gehören, dürfen aber nicht in einer lokalen Tier verwendet werden.

  Wenn die Festplatten partitioniert sind, kann keine der Partitionen in einer lokalen Ebene verwendet werden.

- Die Datenträger dürfen keine selbstverschlüsselnden Datenträger (SED) sein.

  Sie müssen den `storage encryption disk sanitize` Befehl verwenden, um eine SED zu bereinigen.

  "Verschlüsselung von Daten im Ruhezustand"

- Die Festplatten dürfen nicht Teil eines Speicherpools sein.

Schritte

1. Wenn die zu bereinigenden Festplatten partitioniert sind, jede Festplatte entpartitionieren:

   > Der Befehl zum Aufheben der Partitionierung einer Festplatte ist nur auf der Diagnoseebene verfügbar und sollte nur unter Aufsicht des NetApp Supports durchgeführt werden. **Es wird dringend empfohlen, vor dem weiteren Vorgehen den NetApp Support zu kontaktieren.** Es kann auch auf die "NetApp Knowledge Base: Wie eine Ersatzfestplatte in ONTAP entpartitioniert wird" verwiesen werden.

   ```
   disk unpartition <disk_name>
   ```

2. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten:

   ```
   system node run -node <node_name>
   ```

3. Festplattenbereinigung aktivieren:

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   Sie werden gebeten, den Befehl zu bestätigen, da er unwiderruflich ist.

4. Zur erweiterten Berechtigungsstufe der NodeShell wechseln:

   ```
   priv set advanced
   ```

5. Die angegebenen Festplatten bereinigen:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-r]]]
   [-c <cycle_count>] <disk_list>
   ```

   > Schalten Sie den Knoten während der Festplattenbereinigung nicht aus, unterbrechen Sie nicht die Speicherverbindung und entfernen Sie keine Zielfestplatten. Wird die Festplattenbereinigung während der Formatierungsphase unterbrochen, muss die Formatierungsphase neu gestartet und abgeschlossen werden, bevor die Festplatten bereinigt und dem Ersatzspeicherpool wieder zugeführt werden können. Falls der Bereinigungsprozess abgebrochen werden muss, ist dies mit dem Befehl disk sanitize abort möglich. Befinden sich die angegebenen Festplatten in der Formatierungsphase der Festplattenbereinigung, erfolgt der Abbruch erst nach Abschluss dieser Phase.

   `-p <pattern1> -p <pattern2> -p <pattern3>` Gibt einen Zyklus von ein bis drei benutzerdefinierten Hex-Byte-Überschreibungsmustern an, die nacheinander auf die zu bereinigenden Festplatten angewendet werden können. Das Standardmuster besteht aus drei Durchgängen: 0x55 für den ersten Durchgang, 0xaa für den zweiten Durchgang und 0x3c für den dritten Durchgang.

   `-r`Ersetzt ein strukturiertes Überschreiben durch ein zufälliges Überschreiben für einen oder alle Durchläufe.

   `-c <cycle_count>` Gibt an, wie oft die angegebenen Überschreibungsmuster angewendet werden.

   Der Standardwert ist ein Zyklus. Der Maximalwert beträgt sieben Zyklen.

`<disk_list>`gibt eine durch Leerzeichen getrennte Liste der IDs der zu bereinigenden Ersatzfestplatten an.

6. Wenn Sie den Status des Festplattenbereinigungsprozesses überprüfen möchten:

   ```
   disk sanitize status [<disk_list>]
   ```

7. Nach Abschluss des Bereinigungsprozesses werden die Festplatten wieder in den Ersatzteilstatus versetzt:

   ```
   disk sanitize release <disk_name>
   ```

8. Zurückkehren zur Administratorberechtigungsebene der nodeshell:

   ```
   priv set admin
   ```

9. Zurück zur ONTAP CLI:

   ```
   exit
   ```

10. Es sollte festgestellt werden, ob alle Festplatten wieder in den Ersatzteilstatus versetzt wurden:

    ```
    storage aggregate show-spare-disks
    ```

Wenn…	Dann…
Alle bereinigten Datenträger sind als Ersatzteile aufgeführt	Sie sind fertig. Die Festplatten wurden bereinigt und befinden sich im Ersatzteilstatus.

Einige der bereinigten Festplatten sind nicht als Ersatz aufgeführt	Die folgenden Schritte sind auszuführen:
	a. Erweiterten Berechtigungsmodus aktivieren:
	`set -privilege advanced`
	b. Die nicht zugewiesenen, bereinigten Festplatten werden dem jeweils passenden Node zugeordnet:
	`storage disk assign -disk <disk_name> -owner <node_name>`
	c. Die Festplatten werden für jede Festplatte wieder in den Ersatzdatenträgerstatus versetzt:
	`storage disk unfail -disk <disk_name> -s -q`
	d. Zurück in den Administratormodus:
	`set -privilege admin`

Weitere Informationen zu `storage aggregate show-spare-disks` finden sich in der "ONTAP-Befehlsreferenz".

Ergebnis

Die angegebenen Festplatten werden bereinigt und als Hot-Spare-Festplatten gekennzeichnet. Die Seriennummern der bereinigten Festplatten werden in `/etc/log/sanitized_disks` geschrieben.

Die Protokolle der Festplattenbereinigung, die anzeigen, was auf jeder Festplatte abgeschlossen wurde, werden in `/mroot/etc/log/sanitization.log` geschrieben.

Verwandte Informationen

- "storage aggregate show"
- "Speicherdatenträger zuweisen"
- "Speicherfestplatte wiederherstellen"
- "Speicherverschlüsselung Festplattenbereinigung"

ONTAP Befehle zur Verwaltung von Festplatten

Sie können die `storage disk` und `storage aggregate` Befehle verwenden, um Ihre Festplatten zu verwalten.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Eine Liste der Ersatzfestplatten, einschließlich partitionierter Festplatten, nach Besitzer anzeigen	`storage aggregate show-spare-disks`
RAID-Typ der Festplatte, aktuelle Nutzung und RAID-Gruppe nach lokaler Ebene anzeigen	`storage aggregate show-status`
Anzeige des RAID-Typs, der aktuellen Nutzung, der lokalen Ebene und der RAID-Gruppe, einschließlich Ersatzfestplatten, für physische Festplatten	`storage disk show -raid`
Zeigen Sie eine Liste der defekten Festplatten einschließlich des Laufwerksmodells an	`storage disk show -broken`
Den Namen des Laufwerks vor dem Cluster (Nodescope) für eine Festplatte anzeigen	`storage disk show -primary-paths` (fortschrittlich)
Die LED für eine bestimmte Festplatte oder ein bestimmtes Shelf leuchtet auf.	`storage disk set-led`
Den Prüfsummentyp für eine bestimmte Festplatte anzeigen	`storage disk show -fields checksum-compatibility`
Prüfsummentyp für alle Ersatzfestplatten anzeigen	`storage disk show -fields checksum-compatibility -container-type spare`
Informationen zu Festplattenkonnektivität und Platzierung	`storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay`
Die Namen der Datenträger vor der Clusterung für bestimmte Datenträger werden angezeigt	`storage disk show -disk diskname -fields diskpathnames`

Die Liste der Datenträger im Wartungszentrum anzeigen	`storage disk show -maintenance`
SSD-Verschleißlebensdauer anzeigen	`storage disk show -ssd-wear`
Partitionierung einer gemeinsam genutzten Festplatte aufheben	`storage disk unpartition` (verfügbar auf Diagnoseebene)
Alle nicht mit Nullen initialisierten Datenträger auf null setzen	`storage disk zerospares`
Einen laufenden Bereinigungsprozess auf einer oder mehreren angegebenen Festplatten anhalten	`system node run -node nodename -command disk sanitize`
Informationen zur Speicherverschlüsselung von Festplatten anzeigen	`storage encryption disk show`
Authentifizierungsschlüssel von allen verknüpften Schlüsselverwaltungsservern abrufen	`security key-manager restore`

Verwandte Informationen

- "storage aggregate show"
- "Storage Disk Set-LED"
- "Speicherdatenträger anzeigen"
- "Storage Disk ZeroSpares"
- "storage encryption Disk anzeigen"

ONTAP Befehle zur Anzeige von Informationen zur Speicherplatznutzung

Sie verwenden die `storage aggregate`- und `volume`-Befehle, um anzuzeigen, wie der Speicherplatz in Ihren lokalen Tiers und Volumes sowie deren Snapshots genutzt wird.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Informationen über … werden angezeigt.	Verwenden Sie diesen Befehl…

Lokale Ebene, einschließlich Details zu belegten und verfügbaren Speicherplatz-Prozentsätzen, Größe der Snapshot-Reserve und weiteren Informationen zur Speicherplatznutzung	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

Wie Festplatten und RAID-Gruppen in einer lokalen Ebene verwendet werden und der RAID-Status	`storage aggregate show-status`
Die Menge an Speicherplatz, die freigegeben würde, wenn ein bestimmter Snapshot gelöscht wird	`volume snapshot compute-reclaimable`

Der von einem Volume belegte Speicherplatz	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

Der von einem Volumen in der übergeordneten lokalen Ebene belegte Speicherplatz	`volume show-footprint`

Verwandte Informationen

- "storage aggregate show"
- "storage aggregate show-space"
- "storage aggregate show-status"

ONTAP Befehle zur Anzeige von Informationen über Storage Shelves

Der `storage shelf show` Befehl zeigt Konfigurations- und Fehlerinformationen für Ihre Festplattengehäuse an.

Wenn Sie anzeigen möchten…	Verwenden Sie diesen Befehl…
Allgemeine Informationen zur Regalkonfiguration und zum Hardwarestatus	`storage shelf show`
Detaillierte Informationen zu einem bestimmten Shelf, einschließlich Stack-ID	`storage shelf show -shelf`
Ungeklärte, vom Kunden zu behebende Fehler nach Shelf	`storage shelf show -errors`
Informationen zur Bucht	`storage shelf show -bay`
Verbindungsinformationen	`storage shelf show -connectivity`
Informationen zur Kühlung, einschließlich Temperatursensoren und Kühlventilatoren	`storage shelf show -cooling`
Informationen zu E/A-Modulen	`storage shelf show -module`
Port-Informationen	`storage shelf show -port`
Informationen zur Stromversorgung, einschließlich Netzteilen, Stromsensoren und Spannungssensoren	`storage shelf show -power`

Verwandte Informationen

- "Storage Shelf anzeigen"

RAID Konfigurationen verwalten

Standard-RAID-Richtlinien für ONTAP lokale Tiers

Entweder RAID-DP oder RAID-TEC ist die Standard-RAID-Richtlinie für alle neuen lokalen Ebenen. Die RAID-Richtlinie bestimmt den Paritätsschutz im Falle eines Festplattenausfalls.

RAID-DP bietet doppelten Paritätsschutz im Falle eines einzelnen oder doppelten Festplattenausfalls. RAID-

DP ist die Standard-RAID-Richtlinie für die folgenden lokalen Tier-Typen:

- Alle Flash Local Tiers
- Flash Pool lokale Tiers
- Leistungsfähige lokale Festplattenlaufwerk-Ebenen (HDD)

RAID-TEC wird auf allen Festplattentypen und allen Plattformen, einschließlich AFF, unterstützt. Lokale Tiers, die größere Festplatten enthalten, haben eine höhere Wahrscheinlichkeit für gleichzeitige Festplattenausfälle. RAID-TEC hilft, dieses Risiko zu mindern, indem es einen dreifachen Paritätsschutz bietet, sodass Ihre Daten bis zu drei gleichzeitige Festplattenausfälle überstehen können. RAID-TEC ist die Standard-RAID-Richtlinie für lokale Kapazitäts-HDD-Tiers mit Festplatten ab 6 TB.

Jeder RAID-Richtlinientyp erfordert eine Mindestanzahl an Festplatten:

- RAID-DP: mindestens 5 Festplatten
- RAID-TEC: mindestens 7 Festplatten

ONTAP RAID-Schutzstufen für Festplatten

ONTAP unterstützt drei RAID-Schutzstufen für lokale Speicherebenen. Die RAID-Schutzstufe bestimmt die Anzahl der Paritätsfestplatten, die im Falle eines Festplattenausfalls zur Datenwiederherstellung zur Verfügung stehen.

Mit RAID-Schutz kann ONTAP im Falle eines Festplattenausfalls in einer RAID-Gruppe die ausgefallene Festplatte durch eine Ersatzfestplatte ersetzen und mithilfe von Parität die Daten der ausgefallenen Festplatte rekonstruieren.

- **RAID4**

  Mit RAID4-Schutz kann ONTAP eine Ersatzfestplatte verwenden, um die Daten einer ausgefallenen Festplatte innerhalb der RAID-Gruppe zu ersetzen und wiederherzustellen.

- **RAID-DP**

  Mit RAID-DP Schutz kann ONTAP bis zu zwei Ersatzfestplatten verwenden, um die Daten von bis zu zwei gleichzeitig ausgefallenen Festplatten innerhalb der RAID-Gruppe zu ersetzen und wiederherzustellen.

- **RAID-TEC**

  Mit RAID-TEC Schutz kann ONTAP bis zu drei Ersatzfestplatten verwenden, um die Daten von bis zu drei gleichzeitig ausgefallenen Festplatten innerhalb der RAID-Gruppe zu ersetzen und wiederherzustellen.

Anzeigen von Laufwerks- und RAID-Gruppeninformationen für ein ONTAP lokales Tier

Einige Aufgaben der lokalen Tier-Administration erfordern Kenntnisse darüber, aus welchen Laufwerkstypen die lokale Tier besteht, deren Größe, Prüfsumme und Status, ob sie mit anderen lokalen Tiers gemeinsam genutzt werden sowie über die Größe und Zusammensetzung der RAID-Gruppen.

Schritt

1. Die Laufwerke der lokalen Ebene nach RAID-Gruppe anzeigen:

`storage aggregate show-status` *aggr_name*

Die Laufwerke werden für jede RAID-Gruppe in der lokalen Ebene angezeigt.

Der RAID-Typ des Laufwerks (Daten, Parität, dParität) ist in der `Position` Spalte ersichtlich. Wenn in der `Position` Spalte `shared` angezeigt wird, ist das Laufwerk gemeinsam genutzt: Bei einer HDD handelt es sich um eine partitionierte Festplatte, bei einer SSD ist es Teil eines Speicherpools.

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

Verwandte Informationen

- "storage aggregate show-status"

Umstellung von ONTAP RAID-DP auf RAID-TEC

Wenn zusätzlicher Schutz durch dreifache Parität gewünscht ist, ist eine Konvertierung von RAID-DP zu RAID-TEC möglich. RAID-TEC wird empfohlen, wenn die Größe der in Ihrer lokalen Ebene verwendeten Festplatten 4 TiB übersteigt.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff

aggregate. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Die lokale Ebene, die konvertiert werden soll, muss mindestens sieben Festplatten haben.

Über diese Aufgabe

- Lokale Festplatten-Tiers (HDD) können von RAID-DP auf RAID-TEC umgestellt werden. Dies schließt HDD-Tiers in Flash Pool lokalen Tiers ein.

Vorgehensweise für Flashpools/Hybridaggregate, bei denen -disktype verwendet werden muss, um den jeweiligen Festplattentyp zu ändern

[-T, -disktype {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SSD | VMDISK | SSD-NVM | SSD-CAP | SSD-ZNS | VMLUN | VMLUN-SSD}] - Datenträgertyp

Dieser Parameter legt den Festplattentyp der zu ändernden RAID-Gruppen fest. Im Fall von Flash Pool gibt er entweder die HDD-Ebene oder die SSD-Ebene an. Wenn die HDD-Ebene aus mehr als einem Festplattentyp besteht, führt die Angabe eines der verwendeten Festplattentypen dazu, dass diese Ebene geändert wird. Wenn der aktuelle Aggregat-RAID-Typ mixed_raid_type ist, ist dieser Parameter obligatorisch.

Schritte

1. Es wird überprüft, ob die lokale Ebene online ist und mindestens sechs Festplatten vorhanden sind:

   `storage aggregate show-status -aggregate` *`aggregate_name`*

2. Konvertieren der lokalen Tier von RAID-DP zu RAID-TEC:

   `storage aggregate modify -aggregate` *`aggregate_name`* `-raidtype raid_tec`

3. Es sollte sichergestellt werden, dass die lokale RAID-Richtlinie RAID-TEC ist:

   `storage aggregate show` *`aggregate_name`*

Verwandte Informationen

- "storage aggregate ändern"
- "storage aggregate show-status"

Umstellung von ONTAP RAID-TEC auf RAID-DP

Wenn Sie die Größe Ihrer lokalen Ebene reduzieren und keine dreifache Parität mehr benötigen, kann die RAID-Richtlinie von RAID-TEC auf RAID-DP umgestellt und die Anzahl der für die RAID-Parität benötigten Festplatten reduziert werden.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Die maximale RAID-TEC Gruppengröße ist größer als die maximale RAID-DP Gruppengröße. Wenn die größte RAID-TEC Gruppengröße nicht innerhalb der RAID-DP-Grenzwerte liegt, ist eine Konvertierung zu

RAID-DP nicht möglich.

Über diese Aufgabe

Um die Auswirkungen der Konvertierung zwischen RAID-Typen zu verstehen, siehe die "Parameter" für den `storage aggregate modify` Befehl.

Schritte

1. Es wird überprüft, ob die lokale Ebene online ist und mindestens sechs Festplatten vorhanden sind:

   `storage aggregate show-status -aggregate` *`aggregate_name`*

2. Konvertieren der lokalen Tier von RAID-TEC zu RAID-DP:

   `storage aggregate modify -aggregate` *`aggregate_name`* `-raidtype raid_dp`

3. Es sollte sichergestellt werden, dass die lokale RAID-Richtlinie RAID-DP ist:

   `storage aggregate show` *`aggregate_name`*

Verwandte Informationen

- "storage aggregate ändern"
- "storage aggregate show-status"

Faktoren für die Dimensionierung von ONTAP RAID Gruppen

Die Konfiguration einer optimalen RAID-Gruppengröße erfordert einen Kompromiss zwischen verschiedenen Faktoren. Es ist zu entscheiden, welche Faktoren – Geschwindigkeit des RAID-Wiederaufbaus, Schutz vor Datenverlust durch Festplattenausfall, Optimierung der I/O-Leistung und Maximierung des Datenspeicherplatzes – für das (lokale Tier) Datenaggregat, das konfiguriert wird, am wichtigsten sind.

Durch die Erstellung größerer RAID-Gruppen wird der für die Datenspeicherung verfügbare Speicherplatz bei gleicher Menge an Speicherplatz für Parität (auch als „Paritätsteuer“ bekannt) maximiert. Fällt jedoch eine Festplatte in einer größeren RAID-Gruppe aus, verlängert sich die Rekonstruktionszeit, was die Leistung über einen längeren Zeitraum beeinträchtigt. Zudem erhöht eine größere Anzahl von Festplatten in einer RAID-Gruppe die Wahrscheinlichkeit eines mehrfachen Festplattenausfalls innerhalb derselben RAID-Gruppe.

HDD- oder Array-LUN RAID-Gruppen

Bei der Dimensionierung von RAID-Gruppen, die aus HDDs oder Array-LUNs bestehen, sind die folgenden Richtlinien zu berücksichtigen:

- Alle RAID-Gruppen in einer lokalen Ebene (Aggregat) sollten die gleiche Anzahl an Festplatten haben.

  Zwar können Sie auf einer lokalen Ebene bis zu 50 % weniger oder mehr Festplatten in verschiedenen RAID-Gruppen haben, dies kann jedoch in einigen Fällen zu Leistungsengpässen führen, weshalb es möglichst vermieden werden sollte.

- Die empfohlene Anzahl an Festplatten in einer RAID-Gruppe liegt zwischen 12 und 20.

  Die Zuverlässigkeit der Performance-Festplatten kann bei Bedarf eine RAID-Gruppengröße von bis zu 28

unterstützen.

- Wenn Sie die ersten beiden Richtlinien mit mehreren RAID-Gruppen-Festplattenanzahlen erfüllen können, sollte die größere Anzahl an Festplatten gewählt werden.

SSD RAID-Gruppen in Flash Pool lokalen Tiers (Aggregaten)

Die Größe der SSD RAID-Gruppe kann von der Größe der HDD RAID-Gruppen in einem Flash Pool lokalen Tier (Aggregat) abweichen. In der Regel ist darauf zu achten, dass für ein Flash Pool lokales Tier nur eine SSD RAID-Gruppe vorhanden ist, um die Anzahl der für die Parität benötigten SSDs zu minimieren.

SSD RAID-Gruppen in SSD Local Tiers (Aggregaten)

Für die Dimensionierung von RAID-Gruppen, die aus SSDs bestehen, gelten folgende Richtlinien:

- Alle RAID-Gruppen in einer lokalen Ebene (Aggregat) sollten eine ähnliche Anzahl von Laufwerken aufweisen.

  Die RAID-Gruppen müssen nicht exakt die gleiche Größe haben, jedoch sollte nach Möglichkeit vermieden werden, dass eine RAID-Gruppe weniger als die Hälfte der Größe anderer RAID-Gruppen in derselben lokalen Ebene aufweist.

- Für RAID-DP liegt der empfohlene Bereich der RAID-Gruppengröße zwischen 20 und 28.

Passen Sie die Größe Ihrer ONTAP RAID-Gruppen an

Sie können die Größe Ihrer RAID-Gruppen anpassen, um sicherzustellen, dass die RAID-Gruppengrößen für die Speichermenge geeignet sind, die Sie für eine lokale Ebene einplanen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Über diese Aufgabe

Für Standard-Lokalebenen wird die Größe der RAID-Gruppen für jede lokale Ebene separat geändert. Für Flash Pool-Lokalebenen kann die RAID-Gruppengröße für die SSD-RAID-Gruppen und die HDD-RAID-Gruppen unabhängig voneinander geändert werden.

Die folgende Liste enthält einige Fakten zur Änderung der RAID-Gruppengröße:

- Standardmäßig werden, wenn die Anzahl der Festplatten oder Array-LUNs in der zuletzt erstellten RAID-Gruppe kleiner ist als die neue RAID-Gruppengröße, Festplatten oder Array-LUNs zur zuletzt erstellten RAID-Gruppe hinzugefügt, bis diese die neue Größe erreicht.
- Alle anderen bestehenden RAID-Gruppen in dieser lokalen Ebene behalten ihre Größe, es sei denn, Sie fügen ihnen explizit Festplatten hinzu.
- Es ist niemals möglich, eine RAID-Gruppe größer werden zu lassen als die aktuelle maximale RAID-Gruppengröße für die lokale Ebene.
- Die Größe bereits erstellter RAID-Gruppen kann nicht verringert werden.
- Die neue Größe gilt für alle RAID-Gruppen in dieser lokalen Ebene (oder, im Falle einer Flash Pool lokalen Ebene, für alle RAID-Gruppen des betroffenen RAID-Gruppentyps, SSD oder HDD).

Schritte

1. Verwenden Sie den entsprechenden Befehl:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Die maximale RAID-Gruppengröße für die SSD RAID-Gruppen einer Flash Pool lokalen Ebene ändern	`storage aggregate modify -aggregate aggr_name -cache-raid-group-size size`
Die maximale Größe anderer RAID-Gruppen ändern	`storage aggregate modify -aggregate aggr_name -maxraidsize size`

Beispiele

Der folgende Befehl ändert die maximale RAID-Gruppengröße der lokalen Ebene n1_a4 auf 20 Festplatten oder Array-LUNs:

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

Der folgende Befehl ändert die maximale RAID-Gruppengröße der SSD-Cache-RAID-Gruppen des Flash Pool lokalen Tiers n1_cache_a2 auf 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

Verwandte Informationen

- "storage aggregate ändern"

Flash Pool lokale Ebenen verwalten

Flash Pool Caching-Richtlinien für ONTAP lokale Tiers

Caching-Richtlinien für die Volumes in einer Flash Pool lokalen Ebene ermöglichen den Einsatz von Flash als Hochleistungscache für Ihren Arbeitsdatensatz, während kostengünstigere HDDs für weniger häufig genutzte Daten verwendet werden. Wenn Cache für zwei oder mehr Flash Pool lokale Ebenen bereitgestellt wird, empfiehlt sich die Nutzung der Flash Pool SSD-Partitionierung, um SSDs über die lokalen Ebenen im Flash Pool hinweg gemeinsam zu nutzen.

Caching-Richtlinien werden auf Volumes angewendet, die sich in Flash Pool lokalen Tiers befinden. Es ist wichtig, die Funktionsweise von Caching-Richtlinien zu verstehen, bevor Änderungen vorgenommen werden.

In den meisten Fällen ist die Standard-Caching-Richtlinie von `auto` die beste Caching-Richtlinie. Die Caching-Richtlinie sollte nur geändert werden, wenn eine andere Richtlinie eine bessere Performance für Ihre Arbeitslast bietet. Die Konfiguration einer falschen Caching-Richtlinie kann die Volume-Performance erheblich beeinträchtigen, wobei sich die Leistungseinbußen im Laufe der Zeit allmählich verstärken können.

Caching-Richtlinien kombinieren eine Lese-Caching-Richtlinie und eine Schreib-Caching-Richtlinie. Der Richtlinienname setzt sich aus den Namen der Lese-Caching-Richtlinie und der Schreib-Caching-Richtlinie zusammen, getrennt durch einen Bindestrich. Fehlt der Bindestrich im Richtliniennamen, ist die Schreib-Caching-Richtlinie `none`, außer bei der `auto` Richtlinie.

Lesecache-Richtlinien optimieren die zukünftige Leseleistung, indem sie zusätzlich zu den auf HDDs gespeicherten Daten eine Kopie der Daten im Cache ablegen. Bei Lesecache-Richtlinien, die bei

Schreibvorgängen Daten in den Cache einfügen, fungiert der Cache als *Write-Through*-Cache.

Daten, die mithilfe der Schreibcaching-Richtlinie in den Cache eingefügt werden, befinden sich ausschließlich im Cache; es gibt keine Kopie auf den Festplatten. Flash Pool Cache ist RAID-geschützt. Das Aktivieren des Schreibcachings bewirkt, dass Daten aus Schreibvorgängen sofort für Lesezugriffe aus dem Cache zur Verfügung stehen, während das Schreiben der Daten auf die Festplatten aufgeschoben wird, bis sie aus dem Cache entfernt werden.

Wenn ein Volume von einer Flash Pool lokalen Ebene auf eine Einzellaufwerk lokale Ebene verschoben wird, geht seine Caching-Richtlinie verloren; wird es später wieder auf eine Flash Pool lokale Ebene verschoben, erhält es die Standard-Caching-Richtlinie von `auto`. Wird ein Volume zwischen zwei Flash Pool lokalen Ebenen verschoben, bleibt die Caching-Richtlinie erhalten.

Eine Caching-Richtlinie ändern

Die CLI kann verwendet werden, um die Caching-Richtlinie für ein Volume zu ändern, das sich auf einer Flash Pool lokalen Ebene befindet, indem der `-caching-policy` Parameter mit dem `volume create` Befehl genutzt wird.

Wenn Sie ein Volume auf einer Flash Pool lokalen Ebene erstellen, wird dem Volume standardmäßig die `auto` Caching-Richtlinie zugewiesen.

Flash Pool Caching-Richtlinien verwalten

Feststellen, ob eine ONTAP Flash Pool Caching-Richtlinie geändert werden soll

Sie können Volumes in Flash Pool lokalen Tiers Cache-Aufbewahrungsrichtlinien zuweisen, um festzulegen, wie lange die Volume-Daten im Flash Pool Cache verbleiben. In manchen Fällen hat die Änderung der Cache-Aufbewahrungsrichtlinie jedoch keinen Einfluss darauf, wie lange die Daten des Volumes im Cache verbleiben.

Über diese Aufgabe

Wenn Ihre Daten eine der folgenden Bedingungen erfüllen, könnte eine Änderung Ihrer Cache-Retention-Policy keine Auswirkungen haben:

- Ihre Arbeitslast ist sequenziell.
- Ihre Arbeitslast liest die im Solid State Drive (SSD) zwischengespeicherten zufälligen Blöcke nicht erneut.
- Die Cache-Größe des Volumes ist zu klein.

Schritte

Die folgenden Schritte prüfen, ob die Daten die erforderlichen Bedingungen erfüllen. Die Aufgabe muss über die Befehlszeilenschnittstelle (CLI) im erweiterten Berechtigungsmodus ausgeführt werden.

1. Die CLI kann verwendet werden, um das Workload-Volumen anzuzeigen:

   ```
   statistics start -object workload_volume
   ```

2. Das Auslastungsmuster des Volumens bestimmen:

   ```
   statistics show -object workload_volume -instance volume-workload -counter
   sequential_reads
   ```

3. Die Trefferquote des Volumens bestimmen:

   ```
   statistics show -object wafl_hya_vvol -instance volume -counter
   read_ops_replaced_percent|wc_write_blks_overwritten_percent
   ```

4. Bestimmen Sie die `Cacheable Read` und `Project Cache Alloc` des Volumens:

   ```
   system node run -node node_name wafl awa start aggr_name
   ```

5. AWA-Zusammenfassung anzeigen:

   ```
   system node run -node node_name wafl awa print aggr_name
   ```

6. Die Trefferquote des Volumes kann mit der `Cacheable Read` verglichen werden.

   Wenn die Trefferquote des Volumes größer als der `Cacheable Read` ist, liest Ihre Arbeitslast keine zufälligen, auf den SSDs zwischengespeicherten Blöcke erneut.

7. Die aktuelle Cache-Größe des Volumes im Vergleich zur `Project Cache Alloc`.

   Wenn die aktuelle Cache-Größe des Volumes größer als die `Project Cache Alloc` ist, ist die Größe Ihres Volume-Caches zu klein.

Verwandte Informationen

- "Statistiken zeigen"
- "Statistiken Start"

Ändern der Caching-Richtlinien der ONTAP Flash Pool lokalen Ebenen

Die Caching-Richtlinie eines Volumes sollte nur dann geändert werden, wenn eine andere Caching-Richtlinie voraussichtlich eine bessere Leistung bietet. Die Caching-Richtlinie eines Volumes kann auf einer Flash Pool lokalen Ebene geändert werden.

Bevor Sie beginnen

Es ist zu bestimmen, ob die Caching-Richtlinie geändert werden soll.

Über diese Aufgabe

In den meisten Fällen ist die Standard-Caching-Richtlinie von `auto` die beste Caching-Richtlinie, die verwendet werden kann. Die Caching-Richtlinie sollte nur geändert werden, wenn eine andere Richtlinie eine bessere Performance für Ihre Arbeitslast bietet. Die Konfiguration einer falschen Caching-Richtlinie kann die Volume-Performance erheblich beeinträchtigen, wobei sich die Leistungseinbußen im Laufe der Zeit allmählich verstärken können. Beim Ändern von Caching-Richtlinien ist Vorsicht geboten. Treten Leistungsprobleme bei einem Volume auf, für das die Caching-Richtlinie geändert wurde, sollte die Caching-Richtlinie auf `auto` zurückgesetzt werden.

Schritt

1. Die CLI kann verwendet werden, um die Caching-Richtlinie des Volumes zu ändern:

   ```
   volume modify -volume volume_name -caching-policy policy_name
   ```

Beispiel

Das folgende Beispiel ändert die Caching-Richtlinie eines Volumes mit dem Namen `vol2` auf die Richtlinie `none`:

```
volume modify -volume vol2 -caching-policy none
```

Die Cache-Aufbewahrungsrichtlinie für ONTAP Flash Pool lokale Tiers festlegen

Sie können Volumes in Flash Pool lokalen Tiers Cache-Aufbewahrungsrichtlinien zuweisen. Daten in Volumes mit einer hohen Cache-Aufbewahrungsrichtlinie verbleiben länger im Cache, während Daten in Volumes mit einer niedrigen Cache-Aufbewahrungsrichtlinie schneller entfernt werden. Dadurch wird die Leistung Ihrer kritischen Workloads erhöht, da wichtige Informationen für einen längeren Zeitraum schneller zugänglich sind.

Bevor Sie beginnen

Es sollte bekannt sein, ob Ihr System Bedingungen aufweist, die verhindern könnten, dass die Cache-Aufbewahrungsrichtlinie einen Einfluss darauf hat, wie lange Ihre Daten im Cache verbleiben.

Schritte

Die folgenden Schritte werden im erweiterten Berechtigungsmodus der CLI durchgeführt:

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. Die Cache-Aufbewahrungsrichtlinie des Volumes überprüfen:

   Standardmäßig ist die Aufbewahrungsrichtlinie für den Cache “normal”.

3. Cache-Aufbewahrungsrichtlinie festlegen:

   ```
   volume modify -volume volume_name -vserver vserver_name -caching-policy
   policy_name
   ```

4. Es sollte überprüft werden, ob die Cache-Aufbewahrungsrichtlinie des Volumes auf die ausgewählte Option geändert wurde.
5. Die Berechtigungseinstellung wieder auf "admin" setzen:

   ```
   set -privilege admin
   ```

Flash Pool SSD Partitionierung für ONTAP lokale Tiers mit Storage-Pools

Wenn Sie Cache für zwei oder mehr lokale Flash Pool Ebenen bereitstellen, sollte die Flash Pool Solid-State Drive (SSD) Partitionierung verwendet werden. Die Flash Pool SSD Partitionierung ermöglicht die gemeinsame Nutzung von SSDs durch alle lokalen Ebenen, die den Flash Pool verwenden. Dadurch werden die Kosten der Parität auf mehrere lokale Ebenen verteilt, die Flexibilität der SSD-Cache-Zuweisung erhöht und die SSD-Leistung maximiert.

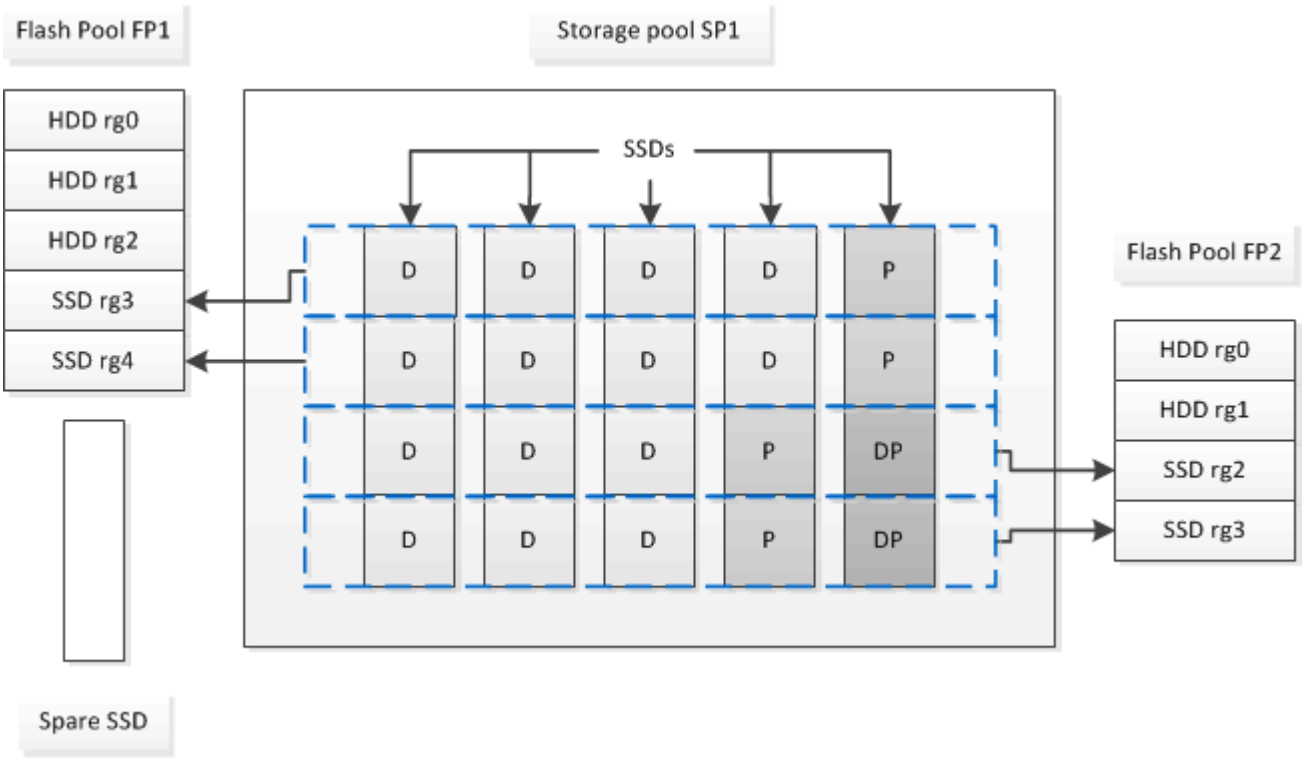
Damit eine SSD in einem Flash Pool lokalen Tier verwendet werden kann, muss die SSD in einen Speicherpool aufgenommen werden. SSDs, die für Root-Data Partitioning partitioniert wurden, können in

einem Speicherpool nicht verwendet werden. Nachdem die SSD in den Speicherpool aufgenommen wurde, kann die SSD nicht mehr als Standalone Laufwerk verwaltet werden und kann nur dann aus dem Speicherpool entfernt werden, wenn die mit dem Flash Pool verbundenen lokalen Tiers zerstört werden und der Speicherpool zerstört wird.

SSD-Speicherpools sind in vier gleich große Zuordnungseinheiten unterteilt. Die dem Speicherpool hinzugefügten SSDs werden in vier Partitionen aufgeteilt, und jeder der vier Zuordnungseinheiten wird eine Partition zugewiesen. Die SSDs im Speicherpool müssen demselben HA-Paar gehören. Standardmäßig werden jedem Knoten im HA-Paar zwei Zuordnungseinheiten zugewiesen. Die Zuordnungseinheiten müssen dem Knoten gehören, der die lokale Tier verwaltet, die er bedient. Wenn für lokale Tiers auf einem der Knoten mehr Flash Cache benötigt wird, kann die Standardanzahl der Zuordnungseinheiten verschoben werden, sodass die Anzahl auf einem Knoten verringert und auf dem Partnerknoten erhöht wird.

Sie verwenden Ersatz-SSDs, um einen SSD-Speicherpool hinzuzufügen. Wenn der Speicherpool Zuordnungseinheiten für Flash Pool lokale Ebenen bereitstellt, die beiden Knoten im HA-Paar gehören, können die Ersatz-SSDs einem der beiden Knoten gehören. Stellt der Speicherpool jedoch Zuordnungseinheiten nur für Flash Pool lokale Ebenen bereit, die einem der Knoten im HA-Paar gehören, müssen die SSD-Ersatzlaufwerke demselben Knoten gehören.

Die folgende Abbildung zeigt ein Beispiel für die SSD-Partitionierung eines Flash Pool. Der SSD-Speicherpool dient als Cache für zwei Flash Pool lokale Tiers:



Der Storage Pool SP1 besteht aus fünf SSDs und einer Hot Spare SSD. Zwei der Allocation Units des Storage Pools sind Flash Pool FP1 zugeordnet, und zwei sind Flash Pool FP2 zugeordnet. FP1 hat einen Cache-RAID-Typ von RAID4. Daher enthalten die FP1 zugewiesenen Allocation Units nur eine Partition, die für Parität vorgesehen ist. FP2 hat einen Cache-RAID-Typ von RAID-DP. Daher enthalten die FP2 zugewiesenen Allocation Units eine Paritätspartition und eine Doppelparitätspartition.

In diesem Beispiel werden jedem Flash Pool lokalen Tier zwei Zuordnungseinheiten zugewiesen. Falls jedoch ein Flash Pool lokales Tier einen größeren Cache benötigt, können drei der Zuordnungseinheiten diesem Flash Pool lokalen Tier und nur eine dem anderen zugewiesen werden.

Bestimmen Sie die ONTAP Flash Pool-Eignung und die optimale Cache-Größe

Bevor eine bestehende lokale Tier in eine Flash Pool lokale Tier umgewandelt wird, kann festgestellt werden, ob die lokale Tier I/O-gebunden ist und welche Flash Pool Cache-Größe für die jeweilige Workload und das Budget am besten geeignet ist. Es kann außerdem überprüft werden, ob der Cache einer bestehenden Flash Pool lokalen Tier korrekt dimensioniert ist.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Bevor Sie beginnen

Es sollte ungefähr bekannt sein, wann die lokale Tier, die analysiert wird, ihre Spitzenlast erreicht.

Schritte

1. Erweiterter Modus:

   ```
   set advanced
   ```

2. Wenn festgestellt werden soll, ob eine bestehende lokale Ebene für die Umwandlung in eine Flash Pool lokale Ebene geeignet ist, sollte ermittelt werden, wie stark die Festplatten in der lokalen Ebene während einer Spitzenlastperiode ausgelastet sind und wie sich dies auf die Latenz auswirkt:

   ```
   statistics show-periodic -object disk:raid_group -instance raid_group_name
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

   Sie können entscheiden, ob es für diese lokale Ebene sinnvoll ist, die Latenz durch Hinzufügen eines Flash Pool Cache zu reduzieren.

   Der folgende Befehl zeigt die Statistiken für die erste RAID-Gruppe der lokalen Tier “aggr1”:

   ```
   statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

3. Automatisierter Workload Analyzer (AWA) starten:

   ```
   storage automated-working-set-analyzer start -node node_name -aggregate
   aggr_name
   ```

   AWA beginnt mit der Erfassung von Workload-Daten für die Volumes, die der angegebenen lokalen Tier zugeordnet sind.

4. Erweiterten Modus beenden:

   ```
   set admin
   ```

   AWA sollte so lange ausgeführt werden, bis ein oder mehrere Intervalle mit Spitzenlast aufgetreten sind. AWA sammelt Workload-Statistiken für die Volumes, die der angegebenen lokalen Ebene zugeordnet sind, und analysiert Daten für einen Zeitraum von bis zu einer rollierenden Woche. Wenn AWA länger als eine Woche ausgeführt wird, werden nur Daten aus der jeweils letzten Woche berücksichtigt. Die Schätzungen

der Cache-Größe basieren auf den höchsten Lasten, die während des Datenerfassungszeitraums beobachtet wurden; die Last muss nicht während des gesamten Datenerfassungszeitraums hoch sein.

5. Erweiterter Modus:

   ```
   set advanced
   ```

6. Anzeige der Arbeitslastanalyse:

   ```
   storage automated-working-set-analyzer show -node node_name -instance
   ```

7. AWA anhalten:

   ```
   storage automated-working-set-analyzer stop node_name
   ```

   Sämtliche Arbeitslastdaten werden gelöscht und stehen nicht mehr zur Analyse zur Verfügung.

8. Erweiterten Modus beenden:

   ```
   set admin
   ```

Verwandte Informationen

- "Statistiken anzeigen periodisch"
- "storage automated-working-set-analyzer show"
- "storage automated-working-set-analyzer start"
- "storage automated-working-set-analyzer stop"

Eine ONTAP Flash Pool lokale Ebene mit physischen SSDs erstellen

Eine lokale Flash Pool-Ebene wird erstellt, indem die Funktion auf einer bestehenden lokalen Ebene aktiviert wird, die aus HDD RAID-Gruppen besteht, und anschließend eine oder mehrere SSD RAID-Gruppen zu dieser lokalen Ebene hinzugefügt werden. Dadurch entstehen zwei Sätze von RAID-Gruppen für diese lokale Ebene: SSD RAID-Gruppen (der SSD-Cache) und HDD RAID-Gruppen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Über diese Aufgabe

Nachdem Sie einem lokalen Tier einen SSD-Cache hinzugefügt haben, um ein Flash Pool lokales Tier zu erstellen, kann der SSD-Cache nicht mehr entfernt werden, um das lokale Tier wieder in seine ursprüngliche Konfiguration zurückzuversetzen.

Standardmäßig entspricht der RAID-Level des SSD-Cache dem RAID-Level der HDD-RAID-Gruppen. Diese Standardeinstellung kann durch Angabe der `raidtype` Option beim Hinzufügen der ersten SSD-RAID-Gruppen überschrieben werden.

Bevor Sie beginnen

- Es muss eine gültige lokale Ebene identifiziert sein, die aus HDDs besteht, um sie in eine Flash Pool lokale Ebene umzuwandeln.
- Die Schreibcache-Berechtigung der mit der lokalen Ebene verbundenen Volumes muss ermittelt und alle erforderlichen Schritte zur Behebung von Berechtigungsproblemen abgeschlossen sein.
- Sie müssen die SSDs, die Sie hinzufügen werden, bestimmt haben, und diese SSDs müssen dem Knoten gehören, auf dem Sie die Flash Pool lokale Ebene erstellen.
- Sie müssen die Prüfsummentypen sowohl der hinzuzufügenden SSDs als auch der bereits im lokalen Tier befindlichen HDDs ermittelt haben.
- Sie müssen die Anzahl der hinzuzufügenden SSDs und die optimale RAID-Gruppengröße für die SSD RAID-Gruppen ermittelt haben.

  Die Verwendung von weniger RAID-Gruppen im SSD-Cache verringert die Anzahl der benötigten Paritätsfestplatten, aber größere RAID-Gruppen erfordern RAID-DP.
- Der gewünschte RAID-Level für den SSD-Cache muss festgelegt sein.
- Sie müssen die maximale Cache-Größe für Ihr System ermittelt und festgestellt haben, dass das Hinzufügen eines SSD-Cache zu Ihrer lokalen Speicherebene nicht dazu führt, dass diese überschritten wird.
- Sie müssen sich mit den Konfigurationsanforderungen für lokale Flash Pool Ebenen vertraut gemacht haben.

Schritte

Sie können eine Flash Pool lokale Ebene mithilfe von System Manager oder der ONTAP CLI erstellen.

System Manager

Ab ONTAP 9.12.1 kann mit System Manager eine Flash Pool lokale Tier mit physischen SSDs erstellt werden.

Schritte

1. **Speicher > Ebenen** auswählen und dann eine vorhandene lokale HDD-Speicherebene auswählen.
2. Wählen Sie ⋮ dann **Add Flash Pool Cache**.
3. **Dedizierte SSDs als Cache verwenden** auswählen.
4. Wählen Sie einen Datenträgertyp und die Anzahl der Datenträger.
5. Einen RAID-Typ auswählen.
6. **Speichern** auswählen.
7. Suchen Sie die Speicherebene und wählen Sie dann ⋮ aus
8. **Weitere Details** auswählen. Es wird überprüft, ob Flash Pool als **Aktiviert** angezeigt wird.

CLI

Schritte

1. Die lokale Tier wird als berechtigt markiert, eine Flash Pool lokale Tier zu werden:

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   Falls dieser Schritt nicht erfolgreich ist, die Schreibcache-Berechtigung für die Zielebene bestimmen.

2. Die SSDs werden mithilfe des `storage aggregate add` Befehls zur lokalen Ebene hinzugefügt.
    - Sie können die SSDs anhand ihrer ID oder mithilfe der `diskcount` und `disktype` Parameter angeben.
    - Wenn die HDDs und die SSDs nicht den gleichen Prüfsummentyp haben oder wenn die lokale Ebene eine lokale Ebene mit gemischtem Prüfsummentyp ist, muss der `checksumstyle` Parameter verwendet werden, um den Prüfsummentyp der Datenträger anzugeben, die der lokalen Ebene hinzugefügt werden.
    - Sie können einen anderen RAID-Typ für den SSD-Cache mithilfe des `raidtype` Parameters angeben.
    - Wenn die Größe der Cache-RAID-Gruppe von der Standardgröße für den verwendeten RAID-Typ abweichen soll, sollte sie jetzt mit dem `-cache-raid-group-size` Parameter geändert werden.

Verwandte Informationen

- "Speicheraggregate hinzufügen"
- "storage aggregate ändern"

Eine lokale Flash Pool Ebene mit SSD-Speicherpools erstellen

Ermitteln, ob eine ONTAP Flash Pool lokale Tier einen SSD-Speicherpool verwendet

Sie können eine Flash Pool lokale Ebene konfigurieren, indem Sie einer bestehenden HDD lokalen Ebene eine oder mehrere Zuordnungseinheiten aus einem SSD-Speicherpool hinzufügen.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Die Verwaltung der lokalen Flash Pool Ebenen unterscheidet sich, wenn SSD-Speicherpools für den Cache verwendet werden, von der Verwaltung diskreter SSDs.

Schritt

1. Die Laufwerke der lokalen Ebene nach RAID-Gruppe werden angezeigt:

   `storage aggregate show-status` *`aggr_name`*

   Wenn die lokale Ebene einen oder mehrere SSD-Speicherpools verwendet, wird der Wert für die `Position` Spalte für die SSD-RAID-Gruppen als `Shared` angezeigt, und der Name des Speicherpools wird neben dem RAID-Gruppennamen angezeigt.

Verwandte Informationen

- "storage aggregate show-status"

Cache zu einer lokalen ONTAP-Tier hinzufügen, indem ein SSD-Speicherpool erstellt wird.

Sie können Cache bereitstellen, indem Sie eine bestehende lokale Ebene durch Hinzufügen von Solid State Drives (SSDs) in eine lokale Flash Pool Ebene umwandeln.

Sie können SSD-Speicherpools erstellen, um SSD-Cache für zwei bis vier Flash Pool lokale Ebenen bereitzustellen. Flash Pool lokale Ebenen ermöglichen den Einsatz von Flash als Hochleistungscache für den aktiven Datensatz, während kostengünstigere HDDs für weniger häufig genutzte Daten verwendet werden.

Über diese Aufgabe

- Beim Erstellen oder Hinzufügen von Datenträgern zu einem Speicherpool muss eine Datenträgerliste angegeben werden.

  Speicherpools unterstützen keinen `diskcount`Parameter.

- Die im Speicherpool verwendeten SSDs sollten die gleiche Größe haben.

System Manager

▼ Mit System Manager einen SSD-Cache hinzufügen (ONTAP 9.12.1 und höher)

Ab ONTAP 9.12.1 kann mit System Manager ein SSD-Cache hinzugefügt werden.

Speicherpooloptionen sind auf AFF Systemen nicht verfügbar.

Schritte

1. Klicken Sie auf **Cluster > Datenträger** und dann auf **Anzeigen/Ausblenden**.
2. **Typ** auswählen und überprüfen, ob im Cluster Ersatz-SSDs vorhanden sind.
3. Klicken Sie auf **Speicher > Ebenen** und klicken Sie auf **Speicherpool hinzufügen**.
4. Wählen Sie den Datenträgertyp aus.
5. Geben Sie eine Festplattengröße ein.
6. Wählen Sie die Anzahl der Festplatten aus, die dem Speicherpool hinzugefügt werden sollen.
7. Die geschätzte Cache-Größe wird angezeigt.

▼ Mit System Manager einen SSD-Cache hinzufügen (nur ONTAP 9.7)

Die CLI-Prozedur ist zu verwenden, wenn eine ONTAP Version genutzt wird, die neuer als ONTAP 9.7 oder älter als ONTAP 9.12.1 ist.

Schritte

1. **(Zur klassischen Version zurückkehren)** auswählen.
2. Klicken Sie auf **Speicher > Aggregate & Festplatten > Aggregate**.
3. Wählen Sie die lokale Ebene aus und klicken Sie dann auf **Aktionen > Cache hinzufügen**.
4. Als Cache-Quelle werden „Speicherpools“ oder „dedizierte SSDs“ ausgewählt.
5. **(Zur neuen Benutzeroberfläche wechseln)** auswählen.
6. Klicken Sie auf **Speicher > Ebenen**, um die Größe der neuen lokalen Ebene zu überprüfen.

CLI

Erstellung eines SSD-Speicherpools über die Befehlszeilenschnittstelle

Schritte

1. Die Namen der verfügbaren Ersatz-SSDs bestimmen:

```
storage aggregate show-spare-disks -disk-type SSD
```

Die in einem Speicherpool verwendeten SSDs können einem der beiden Knoten eines HA-Paars gehören.

2. Den Storage-Pool erstellen:

   `storage pool create -storage-pool sp_name -disk-list disk1,disk2,…`

3. **Optional:** Der neu erstellte Speicherpool kann überprüft werden:

   `storage pool show -storage-pool sp_name`

Ergebnisse

Nachdem die SSDs dem Speicherpool hinzugefügt wurden, werden sie im Cluster nicht mehr als Ersatzfestplatten angezeigt, obwohl der vom Speicherpool bereitgestellte Speicher noch keinem Flash Pool Cache zugewiesen wurde. SSDs können einer RAID-Gruppe nicht als einzelne Laufwerke hinzugefügt werden; ihr Speicher kann nur über die Zuordnungseinheiten des Speicherpools, zu dem sie gehören, bereitgestellt werden.

Verwandte Informationen

- "storage aggregate show"
- "Speicherpool erstellen"
- "storage pool show"

Einen ONTAP Flash Pool lokalen Tier mit SSD-Speicherpool-Zuordnungseinheiten erstellen

Sie können eine Flash Pool lokale Ebene konfigurieren, indem Sie einer bestehenden HDD lokalen Ebene eine oder mehrere Zuordnungseinheiten aus einem SSD-Speicherpool hinzufügen.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Ab ONTAP 9.12.1 kann der neu gestaltete System Manager verwendet werden, um eine Flash Pool lokale Ebene mithilfe von Speicherpool-Zuordnungseinheiten zu erstellen.

Bevor Sie beginnen

- Es muss eine gültige lokale Ebene identifiziert sein, die aus HDDs besteht, um sie in eine Flash Pool lokale Ebene umzuwandeln.
- Die Schreibcache-Berechtigung der mit der lokalen Ebene verbundenen Volumes muss ermittelt und alle erforderlichen Schritte zur Behebung von Berechtigungsproblemen abgeschlossen sein.
- Sie müssen einen SSD-Speicherpool erstellt haben, um den SSD-Cache für diese Flash Pool lokale Ebene bereitzustellen.

  Jede Zuordnungseinheit aus dem Speicherpool, die verwendet werden soll, muss demselben Knoten gehören, dem auch die lokale Flash Pool Ebene gehört.

- Es muss festgelegt sein, wie viel Cache dem lokalen Speicher hinzugefügt werden soll.

Sie fügen dem lokalen Tier Cache durch Zuordnungseinheiten hinzu. Die Größe der Zuordnungseinheiten kann später durch das Hinzufügen von SSDs zum Storage Pool erhöht werden, sofern ausreichend Platz vorhanden ist.

- Der gewünschte RAID-Typ für den SSD-Cache muss festgelegt sein.

  Nachdem Sie einen Cache aus SSD-Speicherpools zur lokalen Speicherebene hinzugefügt haben, kann der RAID-Typ der Cache-RAID-Gruppen nicht mehr geändert werden.

- Sie müssen die maximale Cache-Größe für Ihr System ermittelt und festgestellt haben, dass das Hinzufügen eines SSD-Cache zu Ihrer lokalen Speicherebene nicht dazu führt, dass diese überschritten wird.

  Die Menge des Caches, die zur Gesamtgröße des Caches hinzugefügt wird, lässt sich mit dem `storage pool show` Befehl anzeigen.

- Sie müssen sich mit den Konfigurationsanforderungen für die lokale Ebene von Flash Pool vertraut gemacht haben.

Über diese Aufgabe

Soll der RAID-Typ des Cache von dem der HDD-RAID-Gruppen abweichen, muss der Cache-RAID-Typ beim Hinzufügen der SSD-Kapazität angegeben werden. Nach dem Hinzufügen der SSD-Kapazität zur lokalen Ebene ist eine Änderung des RAID-Typs des Cache nicht mehr möglich.

Nachdem Sie einem lokalen Tier einen SSD-Cache hinzugefügt haben, um ein Flash Pool lokales Tier zu erstellen, kann der SSD-Cache nicht mehr entfernt werden, um das lokale Tier wieder in seine ursprüngliche Konfiguration zurückzuversetzen.

System Manager

Ab ONTAP 9.12.1 ist es möglich, mit System Manager SSDs zu einem SSD-Speicherpool hinzuzufügen.

Schritte

1. Klicken Sie auf **Storage > Tiers** und wählen Sie eine vorhandene lokale HDD Storage-Tier aus.
2. Klicken Sie ⋮ und wählen Sie **Add Flash Pool Cache** aus.
3. **Speicherpools verwenden** auswählen.
4. Wählen Sie einen Speicherpool aus.
5. Eine Cache-Größe und eine RAID-Konfiguration auswählen.
6. Auf **Speichern** klicken.
7. Die Speicherebene erneut suchen und auf ⋮ klicken
8. **Weitere Details** auswählen und überprüfen, dass Flash Pool als **Aktiviert** angezeigt wird.

CLI

Schritte

1. Die lokale Tier wird als berechtigt markiert, eine Flash Pool lokale Tier zu werden:

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   Falls dieser Schritt nicht erfolgreich ist, die Schreibcache-Berechtigung für die Zielebene bestimmen.

2. Verfügbare SSD-Speicherpool-Zuordnungseinheiten:

   `storage pool show-available-capacity`

3. Die SSD-Kapazität wird der lokalen Ebene hinzugefügt:

   `storage aggregate add` *`aggr_name`* `-storage-pool` *`sp_name`* `-allocation-units` *`number_of_units`*

   Wenn der RAID-Typ des Caches sich von dem der HDD-RAID-Gruppen unterscheiden soll, muss dies bei der Eingabe dieses Befehls mit dem `raidtype` Parameter geändert werden.

   Sie müssen keine neue RAID-Gruppe angeben; ONTAP platziert den SSD-Cache automatisch in separate RAID-Gruppen, getrennt von den HDD-RAID-Gruppen.

   Die RAID-Gruppengröße des Caches kann nicht festgelegt werden; sie wird durch die Anzahl der SSDs im Speicherpool bestimmt.

   Der Cache wird der lokalen Ebene hinzugefügt und die lokale Ebene ist nun eine Flash Pool lokale Ebene. Jede der lokalen Ebene hinzugefügte Zuordnungseinheit bildet eine eigene RAID-Gruppe.

4. Das Vorhandensein und die Größe des SSD-Cache bestätigen:

   `storage aggregate show` *`aggregate_name`*

   Die Größe des Caches ist unter `Total Hybrid Cache Size` aufgeführt.

Verwandte Informationen

- "Speicheraggregate hinzufügen"
- "storage aggregate ändern"
- "storage pool show"
- "storage pool show-available-capacity"

Bestimmung der Auswirkungen des Hinzufügens von SSDs zu einem Storage-Pool auf die ONTAP Cache-Größe

Wenn durch das Hinzufügen von SSDs zu einem Speicherpool das Cache-Limit Ihres Plattformmodells überschritten wird, weist ONTAP die neu hinzugefügte Kapazität keinem Flash Pool lokalen Tier zu. Dies kann dazu führen, dass ein Teil oder die gesamte neu hinzugefügte Kapazität nicht verfügbar ist.

Über diese Aufgabe

Wenn Sie SSDs zu einem SSD-Speicherpool hinzufügen, dem bereits Zuordnungseinheiten für Flash Pool lokale Ebenen zugewiesen sind, erhöht sich die Cache-Größe jeder dieser lokalen Ebenen und der gesamte Cache des Systems. Sind noch keine Zuordnungseinheiten des Speicherpools zugewiesen, wirkt sich das Hinzufügen von SSDs zu diesem Speicherpool nicht auf die SSD-Cache-Größe aus, bis eine oder mehrere Zuordnungseinheiten einem Cache zugewiesen werden.

Schritte

1. Die nutzbare Größe der SSDs, die dem Speicherpool hinzugefügt werden, lässt sich wie folgt bestimmen:

```
storage disk show disk_name -fields usable-size
```

2. Ermitteln, wie viele Zuordnungseinheiten für den Speicherpool noch nicht zugeordnet sind:

   ```
   storage pool show-available-capacity sp_name
   ```

   Alle nicht zugewiesenen Zuordnungseinheiten im Speicherpool werden angezeigt.

3. Die Menge des hinzuzufügenden Caches lässt sich mit der folgenden Formel berechnen:

   (4 – Anzahl der nicht zugewiesenen Zuordnungseinheiten) × 25% × nutzbare Größe × Anzahl der SSDs

Verwandte Informationen

- "Speicherdatenträger anzeigen"
- "storage pool show-available-capacity"

SSDs zu einem ONTAP SSD Storage Pool hinzufügen

Durch das Hinzufügen von SSDs zu einem SSD-Speicherpool erhöhen sich die physische und die nutzbare Größe des Speicherpools sowie die Größe der Zuordnungseinheit. Die größere Zuordnungseinheit wirkt sich auch auf Zuordnungseinheiten aus, die bereits lokalen Speicherebenen zugewiesen wurden.

Bevor Sie beginnen

Sie müssen festgestellt haben, dass diese Operation das Cache-Limit Ihres HA-Paares nicht überschreiten wird. ONTAP verhindert nicht, dass das Cache-Limit überschritten wird, wenn SSDs zu einem SSD-Speicherpool hinzugefügt werden, und dies kann dazu führen, dass die neu hinzugefügte Speicherkapazität nicht verfügbar ist.

Über diese Aufgabe

Beim Hinzufügen von SSDs zu einem bestehenden SSD-Speicherpool müssen die SSDs entweder dem einen oder dem anderen Knoten desselben HA-Paares gehören, dem bereits die vorhandenen SSDs im Speicherpool gehören. Es können SSDs hinzugefügt werden, die einem der beiden Knoten des HA-Paares gehören.

Die SSD, die Sie dem Speicherpool hinzufügen, muss die gleiche Größe wie die derzeit im Speicherpool verwendete Festplatte haben.

System Manager

Ab ONTAP 9.12.1 ist es möglich, mit System Manager SSDs zu einem SSD-Speicherpool hinzuzufügen.

Schritte

1. Klicken Sie auf **Speicher > Ebenen** und suchen Sie den Abschnitt **Speicherpools**.
2. Den Speicherpool suchen, auf ⋮ klicken und **Festplatten hinzufügen** auswählen.
3. Wählen Sie den Datenträgertyp und die Anzahl der Datenträger.
4. Die geschätzte Cache-Größe prüfen.

CLI

Schritte

1. **Optional:** Die aktuelle Größe der Zuordnungseinheit und den verfügbaren Speicherplatz für den Speicherpool anzeigen:

   `storage pool show -instance sp_name`

2. Verfügbare SSDs:

   `storage disk show -container-type spare -type SSD`

3. Fügen Sie die SSDs dem Speicherpool hinzu:

   `storage pool add -storage-pool sp_name -disk-list disk1,disk2…`

   Das System zeigt an, welche lokalen Flash Pool Ebenen durch diesen Vorgang vergrößert werden und um welchen Betrag, und fordert Sie zur Bestätigung des Vorgangs auf.

Verwandte Informationen

- "Speicherdatenträger anzeigen"
- "storage pool show"
- "Speicherpool hinzufügen"

ONTAP Befehle zur Verwaltung von SSD-Speicherpools

ONTAP stellt den `storage pool` Befehl zur Verwaltung von SSD-Speicherpools bereit.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Anzeigen, wie viel Speicherplatz ein Speicherpool welcher lokalen Ebene bereitstellt	`storage pool show-aggregate`
Anzeigen, wie viel Cache zur Gesamt-Cache-Kapazität für beide RAID-Typen hinzugefügt würde (Datengröße der Zuordnungseinheit)	`storage pool show -instance`
Die Datenträger in einem Speicherpool anzeigen	`storage pool show-disks`
Nicht zugewiesene Zuordnungseinheiten für einen Speicherpool anzeigen	`storage pool show-available-capacity`
Die Eigentumsrechte an einer oder mehreren Zuordnungseinheiten eines Storage Pools von einem HA-Partner auf den anderen übertragen	`storage pool reassign`

Verwandte Informationen

- "Speicherpool neu zuweisen"
- "storage pool show"
- "storage pool show-aggregate"
- "storage pool show-available-capacity"
- "storage pool show-disks"

FabricPool Tier-Management

Informationen zum Data Tiering mit ONTAP FabricPool

Mit FabricPool kann Daten automatisch je nach Zugriffshäufigkeit in verschiedene Ebenen verschoben werden.

FabricPool ist eine Hybrid-Speicherlösung, die auf AFF Systemen ein All-Flash-Aggregat (ausschließlich SSDs) nutzt und auf FAS Systemen entweder ein All-Flash-Aggregat (ausschließlich SSDs) oder ein HDD-Aggregat als Leistungsebene sowie einen Objektspeicher als Cloud-Ebene einsetzt. Die Nutzung eines FabricPool trägt dazu bei, die Speicherkosten zu senken, ohne Leistung, Effizienz oder Schutz zu beeinträchtigen.

Die Cloud-Ebene kann sich auf NetApp StorageGRID oder ONTAP S3 (ab ONTAP 9.8) oder bei einem der folgenden Dienstanbieter befinden:

- Alibaba Cloud
- Amazon S3
- Amazon Commercial Cloud Services
- Google Cloud
- IBM Cloud
- Microsoft Azure Blob Storage

Ab ONTAP 9.7 können zusätzliche Objektspeicheranbieter, die generische S3-APIs unterstützen, durch Auswahl des S3_Compatible Objektspeicheranbieters verwendet werden.

Anforderungen für die Nutzung von ONTAP FabricPool

Um sicherzustellen, dass Sie Ihre FabricPool Konfigurationen optimieren, ist es hilfreich, sich mit einigen Überlegungen und Anforderungen bezüglich der Verwendung von FabricPool vertraut zu machen.

Allgemeine Überlegungen und Anforderungen

ONTAP 9.4

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.4 oder eine spätere Version ausgeführt werden:
  - Der `auto` "Tiering-Richtlinie"
  - Festlegung der minimalen Kühlungsdauer für das Tiering
  - Meldung inaktiver Daten (IDR)
  - Verwendung von Microsoft Azure Blob Storage für die Cloud als Cloud-Tier für FabricPool
  - Verwendung von FabricPool mit ONTAP Select

ONTAP 9.5

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.5 oder eine spätere Version ausgeführt werden:
  - Festlegung des Schwellenwerts für den Tiering-Füllstand

- Verwendung von IBM Cloud Object Storage als Cloud-Tier für FabricPool
- NetApp Volume Encryption (NVE) der Cloud-Ebene, standardmäßig aktiviert.

ONTAP 9.6

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.6 oder eine spätere Version ausgeführt werden:
  - Die `all`Tiering-Policy
  - Inaktive Datenberichterstattung manuell auf HDD Aggregaten aktiviert
  - Die Meldung inaktiver Daten wird für SSD-Aggregate automatisch aktiviert, wenn auf ONTAP 9.6 aktualisiert wird und wenn das Aggregat erstellt wird, außer auf Low-End-Systemen mit weniger als 4 CPU, weniger als 6 GB RAM oder wenn die WAFL-Puffer-Cache-Größe weniger als 3 GB beträgt.

    ONTAP überwacht die Systemlast, und wenn die Last vier Minuten lang konstant hoch bleibt, wird IDR deaktiviert und nicht automatisch wieder aktiviert. IDR kann manuell wieder aktiviert werden; manuell aktiviertes IDR wird jedoch nicht automatisch deaktiviert.

  - Verwendung von Alibaba Cloud Object Storage als Cloud-Tier für FabricPool
  - Nutzung der Google Cloud Platform als Cloud-Tier für FabricPool
  - Volumenverschiebung ohne Cloud-Tier-Datenkopie

ONTAP 9.7

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.7 oder eine spätere Version ausgeführt werden:
  - Nicht transparenter HTTP- und HTTPS-Proxy, um den Zugriff nur auf zugelassene Zugriffspunkte bereitzustellen sowie Überwachungs- und Berichtsfunktionen zu ermöglichen.
  - FabricPool Spiegelung zur Tierung von kalten Daten gleichzeitig auf zwei Objektspeicher
  - FabricPool Spiegelungen auf MetroCluster Konfigurationen
  - NDMP-Dump und -Wiederherstellung sind auf FabricPool angeschlossenen Aggregaten standardmäßig aktiviert.

    Verwendet die Backup-Anwendung ein anderes Protokoll als NDMP, beispielsweise NFS oder SMB, werden alle im Performance Tier gesicherten Daten als „heiß“ eingestuft, was das Tiering dieser Daten in den Cloud Tier beeinträchtigen kann. Nicht-NDMP-Lesezugriffe können eine Datenmigration vom Cloud Tier zurück in den Performance Tier verursachen.

    "NDMP Backup- und Wiederherstellungsunterstützung für FabricPool"

ONTAP 9.8

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.8 oder höher ausgeführt werden:
  - Cloud Retrieval
  - FabricPool mit SnapLock Enterprise. FabricPool mit SnapLock Enterprise erfordert einen Feature Product Variance Request (FPVR). Für die Erstellung eines FPVR ist das Vertriebsteam zu kontaktieren.
  - Mindestkühlzeit maximal 183 Tage
  - Objektkennzeichnung mithilfe benutzerdefinierter Tags

- HDD FabricPool Aggregate

  HDD FabricPools werden mit SAS-, FSAS-, BSAS- und MSATA-Festplatten nur auf Systemen mit 6 oder mehr CPU-Kernen unterstützt.

Prüfen Sie "Hardware Universe" auf die neuesten unterstützten Modelle.

ONTAP 9.10.1

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.10.1 oder höher ausgeführt werden:
  - PUT-Drosselung
  - Temperaturabhängige Speichereffizienz (TSSE).

ONTAP 9.12.1

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.12.1 oder höher ausgeführt werden:
  - Unterstützung für FabricPool, FlexGroup und SVM-DR, die gemeinsam funktionieren. (Vor Version 9.12.1 funktionierten jeweils zwei dieser Funktionen zusammen, jedoch nicht alle drei in Kombination.)

ONTAP 9.14.1

- Für die folgende FabricPool-Funktionalität muss ONTAP 9.14.1 oder höher ausgeführt werden:
  - Cloud Write
  - Aggressives Readahead

Lokale Ebenen (Aggregate)

FabricPool unterstützt die folgenden Aggregattypen:

- Auf AFF Systemen können nur SSD Aggregate für FabricPool verwendet werden.
- Auf FAS-Systemen können entweder SSD- oder HDD-Aggregate für FabricPool verwendet werden.
- Bei Cloud Volumes ONTAP und ONTAP Select können entweder SSD- oder HDD-Aggregate für FabricPool verwendet werden. Die Verwendung von SSD-Aggregaten wird empfohlen.

Flash Pool Aggregate, die sowohl SSDs als auch HDDs enthalten, werden nicht unterstützt.

Cloud-Tiers

FabricPool unterstützt die Verwendung der folgenden Objektspeicher als Cloud-Tier:

- Alibaba Cloud Objektspeicherdienst (Standard, Seltener Zugriff)
- Amazon S3 (Standard, Standard-IA, One Zone-IA, Intelligent-Tiering, Glacier Instant Retrieval)
- Amazon Commercial Cloud Services (C2S)
- Google Cloud Storage (Multi-Regional, Regional, Nearline, Coldline, Archive)
- IBM Cloud Object Storage (Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (Hot und Cool)
- NetApp ONTAP S3 (ONTAP 9.8 und höher)
- NetApp StorageGRID (StorageGRID 10.3 und höher)

Glacier Flexible Retrieval und Glacier Deep Archive werden nicht unterstützt.

- Der Objektspeicher “bucket” (Container), den Sie verwenden möchten, muss bereits eingerichtet sein, mindestens 10 GB Speicherplatz haben und darf nicht umbenannt werden.
- Eine Cloud-Ebene kann nach dem Verbinden nicht mehr von einer lokalen Ebene getrennt werden; allerdings kann "FabricPool Spiegel" verwendet werden, um eine lokale Ebene mit einer anderen Cloud-Ebene zu verbinden.

Intercluster-LIFs

Cluster-Hochverfügbarkeitspaare (HA-Paare), die FabricPool verwenden, benötigen zwei Intercluster-LIFs, um mit der Cloud-Ebene zu kommunizieren. NetApp empfiehlt, auch auf zusätzlichen HA-Paaren einen Intercluster-LIF zu erstellen, um Cloud-Ebenen nahtlos mit lokalen Ebenen auf diesen Knoten zu verbinden.

Das Deaktivieren oder Löschen eines Intercluster-LIF unterbricht die Kommunikation mit der Cloud-Tier.

Da parallele SnapMirror und SnapVault Replikationsvorgänge die Netzwerkverbindung zur Cloud-Ebene gemeinsam nutzen, hängen Initialisierung und RTO von der verfügbaren Bandbreite und Latenz zur Cloud-Ebene ab. Bei Überlastung der Verbindungsressourcen kann es zu Leistungseinbußen kommen. Die proaktive Konfiguration mehrerer LIFs kann diese Art der Netzwerküberlastung deutlich reduzieren.

Wenn Sie auf einem Knoten mit unterschiedlichem Routing mehr als eine Intercluster-LIF verwenden, empfiehlt NetApp, diese in verschiedenen IPspaces zu platzieren. Während der Konfiguration kann FabricPool aus mehreren IPspaces auswählen, jedoch keine spezifischen Intercluster-LIFs innerhalb eines IPspaces auswählen.

Network Time Protocol (NTP)

Die Konfiguration des Network Time Protocol (NTP) ist erforderlich, um die Zeit zwischen den Clustern zu synchronisieren. "Informationen zur Konfiguration von NTP".

ONTAP Speicher-Effizienzen

Speichereffizienzen wie Komprimierung, Deduplizierung und Verdichtung bleiben beim Verschieben von Daten in die Cloud-Tier erhalten, wodurch die benötigte Objektspeicherkapazität und die Transportkosten reduziert werden.

Ab ONTAP 9.15.1 unterstützt FabricPool die Intel QuickAssist Technology (QAT4), die aggressivere und leistungsfähigere Einsparungen bei der Speichereffizienz bietet.

Die Inline-Deduplizierung auf Aggregatebene wird auf der lokalen Ebene unterstützt, die damit verbundenen Speichereffizienzen werden jedoch nicht auf Objekte übertragen, die auf der Cloud-Ebene gespeichert sind.

Bei Verwendung der All Volume Tiering-Richtlinie können die mit Hintergrunddeduplizierungsprozessen verbundenen Speichereffizienzen reduziert werden, da die Daten wahrscheinlich gestaffelt werden, bevor die zusätzlichen Speichereffizienzen angewendet werden können.

Kapazitätslizenz

FabricPool erfordert eine kapazitätsbasierte Lizenz, wenn Drittanbieter von Objektspeichern (wie Amazon S3) als Cloud-Tiers für AFF und FAS Systeme angebunden werden.

StorageGRID Konsistenzkontrollen

Die Konsistenzsteuerung von StorageGRID beeinflusst, wie die Metadaten, die StorageGRID zur Nachverfolgung von Objekten verwendet, zwischen den Knoten verteilt werden und wie verfügbar die Objekte für Clientanfragen sind. NetApp empfiehlt die Verwendung der standardmäßigen Konsistenzsteuerung „Read-After-New-Write“ für Buckets, die als FabricPool Ziele genutzt werden.

> Die verfügbare Konsistenzkontrolle sollte nicht für Buckets verwendet werden, die als FabricPool Ziele genutzt werden.

Zusätzliche Überlegungen zum Tiering von Daten, auf die über SAN-Protokolle zugegriffen wird

Beim Tiering von Daten, auf die über SAN-Protokolle zugegriffen wird, empfiehlt NetApp aufgrund von Konnektivitätsaspekten die Nutzung privater Clouds wie ONTAP S3 oder StorageGRID.

> Es ist zu beachten, dass bei der Verwendung von FabricPool in einer SAN-Umgebung mit einem Windows-Host Dateien auf der NetApp LUN des Windows-Hosts unzugänglich werden oder verschwinden können, wenn der Objektspeicher während der Tiering-Vorgänge in die Cloud über einen längeren Zeitraum nicht verfügbar ist. Siehe "NetApp Knowledge Base: Während FabricPool S3-Objektspeicher nicht verfügbar war, wurde vom Windows SAN-Host eine Dateisystembeschädigung gemeldet.".

Servicequalität

- Wenn Sie Durchsatzuntergrenzen (QoS Min) verwenden, muss die Tiering-Richtlinie für die Volumes auf `none` festgelegt werden, bevor das Aggregat an FabricPool angehängt werden kann.

  Andere Tiering-Richtlinien verhindern, dass das Aggregat an FabricPool angehängt wird. Eine QoS-Richtlinie erzwingt keine Durchsatzuntergrenzen, wenn FabricPool aktiviert ist.

Funktionen oder Merkmale, die von FabricPool nicht unterstützt werden

- Objektspeicher mit aktiviertem WORM und aktivierter Objektversionierung.
- Richtlinien für das Informationslebenszyklusmanagement (ILM), die auf Objektspeicher Buckets angewendet werden

  FabricPool unterstützt die Information Lifecycle Management (ILM)-Richtlinien von StorageGRID ausschließlich für Datenreplizierung und Erasure Coding, um Cloud-Tier-Daten vor Ausfällen zu schützen. Erweiterte ILM-Regeln wie das Filtern anhand von Benutzermetadaten oder Tags werden von FabricPool jedoch nicht unterstützt. ILM umfasst typischerweise verschiedene Richtlinien zur Bewegung und Löschung von Daten. Diese Richtlinien können für die Daten im Cloud-Tier von FabricPool nachteilig sein. Die Nutzung von FabricPool mit ILM-Richtlinien, die auf Objektspeichern konfiguriert sind, kann zu Datenverlust führen.

- 7-Mode Datenmigration mithilfe der ONTAP CLI-Befehle oder des 7-Mode Transition Tool
- RAID SyncMirror, außer in einer MetroCluster Konfiguration
- SnapLock Volumes bei Verwendung von ONTAP 9.7 und früheren Versionen
- "Manipulationssichere Schnappschüsse"

  Manipulationssichere Snapshots bieten unveränderlichen Schutz, der nicht gelöscht werden kann. Da FabricPool die Möglichkeit zum Löschen von Daten benötigt, können FabricPool und Snapshot-Sperren nicht auf demselben Volume aktiviert werden.

- Bandsicherung mit SMTape für FabricPool aktivierte Aggregate
- Volumes mit einer anderen Speicherplatzzusage als `none`

  Mit Ausnahme von Root-SVM-Volumes und CIFS-Audit-Staging-Volumes unterstützt FabricPool das Anhängen einer Cloud-Ebene an ein Aggregat, das Volumes mit einer anderen Speicherplatzzusage als `none` enthält, nicht. Beispielsweise wird ein Volume mit einer Speicherplatzzusage von `volume` (`-space -guarantee volume` nicht unterstützt.

- Cluster mit "DP_Optimized Lizenz"
- Flash Pool Aggregate

ONTAP FabricPool Volume-Tiering-Richtlinien

FabricPool Volumen-Tiering-Richtlinien legen fest, welche Daten in einem Volume für das Tiering infrage kommen, und der Parameter für die minimale Anzahl an Kühl-Tagen beim Tiering bestimmt, wann die Daten als inaktiv gelten und für das Tiering infrage kommen.

Zugriffskontrolllisten (ACLs), Verzeichnisstrukturen und Metadaten werden niemals gestuft, sondern verbleiben immer auf der lokalen Tier.

Ein täglicher Hintergrundscan sucht nach selten genutzten Datenblöcken. Sobald genügend 4-KB-Blöcke desselben Volumes erfasst wurden, werden diese zu einem 4-MB-Objekt zusammengefasst und gemäß der Volume Tiering-Richtlinie in die Cloud-Ebene verschoben.

Das Verständnis der Funktionsweise von Tiering-Richtlinien unterstützt bei der Auswahl der passenden Richtlinie für die Anforderungen an das Speichermanagement.

Optionen für Volume-Tiering-Richtlinien

Standardmäßig verwenden Volumes die Volume-Tiering-Richtlinie „Keine“. Eine Ausnahme bilden neu erstellte FlexVol Volumes auf FabricPool Aggregaten, die die Volume-Tiering-Richtlinie „Nur Snapshots“ verwenden.

Der `volume object-store tiering show`Befehl kann verwendet werden, um den Tiering-Status eines FabricPool Volumes anzuzeigen. Weitere Informationen zu `volume object-store tiering show` finden sich in der "ONTAP-Befehlsreferenz".

Die FabricPool Tiering-Richtlinie wird auf Volume-Ebene festgelegt. Vier Optionen sind verfügbar:

Nur Snapshot

Die `snapshot-only`Tiering-Richtlinie verschiebt Snapshot-Daten, die nicht mehr mit dem aktiven Dateisystem verbunden sind, in eine andere Ebene. Standardmäßig sind zwei Tage Inaktivität erforderlich, bevor ein Snapshot für das Tiering in Frage kommt. Die meisten Datensicherungspläne sind stündlich oder täglich und lesen die Daten lokal, bevor sie getiert werden.

Die Standardeinstellung für die Mindestkühlzeit nach Stufen kann mit dem `-tiering-minimum-cooling -days` Parameter auf der erweiterten Berechtigungsebene der `volume create` und `volume modify` Befehle geändert werden. Gültige Werte sind 2 bis 183 Tage bei Verwendung von ONTAP 9.8 und höher. Bei Verwendung einer ONTAP-Version vor 9.8 sind gültige Werte 2 bis 63 Tage.

Beim Lesen bleiben kalte Blöcke, die mit Snapshot-Kopien verknüpft sind, kalt und werden nicht zurück in die lokale Tier geschrieben.

Automatisch

Die `auto`Tiering-Richtlinie verschiebt alle kalten Daten im Volume, sowohl die Snapshots als auch das aktive Dateisystem, in die Cloud-Tier. Die standardmäßige Mindestkühlzeit für das Tiering beträgt 31 Tage und gilt für das gesamte Volume, sowohl für das aktive Dateisystem als auch für die Snapshots.

Die Standardeinstellung für die Mindestkühlzeit nach Stufen kann mit dem `-tiering-minimum-cooling-days` Parameter auf der erweiterten Berechtigungsebene der `volume create` und `volume modify` Befehle geändert werden. Gültige Werte sind 2 bis 183 Tage.

Beim zufälligen Lesen werden kalte Blöcke in einem Volume mit auf Auto eingestellter Tiering-Richtlinie als hot markiert und zurück in die lokale Tier geschrieben.

Beim sequenziellen Lesen bleiben kalte Blöcke in einem Volume mit der Tiering-Richtlinie Auto kalt und verbleiben auf der Cloud-Ebene. Sie werden nicht zurück in den lokalen Tier geschrieben.

Alle

Die `all` Tiering-Richtlinie kennzeichnet sofort alle Daten im Volume als kalt und beginnt, sie so schnell wie möglich in die Cloud-Tier zu verschieben. Ein Warten von 48 Stunden, bis neue Blöcke in einem Volume mit der `all` Tiering-Richtlinie als kalt gelten, ist nicht erforderlich.

Die Mindestkühlzeit für Tiering findet keine Anwendung, da die Daten in die Cloud-Tier verschoben werden, sobald der Tiering-Scan ausgeführt wird, und diese Einstellung nicht geändert werden kann.

Wenn kalte Blöcke in einem Volume mit der Tiering-Richtlinie „All“ gelesen werden, bleiben sie kalt und verbleiben im Cloud-Tier. Sie werden nicht zurück in den lokalen Tier geschrieben.

> Die `all`Volume Tiering-Richtlinie sollte nicht auf lesen/schreiben Volumes angewendet werden, die normalen Client-Datenverkehr aufweisen.
>
> Objektspeicherung ist nicht transaktionsorientiert wie Datei- oder Blockspeicherung. Änderungen an Dateien, die als Objekte in Volumes mit der All Tiering-Richtlinie gespeichert werden, können zur Erstellung neuer Objekte, zur Fragmentierung vorhandener Objekte, zu einer verringerten Leseleistung und zu zusätzlichen Speicherineffizienzen führen.

Keine

Die `none`Tiering-Richtlinie behält die Daten eines Volumes in der Performance-Tier und verschiebt keine Daten in andere Tiers.

Das Festlegen der Tiering-Richtlinie auf `none` verhindert neues Tiering. Volumendaten, die zuvor in die Cloud-Tier verschoben wurden, verbleiben in der Cloud-Tier, bis sie wieder aktiv werden und automatisch zurück in die lokale Tier verschoben werden.

Die Mindestkühlzeit für das Tiering findet keine Anwendung, da die Daten nie in die Cloud-Tier verschoben werden und die Einstellung nicht geändert werden kann.

Wenn kalte Blöcke in einem Volume mit einer auf `none` gesetzten Tiering-Richtlinie gelesen werden, werden sie heiß gemacht und in das lokale Tier geschrieben.

Die `volume show` Befehlsausgabe zeigt die Tiering-Richtlinie eines Volumes an. Ein Volume, das noch nie mit FabricPool verwendet wurde, zeigt die `none` Tiering-Richtlinie in der Ausgabe an.

Bei einer SVM DR-Beziehung müssen Quell- und Ziel-Volumes keine FabricPool Aggregate verwenden, sie müssen jedoch dieselbe Tiering-Richtlinie nutzen.

Was geschieht, wenn eine Volume-Tiering-Richtlinie geändert wird?

Die Tiering-Richtlinie eines Volumes kann durch einen `volume modify` Vorgang geändert werden. Es ist wichtig zu verstehen, wie sich eine Änderung der Tiering-Richtlinie auf die Dauer auswirken kann, bis Daten als kalt gelten und in die Cloud-Tier verschoben werden.

- Eine Änderung der Tiering-Richtlinie von `snapshot-only` oder `none` zu `auto` bewirkt, dass ONTAP Benutzerdatenblöcke im aktiven Dateisystem, die bereits kalt sind, an die Cloud-Tier sendet, selbst wenn diese Benutzerdatenblöcke zuvor nicht für die Cloud-Tier geeignet waren.
- Die Änderung der Tiering-Richtlinie zu `all` von einer anderen Richtlinie bewirkt, dass ONTAP alle Benutzerblöcke im aktiven Dateisystem und in den Snapshots so schnell wie möglich in die Cloud verschiebt. Vor ONTAP 9.8 mussten Blöcke warten, bis der nächste Tiering-Scan ausgeführt wurde.

  Das Zurückverschieben von Blöcken in die Performance Ebene ist nicht zulässig.

- Eine Änderung der Tiering-Richtlinie von `auto` zu `snapshot-only` oder `none` führt nicht dazu, dass aktive Dateisystemblöcke, die bereits in die Cloud-Ebene verschoben wurden, wieder in die Performance-Ebene zurückverschoben werden.

  Für die Rückführung der Daten in die Performance-Tier sind Volume-Lesevorgänge erforderlich.

- Jedes Mal, wenn die Tiering-Richtlinie für ein Volume geändert wird, wird die minimale Abkühlperiode des Tierings auf den Standardwert der Richtlinie zurückgesetzt.

Was geschieht mit der Tiering-Richtlinie, wenn ein Volume verschoben wird?

- Sofern nicht explizit eine andere Tiering-Richtlinie festgelegt wird, behält ein Volume seine ursprüngliche Tiering-Richtlinie bei, wenn es in ein FabricPool fähiges Aggregat verschoben wird oder dieses verlässt.

  Die Tiering-Richtlinie greift jedoch nur, wenn das Volume sich in einem FabricPool fähigen Aggregat befindet.

- Der bestehende Wert des `-tiering-minimum-cooling-days` Parameters für ein Volume wird mit dem Volume übertragen, sofern keine andere Tiering-Richtlinie für das Ziel angegeben wird.

  Wenn Sie eine andere Tiering-Richtlinie festlegen, verwendet das Volume die standardmäßige minimale Abkühlperiode für diese Richtlinie. Dies ist der Fall, unabhängig davon, ob das Ziel FabricPool ist oder nicht.

- Ein Volume kann zwischen Aggregaten verschoben und gleichzeitig die Tiering-Richtlinie geändert werden.
- Besondere Aufmerksamkeit ist erforderlich, wenn ein `volume move`Vorgang die `auto`Tiering-Policy betrifft.

  Unter der Annahme, dass sowohl die Quelle als auch das Ziel FabricPool-fähige Aggregate sind, fasst die folgende Tabelle das Ergebnis einer `volume move`Operation zusammen, die Richtlinienänderungen im Zusammenhang mit `auto` zusammenfasst:

Wenn ein Volume mit einer Tiering-Richtlinie von … verschoben wird	Und die Tiering-Richtlinie wird mit dem Wechsel zu … geändert	Dann nach der Volume-Verschiebung…
`all`	`auto`	Alle Daten werden in die Performance-Tier verschoben.
`snapshot-only`, `none`, oder `auto`	`auto`	Die Datenblöcke werden auf dieselbe Ebene des Zielsystems verschoben, auf der sie sich zuvor auf dem Quellsystem befanden.
`auto` oder `all`	`snapshot-only`	Alle Daten werden in die Performance-Tier verschoben.
`auto`	`all`	Alle Benutzerdaten werden in die Cloud-Tier verschoben.
`snapshot-only`,`auto` oder `all`	`none`	Alle Daten verbleiben auf der Leistungsebene.

Was geschieht mit der Tiering-Richtlinie, wenn ein Volume geklont wird

- Ab ONTAP 9.8 erbt ein geklontes Volume immer sowohl die Tiering-Richtlinie als auch die Cloud-Abrufrichtlinie vom übergeordneten Volume.

  In Versionen vor ONTAP 9.8 übernimmt ein Klon die Tiering-Richtlinie vom übergeordneten Volume, außer wenn das übergeordnete Volume die `all` Tiering-Richtlinie hat.

- Wenn das übergeordnete Volume die `never` Cloud Retrieval Policy hat, muss sein Klon-Volume entweder die `never` Cloud Retrieval Policy oder die `all` Tiering Policy sowie eine entsprechende Cloud Retrieval Policy `default` haben.
- Die Cloud-Abrufrichtlinie des übergeordneten Volumes kann nicht in `never` geändert werden, es sei denn, alle seine Klon-Volumes haben eine Cloud-Abrufrichtlinie `never`.

Beim Klonen von Volumes sind die folgenden bewährten Vorgehensweisen zu beachten:

- Die `-tiering-policy` Option und `tiering-minimum-cooling-days` Option des Klons steuern ausschließlich das Tiering-Verhalten von Blöcken, die nur in diesem Klon vorkommen. Daher wird empfohlen, für das übergeordnete FlexVol Tiering-Einstellungen zu verwenden, die entweder die gleiche Datenmenge verschieben oder weniger Daten verschieben als einer der Klone.
- Die Cloud-Abrufrichtlinie des übergeordneten FlexVol sollte entweder die gleiche Datenmenge oder mehr Daten übertragen als die Abrufrichtlinie eines der Klone.

Wie Cloud-Abrufrichtlinien mit Tiering-Richtlinien funktionieren

FabricPool Cloud-Datenabruf wird durch Abrufrichtlinien gesteuert, die festlegen, wann Daten in die lokale Ebene zurückgeschrieben werden. Lesemuster können entweder sequenziell oder zufällig sein.

Die folgende Tabelle listet die Volume-Tiering-Richtlinien und das Standardabrufverhalten für jede Richtlinie auf.

Tiering-Richtlinie	Standardmäßiges Abrufverhalten
keine	Sequenzielle und zufällige Lesevorgänge

nur Snapshot	Sequenzielle und zufällige Lesevorgänge
Auto	Zufällige Lesevorgänge
alle	Kein Datenabruf

Ab ONTAP 9.8 überschreibt die Option zur Steuerung der Cloud-Migration `cloud-retrieval-policy` das standardmäßige Cloud-Migrations- oder Abrufverhalten, das durch die Tiering-Richtlinie gesteuert wird.

Die folgende Tabelle listet die unterstützten Cloud-Abrufrichtlinien und deren Abrufverhalten auf.

Cloud-Abrufrichtlinie	Abrufverhalten
Standard	Beim Lesen von kalten Blöcken in einem Volume wird das Standardverhalten der Volume-Tiering-Richtlinie des Volumes verwendet. Diese Richtlinie ist der Standardwert für jedes Volume, unabhängig vom Typ des gehosteten Aggregats.
on-read	Wenn kalte Blöcke in einem Volume mit einer Cloud-Abrufrichtlinie, die auf “On-Read” gesetzt ist, zufällig oder sequenziell gelesen werden, werden sie zu heißen Blöcken und in die lokale Ebene geschrieben. Anwendungen, die sequenzielle Lesevorgänge nutzen, lösen Rückschreibvorgänge auf die lokale Ebene aus, indem die Abrufrichtlinie für das Volume aus der Cloud auf „On-Read“ gesetzt wird. Dies kann für Anwendungen von Vorteil sein, die lokale Ebenenleistung für zuvor kalte Daten benötigen, die nun von aktiven Workloads gelesen werden.
niemals	Wenn kalte Blöcke in einem Volume mit einer Cloud-Abrufrichtlinie, die auf „Nie“ gesetzt ist, gelesen werden, bleiben sie kalt und verbleiben auf der Cloud-Ebene. Sie werden nicht zurück auf die lokale Ebene geschrieben. Die Einstellung der Cloud-Abrufrichtlinie auf „`Never`“ ist ähnlich wie die All Tiering-Richtlinie, da Daten nicht auf die lokale Ebene zurückkehren dürfen, unterscheidet sich jedoch von der All Tiering-Richtlinie dadurch, dass weiterhin die Einstellung „tiering-minimum-cooling-days“ des Volumes verwendet wird, anstatt die Daten so schnell wie möglich zu verschieben. Beispielsweise würde ein Volume, das die Standardeinstellung der Auto Tiering-Richtlinie verwendet, Daten erst nach 31 Tagen Inaktivität als kalt markieren. Nach 31 Tagen würden die inaktiven Daten in den Objektspeicher verschoben und kämen beim Lesen nicht zurück, da die Cloud Retrieval Policy des Volumes auf "Never" gesetzt wurde.

promoten	• Für die Tiering-Richtlinie “none,” werden alle gestuften Daten zurück auf die lokale Tier geschrieben. • Für die Tiering-Richtlinie „`snapshot-only`“ werden gestaffelte, nicht-Snapshot-Daten zurück in die lokale Ebene geschrieben.

Beispiel für die Änderung der Cloud Retrieval-Richtlinie

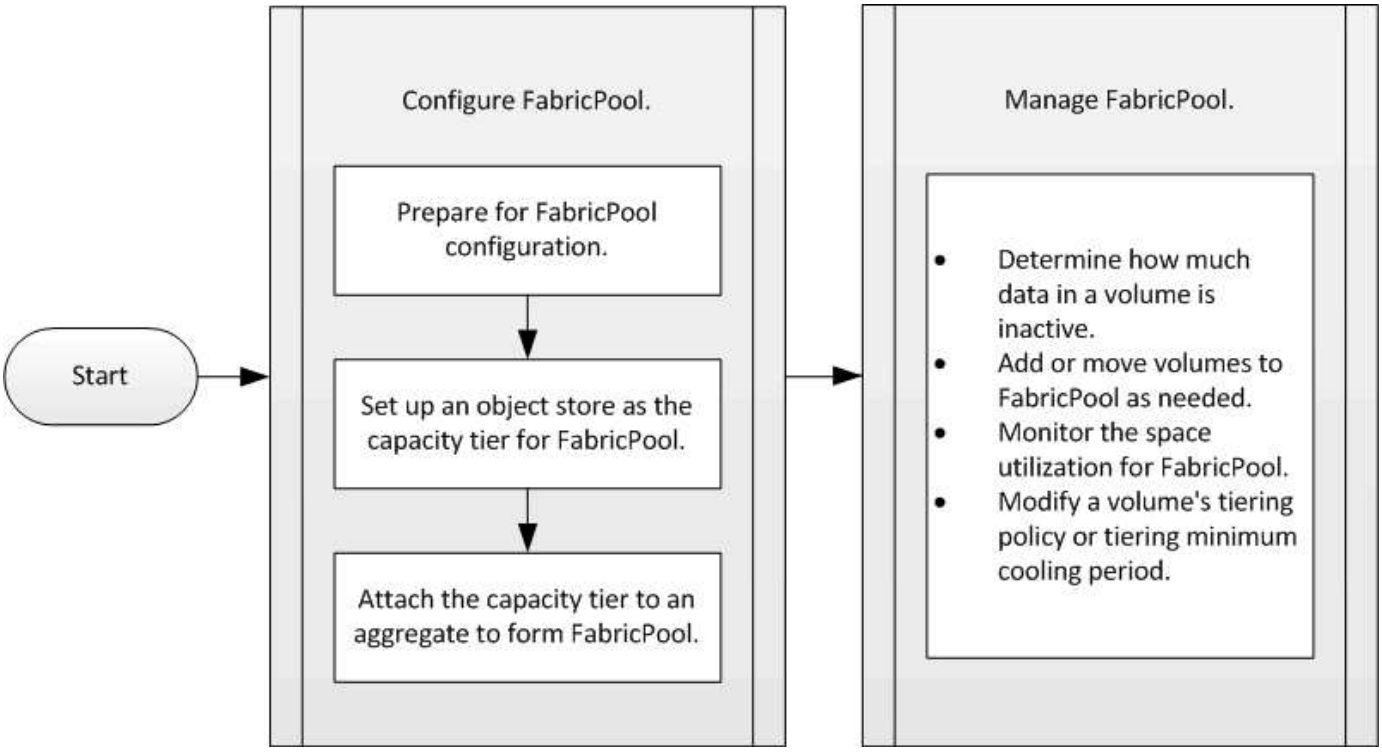
Das folgende Beispiel ändert die Tiering-Richtlinie des Volumes auf `none` und die Abrufrichtlinie auf `promote`:

```
set -privilege advanced

volume modify -vserver vs1 -volume myvol -tiering-policy none -cloud
-retrieval-policy promote
```

ONTAP FabricPool Konfigurations- und Verwaltungsworkflow

Das FabricPool Workflow-Diagramm kann zur Planung der Konfigurations- und Verwaltungsaufgaben verwendet werden.



Konfiguration von FabricPool

Einstieg in ONTAP FabricPool

Die Konfiguration von FabricPool hilft dabei, zu steuern, auf welcher Speicherebene (lokale Performance-Ebene oder Cloud-Ebene) Daten gespeichert werden sollten,

abhängig davon, ob häufig auf die Daten zugegriffen wird.

Die für die FabricPool Konfiguration erforderliche Vorbereitung hängt vom Objektspeicher ab, der als Cloud-Tier verwendet wird.

Installieren einer FabricPool-Lizenz auf einem ONTAP Cluster

NetApp Cloud Tiering ist ab dem 26. April 2026 nicht mehr zum Kauf oder zur Lizenzverlängerung verfügbar. Wenn Sie NetApp Cloud Tiering verwenden, empfiehlt NetApp, dass Sie mit Ihrem NetApp Ansprechpartner zusammenarbeiten, um Ihre bestehenden Tiering-Lizenzen auf ONTAP FabricPool Lizenzen umzustellen.

Bestehende Kunden können NetApp Cloud Tiering weiterhin nutzen und Support dafür erhalten, bis ihr Abonnement oder Lizenzvertrag abläuft. Nach Ablauf des Abonnements haben Sie keinen Zugriff mehr auf NetApp Cloud Tiering-Funktionen oder Support.

Wenn Sie derzeit Cloud-Tiering-Lizenzierung nutzen, sind Sie erst betroffen, wenn Ihre Cloud-Tiering-Lizenz abläuft oder ihre maximale Kapazität erreicht. Kontaktieren Sie NetApp, wenn Sie Ihre Lizenz aktualisieren müssen oder auch früher, um sicherzustellen, dass Ihre Fähigkeit, Daten in die Cloud zu verschieben, nicht unterbrochen wird.

"Erfahren Sie mehr über NetApp Cloud-Tiering-Lizenzänderungen".

Sie können eine FabricPool-Lizenz mit dem System Manager herunterladen und aktivieren.

Die FabricPool-Lizenz ist eine clusterweite Lizenz. Sie umfasst ein berechtigtes Nutzungslimit, das für den Objektspeicher erworben wird, der im Cluster mit FabricPool verknüpft ist. Die Nutzung im gesamten Cluster darf die Kapazität des berechtigten Nutzungslimits nicht überschreiten. Für eine Erhöhung des Nutzungslimits der Lizenz ist der jeweilige Vertriebsmitarbeiter zu kontaktieren.

FabricPool Lizenzen sind als unbefristete oder befristete Lizenzen mit einer Laufzeit von 1 oder 3 Jahren erhältlich.

Eine Lizenz ist nicht erforderlich, wenn Sie NetApp StorageGRID oder ONTAP S3 für die Cloud-Ebene verwenden. Cloud Volumes ONTAP benötigt unabhängig vom verwendeten Anbieter keine FabricPool-Lizenz.

Bevor Sie beginnen

Sie benötigen Ihre Cluster-UUID, um Ihre NetApp License File (NLF) von der NetApp Support Site abzurufen.

Schritte

Diese Aufgabe wird nur unterstützt, wenn die Lizenzdatei mithilfe von System Manager in den Cluster hochgeladen wird.

1. Laden Sie die NetApp License File (NLF) für die FabricPool Lizenz von der "NetApp Support Site" herunter.
2. Die folgenden Aktionen werden mit dem System Manager durchgeführt, um die FabricPool Lizenz auf das Cluster hochzuladen:
   a. Im Bereich **Cluster > Einstellungen** auf der Karte **Lizenzen** auf → klicken.
   b. Auf der Seite **Lizenz** auf + Add klicken.
   c. Im Dialogfeld **Lizenz hinzufügen** auf **Durchsuchen** klicken, um die heruntergeladene NLF auszuwählen, und anschließend auf **Hinzufügen** klicken, um die Datei in den Cluster hochzuladen.

Verwandte Informationen

"ONTAP FabricPool (FP) Lizenzübersicht"

"NetApp Softwarelizenzsuche"

"NetApp TechComm TV: FabricPool Wiedergabeliste"

Installation eines CA-Zertifikats auf einem ONTAP Cluster für StorageGRID

Die Verwendung von CA-Zertifikaten schafft eine vertrauenswürdige Beziehung zwischen Client-Anwendungen und StorageGRID.

Sofern Sie nicht vorhaben, die Zertifikatsprüfung für StorageGRID zu deaktivieren, müssen Sie ein StorageGRID CA-Zertifikat auf dem Cluster installieren, damit ONTAP sich bei StorageGRID als Objektspeicher für FabricPool authentifizieren kann.

Obwohl StorageGRID selbstsignierte Zertifikate generieren kann, gilt die Verwendung signierter Zertifikate einer Drittanbieter-Zertifizierungsstelle als empfohlene Best Practice.

Über diese Aufgabe

Obwohl die Installation und Verwendung von Zertifikaten der Zertifizierungsstelle (CA) als empfohlene Best Practice gilt, ist ab ONTAP 9.4 die Installation von CA-Zertifikaten für StorageGRID nicht erforderlich.

Schritte

1. Wenden Sie sich an Ihren StorageGRID Administrator, um die "CA-Zertifikat des StorageGRID Systems" zu erhalten.
2. Der `security certificate install`-Befehl mit dem `-type server-ca`-Parameter dient zur Installation des StorageGRID CA-Zertifikats auf dem Cluster.

   Der vollqualifizierte Domainname (FQDN), den Sie eingeben, muss mit dem benutzerdefinierten allgemeinen Namen auf dem StorageGRID CA-Zertifikat übereinstimmen.

Ein abgelaufenes Zertifikat aktualisieren

Um ein abgelaufenes Zertifikat zu aktualisieren, empfiehlt es sich, das neue Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) generieren zu lassen. Zusätzlich sollte sichergestellt werden, dass das Zertifikat sowohl auf dem StorageGRID Server als auch auf dem ONTAP Cluster gleichzeitig aktualisiert wird, um Ausfallzeiten auf ein Minimum zu beschränken.

Verwandte Informationen

- "StorageGRID Ressourcen"
- "Sicherheitszertifikat installieren"

Installation eines CA-Zertifikats auf einem Cluster für ONTAP S3

Durch die Verwendung von CA-Zertifikaten wird eine vertrauenswürdige Beziehung zwischen Client-Anwendungen und dem ONTAP S3 Objektspeicher Server geschaffen. Ein CA-Zertifikat sollte auf ONTAP installiert sein, bevor ONTAP als Objektspeicher verwendet wird, der für Remote-Clients zugänglich ist.

Sofern Sie nicht vorhaben, die Zertifikatsprüfung für ONTAP S3 zu deaktivieren, muss ein ONTAP S3 CA-Zertifikat auf dem Cluster installiert werden, damit ONTAP sich bei ONTAP S3 als Objektspeicher für FabricPool authentifizieren kann.

Obwohl ONTAP selbstsignierte Zertifikate generieren kann, gilt die Verwendung signierter Zertifikate einer externen Zertifizierungsstelle als empfohlene Best Practice.

Schritte

1. Das CA-Zertifikat des ONTAP S3-Systems beschaffen.
2. Mit dem Befehl `security certificate install` und dem Parameter `-type server-ca` wird das ONTAP S3-CA-Zertifikat auf dem Cluster installiert.

   Der vollqualifizierte Domainname (FQDN), den Sie eingeben, muss mit dem benutzerdefinierten allgemeinen Namen auf dem ONTAP S3 CA-Zertifikat übereinstimmen.

Ein abgelaufenes Zertifikat aktualisieren

Um ein abgelaufenes Zertifikat zu aktualisieren, empfiehlt es sich, das neue Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (CA) generieren zu lassen. Zudem sollte das Zertifikat sowohl auf dem ONTAP S3-Server als auch auf dem ONTAP Cluster gleichzeitig aktualisiert werden, um Ausfallzeiten auf ein Minimum zu beschränken.

Mit System Manager lässt sich ein abgelaufenes Zertifikat auf einem ONTAP Cluster erneuern.

Schritte

1. Zu **Cluster > Einstellungen** navigieren.
2. Zum Abschnitt **Sicherheit** scrollen, den Bereich **Zertifikate** suchen und auf → klicken.
3. Auf der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** befindet sich der Name des Zertifikats, das erneuert werden soll.
4. Neben dem Zertifikatsnamen auf ⋮ klicken und **Erneuern** auswählen.
5. Im Fenster **Vertrauenswürdige Zertifizierungsstelle erneuern** werden die Zertifikatsinformationen in den Bereich **Zertifikatsdetails** kopiert und eingefügt oder importiert.
6. Auf **Verlängern** klicken.

Verwandte Informationen

- "S3 Konfiguration"
- "Sicherheitszertifikat installieren"

Einen Objektspeicher als Cloud-Ebene für FabricPool einrichten

Workflows zur Einrichtung des Objektspeichers für die ONTAP FabricPool Cloud-Ebene

Die Einrichtung von FabricPool beinhaltet die Angabe der Konfigurationsinformationen des Objektspeichers (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage oder Microsoft Azure Blob Storage für die Cloud), den Sie als Cloud-Tier für FabricPool verwenden möchten.

StorageGRID als ONTAP FabricPool Cloud-Tier einrichten

StorageGRID kann als Cloud-Tier für FabricPool eingerichtet werden. Beim Tiering von Daten, auf die über SAN-Protokolle zugegriffen wird, empfiehlt NetApp aufgrund von Konnektivitätsaspekten die Nutzung privater Clouds wie StorageGRID.

Überlegungen zur Verwendung von StorageGRID mit FabricPool

- Ein CA-Zertifikat für StorageGRID ist erforderlich, es sei denn, die Zertifikatsprüfung wird explizit deaktiviert.
- Die StorageGRID Objektversionierung sollte für den Objektspeicher-Bucket nicht aktiviert werden.
- Eine FabricPool Lizenz ist nicht erforderlich.
- Wenn ein StorageGRID Knoten in einer virtuellen Maschine mit Speicherzuweisung aus einem NetApp AFF System bereitgestellt wird, ist zu bestätigen, dass für das Volume keine FabricPool Tiering-Richtlinie aktiviert ist.

  Das Deaktivieren des FabricPool Tierings für Volumes, die mit StorageGRID Knoten verwendet werden, vereinfacht die Fehlersuche und den Speicherbetrieb.

> Es sollte niemals FabricPool verwendet werden, um Daten, die mit StorageGRID in Zusammenhang stehen, wieder auf StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück auf StorageGRID erhöht die Komplexität bei der Fehlerbehebung und im Betrieb.

Über diese Aufgabe

Lastausgleich ist für StorageGRID in ONTAP 9.8 und höher aktiviert. Wenn der Hostname des Servers zu mehr als einer IP-Adresse aufgelöst wird, stellt ONTAP Client-Verbindungen mit allen zurückgegebenen IP-Adressen her (bis zu maximal 16 IP-Adressen). Die IP-Adressen werden beim Verbindungsaufbau nach dem Round-Robin-Verfahren ausgewählt.

Schritte

StorageGRID kann als Cloud-Tier für FabricPool mit ONTAP System Manager oder der ONTAP CLI eingerichtet werden.

System Manager

1. Wählen Sie **Speicher > Ebenen > Cloud-Ebene hinzufügen** und dann StorageGRID als Objektspeicher-Anbieter aus.
2. Die angeforderten Informationen sind auszufüllen.
3. Zum Erstellen eines Cloud-Mirrors auf **Als FabricPool Mirror hinzufügen** klicken.

Ein FabricPool Mirror bietet eine Methode, einen Datenspeicher nahtlos zu ersetzen, und trägt dazu bei, dass Ihre Daten im Katastrophenfall verfügbar sind.

CLI

1. Die StorageGRID Konfigurationsinformationen werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type SGWS` Parameter angegeben.

   - Der `storage aggregate object-store config create`Befehl schlägt fehl, wenn ONTAP mit den angegebenen Informationen nicht auf StorageGRID zugreifen kann.
   - Der `-access-key`Parameter wird verwendet, um den Zugriffsschlüssel für die Autorisierung von Anfragen an den StorageGRID Objektspeicher anzugeben.
   - Der `-secret-password` Parameter wird verwendet, um das Passwort (Secret Access Key) für die Authentifizierung von Anfragen an den StorageGRID Objektspeicher anzugeben.
   - Wenn das StorageGRID Passwort geändert wird, sollte das entsprechende in ONTAP gespeicherte Passwort umgehend aktualisiert werden.

Dadurch kann ONTAP ohne Unterbrechung auf die Daten in StorageGRID zugreifen.

- Das Setzen des `-is-certificate-validation-enabled`-Parameters auf `false`deaktiviert die Zertifikatsprüfung für StorageGRID. Die Verwendung signierter Zertifikate (-is-certificate-validation-enabled true`von einer Drittanbieter-Zertifizierungsstelle gilt als empfohlene Best Practice.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Die StorageGRID-Konfigurationsinformationen lassen sich mit dem `storage aggregate object-store config show` Befehl anzeigen und überprüfen.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der StorageGRID-Konfigurationsinformationen für FabricPool.

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

ONTAP S3 als FabricPool Cloud-Tier einrichten

Wenn Sie ONTAP 9.8 oder höher verwenden, kann ONTAP S3 als Cloud-Tier für FabricPool eingerichtet werden.

Bevor Sie beginnen

- Sie benötigen den ONTAP S3-Servernamen und die IP-Adresse der zugehörigen LIFs auf dem Remote-Cluster.

  Der Servername wird von Clientanwendungen als vollqualifizierte Domain (FQDN) verwendet. Außerhalb von ONTAP sollte bestätigt werden, dass die DNS-Einträge auf die verwendeten SVM-Daten-LIFs verweisen.

- Es muss Intracluster LIFs auf dem lokalen Cluster vorhanden sein.

  Bei der Konfiguration für lokales Cluster-Tiering wird eine lokale Tier (in der ONTAP CLI auch als Storage Aggregate bezeichnet) an einen lokalen Bucket angehängt. FabricPool verwendet Cluster-LIFs für den Intracluster-Datenverkehr.

  Bei Überlastung der Cluster-LIF-Ressourcen kann es zu Leistungseinbußen kommen. Um dies zu vermeiden, empfiehlt NetApp, beim Tiering auf einen lokalen Bucket Cluster mit mindestens vier Knoten sowie ein HA-Paar für das lokale Tier und ein weiteres HA-Paar für den lokalen Bucket zu verwenden. Das Tiering auf lokale Buckets auf einem einzelnen HA-Paar wird nicht empfohlen.

- Um Remote-FabricPool-Kapazitäts-Tiering (Cloud-Tiering) mit ONTAP S3 zu ermöglichen, ist "Intercluster

LIFs konfigurieren" auf dem FabricPool-Client und "Daten-LIFs konfigurieren" auf dem Objektspeicher-Server erforderlich.

Über diese Aufgabe

Lastverteilung ist für ONTAP S3 Server ab ONTAP 9.8 aktiviert. Wenn der Hostname des Servers zu mehr als einer IP-Adresse aufgelöst wird, stellt ONTAP Client-Verbindungen mit allen zurückgegebenen IP-Adressen her (bis zu maximal 16 IP-Adressen). Die IP-Adressen werden beim Verbindungsaufbau nach dem Round-Robin-Verfahren ausgewählt.

Die ONTAP S3 Cloud-Tier für FabricPool einrichten

Schritte

ONTAP S3 kann als Cloud-Tier für FabricPool mit ONTAP System Manager oder der ONTAP CLI eingerichtet werden.

System Manager

1. Klicken Sie auf **Speicher > Ebenen > Cloud-Ebene hinzufügen** und wählen Sie ONTAP S3 als Objektspeicher-Anbieter.
2. Die angeforderten Informationen sind auszufüllen.
3. Zum Erstellen eines Cloud-Mirrors auf **Als FabricPool Mirror hinzufügen** klicken.

Ein FabricPool Mirror bietet eine Methode, einen Datenspeicher nahtlos zu ersetzen, und trägt dazu bei, dass Ihre Daten im Katastrophenfall verfügbar sind.

CLI

1. Fügen Sie Einträge für den S3-Server und die LIFs zu Ihrem DNS-Server hinzu.

Option	Beschreibung
Wenn Sie einen externen DNS-Server verwenden	Dem DNS-Serveradministrator werden der Name und die IP-Adressen des S3-Servers bereitgestellt.
Wenn Sie die DNS-Hosttabelle Ihres lokalen Systems verwenden	Führen Sie den folgenden Befehl aus: `dns host create -vserver <svm_name> -address ip_address -hostname <s3_server_name>`

2. Die ONTAP S3 Konfigurationsinformationen werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type ONTAP_S3` Parameter angegeben.
   - Der `storage aggregate object-store config create`Befehl schlägt fehl, wenn das lokale ONTAP System mit den angegebenen Informationen nicht auf den ONTAP S3 Server zugreifen kann.
   - Der `-access-key`Parameter wird verwendet, um den Zugriffsschlüssel für die Autorisierung von Anfragen an den ONTAP S3 Server anzugeben.
   - Der `-secret-password` Parameter dient zur Angabe des Passworts (geheimer Zugriffsschlüssel) für die Authentifizierung von Anfragen an den ONTAP S3 Server.

- Wenn das Passwort des ONTAP S3 Servers geändert wird, sollte das entsprechende Passwort, das im lokalen ONTAP System gespeichert ist, umgehend aktualisiert werden.

  Dadurch ist der Zugriff auf die Daten im ONTAP S3 Objektspeicher ohne Unterbrechung möglich.

- Das Setzen des `-is-certificate-validation-enabled`Parameters auf `false`deaktiviert die Zertifikatsprüfung für ONTAP S3. Die Verwendung signierter Zertifikate (-is-certificate-validation-enabled true`von einer Drittanbieter-Zertifizierungsstelle gilt als empfohlene Best Practice.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Die ONTAP_S3 Konfigurationsinformationen lassen sich mit dem `storage aggregate object-store config show` Befehl anzeigen und überprüfen.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der `ONTAP_S3`Konfigurationsinformationen für FabricPool.

Den ONTAP S3 FQDN für FabricPool Tiering ändern

Wenn Änderungen an Ihrem Netzwerk erforderlich sind, die FQDN-Aktualisierungen beinhalten, sollte der für das FabricPool-Tiering verwendete ONTAP S3 FQDN geändert werden, um Netzwerkunterbrechungen zu vermeiden.

Schritte

1. Zertifikatsprüfung für die FabricPool Stufe deaktivieren:

   ```
   storage aggregate object-store config modify -object-store-name <object store>
   -is-certificate-validation-enabled false
   ```

2. Den FQDN für den ONTAP S3 Server ändern:

   ```
   vserver object-store-server modify -vserver <vserver> -object-store-server
   <new fqdn>
   ```

3. (Optional) Falls eine Zertifikatsvalidierung erforderlich ist und der Hostname geändert wurde, "das Zertifikat erneuern".
4. Die FabricPool Tier mit dem neuen FQDN aktualisieren:

   ```
   storage aggregate object-store config modify -object-store-name
   <object_store_name> -server <new fqdn>
   ```

5. Es wird geprüft, ob alle Objektspeicher und gegebenenfalls deren Spiegel in der FabricPool-Ebene verfügbar sind:

   ```
   storage aggregate object-store show -fields object-store-availability,mirror-
   type,is-mirror-degraded
   ```

Weitere Informationen finden Sie unter "storage aggregate object-store show".

6. Diese Schritte sind für alle weiteren Objektspeicher zu wiederholen.
7. Wenn die Zertifikate auf dem ONTAP S3-Server und die Zertifikate auf der FabricPool Ebene erneuert wurden, sollte die Zertifikatsprüfung erneut aktiviert werden:

```
storage aggregate object-store config modify -object-store-name <object store>
-is-certificate-validation-enabled true
```

Verwandte Informationen

- "LIF für SMB erstellen"
- "LIF für NFS erstellen"
- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

Alibaba Cloud Object Storage als ONTAP FabricPool Cloud-Tier einrichten

Wenn Sie ONTAP 9.6 oder höher verwenden, kann Alibaba Cloud Object Storage als Cloud-Tier für FabricPool eingerichtet werden.

Überlegungen zur Verwendung von Alibaba Cloud Object Storage mit FabricPool

- A "FabricPool Lizenz" ist erforderlich, wenn von lokalen ONTAP Clustern zu Alibaba Cloud Object Storage migriert wird.
- Auf AFF und FAS Systemen sowie ONTAP Select unterstützt FabricPool die folgenden Alibaba Object Storage Service Klassen:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service Infrequent Access

    "Alibaba Cloud: Einführung in die Speicherklassen"

Ihr NetApp Vertriebsmitarbeiter kann Informationen zu nicht aufgeführten Speicherklassen bereitstellen.

Schritte

1. Die Konfigurationsinformationen für Alibaba Cloud Object Storage werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type AliCloud` Parameter angegeben.
   - Der `storage aggregate object-store config create` Befehl schlägt fehl, wenn ONTAP mit den angegebenen Informationen nicht auf Alibaba Cloud Object Storage zugreifen kann.
   - Der `-access-key`Parameter wird verwendet, um den Zugriffsschlüssel für die Autorisierung von Anfragen an den Alibaba Cloud Object Storage Objektspeicher anzugeben.
   - Wenn das Passwort für Alibaba Cloud Object Storage geändert wird, ist das entsprechende in ONTAP gespeicherte Passwort umgehend zu aktualisieren.

     Dadurch kann ONTAP ohne Unterbrechung auf die Daten im Alibaba Cloud Object Storage zugreifen.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
```

```
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Die Konfigurationsinformationen von Alibaba Cloud Object Storage lassen sich mit dem `storage aggregate object-store config show` Befehl anzeigen und überprüfen.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der Alibaba Cloud Object Storage-Konfigurationsinformationen für FabricPool.

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

Amazon S3 als ONTAP FabricPool Cloud-Tier einrichten

Amazon S3 kann als Cloud-Tier für FabricPool eingerichtet werden. Bei Verwendung von ONTAP 9.5 oder höher kann Amazon Commercial Cloud Services (C2S) für FabricPool eingerichtet werden.

Überlegungen zur Verwendung von Amazon S3 mit FabricPool

- A "FabricPool Lizenz" ist erforderlich, wenn von lokalen Clustern zu Amazon S3 migriert wird.
- Es wird empfohlen, dass der LIF, den ONTAP zur Verbindung mit dem Amazon S3 Objektserver verwendet, an einem 10 Gbit/s Port angeschlossen ist.
- Auf AFF und FAS Systemen sowie ONTAP Select unterstützt FabricPool die folgenden Amazon S3-Speicherklassen:
  - Amazon S3 Standard
  - Amazon S3 Standard - Seltener Zugriff (Standard - IA)
  - Amazon S3 One Zone - Seltener Zugriff (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services
  - Ab ONTAP 9.11.1 wird Amazon S3 Glacier Instant Retrieval unterstützt (FabricPool unterstützt Glacier Flexible Retrieval oder Glacier Deep Archive nicht)

    "Amazon Web Services Dokumentation: Amazon S3 Storage Classes"

  Für Informationen zu nicht aufgeführten Speicherklassen steht Ihr Vertriebsmitarbeiter zur Verfügung.
- Auf Cloud Volumes ONTAP unterstützt FabricPool das Tiering von General Purpose SSD (gp2) und Throughput Optimized HDD (st1) Volumes von Amazon Elastic Block Store (EBS).

Schritte

1. Die Amazon S3-Konfigurationsinformationen werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type AWS_S3` Parameter angegeben.
   - Sie verwenden den `-auth-type` `CAP`Parameter, um Anmeldeinformationen für den C2S-Zugriff zu erhalten.

Wenn Sie den `-auth-type CAP` Parameter verwenden, müssen Sie den `-cap-url` Parameter verwenden, um die vollständige URL anzugeben, mit der temporäre Anmeldeinformationen für den C2S-Zugriff angefordert werden.

- Der `storage aggregate object-store config create` Befehl schlägt fehl, wenn ONTAP mit den angegebenen Informationen nicht auf Amazon S3 zugreifen kann.
- Der `-access-key` Parameter wird verwendet, um den Zugriffsschlüssel für die Autorisierung von Anfragen an den Amazon S3 Objektspeicher anzugeben.
- Der `-secret-password`-Parameter wird verwendet, um das Passwort (den geheimen Zugriffsschlüssel) für die Authentifizierung von Anfragen an den Amazon S3 Objektspeicher anzugeben.
- Wenn das Amazon S3-Passwort geändert wird, ist das entsprechende Passwort, das in ONTAP gespeichert ist, umgehend zu aktualisieren.

  Dadurch kann ONTAP ohne Unterbrechung auf die Daten in Amazon S3 zugreifen.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. Die Amazon S3-Konfigurationsinformationen lassen sich mit dem `storage aggregate object-store config show` Befehl anzeigen und überprüfen.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der Amazon S3-Konfigurationsinformationen für FabricPool.

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

Google Cloud Storage als ONTAP FabricPool Cloud-Tier einrichten

Wenn Sie ONTAP 9.6 oder höher verwenden, kann Google Cloud Storage als Cloud-Ebene für FabricPool eingerichtet werden.

Weitere Überlegungen zur Verwendung von Google Cloud Storage mit FabricPool

- Ein "FabricPool Lizenz" ist erforderlich, wenn von lokalen Clustern zu Google Cloud Storage getiert wird.
- Es wird empfohlen, dass der LIF, den ONTAP zur Verbindung mit dem Google Cloud Storage Objektspeicher verwendet, an einem 10 Gbit/s Port angeschlossen ist.
- Auf AFF und FAS Systemen sowie ONTAP Select unterstützt FabricPool die folgenden Google Cloud Objektspeicherklassen:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline
  - Google Cloud Coldline

  "Google Cloud: Speicherklassen"

Schritte

1. Die Konfigurationsinformationen für Google Cloud Storage werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type GoogleCloud` Parameter angegeben.

   - Der `storage aggregate object-store config create` Befehl schlägt fehl, wenn ONTAP mit den angegebenen Informationen nicht auf Google Cloud Storage zugreifen kann.
   - Der `-access-key`Parameter wird verwendet, um den Zugriffsschlüssel für die Autorisierung von Anfragen an den Google Cloud Storage Objektspeicher anzugeben.
   - Wenn das Passwort für Google Cloud Storage geändert wird, ist das entsprechende in ONTAP gespeicherte Passwort umgehend zu aktualisieren.

     Dadurch kann ONTAP ohne Unterbrechung auf die Daten in Google Cloud Storage zugreifen.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud  -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Die Konfigurationsinformationen von Google Cloud Storage lassen sich mit dem `storage aggregate object-store config show` Befehl anzeigen und überprüfen.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der Google Cloud Storage-Konfigurationsinformationen für FabricPool.

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

IBM Cloud Object Storage als ONTAP FabricPool Cloud-Tier einrichten

Wenn Sie ONTAP 9.5 oder höher verwenden, kann IBM Cloud Object Storage als Cloud-Ebene für FabricPool eingerichtet werden.

Überlegungen zur Verwendung von IBM Cloud Object Storage mit FabricPool

- A "FabricPool Lizenz" ist erforderlich, wenn von lokalen Clustern zu IBM Cloud Object Storage migriert wird.
- Es wird empfohlen, dass der LIF, den ONTAP zur Verbindung mit dem IBM Cloud Objektspeicher verwendet, an einem 10 Gbit/s Port angeschlossen ist.

Schritte

1. Die Konfigurationsinformationen für IBM Cloud Object Storage werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type IBM_COS` Parameter angegeben.

   - Der `storage aggregate object-store config create` Befehl schlägt fehl, wenn ONTAP mit den angegebenen Informationen nicht auf IBM Cloud Object Storage zugreifen kann.
   - Der `-access-key`Parameter wird verwendet, um den Zugriffsschlüssel für die Autorisierung von Anfragen an den IBM Cloud Object Storage Objektspeicher anzugeben.
   - Der `-secret-password`Parameter wird verwendet, um das Passwort (geheimer Zugriffsschlüssel) für die Authentifizierung von Anfragen an den IBM Cloud Object Storage Objektspeicher anzugeben.
   - Wenn das Passwort für IBM Cloud Object Storage geändert wird, ist das entsprechende in ONTAP gespeicherte Passwort umgehend zu aktualisieren.

     Dadurch kann ONTAP ohne Unterbrechung auf die Daten im IBM Cloud Object Storage zugreifen.

   ```
   storage aggregate object-store config create
   -object-store-name MyIBM -provider-type IBM_COS
   -server s3.us-east.objectstorage.softlayer.net
   -container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
   ```

2. Die Konfigurationsinformationen von IBM Cloud Object Storage werden mit dem `storage aggregate object-store config show` Befehl angezeigt und überprüft.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der IBM Cloud Object Storage-Konfigurationsinformationen für FabricPool.

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

Azure Blob Storage als ONTAP FabricPool Cloud-Tier einrichten

Wenn Sie ONTAP 9.4 oder höher verwenden, kann Azure Blob Storage als Cloud-Ebene für FabricPool eingerichtet werden.

Überlegungen zur Verwendung von Microsoft Azure Blob Storage mit FabricPool

- A "FabricPool Lizenz" ist erforderlich, wenn das Tiering von lokalen ONTAP Clustern auf Azure Blob Storage erfolgt.
- Für die Nutzung von Azure Blob Storage über Cloud Volumes ONTAP oder Azure NetApp Files ist keine Lizenz erforderlich.

- Es wird empfohlen, dass der LIF, den ONTAP zur Verbindung mit dem Azure Blob Storage Objektspeicher verwendet, an einem 10 Gbit/s Port angeschlossen ist.
- FabricPool unterstützt derzeit Azure Stack nicht, bei dem es sich um lokale Azure-Dienste handelt.
- Auf Kontoebene in Microsoft Azure Blob Storage unterstützt FabricPool nur die Speicherebenen Hot und Cool.

  FabricPool unterstützt kein Tiering auf Blob-Ebene. Ebenso wird Tiering auf die Archivspeicher-Ebene von Azure nicht unterstützt.

Über diese Aufgabe

FabricPool unterstützt derzeit Azure Stack nicht, bei dem es sich um lokale Azure-Dienste handelt.

Schritte

1. Die Konfigurationsinformationen für Azure Blob Storage werden mit dem `storage aggregate object-store config create` Befehl und dem `-provider-type Azure_Cloud` Parameter angegeben.

   - Der `storage aggregate object-store config create` Befehl schlägt fehl, wenn ONTAP mit den angegebenen Informationen nicht auf Azure Blob Storage zugreifen kann.
   - Sie verwenden den `-azure-account` Parameter, um das Azure Blob Storage Konto anzugeben.
   - Der `-azure-private-key`Parameter wird verwendet, um den Zugriffsschlüssel für die Authentifizierung von Anfragen an Azure Blob Storage anzugeben.
   - Wenn das Kennwort für Azure Blob Storage geändert wird, ist das entsprechende in ONTAP gespeicherte Kennwort umgehend zu aktualisieren.

     Dadurch kann ONTAP ohne Unterbrechung auf die Daten in Azure Blob Storage zugreifen.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyAzure -provider-type Azure_Cloud
   -server blob.core.windows.net -container-name myAzureContainer
   -azure-account myAzureAcct -azure-private-key myAzureKey
   ```

2. Die Konfigurationsinformationen von Azure Blob Storage lassen sich mit dem `storage aggregate object-store config show` Befehl anzeigen und überprüfen.

   Der `storage aggregate object-store config modify`Befehl ermöglicht die Änderung der Azure Blob Storage-Konfigurationsinformationen für FabricPool.

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher config modify"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"

Objektspeicher für ONTAP FabricPool in einer MetroCluster Konfiguration einrichten

Wenn Sie ONTAP 9.7 oder höher verwenden, kann ein gespiegeltes FabricPool auf einer MetroCluster Konfiguration eingerichtet werden, um kalte Daten in Objektspeicher in zwei verschiedenen Fehlerzonen zu verschieben.

Über diese Aufgabe

- FabricPool in MetroCluster erfordert, dass das zugrunde liegende gespiegelte Aggregat und die zugehörige Objektspeicher-Konfiguration von derselben MetroCluster Konfiguration verwaltet werden.
- Es ist nicht möglich, ein Aggregat an einen Objektspeicher anzubinden, der am Remote-MetroCluster-Standort erstellt wurde.
- Objektspeicher-Konfigurationen sind auf der MetroCluster Konfiguration zu erstellen, die das Aggregat besitzt.

Bevor Sie beginnen

- Die MetroCluster Konfiguration ist eingerichtet und ordnungsgemäß konfiguriert.
- Zwei Objektspeicher sind an den entsprechenden MetroCluster Standorten eingerichtet.
- Auf jedem der Objektspeicher werden Container konfiguriert.
- In den beiden MetroCluster Konfigurationen werden IP-Adressräume erstellt oder identifiziert, und ihre Namen stimmen überein.

Schritt

1. Die Objektspeicher Konfigurationsinformationen werden an jedem MetroCluster Standort mithilfe des `storage object-store config create` Befehls angegeben.

   In diesem Beispiel ist FabricPool nur auf einem Cluster in der MetroCluster Konfiguration erforderlich. Für diesen Cluster werden zwei Objektspeicherkonfigurationen erstellt, eine für jeden Objektspeicher-Bucket.

   ```
   storage aggregate
       object-store config create -object-store-name mcc1-ostore-config-s1
   -provider-type SGWS -server
       <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
   -secret-password <password> -encrypt
       <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
   ipspace
       <IPSpace>
   ```

   ```
   storage aggregate object-store config create -object-store-name mcc1-
   ostore-config-s2
       -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
   bucket-2> -access-key <key> -secret-password <password> -encrypt
   <true|false> -provider <provider-type>
       -is-ssl-enabled <true|false> ipspace <IPSpace>
   ```

   In diesem Beispiel wird FabricPool auf dem zweiten Cluster in der MetroCluster Konfiguration eingerichtet.

   ```
   storage aggregate
       object-store config create -object-store-name mcc2-ostore-config-s1
   -provider-type SGWS -server
       <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
   ```

```
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

Verwandte Informationen

- "storage object-store config create"

Die Latenz- und Durchsatzleistung der ONTAP Cloud-Tier wird getestet.

Bevor ein Objektspeicher an eine lokale Ebene angebunden wird, lässt sich die Latenz und die Durchsatzleistung des Objektspeichers mithilfe des Object Store Profilers testen.

> Die Ergebnisse des Objektspeicherprofilers sind eine Messung der Konnektivität zwischen ONTAP und dem Cloud-Tier Objektspeicher mithilfe von 4MB PUTs und zufälligen lesen/schreiben Bytebereichs-GETs im Bereich von 4MB bis 256KB. (Nur interne ONTAP Features, wie SnapMirror, können GETs größer als 32KB nutzen.)
>
> Da konkurrierende Arbeitslasten oder das individuelle Verhalten von Clientanwendungen nicht berücksichtigt werden, sind die Ergebnisse des Objektspeicherprofilers kein perfekter Indikator für die Tiering-Performance.

Bevor Sie beginnen

- Die Cloud-Ebene muss zu ONTAP hinzugefügt werden, bevor sie mit dem Objektspeicher-Profiling verwendet werden kann.
- Sie müssen sich im erweiterten Berechtigungsmodus der ONTAP CLI befinden.

Schritte

1. Objektspeicher-Profiling starten:

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. Ergebnisse anzeigen:

   ```
   storage aggregate object-store profiler show
   ```

Verwandte Informationen

- "storage aggregate Objektspeicher Profiler anzeigen"
- "storage aggregate Objektspeicher Profiler starten"

Die ONTAP Cloud-Tier mit einer lokalen Tier verknüpfen

Nachdem ein Objektspeicher als Cloud-Ebene eingerichtet wurde, wird die zu verwendende lokale Ebene angegeben, indem sie an FabricPool angehängt wird. In ONTAP 9.5 und höher können auch lokale Ebenen angehängt werden, die qualifizierte FlexGroup Volume-Bestandteile enthalten.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Über diese Aufgabe

Das Verbinden einer Cloud-Ebene mit einer lokalen Ebene ist ein dauerhafter Vorgang. Eine Cloud-Ebene kann nach dem Verbinden nicht mehr von einer lokalen Ebene getrennt werden. Es besteht jedoch die Möglichkeit, "FabricPool Spiegel" eine lokale Ebene mit einer anderen Cloud-Ebene zu verbinden.

Bevor Sie beginnen

Wenn die ONTAP CLI verwendet wird, um eine lokale Ebene für FabricPool einzurichten, muss die lokale Ebene bereits existieren.

> Wenn der System Manager zur Einrichtung einer lokalen Ebene für FabricPool verwendet wird, kann die lokale Ebene erstellt und gleichzeitig für FabricPool eingerichtet werden.

Schritte

Eine lokale Ebene kann mit ONTAP System Manager oder der ONTAP CLI an einen FabricPool Objektspeicher angebunden werden.

System Manager

1. Navigieren Sie zu **Speicher > Ebenen**, wählen Sie eine Cloud-Ebene aus und klicken Sie dann auf ⋮.
2. **Lokale Ebenen anhängen** auswählen.
3. Unter **Als primär hinzufügen** wird überprüft, ob die Volumes zum Anhängen geeignet sind.
4. Gegebenenfalls **Volumes in Thin Provisioning konvertieren** auswählen.
5. Auf **Speichern** klicken.

CLI

Einen Objektspeicher mit der CLI an ein Aggregat anbinden:

1. **Optional**: Um anzuzeigen, wie viele Daten in einem Volume inaktiv sind, die Schritte in "Ermittlung des Anteils inaktiver Daten in einem Volume mithilfe der Berichterstattung über inaktive Daten" befolgen.

   Zu sehen, wie viele Daten in einem Volume inaktiv sind, kann bei der Entscheidung helfen, welches Aggregat für FabricPool verwendet wird.

2. Den Objektspeicher mit dem `storage aggregate object-store attach` Befehl an ein

Aggregat anbinden.

Wenn das Aggregat noch nie mit FabricPool verwendet wurde und bereits vorhandene Volumes enthält, wird den Volumes die Standard `snapshot-only` Tiering-Richtlinie zugewiesen.

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

Sie können die `allow-flexgroup true` Option verwenden, um Aggregate anzuhängen, die FlexGroup-Volume-Bestandteile enthalten.

3. Die Objektspeicherinformationen werden angezeigt und mit dem `storage aggregate object-store show` Befehl lässt sich überprüfen, ob der angeschlossene Objektspeicher verfügbar ist.

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
myaggr       Amazon01B1           available
```

Verwandte Informationen

- "storage aggregate Objektspeicher anhängen"
- "storage aggregate object-store show"

Tier-Daten in einen lokalen ONTAP S3 Bucket

Ab ONTAP 9.8 ist das Tiering von Daten in lokalen Objektspeicher mithilfe von ONTAP S3 möglich.

Das Tiering von Daten in einen lokalen Bucket bietet eine einfache Alternative zum Verschieben von Daten in eine andere lokale Ebene. Dieses Verfahren verwendet entweder einen vorhandenen Bucket im lokalen Cluster, oder ONTAP kann automatisch eine neue Storage-VM und einen neuen Bucket erstellen.

Beachten Sie, dass der primäre lokale Bucket nach dem Anhängen nicht mehr getrennt werden kann.

Bevor Sie beginnen

- Für diesen Workflow, der einen neuen S3-Server und einen neuen Bucket erstellt oder bestehende verwendet, ist eine S3-Lizenz erforderlich. Diese Lizenz ist in "ONTAP One" enthalten. Für diesen Workflow ist keine FabricPool Lizenz erforderlich.
- "ONTAP S3-Zugriff für lokales FabricPool Tiering aktivieren".

Schritte

1. Daten auf einen lokalen Bucket verschieben: Auf **Storage > Tiers** klicken, im Bereich **SSD** ein lokales Tier auswählen, auf ⋮ klicken und **Tier zu lokalem Bucket** auswählen.
2. Im Abschnitt **Primäre Ebene** entweder **Vorhanden** oder **Neu** auswählen.
3. Auf **Speichern** klicken.

Verwaltung von FabricPool

Inaktive ONTAP Daten mit der Berichterstattung über inaktive Daten analysieren

Die Meldung inaktiver Daten (IDR) ist ein hervorragendes Werkzeug, um die Menge inaktiver (kalter) Daten zu ermitteln, die aus einer lokalen Ebene ausgelagert werden können.

Standardmäßig verwendet IDR eine 31-tägige Abkühlphase, um zu bestimmen, welche Daten als inaktiv gelten. Die Menge der kalten Daten, die ausgelagert werden, hängt von den auf den Volumes festgelegten Tiering-Richtlinien ab. In Versionen vor ONTAP 9.8 verwendete IDR eine feste 31-tägige Abkühlphase.

Bevor Sie beginnen

ONTAP 9.4

- IDR ist standardmäßig auf allen FabricPool Aggregaten aktiviert.
- IDR kann auf Nicht-FabricPool SSD-Aggregaten aktiviert werden.

ONTAP 9.6

- IDR ist standardmäßig auf allen Nicht-FabricPool SSD-Aggregaten aktiviert.
- IDR kann auf Nicht-FabricPool HDD-Aggregaten aktiviert werden.

ONTAP 9.8

- Die IDR-Kühlperiode kann über die Einstellung volume-tiering-minimum-cooling-days angepasst werden.

Über diese Aufgabe

- IDR meldet inaktive Daten, die ausgelagert werden können, nicht jedoch inaktive Daten, die bereits ausgelagert wurden. Wenn FabricPool aktiviert ist und inaktive Daten ausgelagert wurden, werden sie nicht mehr von IDR gemeldet.

> Obwohl IDR auf allen SSD-Aggregaten (ONTAP 9.6 und höher) standardmäßig aktiviert ist, wird IDR automatisch deaktiviert und die Kühltage auf null zurückgesetzt, sobald eine Client-Workload 90 % der Systemressourcen benötigt. In diesem Fall wird IDR nicht automatisch wieder aktiviert.
>
> Um zu vermeiden, dass der automatische Prozess IDR abschaltet, um Ressourcen für andere Workloads freizugeben, aktivieren Sie -is-inactive-data-reporting-enabled manuell auf true.

- Inaktive Datenberichterstattung, wenn FabricPool nicht aktiviert werden kann, einschließlich der folgenden Fälle:
  - Wurzelaggregate
  - Aggregate, die Volumes mit einer anderen Speicherplatzzusage als „keine“ enthalten. (Thick-Provisioned Volumes werden nicht unterstützt.)
  - MetroCluster Aggregate mit ONTAP Versionen vor 9.7
  - Flash Pool (Hybridaggregate oder SnapLock Aggregate)

Verfahren

Mit ONTAP System Manager oder der ONTAP CLI lässt sich ermitteln, wie viele Daten inaktiv sind.

System Manager

1. Wählen Sie eine der folgenden Optionen:
   - Wenn bereits HDD-Aggregate vorhanden sind, zu **Speicher > Ebenen** navigieren und ⋮ für das Aggregat auswählen, für das die Berichterstattung über inaktive Daten aktiviert werden soll.
   - Wenn keine Cloud-Ebenen konfiguriert sind, auf **Dashboard** wechseln und unter **Kapazität** auf den Link **Aktivieren der Berichterstattung über inaktive Daten** klicken.

CLI

Aktivierung der Meldung inaktiver Daten über die CLI:

1. Wenn das Aggregat, für das Sie die Berichterstattung über inaktive Daten anzeigen möchten, nicht in FabricPool verwendet wird, kann die Berichterstattung über inaktive Daten für das Aggregat mit dem `storage aggregate modify` Befehl und dem `-is-inactive-data-reporting-enabled true` Parameter aktiviert werden.

   ```
   cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
   -data-reporting-enabled true
   ```

   Die Funktion zur Meldung inaktiver Daten muss explizit für ein Aggregat aktiviert werden, das nicht für FabricPool verwendet wird.

   Sie können die Meldung inaktiver Daten für ein FabricPool-fähiges Aggregat nicht aktivieren und müssen dies auch nicht, da das Aggregat bereits die Meldung inaktiver Daten enthält. Der `-is -inactive-data-reporting-enabled` Parameter funktioniert bei FabricPool-fähigen Aggregaten nicht.

   Der `-fields is-inactive-data-reporting-enabled`Parameter des `storage aggregate show`Befehls zeigt, ob die Meldung inaktiver Daten für ein Aggregat aktiviert ist.

2. Um anzuzeigen, wie viele Daten auf einem Volume inaktiv sind, kann der `volume show` Befehl mit dem `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` Parameter verwendet werden.

   ```
   cluster1::> volume show -fields performance-tier-inactive-user-
   data,performance-tier-inactive-user-data-percent

   vserver volume performance-tier-inactive-user-data performance-tier-
   inactive-user-data-percent
   ------- ------ ----------------------------------
   ----------------------------------------
   vsim1   vol0   0B                                 0%
   vs1     vs1rv1 0B                                 0%
   vs1     vv1    10.34MB                            0%
   vs1     vv2    10.38MB                            0%
   ```

```
4 entries were displayed.
```

- Das `performance-tier-inactive-user-data` Feld zeigt an, wie viele der im Aggregat gespeicherten Benutzerdaten inaktiv sind.
- Das `performance-tier-inactive-user-data-percent` Feld zeigt an, welcher Prozentsatz der Daten im gesamten aktiven Dateisystem und in den Snapshots inaktiv ist.
- Für ein Aggregat, das nicht für FabricPool verwendet wird, nutzt die Meldung inaktiver Daten die Tiering-Richtlinie, um zu entscheiden, wie viele Daten als kalt gemeldet werden.
  - Für die `none`Tiering-Policy werden 31 Tage verwendet.
  - Für die `snapshot-only` und `auto` verwendet die Meldung inaktiver Daten `tiering-minimum-cooling-days`.
  - Für die `ALL`Richtlinie wird bei der Meldung inaktiver Daten angenommen, dass die Daten innerhalb eines Tages in eine andere Ebene verschoben werden.

    Bis zum Erreichen der Periode zeigt die Ausgabe "-" für die Menge der inaktiven Daten anstelle eines Wertes.
- Bei einem Volume, das Teil von FabricPool ist, hängt das, was ONTAP als inaktiv meldet, von der auf dem Volume festgelegten Tiering-Richtlinie ab.
  - Für die `none`Tiering-Policy meldet ONTAP die Menge des gesamten Volumens, die seit mindestens 31 Tagen inaktiv ist. Der `-tiering-minimum-cooling-days`Parameter kann nicht mit der `none`Tiering-Policy verwendet werden.
  - Für die `ALL`, `snapshot-only` und `auto` Tiering-Richtlinien wird die Meldung inaktiver Daten nicht unterstützt.

Verwandte Informationen

- "storage aggregate ändern"

Volumen für FabricPool verwalten

Ein Volume auf einer FabricPool ONTAP lokalen Ebene erstellen

Volumes können zu FabricPool hinzugefügt werden, indem neue Volumes direkt in der FabricPool-aktivierten lokalen Ebene erstellt oder vorhandene Volumes von einer anderen lokalen Ebene in die FabricPool-aktivierte lokale Ebene verschoben werden.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Wenn ein Volume für FabricPool erstellt wird, besteht die Möglichkeit, eine Tiering-Richtlinie anzugeben. Wird keine Tiering-Richtlinie angegeben, verwendet das erstellte Volume die Standard `snapshot-only` Tiering-Richtlinie. Für ein Volume mit der `snapshot-only` oder `auto` Tiering-Richtlinie kann auch die minimale Abkühlperiode für das Tiering angegeben werden.

Bevor Sie beginnen

- Das Festlegen eines Volumes zur Verwendung der `auto` Tiering-Policy oder das Angeben der minimalen Kühlperiode für das Tiering erfordert ONTAP 9.4 oder höher.
- Die Verwendung von FlexGroup Volumes erfordert ONTAP 9.5 oder höher.
- Das Festlegen eines Volumes zur Verwendung der `all` Tiering-Policy erfordert ONTAP 9.6 oder höher.
- Das Festlegen eines Volumes zur Verwendung des `-cloud-retrieval-policy` Parameters erfordert ONTAP 9.8 oder höher.

Schritte

1. Ein neues Volume für FabricPool kann mit dem `volume create` Befehl erstellt werden.
   - Der `-tiering-policy`optionale Parameter ermöglicht die Angabe der Tiering-Richtlinie für das Volume.

     Eine der folgenden Tiering-Richtlinien kann angegeben werden:

     - `snapshot-only` (Standard)
     - `auto`
     - `all`
     - `backup` (veraltet)
     - `none`

       "FabricPool Volume-Tiering-Richtlinien"
   - Der `-cloud-retrieval-policy`optionale Parameter ermöglicht Cluster-Administratoren mit erweitertem Berechtigungsniveau, das durch die Tiering-Richtlinie gesteuerte Standardverhalten bei der Cloud-Migration oder beim Abrufen zu überschreiben.

     Sie können eine der folgenden Cloud-Abrufrichtlinien festlegen:

     - `default`

       Die Tiering-Richtlinie legt fest, welche Daten zurückgeholt werden, daher gibt es keine Änderung beim Abruf von Cloud-Daten mit `default` cloud-retrieval-policy. Das Verhalten ist somit identisch mit dem in Versionen vor ONTAP 9.8:

       - Wenn die Tiering-Richtlinie `none` oder `snapshot-only` ist, bedeutet „`default`“, dass alle von Clients gelesenen Daten vom Cloud-Tier in den Performance-Tier übertragen werden.
       - Wenn die Tiering-Richtlinie `auto` ist, werden alle clientseitig gesteuerten zufälligen Lesevorgänge abgerufen, jedoch keine sequenziellen Lesevorgänge.
       - Wenn die Tiering-Richtlinie `all`ist, werden keine clientseitig gesteuerten Daten aus dem Cloud-Tier abgerufen.
     - `on-read`

       Alle clientseitigen Datenlesevorgänge werden von der Cloud-Tier in die Performance-Tier übertragen.
     - `never`

       Es werden keine clientgesteuerten Daten von der Cloud-Ebene in die Performance-Ebene übertragen.

- `promote`
  - Bei der Tiering-Richtlinie `none`werden alle Cloud-Daten vom Cloud-Tier in den Performance-Tier verschoben.
  - Für die Tiering-Richtlinie `snapshot-only` werden alle aktiven Dateisystemdaten vom Cloud-Tier auf den Performance-Tier verschoben.

◦ Der `-tiering-minimum-cooling-days` optionale Parameter auf der erweiterten Berechtigungsstufe ermöglicht die Angabe der minimalen Abkühlperiode für ein Volume, das die `snapshot-only` oder `auto` Tiering-Richtlinie verwendet.

Ab ONTAP 9.8 kann ein Wert zwischen 2 und 183 für die Mindestanzahl an Kühltagen pro Stufe angegeben werden. Wenn eine Version von ONTAP vor 9.8 verwendet wird, kann ein Wert zwischen 2 und 63 für die Mindestanzahl an Kühltagen für das Tiering angegeben werden.

Beispiel für die Erstellung eines Volumens für FabricPool

Das folgende Beispiel erstellt ein Volume mit dem Namen “myvol1” im “myFabricPool” FabricPool-fähigen lokalen Tier. Die Tiering-Richtlinie ist auf `auto` gesetzt und die minimale Tiering-Abkühlperiode beträgt 45 Tage:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

Verwandte Informationen

"FlexGroup Volumenmanagement"

Ein Volume auf eine FabricPool aktivierte ONTAP lokale Ebene verschieben

Ein "Volume verschieben" verschiebt ein Volume unterbrechungsfrei von einer lokalen ONTAP Ebene (Quelle) auf eine andere (Ziel), meist für das Hardware-Lifecycle-Management, die Cluster-Erweiterung oder den Lastausgleich. Wird ein Volume auf eine für FabricPool aktivierte lokale Ebene verschoben, hilft das Verständnis der Auswirkungen der Verschiebung auf ausgelagerte Daten und Tiering-Richtlinien, unnötigen Netzwerkverkehr und Objektspeicherkosten zu vermeiden.

Änderungen, die eine Volume-Verschiebung am lokalen Tier, am angehängten Cloud-Tier und an den Volume-Tiering-Richtlinien vornimmt, können erhebliche Auswirkungen auf die Funktionalität von FabricPool haben.

> Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Ziel-Lokale Tier

Wenn die lokale Ziel-Tier einer Volume Verschiebung keine angebundene Cloud Tier hat, werden Daten auf dem Quell-Volume, die auf der Cloud Tier gespeichert sind, in die lokale Ziel-Tier geschrieben.

Ab ONTAP 9.8 stellt FabricPool, wenn für ein Volume "Meldung inaktiver Daten" aktiviert ist, anhand der Heatmap des Volumes kalte Daten für das Tiering in die Warteschlange, sobald die Daten auf die lokale

Zielebene geschrieben werden.

In ONTAP 9.7 und früheren Versionen setzt das Verschieben eines Volumes auf ein anderes lokales Tier die Inaktivitätsdauer von Blöcken auf dem lokalen Tier zurück. Wenn beispielsweise ein Volume die Auto Volume-Tiering-Richtlinie verwendet und Daten auf dem lokalen Tier enthält, die seit 20 Tagen inaktiv sind, aber noch nicht tiered wurden, setzt das Verschieben eines Volumes die Temperatur dieser Daten auf 0 Tage zurück.

Optimierte Volumenverschiebungen

Ab ONTAP 9.6 werden bei einer Volume-Verschiebung Daten auf dem Quell-Volume, die im Bucket gespeichert sind, nicht zurück in das lokale Tier verschoben, wenn das Ziel-Local-Tier denselben Bucket verwendet wie das Quell-Local-Tier. Tiering-Daten bleiben unverändert, und nur häufig benötigte Daten müssen von einem lokalen Tier in ein anderes verschoben werden. Diese optimierte Volume-Verschiebung führt zu einer deutlich höheren Netzwerkeffizienz.

Beispielsweise löst bei einer optimierten Volume-Verschiebung von 300 TB die Verschiebung von 300 TB kalter Daten von einer lokalen Ebene auf eine andere weder 300 TB an Lesevorgängen noch 300 TB an Schreibvorgängen im Objektspeicher aus.

Nicht optimierte Volume-Verschiebungen erzeugen zusätzlichen Netzwerk- und Rechenverkehr (Lese-/GET- und Schreib-/PUT-Vorgänge), wodurch die Anforderungen an den ONTAP Cluster und den Objektspeicher steigen und beim Tiering auf öffentliche Objektspeicher potenziell höhere Kosten entstehen.



Einige Konfigurationen sind mit optimierten Volumenverschiebungen nicht kompatibel:

- Änderung der Tiering-Richtlinie während einer Volumenverschiebung
- Quell- und Ziel-Lokalschichten verwenden unterschiedliche Verschlüsselungsschlüssel
- FlexClone Volumes
- FlexClone übergeordnete Volumes
- MetroCluster (unterstützt optimierte Volumenverschiebungen in ONTAP 9.8 und höher)
- Nicht synchronisierte FabricPool Mirror Buckets
- Volume wird von einer Plattform, die QuickAssist Technologie (QAT) unterstützt, zu einer Plattform verschoben, die dies nicht unterstützt

Weitere Informationen zu "wie QAT Volume-Verschiebungen beeinflusst".

Wenn die lokale Ziel-Speicherebene eines verschobenen Volumes über eine zugeordnete Cloud-Speicherebene verfügt, werden die Daten des Quell-Volumes, die auf der Cloud-Speicherebene gespeichert sind, zunächst auf die lokale Speicherebene der lokalen Ziel-Speicherebene geschrieben. Anschließend werden die Daten, sofern die Tiering-Richtlinie des Volumes dies zulässt, auf die Cloud-Speicherebene geschrieben, die der lokalen Ziel-Speicherebene zugeordnet ist.

Das Schreiben von Daten zuerst auf den lokalen Tier verbessert die Performance beim Verschieben eines Volumes und verkürzt die Cutover-Zeit. Wenn Sie beim Verschieben eines Volumes keine Volume-Tiering-Richtlinie festlegen, verwendet das Ziel-Volume die Tiering-Richtlinie des Quell-Volumes.

Wenn Sie beim Verschieben des Volumes eine andere Tiering-Richtlinie festlegen, wird das Zielvolume mit der festgelegten Tiering-Richtlinie erstellt, und die Volume-Verschiebung ist nicht optimiert.

Volume Metadaten

Unabhängig davon, ob eine Volume Verschiebung optimiert ist, speichert ONTAP eine erhebliche Menge an Metadaten zu allen Daten, sowohl zu lokalen als auch zu per Tiering verschobenen Daten, einschließlich ihres Speicherorts, der Storage Effizienz, der Berechtigungen und der Nutzungsmuster. Metadaten verbleiben immer auf dem lokalen Tier und unterliegen nicht dem Tiering. Wenn ein Volume von einem lokalen Tier auf einen anderen verschoben wird, müssen diese Informationen ebenfalls auf den lokalen Ziel Tier verschoben werden.

Dauer

Volume-Verschiebungen benötigen weiterhin Zeit. Es ist davon auszugehen, dass eine optimierte Volume-Verschiebung ungefähr genauso lange dauert wie die Verschiebung einer gleich großen Menge nicht abgestufter Daten.

Der vom `volume move show`Befehl gemeldete Durchsatz stellt lokal aktualisierte Volumendaten dar, nicht Daten, die aus dem Cloud-Tier verschoben wurden.

> Wenn sich Volumes in einer SVM DR Beziehung befinden, müssen Quell- und Ziel-Volumes dieselbe Tiering-Richtlinie verwenden.

Schritte

1. Mit dem `volume move start` Befehl lässt sich ein Volume von einer lokalen Quellebene auf eine lokale Zielebene verschieben.

Beispiel für das Verschieben eines Volumens

Im folgenden Beispiel wird ein Volume mit dem Namen `myvol2` der `vs1` SVM auf `dest_FabricPool` verschoben, eine FabricPool-fähige lokale Ebene.

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool
```

Cloud-Schreibmodus auf ONTAP Volumes in FabricPool aktivieren oder deaktivieren

Ab ONTAP 9.14.1 kann das direkte Schreiben in die Cloud auf einem neuen oder bestehenden Volume in einer FabricPool aktiviert oder deaktiviert werden, sodass NFS-Clients Daten direkt in die Cloud schreiben können, ohne auf Tiering-Scans warten zu müssen. SMB-Clients schreiben weiterhin auf die Performance-Ebene in einem Volume mit aktiviertem Cloud-Schreibmodus. Der Cloud-Schreibmodus ist standardmäßig deaktiviert.

Die Möglichkeit, direkt in die Cloud zu schreiben, ist beispielsweise bei Migrationen hilfreich, bei denen große Datenmengen in einen Cluster übertragen werden, die der Cluster auf der lokalen Ebene nicht verarbeiten kann. Ohne Cloud-Schreibmodus werden während einer Migration kleinere Datenmengen übertragen, dann gestuft, dann erneut übertragen und wieder gestuft, bis die Migration abgeschlossen ist. Mit Cloud-Schreibmodus ist diese Art der Verwaltung nicht mehr erforderlich, da die Daten nie auf die lokale Ebene übertragen werden.

Bevor Sie beginnen

- Sie sind als Cluster- oder SVM-Administrator tätig.

- Sie müssen sich auf der erweiterten Berechtigungsstufe befinden.
- Das Volume muss ein Lese-/Schreib-Volume sein.
- Das Volumen muss die ALL Tiering-Richtlinie aufweisen.

Direktes Schreiben in die Cloud während der Volume-Erstellung ermöglichen

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Ein Volume wird erstellt und der Cloud-Schreibmodus aktiviert:

```
volume create -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled <true|false> -aggregate <local tier name>
```

Im folgenden Beispiel wird ein Volume mit dem Namen vol1 erstellt, bei dem Cloud Write auf der FabricPool lokalen Ebene (aggr1) aktiviert ist:

```
volume create -vserver vs1 -volume vol1 -is-cloud-write-enabled true
-aggregate aggr1
```

Direktes Schreiben in die Cloud auf einem vorhandenen Volume aktivieren

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Ein Volume kann so geändert werden, dass der Cloud-Schreibmodus aktiviert wird:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled true
```

Das folgende Beispiel ändert das Volume mit dem Namen vol1, um Cloud-Schreibvorgänge zu ermöglichen:

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled true
```

Das direkte Schreiben in die Cloud auf einem Volume deaktivieren

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Cloud-Schreibmodus für ein Volume deaktivieren:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled false
```

Das folgende Beispiel deaktiviert den Cloud-Schreibmodus für das Volume mit dem Namen vol1:

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled false
```

Aggressiven Read-Ahead-Modus für ONTAP FabricPool Volumes verwalten

Ab ONTAP 9.14.1 kann der aggressive Lesevorlaufmodus auf Volumes in FabricPools aktiviert und deaktiviert werden. In ONTAP 9.13.1 wurde der aggressive Lesevorlaufmodus nur auf Cloud-Plattformen eingeführt. Ab ONTAP 9.14.1 ist der aggressive Lesevorlaufmodus auf allen Plattformen verfügbar, die FabricPool unterstützt, einschließlich lokaler Plattformen. Die Funktion ist standardmäßig deaktiviert.

Wenn aggressives Vorlesen deaktiviert ist, liest FabricPool nur die Dateiblöcke, die eine Clientanwendung benötigt; es ist nicht erforderlich, die gesamte Datei zu lesen. Dies kann zu reduziertem Netzwerkverkehr führen, insbesondere bei großen Dateien im GB- und TB-Bereich. Das *Aktivieren* von aggressivem Vorlesen auf einem Volume schaltet diese Funktionalität ab, und FabricPool liest die gesamte Datei vorab sequenziell aus dem Objektspeicher, wodurch der GET-Durchsatz erhöht und die Latenzzeit für Client-Lesezugriffe auf die Datei verringert wird. Standardmäßig bleiben gestaffelte Daten beim sequenziellen Lesen kalt und werden nicht auf die lokale Ebene geschrieben.

Aggressives Vorlesen tauscht Netzwerkeffizienz gegen eine gesteigerte Leistung von gestuften Daten.

Über diese Aufgabe

Der `aggressive-readahead-mode` Befehl hat zwei Optionen:

- `none`: Das Read-Ahead ist deaktiviert.
- `file_prefetch`: Das System liest die gesamte Datei vor der Clientanwendung in den Speicher ein.

Bevor Sie beginnen

- Sie sind als Cluster- oder SVM-Administrator tätig.
- Sie müssen sich auf der erweiterten Berechtigungsstufe befinden.

Aggressiver Lesevorlaufmodus während der Volume-Erstellung aktivieren

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Ein Volume wird erstellt und der aggressive Read-Ahead-Modus aktiviert:

```
volume create -volume <volume name>  -aggressive-readahead-mode
<none|file_prefetch>
```

Das folgende Beispiel erstellt ein Volume namens vol1 mit aktiviertem aggressivem Vorlesen über die Option file_prefetch:

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

Aggressiver Read-Ahead-Modus deaktivieren

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Aggressiven Read-Ahead-Modus deaktivieren:

```
volume modify -volume <volume name>  -aggressive-readahead-mode none
```

Das folgende Beispiel ändert ein Volume mit dem Namen vol1, sodass der aggressive Lesevorlaufmodus deaktiviert wird:

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

Aggressiver Lesevorlaufmodus auf einem Volume anzeigen

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Den aggressiven Vorlesemodus anzeigen:

```
volume show -fields aggressive-readahead-mode
```

ONTAP FabricPool Volumes mit benutzerdefinierten, vom Benutzer erstellten Tags verwalten

Ab ONTAP 9.8 unterstützt FabricPool die Objektkennzeichnung mit benutzerdefinierten, vom Benutzer erstellten Tags, sodass Objekte zur einfacheren Verwaltung klassifiziert und sortiert werden können. Wenn Sie über die Admin-Berechtigungsstufe verfügen, können neue Objekt-Tags erstellt sowie bestehende Tags geändert, gelöscht und angezeigt werden.

Während der Volume-Erstellung ein neues Tag zuweisen

Sie können ein neues Objekt-Tag erstellen, wenn Sie einem oder mehreren neuen Objekten, die aus einem von Ihnen erstellten neuen Volume ausgelagert werden, Tags zuweisen möchten. Tags können zur Klassifizierung und Sortierung von Tiering-Objekten verwendet werden, um die Datenverwaltung zu erleichtern. Ab ONTAP 9.8 kann der System Manager zur Erstellung von Objekt-Tags verwendet werden.

Über diese Aufgabe

Tags können nur auf FabricPool Volumes vergeben werden, die an StorageGRID angebunden sind. Diese Tags bleiben beim Verschieben eines Volumes erhalten.

- Pro Volume sind maximal vier Tags zulässig.
- In der CLI muss jedes Objekt-Tag ein Schlüssel-Wert-Paar sein, das durch ein Gleichheitszeichen getrennt ist.
- In der CLI müssen mehrere Tags durch ein Komma getrennt werden.
- Jeder Tag-Wert kann maximal 127 Zeichen enthalten.
- Jeder Tag-Schlüssel muss entweder mit einem alphabetischen Zeichen oder einem Unterstrich beginnen.

  Schlüssel dürfen nur alphanumerische Zeichen und Unterstriche enthalten, und die maximal zulässige Zeichenanzahl beträgt 127.

Sie können Objekt-Tags mit ONTAP System Manager oder ONTAP CLI zuweisen.

Beispiel 1. Schritte

System Manager

1. Zu **Storage > Tiers** navigieren.
2. Eine Speicherebene mit Volumes, die getaggt werden sollen, finden.
3. Die Registerkarte **Volumes** auswählen.
4. Suchen Sie das Volume, das Sie taggen möchten, und wählen Sie in der Spalte **Objekt-Tags Klicken zum Eingeben von Tags** aus.
5. Geben Sie einen Schlüssel und einen Wert ein.
6. Auf **Anwenden** klicken.

CLI

1. Der `volume create` Befehl mit der `-tiering-object-tags` Option ermöglicht das Erstellen eines neuen Volumes mit den angegebenen Tags. Mehrere Tags können als durch Kommas

getrennte Paare angegeben werden:

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1>
[,<key2=value2>,<key3=value3>,<key4=value4> ]
```

Im folgenden Beispiel wird ein Volume mit dem Namen fp_volume1 und drei Objekttags erstellt.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

Ein vorhandenes Tag ändern

Sie können den Namen eines Tags ändern, Tags bei bestehenden Objekten im Objektspeicher ersetzen oder neuen Objekten, die Sie später hinzufügen möchten, einen anderen Tag hinzufügen.

Beispiel 2. Schritte

System Manager

1. Zu **Storage > Tiers** navigieren.
2. Eine Speicherebene mit Volumes, die die zu ändernden Tags enthalten, kann gefunden werden.
3. Die Registerkarte **Volumes** auswählen.
4. Das Volume mit den Tags, die geändert werden sollen, in der Spalte **Objekt-Tags** suchen und auf den Tag-Namen klicken.
5. Das Tag ändern.
6. Auf **Anwenden** klicken.

CLI

1. Der `volume modify`Befehl mit der `-tiering-object-tags`Option dient dazu, ein vorhandenes Tag zu ändern.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [ ,<key2=value2>,
<key3=value3>,<key4=value4> ]
```

Das folgende Beispiel ändert den Namen des vorhandenen Tags `type=abc` zu `type=xyz`.

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

Tag löschen

Sie können Objekt-Tags löschen, wenn Sie diese nicht mehr für ein Volume oder für Objekte im Objektspeicher festlegen möchten.

Beispiel 3. Schritte

System Manager

1. Zu **Storage > Tiers** navigieren.
2. Eine Speicherebene mit Volumes, die Tags enthalten, die gelöscht werden sollen, ermitteln.
3. Die Registerkarte **Volumes** auswählen.
4. Suchen Sie das Volume mit den Tags, die Sie löschen möchten, und klicken Sie in der Spalte **Objekt-Tags** auf den Tagnamen.
5. Zum Löschen des Tags auf das Papierkorbsymbol klicken.
6. Auf **Anwenden** klicken.

CLI

1. Der `volume modify`Befehl mit der `-tiering-object-tags`Option, gefolgt von einem leeren Wert (`""`), löscht ein vorhandenes Tag.

   Das folgende Beispiel löscht die vorhandenen Tags auf fp_volume1.

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

Vorhandene Tags eines Volumes anzeigen

Sie können die vorhandenen Tags eines Volumes anzeigen, um zu sehen, welche Tags verfügbar sind, bevor neue Tags zur Liste hinzugefügt werden.

Schritte

1. Der `volume show`Befehl kann mit der `tiering-object-tags`Option verwendet werden, um vorhandene Tags auf einem Volume anzuzeigen.

   ```
   volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
   tiering-object-tags
   ```

Objekt-Tagging-Status auf FabricPool Volumes prüfen

Sie können überprüfen, ob die Verschlagwortung auf einem oder mehreren FabricPool Volumes abgeschlossen ist.

Schritte

1. Der `vol show`Befehl mit der `-fields needs-object-retagging`Option zeigt an, ob die Verschlagwortung läuft, abgeschlossen ist oder nicht festgelegt wurde.

   ```
   vol show -fields needs-object-retagging  [ -instance | -volume <volume
   ```

```
name>]
```

Einer der folgenden Werte wird angezeigt:

- `true`: Der Objekt-Tagging-Scanner wurde für dieses Volume noch nicht ausgeführt oder muss erneut ausgeführt werden.
- `false`: Der Objekt-Tagging-Scanner hat das Tagging für dieses Volume abgeschlossen.
- `<->`: Der Objekt-Tagging-Scanner ist für dieses Volume nicht anwendbar. Dies tritt bei Volumes auf, die sich nicht auf FabricPools befinden.

Speichernutzung einer FabricPool aktivierten ONTAP lokalen Tier überwachen

Sie müssen wissen, wie viele Daten in den Performance- und Cloud-Tiers für FabricPool gespeichert sind. Diese Information hilft dabei festzustellen, ob die Tiering-Richtlinie eines Volumes geändert, das FabricPool lizenzierte Nutzungslimit erhöht oder der Speicherplatz des Cloud-Tiers erweitert werden sollte.

Vor ONTAP 9.7 verwendet System Manager den Begriff *aggregate*, um eine *lokale Ebene* zu beschreiben. Unabhängig von der ONTAP Version verwendet die ONTAP CLI den Begriff *aggregate*. Weitere Informationen zu lokalen Ebenen finden sich unter "Festplatten und lokale Ebenen".

Über diese Aufgabe

Ab ONTAP 9.18.1 ändert der `storage aggregate show-space` Befehl die Art und Weise, wie die logische referenzierte Kapazität und die logische nicht referenzierte Kapazität gemeldet werden. Die logische referenzierte Kapazität meldet referenzierte Blöcke in allen Objekten und nicht referenzierte Blöcke in fragmentierten Objekten. Die logische nicht referenzierte Kapazität meldet nur nicht referenzierte Blöcke in Objekten, die den Füllschwellenwert überschritten haben und für die Objektlöschung und Defragmentierung in Frage kommen.

Wenn Sie beispielsweise den standardmäßigen Schwellenwert für die aggregierte Auslastung von 40 % für ONTAP S3 und StorageGRID verwenden, müssen 60 % der Blöcke in einem Objekt nicht referenziert sein, bevor die Blöcke als nicht referenzierte Kapazität gemeldet werden.

In Versionen vor ONTAP 9.18.1 meldet die logische referenzierte Kapazität referenzierte Blöcke in allen Objekten (sowohl vollständigen als auch fragmentierten Objekten). Die logische nicht referenzierte Kapazität meldet nicht referenzierte Blöcke in allen Objekten.

Schritte

1. Die Speichernutzung für FabricPool aktivierte lokale Ebenen lässt sich mit einem der folgenden Befehle anzeigen:

Wenn Sie anzeigen möchten…	Verwenden Sie dann diesen Befehl:
Die genutzte Größe der Cloud-Tier in einer lokalen Tier	`storage aggregate show` mit dem `-instance` Parameter
Einzelheiten zur Speichernutzung innerhalb einer lokalen Ebene, einschließlich der referenzierten Kapazität des Objektspeichers	`storage aggregate show-space` mit dem `-instance` Parameter

Speichernutzung der Objektspeicher, die den lokalen Ebenen zugeordnet sind, einschließlich des genutzten Lizenzspeicherplatzes	`storage aggregate object-store show-space`
Eine Liste der Volumes in einer lokalen Ebene sowie die Footprints ihrer Daten und Metadaten	`volume show-footprint`

Zusätzlich zur Verwendung von CLI-Befehlen kann Active IQ Unified Manager (ehemals OnCommand Unified Manager) zusammen mit FabricPool Advisor, das auf ONTAP 9.4 und späteren Clustern unterstützt wird, oder System Manager zur Überwachung der Speichernutzung eingesetzt werden.

Das folgende Beispiel zeigt Möglichkeiten zur Anzeige der Speicherplatzauslastung und zugehöriger Informationen für FabricPool:

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                    ...
                                        Aggregate Display Name:
MyFabricPool
                                                                    ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                    ...
                                                    Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                 Total Logical Used
Size: -
                                                 Logical Used
Percentage: -
                                           Logical Unreferenced
Capacity: -
                                        Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
```

```
                                    ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume : rootvol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Volume Guarantee                 MB          %
Flexible Volume Metadata         KB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %

Vserver : vs1
Volume : vol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Footprint in Performance Tier    KB          %
Footprint in Amazon01            KB          %
Flexible Volume Metadata         MB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %
...
```

2. Je nach Bedarf ist eine der folgenden Maßnahmen zu ergreifen:

Wenn Sie möchten…	Dann…
Die Tiering-Richtlinie eines Volumens ändern	Die Vorgehensweise in "Verwaltung des Speicher-Tierings durch Ändern der Tiering-Richtlinie eines Volumes oder der minimalen Abkühlzeit für Tiering" ist zu beachten.
Das Limit für die lizenzierte Nutzung von FabricPool erhöhen	Ihr NetApp Vertriebsmitarbeiter oder Vertriebspartner steht als Ansprechpartner zur Verfügung. "NetApp Support"
Den Speicherplatz der Cloud-Tier erhöhen	Wenden Sie sich an den Anbieter des Objektspeichers, den Sie für die Cloud-Tier verwenden.

Verwandte Informationen

- "Speicher-Aggregatobjekt"
- "storage aggregate show"
- "storage aggregate show-space"

Die Tiering-Richtlinie und die minimale Kühlzeit eines ONTAP-Volumes anpassen

Sie können die Tiering-Richtlinie eines Volumes ändern, um festzulegen, ob Daten in die Cloud-Ebene verschoben werden, wenn sie inaktiv werden (*cold*). Für ein Volume mit der `snapshot-only` oder `auto` Tiering-Richtlinie kann außerdem die minimale Abkühlphase festgelegt werden, die Benutzerdaten inaktiv bleiben müssen, bevor sie in die Cloud-Ebene verschoben werden.

Bevor Sie beginnen

Das Ändern eines Volumens auf die `auto` Tiering-Richtlinie oder das Anpassen der minimalen Tiering-Kühlzeit erfordert ONTAP 9.4 oder höher.

Über diese Aufgabe

Durch die Änderung der Tiering-Richtlinie eines Volumes ändert sich lediglich das nachfolgende Tiering-Verhalten dieses Volumes. Dadurch werden Daten nicht rückwirkend in die Cloud-Tier verschoben.

Eine Änderung der Tiering-Richtlinie kann beeinflussen, wie lange es dauert, bis Daten als „kalt“ gelten und in die Cloud-Tier verschoben werden.

"Was geschieht, wenn eine Volume-Tiering-Richtlinie geändert wird?"

Bei einer SVM DR-Beziehung müssen Quell- und Ziel-Volumes keine FabricPool Aggregate verwenden, sie müssen jedoch dieselbe Tiering-Richtlinie nutzen.

Schritte

1. Die Tiering-Richtlinie für ein vorhandenes Volume kann mit dem `volume modify` Befehl und dem `-tiering-policy` Parameter geändert werden:

   Eine der folgenden Tiering-Richtlinien kann angegeben werden:

   - `snapshot-only` (Standard)
   - `auto`
   - `all`
   - `none`

     "FabricPool Volume-Tiering-Richtlinien"

2. Wenn das Volume die `snapshot-only` oder `auto` Tiering-Richtlinie verwendet und die minimale Abkühlperiode für das Tiering geändert werden soll, kann der `volume modify` Befehl mit dem `-tiering-minimum-cooling-days` optionalen Parameter auf der erweiterten Berechtigungsstufe genutzt werden.

   Sie können einen Wert zwischen 2 und 183 für die Mindestanzahl an Kühltagen für das Tiering angeben. Wenn eine Version von ONTAP vor 9.8 verwendet wird, kann ein Wert zwischen 2 und 63 für die Mindestanzahl an Kühltagen für das Tiering angegeben werden.

Beispiel für die Änderung der Tiering-Richtlinie und der Mindestkühlzeit für das Tiering eines Volumens

Das folgende Beispiel ändert die Tiering-Richtlinie des Volumes "myvol" in der SVM "vs1" zu `auto` und die minimale Kühlperiode für das Tiering auf 45 Tage:

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

ONTAP FabricPool Volume-Archivierungsvideo

Dieses Video bietet einen kurzen Überblick über die Verwendung von System Manager zum Archivieren eines Volumes in eine Cloud-Ebene mit FabricPool.

"NetApp Video: Archivierung von Volumes mit FabricPool (Backup + Volume-Verschiebung)"

Verwandte Informationen

"NetApp TechComm TV: FabricPool Wiedergabeliste"

Die Cloud-Abrufrichtlinie eines ONTAP Volumes ändern

FabricPool Cloud-Datenabruf wird durch Abrufrichtlinien gesteuert, die festlegen, wann Daten in die lokale Ebene zurückgeschrieben werden. Lesemuster können entweder sequenziell oder zufällig sein.

Wenn beispielsweise die Volume-Tiering-Richtlinie „Auto“ verwendet wird und kalte Blöcke sequenziell gelesen werden, bleiben diese kalt und verbleiben auf der Cloud-Tier. Für die meisten Clientanwendungen ist dies erwünschtes Verhalten und verhindert, dass bei den für Antiviren- und Analyseanwendungen typischen Tiefenscans kalte Daten zurück auf die lokale Tier geschrieben werden.

Ab ONTAP 9.8 kann die Cloud-Abrufrichtlinie eines Volumes geändert werden, um das "Standard Cloud Retrieval" Verhalten zu überschreiben.

Bevor Sie beginnen

- Die Änderung eines Volumes mit der `-cloud-retrieval-policy` Option erfordert ONTAP 9.8 oder höher.
- Für diese Operation ist die erweiterte Berechtigungsebene erforderlich.
- Das Verhalten von Tiering-Richtlinien mit `-cloud-retrieval-policy` sollte verstanden werden.

  "Wie Cloud-Abrufrichtlinien mit Tiering-Richtlinien funktionieren"

Schritt

1. Die Cloud-Abrufrichtlinie für ein vorhandenes Volume kann mit dem `volume modify` Befehl und der `-cloud-retrieval-policy` Option geändert werden:

   ```
   volume create -volume <volume_name> -vserver <vserver_name> - tiering-
   policy <policy_name> -cloud-retrieval-policy
   ```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
promote
```

Schwellenwerte für die ONTAP FabricPool PUT-Rate pro Knoten festlegen

Als Storage-Administrator kann die PUT-Drosselung verwendet werden, um einen oberen Schwellenwert für die maximale PUT-Rate pro Node festzulegen.

PUT-Drosselung ist sinnvoll, wenn Netzwerkressourcen oder der Objektspeicher-Endpunkt ressourcenbeschränkt sind. Obwohl selten, können Ressourcenbeschränkungen bei leistungsschwachen Objektspeichern oder während der ersten Tage der FabricPool Nutzung auftreten, wenn TB oder PB an kalten Daten ausgelagert werden.

Die PUT-Drosselung erfolgt pro Knoten. Das minimale PUT-Drosselungs-Limit beträgt 8 MB/s. Wenn das PUT-Drosselungs-Limit auf einen Wert unter 8 MB/s gesetzt wird, beträgt der Durchsatz an diesem Knoten 8 MB/s. Mehrere Knoten, die gleichzeitig Tiering durchführen, können mehr Bandbreite verbrauchen und möglicherweise eine Netzwerkverbindung mit extrem begrenzter Kapazität auslasten.

> FabricPool PUT-Operationen konkurrieren nicht mit anderen Anwendungen um Ressourcen. FabricPool PUT-Operationen werden von Clientanwendungen und anderen ONTAP Workloads, wie SnapMirror, automatisch niedriger priorisiert („nachrangig behandelt“). PUT-Drosselung mithilfe von `put-rate-limit` kann hilfreich sein, um den Netzwerkverkehr im Zusammenhang mit FabricPool Tiering zu reduzieren, steht jedoch in keinem Zusammenhang mit gleichzeitigem ONTAP-Verkehr.

Bevor Sie beginnen

Es ist eine erweiterte Berechtigungsstufe erforderlich.

Schritte

1. Drosselung von FabricPool PUT-Operationen mithilfe der ONTAP CLI:

```
storage aggregate object-store put-rate-limit modify -node <name>
-default <true|false> -put-rate-bytes-limit <integer>[KB|MB|GB|TB|PB]
```

Verwandte Informationen

- "storage aggregate Objektspeicher Schreibratenlimit ändern"

Anpassen der ONTAP FabricPool Objektlöschung und Defragmentierung

FabricPool löscht keine Blöcke aus angehängten Objektspeichern. Stattdessen löscht FabricPool Objekte, nachdem ein bestimmter Prozentsatz der Blöcke im Objekt nicht mehr von ONTAP referenziert wird.

Beispielsweise gibt es 1.024 4-KB-Blöcke in einem 4-MB-Objekt, das in Amazon S3 ausgelagert ist. Defragmentierung und Löschung finden erst statt, wenn weniger als 205 4-KB-Blöcke (20 % von 1.024) von ONTAP referenziert werden. Wenn genügend (1.024) Blöcke keine Referenzen mehr haben, werden ihre ursprünglichen 4-MB-Objekte gelöscht und ein neues Objekt wird erstellt.

Sie können den Schwellenwert für den nicht freigegebenen Speicherplatz in Prozent anpassen und für verschiedene Objektspeicher unterschiedliche Standardwerte festlegen. Die Standardeinstellungen sind:

Objektspeicher	ONTAP 9.8 und höher	ONTAP 9.7 bis 9.4	ONTAP 9.3 und früher	Cloud Volumes ONTAP
Amazon S3	20%	20%	0%	30%
Google Cloud Storage	20%	12%	n/a	35%
Microsoft Azure Blob Storage	25%	15%	n/a	35%
NetApp ONTAP S3	40%	n/a	n/a	n/a
NetApp StorageGRID	40%	40%	0%	n/a

Schwellenwert für nicht zurückgewonnenen Speicherplatz

Durch Ändern der Standardeinstellungen für den Schwellenwert des nicht freigegebenen Speicherplatzes wird die zulässige Objektfragmentierung erhöht oder verringert. Eine geringere Fragmentierung reduziert die vom Cloud-Tier genutzte physische Kapazität, erfordert jedoch zusätzliche Objektspeicherressourcen (Lese- und Schreibvorgänge).

Interpretation des Werts

- Ein höherer Schwellenwert bedeutet, dass ONTAP Objekte früher defragmentiert oder zurückgewinnt, was die verschwendete Objektspeicherkapazität reduziert, aber zu mehr Lese- und Schreibvorgängen im Objektspeicher führt.
- Ein niedrigerer Schwellenwert bedeutet, dass ONTAP länger wartet, bevor Speicherplatz freigegeben wird, wodurch Defragmentierungs-E/A und die Kosten für Objektspeichertransaktionen reduziert werden, aber mehr nicht referenzierte Daten länger abrechnungsfähig bleiben.

Beispiel:

+ Bei einer Schwelle von 25 % kann ein Objekt zurückgefordert werden, wenn weniger als 25 % seiner Blöcke noch von ONTAP referenziert werden; mit anderen Worten, wenn mehr als 75 % dieses Objekts ungenutzt sind.

Schwellenwertreduzierung

Um zusätzliche Kosten zu vermeiden, empfiehlt es sich, die Schwellenwerte für nicht freigegebenen Speicherplatz zu reduzieren, wenn Objektspeicher Preismodelle verwendet werden, die zwar die Speicherkosten senken, aber die Lesekosten erhöhen. Beispiele hierfür sind Amazon Standard-IA und Azure Blob Storage Cool.

Die Staffelung eines Volumens von zehn Jahre alten Projekten, das aus rechtlichen Gründen aufbewahrt wurde, kann beispielsweise mit einem Preismodell wie Standard-IA oder Cool günstiger sein als mit herkömmlichen Preismodellen. Obwohl Lesevorgänge für ein solches Volumen, einschließlich der für die Objektdefragmentierung erforderlichen Lesevorgänge, teurer sind, treten sie wahrscheinlich nicht häufig auf.

Schwellenwerterhöhungen

Alternativ kann eine Erhöhung der Schwellenwerte für nicht freigegebenen Speicherplatz in Betracht gezogen

werden, wenn die Objektfragmentierung dazu führt, dass deutlich mehr Objektspeicher-Kapazität genutzt wird, als für die von ONTAP referenzierten Daten erforderlich ist. Beispielsweise bedeutet die Verwendung eines Schwellenwerts von 20 % für nicht freigegebenen Speicherplatz in einem Worst-Case-Szenario, in dem alle Objekte maximal zulässig fragmentiert sind, dass bis zu 80 % der Gesamtkapazität in der Cloud-Tier von ONTAP nicht referenziert werden. Beispiel:

2 TB von ONTAP referenziert + 8 TB nicht von ONTAP referenziert = 10 TB Gesamtkapazität, die von der Cloud-Tier genutzt wird.

In dieser Situation könnte es vorteilhaft sein, den Schwellenwert für nicht zurückgewonnenen Speicherplatz anzuheben oder die Mindestanzahl an Kühltagen für Volumes zu erhöhen, um die von nicht referenzierten Blöcken beanspruchte Kapazität zu reduzieren.

> Während das System Objekte defragmentiert und deren Speichereffizienz erhöht, kann es zu einer Fragmentierung der zugrunde liegenden Dateien kommen, da referenzierte Blöcke in neue, effizientere Objekte geschrieben werden. Wenn der Schwellenwert für nicht zurückgewonnenen Speicherplatz deutlich erhöht wird, können Objekte entstehen, die speichereffizienter sind, jedoch eine geringere sequenzielle Leseleistung aufweisen.
>
> Diese zusätzliche Aktivität führt zu höheren Kosten bei externen S3-Anbietern wie AWS, Azure und Google.
>
> NetApp empfiehlt, den Schwellenwert für nicht zurückgewonnenen Speicherplatz nicht über 60% anzuheben.

Schwellenwert für nicht zurückgewonnenen Speicherplatz ändern

Sie können den Schwellenwert für den Prozentsatz des nicht zurückgewonnenen Speicherplatzes für verschiedene Objektspeicher anpassen.

Bevor Sie beginnen

Es ist eine erweiterte Berechtigungsstufe erforderlich.

Schritte

1. Um den Standardschwellenwert für nicht zurückgewonnenen Speicherplatz zu ändern, kann der folgende Befehl angepasst und ausgeführt werden:

```
storage aggregate object-store modify -aggregate <name> -object-store
-name <name> -unreclaimed-space-threshold <%> (0%-99%)
```

Verwandte Informationen

- "storage aggregate object-store modify"

ONTAP Daten in die Leistungsebene hochstufen

Ab ONTAP 9.8 können Sie als Cluster-Administrator mit erweiterten Berechtigungen Daten proaktiv von der Cloud-Ebene in die Performance-Ebene verschieben, indem Sie eine Kombination aus der `tiering-policy` und der `cloud-retrieval-policy` Einstellung verwenden.

Über diese Aufgabe

Dies kann sinnvoll sein, wenn Sie FabricPool auf einem Volume nicht mehr verwenden möchten oder wenn Sie eine `snapshot-only` Tiering-Richtlinie haben und wiederhergestellte Snapshot-Daten zurück in die Performance-Ebene verschieben möchten.

Alle Daten von einem FabricPool Volume auf die Leistungsebene verschieben

Sie können proaktiv alle Daten eines FabricPool Volumes in der Cloud-Ebene abrufen und sie in die Performance-Ebene verschieben.

Schritte

1. Mit dem `volume modify`Befehl wird `tiering-policy`auf `none` und `cloud-retrieval-policy` auf `promote` gesetzt.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

Dateisystemdaten in die Performance-Ebene verschieben

Sie können proaktiv aktive Dateisystemdaten aus einem wiederhergestellten Snapshot in der Cloud-Ebene abrufen und in die Performance-Ebene hochstufen.

Schritte

1. Mit dem `volume modify`Befehl wird `tiering-policy`auf `snapshot-only` und `cloud-retrieval-policy` auf `promote` gesetzt.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

Status einer Leistungsstufenbeförderung prüfen

Sie können den Status der Performance-Tier-Promotion überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist.

Schritte

1. Den `object-store`Befehl volume mit der `tiering`Option verwenden, um den Status der Leistungsstufenaufwertung zu prüfen.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                  Vserver: vs1
```

```
                                    Volume: v1
                                 Node Name: node1
                              Volume DSID: 1023
                            Aggregate Name: a1
                                     State: ready
                       Previous Run Status: completed
                  Aborted Exception Status: -
              Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                Scanner Percent Complete: -
                     Scanner Current VBN: -
                        Scanner Max VBNs: -
    Time Waiting Scan will be scheduled: -
                          Tiering Policy: snapshot-only
   Estimated Space Needed for Promotion: -
                       Time Scan Started: -
 Estimated Time Remaining for scan to complete: -
                   Cloud Retrieve Policy: promote
```

Geplante Migration und Tiering auslösen

Ab ONTAP 9.8 kann eine Tiering-Scan-Anforderung jederzeit ausgelöst werden, wenn nicht auf den standardmäßigen Tiering-Scan gewartet werden soll.

Schritte

1. Mit dem `volume object-store`Befehl und der `trigger`Option kann Migration und Tiering angefordert werden.

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

Spiegel von FabricPool verwalten

Informationen zu ONTAP FabricPool Spiegeln

Um sicherzustellen, dass Daten in Datenspeichern im Katastrophenfall zugänglich sind und um den Austausch eines Datenspeichers zu ermöglichen, kann eine FabricPool Spiegelung konfiguriert werden, indem ein zweiter Datenspeicher hinzugefügt wird, sodass Daten synchron auf zwei Datenspeicher gestuft werden. Ein zweiter Datenspeicher kann zu neuen oder bestehenden FabricPool Konfigurationen hinzugefügt, der Spiegelungsstatus überwacht, FabricPool Spiegelungsdetails angezeigt, eine Spiegelung hochgestuft und eine Spiegelung entfernt werden. ONTAP 9.7 oder höher muss ausgeführt werden.

Eine ONTAP FabricPool Spiegelung erstellen

Um eine FabricPool Spiegelung zu erstellen, werden zwei Objektspeicher an eine

einzelne FabricPool angehängt. Eine FabricPool Spiegelung kann entweder durch das Anhängen eines zweiten Objektspeichers an eine bestehende, einzelne Objektspeicher FabricPool Konfiguration erstellt werden, oder es wird eine neue, einzelne Objektspeicher FabricPool Konfiguration erstellt und anschließend ein zweiter Objektspeicher daran angehängt. FabricPool Spiegelungen können auch auf MetroCluster Konfigurationen erstellt werden.

Bevor Sie beginnen

- Die beiden Objektspeicher müssen bereits mit dem `storage aggregate object-store config` Befehl erstellt worden sein.
- Wenn FabricPool Spiegel auf MetroCluster Konfigurationen erstellt werden:
  - Die MetroCluster muss bereits eingerichtet und konfiguriert sein.
  - Die Objektspeicher-Konfigurationen müssen auf dem ausgewählten Cluster erstellt worden sein.

    Wenn FabricPool Spiegel auf beiden Clustern in einer MetroCluster Konfiguration erstellt werden, müssen auf beiden Clustern Objektspeicherkonfigurationen vorhanden sein.

  - Wenn Sie keine lokalen Objektspeicher für MetroCluster Konfigurationen verwenden, sollte sichergestellt sein, dass eines der folgenden Szenarien vorliegt:
    - Objektspeicher befinden sich in unterschiedlichen Verfügbarkeitszonen
    - Objektspeicher sind so konfiguriert, dass Kopien von Objekten in mehreren Verfügbarkeitszonen aufbewahrt werden.

      "Einrichten von Objektspeichern für FabricPool in einer MetroCluster Konfiguration"

Über diese Aufgabe

Der Objektspeicher, den Sie für den FabricPool Spiegel verwenden, muss sich vom primären Objektspeicher unterscheiden.

Das Verfahren zum Erstellen eines FabricPool Spiegels ist für MetroCluster und Nicht-MetroCluster Konfigurationen gleich.

Schritte

1. Wenn keine bestehende FabricPool Konfiguration verwendet wird, kann eine neue erstellt werden, indem ein Objektspeicher mit dem `storage aggregate object-store attach` Befehl an eine lokale Ebene angehängt wird.

   Dieses Beispiel erstellt ein neues FabricPool, indem ein Objektspeicher an eine lokale Ebene angehängt wird.

   ```
   cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
   my-store-1
   ```

2. Ein zweiter Objektspeicher kann mit dem `storage aggregate object-store mirror` Befehl an die lokale Ebene angehängt werden.

   Dieses Beispiel bindet einen zweiten Objektspeicher an eine lokale Ebene an, um einen FabricPool Spiegel zu erstellen.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

Verwandte Informationen

- "storage aggregate Objektspeicher anhängen"
- "storage aggregate Objektspeicher-Konfiguration"
- "Speicheraggregate Objektspeicher Spiegelung"

Details zum ONTAP FabricPool Spiegel anzeigen

Es lassen sich Details zu einem FabricPool Spiegel anzeigen, um zu sehen, welche Objektspeicher in der Konfiguration enthalten sind und ob der Objektspeicher Spiegel mit dem primären Objektspeicher synchron ist.

Schritt

1. Informationen über einen FabricPool Spiegel werden mit dem `storage aggregate object-store show` Befehl angezeigt.

   Dieses Beispiel zeigt die Details zu den primären und gespiegelten Objektspeichern in einem FabricPool Spiegel.

   ```
   cluster1::> storage aggregate object-store show
   ```

   ```
   Aggregate      Object Store Name Availability    Mirror Type
   -------------- ----------------- -------------   ----------
   aggr1          my-store-1        available       primary
                  my-store-2        available       mirror
   ```

   Dieses Beispiel zeigt Details zum FabricPool Spiegel an, einschließlich der Information, ob der Spiegel aufgrund einer Resync-Operation beeinträchtigt ist.

   ```
   cluster1::> storage aggregate object-store show -fields mirror-type,is-
   mirror-degraded
   ```

   ```
   aggregate      object-store-name mirror-type     is-mirror-degraded
   -------------- ----------------- ------------- ------------------
   aggr1          my-store-1        primary           -
                  my-store-2        mirror          false
   ```

Verwandte Informationen

- "storage aggregate object-store show"

Einen ONTAP FabricPool Spiegel promoten

Der Objektspeicher Spiegel kann durch Hochstufen als primärer Objektspeicher zugewiesen werden. Wenn der Objektspeicher Spiegel zum primären Objektspeicher wird, wird der ursprüngliche primäre Objektspeicher automatisch zum Spiegel.

Bevor Sie beginnen

- Der FabricPool Spiegel muss synchron sein
- Der Objektspeicher muss betriebsbereit sein

Über diese Aufgabe

Sie können den ursprünglichen Objektspeicher durch einen Objektspeicher eines anderen Cloud-Anbieters ersetzen. Beispielsweise könnte Ihr ursprünglicher Spiegel ein AWS Objektspeicher sein, der durch einen Azure Objektspeicher ersetzt werden kann.

Schritte

1. Es kann überprüft werden, ob der FabricPool-Spiegel synchron ist, indem der `storage aggregate object-store show-resync-status` Befehl verwendet wird. Wenn der FabricPool-Spiegel synchron ist, werden keine Einträge angezeigt. Ist der Spiegel nicht synchron, sollte auf den Abschluss der Resynchronisierung gewartet werden.

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

```
                                          Complete
Aggregate    Primary       Mirror         Percentage
---------    -----------   ----------     ----------
aggr1        my-store-1     my-store-2      40%
```

2. Einen Objektspeicher-Mirror mit dem `storage aggregate object-store modify -aggregate` Befehl aktivieren.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-store-2 -mirror-type primary
```

Verwandte Informationen

- "storage aggregate object-store modify"
- "storage aggregate object-store show-resync-status"

Einen ONTAP FabricPool Spiegel entfernen

Ein FabricPool Spiegel kann entfernt werden, wenn keine Replikation eines Objektspeichers mehr erforderlich ist.

Bevor Sie beginnen

Der primäre Objektspeicher muss betriebsbereit sein, andernfalls schlägt der Befehl fehl.

> Dieser Vorgang löscht dauerhaft alle Objekte im Objektspeicher-Container und kann nicht rückgängig gemacht werden. Die Objektlöschung läuft nach Abschluss des Entspiegelungsvorgangs im Hintergrund weiter. Der Container sollte erst wiederverwendet oder einer anderen Zweckbestimmung zugeführt werden, nachdem der Hintergrundlöschprozess abgeschlossen ist.

Schritt

1. Einen Objektspeicher-Spiegel in einem FabricPool mit dem `storage aggregate object-store unmirror -aggregate` Befehl entfernen.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

Verwandte Informationen

- "storage aggregate Objektspeicher Spiegelung aufheben"

Einen vorhandenen Objektspeicher durch einen ONTAP FabricPool Spiegel ersetzen

Sie können die FabricPool Spiegeltechnologie verwenden, um einen Objektspeicher durch einen anderen zu ersetzen. Der neue Objektspeicher muss nicht denselben Cloud-Anbieter wie der ursprüngliche Objektspeicher verwenden.

Über diese Aufgabe

Sie können den ursprünglichen Objektspeicher durch einen Objektspeicher ersetzen, der einen anderen Cloud-Anbieter verwendet. Beispielsweise könnte Ihr ursprünglicher Objektspeicher AWS als Cloud-Anbieter nutzen, er kann jedoch durch einen Objektspeicher ersetzt werden, der Azure als Cloud-Anbieter verwendet, und umgekehrt. Der neue Objektspeicher muss jedoch die gleiche Objektgröße wie der ursprüngliche beibehalten.

Schritte

1. Einen FabricPool-Spiegel erstellen, indem ein neuer Objektspeicher zu einem bestehenden FabricPool mit dem `storage aggregate object-store mirror` Befehl hinzugefügt wird.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. Der Status der Spiegel-Resynchronisierung kann mit dem `storage aggregate object-store show-resync-status` Befehl überwacht werden.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                                Complete
      Aggregate    Primary          Mirror      Percentage
```

```
---------    -----------      ----------    ----------
aggr1        my-AWS-store     my-AZURE-store     40%
```

3. Mit dem `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded`Befehl kann überprüft werden, ob der Spiegel synchronisiert ist.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. Den primären Objektspeicher mit dem gespiegelten Objektspeicher mithilfe des `storage aggregate object-store modify` Befehls austauschen.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. Details zum FabricPool Spiegel werden mit dem `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` Befehl angezeigt.

   Dieses Beispiel zeigt die Informationen über den FabricPool Spiegel an, einschließlich der Information, ob der Spiegel defekt ist (nicht synchronisiert).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. Den FabricPool Spiegel mit dem `storage aggregate object-store unmirror` Befehl entfernen.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Überprüfen Sie, ob sich das FabricPool wieder in einer einzelnen Objektspeicherkonfiguration befindet, indem Sie den `storage aggregate object-store show -fields mirror-type,is-mirror-`

`degraded` Befehl verwenden.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

Verwandte Informationen

- "Speicheraggregate Objektspeicher Spiegelung"
- "storage aggregate object-store modify"
- "storage aggregate object-store show-resync-status"
- "storage aggregate object-store show"
- "storage aggregate Objektspeicher Spiegelung aufheben"

Einen FabricPool Spiegel in einer ONTAP MetroCluster Konfiguration ersetzen

Wenn einer der Objektspeicher in einem FabricPool Spiegel zerstört wird oder in einer MetroCluster Konfiguration dauerhaft nicht mehr verfügbar ist, kann der Objektspeicher zum Spiegel gemacht werden, falls er nicht bereits der Spiegel ist, der beschädigte Objektspeicher aus dem FabricPool Spiegel entfernt und anschließend ein neuer Objektspeicher Spiegel zum FabricPool hinzugefügt werden.

Schritte

1. Falls der beschädigte Objektspeicher noch nicht der Spiegel ist, wird der Objektspeicher mit dem `storage aggregate object-store modify` Befehl zum Spiegel gemacht.

   ```
   storage aggregate object-store modify -aggregate aggr1 -name
   mcc1_ostore1 -mirror-type mirror
   ```

2. Die Objektspeicherspiegelung wird mithilfe des Befehls `storage aggregate object-store unmirror` aus dem FabricPool entfernt.

   ```
   storage aggregate object-store unmirror -aggregate <aggregate name>
   -name mcc1_ostore1
   ```

3. Sie können das Tiering auf dem primären Datenspeicher fortsetzen, nachdem Sie den gespiegelten Datenspeicher entfernt haben, indem Sie `storage aggregate object-store modify` mit der `-force-tiering-on-metrocluster true` Option verwenden.

   Das Fehlen eines Spiegels beeinträchtigt die Replikationsanforderungen einer MetroCluster Konfiguration.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. Zum Erstellen eines Ersatzobjektspeichers, der nicht denselben Bucket wie der zuvor entspiegelte Objektspeicher verwendet, dient der `storage aggregate object-store config create` Befehl.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt <true|false> -port <port> -is-ssl
-enabled <true|false> -ipspace <IPSpace>
```

5. Den Objektspeicher-Mirror zur FabricPool Mirror mithilfe des `storage aggregate object-store mirror` Befehls hinzufügen.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Die Objektspeicherinformationen werden mit dem `storage aggregate object-store show` Befehl angezeigt.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary           -
               mcc1_ostore3-mc    mirror          true
```

7. Der Status der Spiegel-Resynchronisierung kann mit dem `storage aggregate object-store show-resync-status` Befehl überwacht werden.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                          Complete
     Aggregate    Primary        Mirror    Percentage
     ---------    -----------    ----------      ----------
     aggr1        mcc1_ostore1-mc mcc1_ostore3-mc   40%
```

Verwandte Informationen

- "storage aggregate Objektspeicher config create"
- "Speicheraggregate Objektspeicher Spiegelung"
- "storage aggregate object-store modify"
- "storage aggregate object-store show"
- "storage aggregate object-store show-resync-status"
- "storage aggregate Objektspeicher Spiegelung aufheben"

ONTAP-Befehle für die Verwaltung von FabricPool-Ressourcen

Sie verwenden die `storage aggregate object-store` Befehle zur Verwaltung von Objektspeichern für FabricPool. Sie verwenden die `storage aggregate` Befehle zur Verwaltung von Aggregaten für FabricPool. Sie verwenden die `volume` Befehle zur Verwaltung von Volumes für FabricPool.

Wenn Sie möchten…	Dazu wird folgender Befehl verwendet:
Die Konfiguration für einen Objektspeicher wird definiert, sodass ONTAP darauf zugreifen kann	`storage aggregate object-store config create`
Objektspeicher-Konfigurationsattribute ändern	`storage aggregate object-store config modify`
Eine vorhandene Objektspeicher-Konfiguration umbenennen	`storage aggregate object-store config rename`
Konfiguration eines Objektspeichers löschen	`storage aggregate object-store config delete`
Eine Liste der Objektspeicherkonfigurationen anzeigen	`storage aggregate object-store config show`
Einen zweiten Objektspeicher als Spiegel an eine neue oder bestehende FabricPool anhängen	`storage aggregate object-store mirror` mit dem `-aggregate` und `-name` Parameter in der Administratorberechtigungsstufe
Einen Objektspeicher-Spiegel aus einer vorhandenen FabricPool Spiegelung entfernen	`storage aggregate object-store unmirror` mit dem `-aggregate` und `-name` Parameter in der Administratorberechtigungsstufe
Status der Spiegelungs-Resynchronisierung von FabricPool überwachen	`storage aggregate object-store show-resync-status`
Details zum FabricPool-Spiegel anzeigen	`storage aggregate object-store show`
Eine Objektspeicher-Spiegelung kann verwendet werden, um einen primären Objektspeicher in einer FabricPool Spiegelkonfiguration zu ersetzen.	`storage aggregate object-store modify` mit dem `-aggregate` Parameter auf der Administrator-Berechtigungsstufe
Die Latenz und Leistung eines Objektspeichers können getestet werden, ohne den Objektspeicher an ein Aggregat anzubinden.	`storage aggregate object-store profiler start` mit dem `-object-store-name` und `-node` Parameter in der erweiterten Berechtigungsstufe

Status des Objektspeicherprofilers überwachen	`storage aggregate object-store profiler show` mit dem `-object-store-name` und `-node` Parameter in der erweiterten Berechtigungsstufe
Den Objektspeicher-Profiler abbrechen, wenn er ausgeführt wird	`storage aggregate object-store profiler abort` mit dem `-object-store-name` und `-node` Parameter in der erweiterten Berechtigungsstufe
Einen Objektspeicher an ein Aggregat anbinden, um FabricPool zu verwenden	`storage aggregate object-store attach`
Einen Objektspeicher an ein Aggregat anhängen, das ein FlexGroup Volume enthält, um FabricPool zu verwenden	`storage aggregate object-store attach` mit dem `allow-flexgroup true`
Details der Objektspeicher, die an FabricPool-aktivierte Aggregate angehängt sind, anzeigen	`storage aggregate object-store show`
Der vom Tiering-Scan verwendete Schwellenwert für die Aggregatauslastung wird angezeigt.	`storage aggregate object-store show` mit dem `-fields tiering-fullness-threshold` Parameter auf der erweiterten Berechtigungsstufe
Anzeige der Speichernutzung der Objektspeicher, die an FabricPool-fähige Aggregate angebunden sind	`storage aggregate object-store show-space`
Die Berichterstattung über inaktive Daten kann für ein Aggregat aktiviert werden, das nicht für FabricPool verwendet wird	`storage aggregate modify` mit dem `-is-inactive-data-reporting-enabled true` Parameter
Anzeigen, ob die Berichterstattung über inaktive Daten auf einem Aggregat aktiviert ist	`storage aggregate show` mit dem `-fields is-inactive-data-reporting-enabled` Parameter
Informationen darüber, wie viele Nutzerdaten innerhalb eines Aggregats kalt sind, anzeigen	`storage aggregate show-space` mit dem `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` Parameter
Ein Volume für FabricPool erstellen, einschließlich der folgenden Angaben: • Die Tiering-Richtlinie • Die Mindestkühlzeit für das Tiering (für die `snapshot-only` oder `auto` Tiering-Richtlinie)	`volume create` • Der `-tiering-policy`Parameter wird verwendet, um die Tiering-Richtlinie anzugeben. • Der `-tiering-minimum-cooling-days` Parameter auf der erweiterten Berechtigungsstufe gibt den Mindestkühlzeitraum für das Tiering an.
Ein Volume für FabricPool kann geändert werden, einschließlich der folgenden Anpassungen: • Die Tiering-Richtlinie • Die Mindestkühlzeit für das Tiering (für die `snapshot-only` oder `auto` Tiering-Richtlinie)	`volume modify` • Der `-tiering-policy`Parameter wird verwendet, um die Tiering-Richtlinie anzugeben. • Der `-tiering-minimum-cooling-days` Parameter auf der erweiterten Berechtigungsstufe gibt den Mindestkühlzeitraum für das Tiering an.

Informationen zu FabricPool in Bezug auf ein Volumen, einschließlich der folgenden: • Die Mindestkühlperiode für das Tiering • Wie viele Nutzerdaten sind kalt	`volume show` • Sie verwenden den `-fields tiering-minimum-cooling-days` Parameter in der erweiterten Berechtigungsstufe, um die Mindestkühlzeit für das Tiering anzuzeigen. • Der `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent`Parameter zeigt an, wie viele Benutzerdaten kalt sind.
Ein Volume in oder aus FabricPool verschieben	`volume move start`Der `-tiering-policy`optionale Parameter gibt die Tiering-Richtlinie für das Volume an.
Den Schwellenwert für die Rückgewinnung von nicht referenziertem Speicherplatz (den Defragmentierungsschwellenwert) für FabricPool anpassen	`storage aggregate object-store modify` mit dem `-unreclaimed-space-threshold` Parameter auf der erweiterten Berechtigungsstufe
Den Schwellenwert für den Prozentsatz festlegen, bei dem das Aggregat als voll gilt, bevor der Tiering-Scan mit dem Tiering von Daten für FabricPool beginnt FabricPool lagert weiterhin kalte Daten in eine Cloud-Tier aus, bis die lokale Tier 98 % Kapazität erreicht.	`storage aggregate object-store modify` mit dem `-tiering-fullness-threshold` Parameter auf der erweiterten Berechtigungsstufe
Schwellenwert für die Rückgewinnung von nicht referenziertem Speicherplatz für FabricPool anzeigen	`storage aggregate object-store show` oder `storage aggregate object-store show-space` Befehl mit dem `-unreclaimed-space-threshold` Parameter in der erweiterten Berechtigungsstufe

Verwandte Informationen

- "storage aggregate ändern"
- "Speicher-Aggregatobjekt"
- "storage aggregate show-space"

SVM Datenmobilität

Informationen zu ONTAP Datenmobilität

Ab ONTAP 9.10.1 können Cluster-Administratoren eine SVM unterbrechungsfrei von einem Quell-Cluster zu einem Ziel-Cluster verlagern, um die Kapazität und den Lastausgleich zu verwalten oder um Geräte-Upgrades oder Rechenzentrumskonsolidierungen zu ermöglichen.

Die unterbrechungsfreie SVM-Verschiebung wird auf AFF Systemen in ONTAP 9.10.1 und 9.11.1 unterstützt. Ab ONTAP 9.12.1 ist diese Funktion sowohl auf FAS als auch auf AFF Systemen und auf Hybridaggregaten verfügbar.

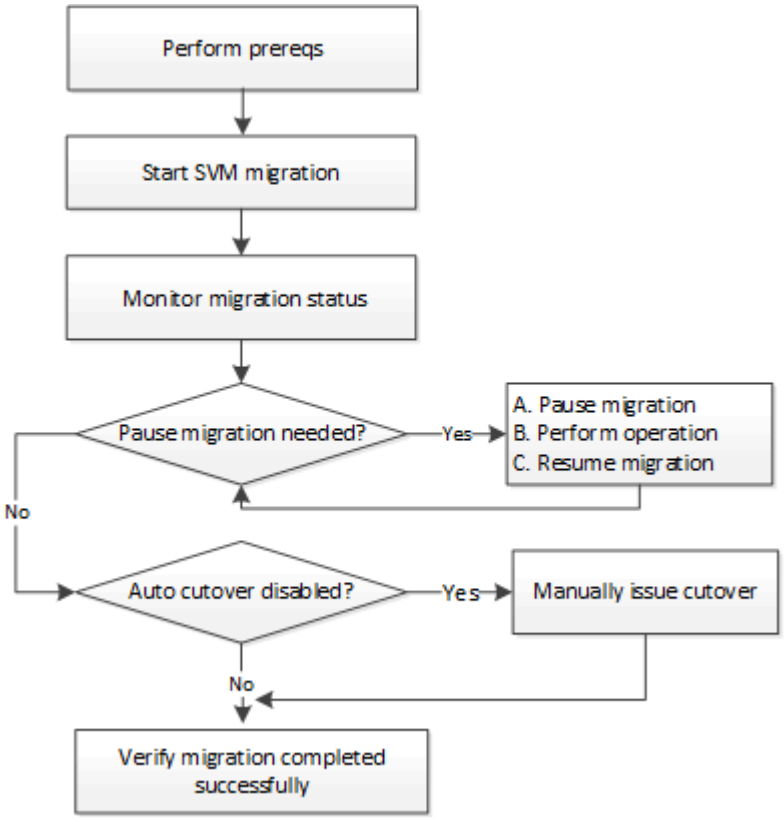
Der Name und die UUID der SVM bleiben nach der Migration unverändert, ebenso wie der Name der Daten-

LIF, die IP-Adresse und Objektnamen wie der Volume-Name. Die UUID der Objekte in der SVM wird jedoch unterschiedlich sein.

Ab ONTAP 9.18.1 wird die SVM Migration von ASA Speichersystemen auf ASA r2 Speichersysteme unterstützt. Wenn Sie ein ASA r2 Speichersystem (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) besitzen und eine SVM von einem ASA System auf Ihr ASA r2 System migrieren möchten, siehe "diese Schritte".

SVM Migrationsworkflow

Das Diagramm veranschaulicht den typischen Workflow einer SVM-Migration. Eine SVM-Migration wird vom Ziel-Cluster aus gestartet. Die Migration kann entweder vom Quell-Cluster oder vom Ziel-Cluster aus überwacht werden. Ein manueller oder ein automatischer Cutover kann durchgeführt werden. Standardmäßig wird ein automatischer Cutover durchgeführt.



SVM Migration Systemunterstützung

Controller Familie	Unterstützte ONTAP-Versionen
ASA	ONTAP 9.18.1 und höher: "diese Schritte" für die SVM-Migration von ASA auf ASA r2-Systeme beachten.
AFF C-Series	ONTAP 9.12.1 Patch 4 und höher
FAS	ONTAP 9.12.1 und höher
AFF A-Series	ONTAP 9.10.1 und höher

Bei der Migration von einem AFF Cluster zu einem FAS Cluster mit Hybridaggregaten versucht

die automatische Volume-Platzierung, eine Zuordnung gleichartiger Aggregate vorzunehmen. Wenn der Quell-Cluster 60 Volumes enthält, versucht die Volume-Platzierung, ein AFF-Aggregat auf dem Ziel-Cluster zu finden, um die Volumes dort zu platzieren. Wenn nicht genügend Speicherplatz auf den AFF-Aggregaten vorhanden ist, werden die Volumes auf Aggregaten mit Nicht-Flash-Festplatten platziert.

Skalierbarkeitsunterstützung nach ONTAP Version

ONTAP Version	HA-Paare in Quell- und Ziel-Cluster
ONTAP 9.14.1 und höher	12
ONTAP 9.13.1	6
ONTAP 9.11.1	3
ONTAP 9.10.1	1

Anforderungen an die Netzwerkinfrastrukturleistung für die TCP Round Trip Time (RTT) zwischen Quell-Cluster und Ziel-Cluster

Abhängig von der auf dem Cluster installierten ONTAP-Version muss das Netzwerk, das Quell-Cluster und Ziel-Cluster verbindet, eine maximale Roundtrip-Zeit wie angegeben aufweisen:

ONTAP Version	Maximale RTT
ONTAP 9.12.1 und höher	10 ms
ONTAP 9.11.1 und früher	2 ms

Maximal unterstützte Volumes pro SVM

Die maximale Anzahl an Volumes, die pro SVM in einem gemischten oder hybriden Cluster migriert werden kann, richtet sich nach dem Cluster-Mitglied, das die geringere Anzahl an Volumes unterstützt.

Quelle	Ziel	ONTAP 9.14.1 und höher	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1 und früher
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	k. A.
FAS	AFF	80	80	80	k. A.
AFF	FAS	80	80	80	k. A.

Voraussetzungen

Bevor Sie eine SVM Migration starten, müssen die folgenden Voraussetzungen erfüllt sein:

- Sie sind ein Cluster-Administrator.
- "Die Quell- und Ziel-Cluster sind miteinander verbunden.".
- Die Quell- und Ziel-Cluster verfügen über die SnapMirror synchron "Lizenz installiert". Diese Lizenz ist mit "ONTAP One" enthalten.

- Alle Knoten im Quell-Cluster verwenden ONTAP 9.10.1 oder höher. Für spezifische ONTAP Array Controller-Unterstützung siehe "Hardware Universe".
- Auf allen Knoten im Quell-Cluster läuft die gleiche ONTAP Version.
- Auf allen Knoten im Ziel-Cluster läuft die gleiche ONTAP Version.
- Die ONTAP Version des Ziel-Cluster ist gleich oder höchstens zwei Hauptversionen neuer als die des Quell-Cluster.
- Die Quell- und Ziel-Cluster unterstützen dasselbe IP-Subnetz für den Daten-LIF-Zugriff.
- Sowohl der Quell-Cluster als auch der Ziel-Cluster müssen über mindestens eine Schnittstelle verfügen, die Zugriff auf alle Netzwerke der migrierenden SVMs hat, andernfalls schlägt die Migrationsvorprüfung fehl.
- Die Quell-SVM enthält weniger als die Maximale Anzahl unterstützter Datenvolumes für die Version.
- Am Ziel ist ausreichend Platz für die Volumenplatzierung vorhanden.
- Der Onboard Key Manager oder die externe Schlüsselverwaltung wird auf Clusterebene auf dem Ziel-Cluster konfiguriert, wenn die Quell-SVM verschlüsselte Volumes besitzt.
  - In diesem Fall werden die auf SVM-Ebene auf dem Quell-Cluster konfigurierten Schlüsselmanager nicht zum Ziel-Cluster migriert. Der Ziel-Cluster verwendet den Schlüsselmanager auf Cluster-Ebene.
- Wenn die Quelle verschlüsselte Datenträger verwendet und für NetApp Aggregate Encryption (NAE) konfiguriert ist, muss auch das Ziel für NAE konfiguriert sein.
- Wenn eine SVM zwischen einer Nicht-MetroCluster Konfiguration und einer MetroCluster Konfiguration oder zwischen zwei MetroCluster Konfigurationen migriert wird, sollte die Konfiguration die folgenden Anforderungen erfüllen:

  Die Migration einer SVM zwischen dem lokalen Cluster und dem Partner-Cluster in einer MetroCluster Konfiguration wird nicht unterstützt.

  - Die Quell- und Ziel-MetroCluster-Cluster befinden sich im „normalen“ Zustand. Das bedeutet, dass sie sich weder im Switchover-Modus noch im Zustand „Warten auf Switchback“ befinden.
  - Die Quell- und Ziel-MetroCluster-Cluster befinden sich nicht in einem FC-zu-IP-Übergang oder einer Hardware-Aktualisierung.
  - Sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster muss ONTAP 9.16.1 oder höher ausgeführt werden.
  - Wenn es sich bei der Quelle um einen MetroCluster Cluster handelt, lautet der SVM-Subtyp "sync-source" (nicht "sync-destination").

    Wenn das Ziel ein MetroCluster Cluster ist, ist die auf dem Ziel erstellte SVM immer „sync-source“. Wenn das Ziel kein MetroCluster Cluster ist, ist der SVM-Subtyp immer „default“.

Bewährte Vorgehensweise

Bei der Durchführung einer SVM-Migration ist es eine bewährte Methode, sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster 30 % CPU-Reserve zu lassen, damit die CPU-Workload ausgeführt werden kann.

SVM Operationen

Es sollte geprüft werden, ob Vorgänge mit einer SVM-Migration in Konflikt stehen können:

- Es sind keine Failover-Operationen im Gange
- WAFLIRON kann nicht ausgeführt werden
- Fingerabdruck ist nicht in Bearbeitung
- Vol move, rehost, clone, create, convert oder Analytics werden nicht ausgeführt
- Auf dem Ziel-Cluster läuft keine SVM-Migration. Es ist jeweils nur eine SVM-Migration zulässig.

Unterstützte und nicht unterstützte Funktionen

Die Tabelle zeigt die von SVM Datenmobilität unterstützten ONTAP Funktionen und die ONTAP Versionen, in denen diese Unterstützung verfügbar ist.

Informationen zur Interoperabilität der ONTAP-Versionen zwischen Quell- und Zielsystem bei einer SVM-Migration sind unter "Kompatible ONTAP Versionen für SnapMirror Beziehungen" zu finden.

Funktion	Erste unterstützte Release	Kommentare
Revisionsprotokolle (NFS und SMB)	ONTAP 9.13.1	Für die Migration einer lokalen SVM mit aktiviertem Revisionsprotokoll empfiehlt es sich, das Revisionsprotokoll auf der Quell-SVM zu deaktivieren und anschließend die Migration durchzuführen. Vor der SVM Migration: • "Das Revisionsprotokoll muss auf dem Ziel-Cluster aktiviert sein". • "Der Revisionsprotokoll-Zielpfad vom Quell-SVM muss auf dem Ziel-Cluster erstellt werden".
Autonomous Ransomware Protection	ONTAP 9.12.1	
Cloud Instanzen	Nicht unterstützt	Die Migration von SVMs zwischen lokalen Instanzen und der Cloud wird nicht unterstützt.
Cloud Volumes ONTAP	Nicht unterstützt	
Externer Schlüsselmanager	ONTAP 9.11.1	
FabricPool	Nicht unterstützt	
Fanout-Beziehung (die migrierende Quelle verfügt über ein SnapMirror Quellvolume mit mehr als einem Zielvolume)	ONTAP 9.11.1	
FC SAN	Nicht unterstützt	

Flash Pool	ONTAP 9.12.1	
FlexCache Volumes	Nicht unterstützt	
FlexGroup Volumes	Nicht unterstützt	
IPsec Richtlinien	Nicht unterstützt	
IPv6-LIFs	Nicht unterstützt	
iSCSI SAN	Nicht unterstützt	
Jobplanreplikation	ONTAP 9.11.1	In ONTAP 9.10.1 werden Jobpläne während der Migration nicht repliziert und müssen auf dem Zielsystem manuell erstellt werden. Ab ONTAP 9.11.1 werden die vom Quellsystem verwendeten Jobpläne während der Migration automatisch repliziert.
Load-sharing-Spiegel	Nicht unterstützt	

MetroCluster SVMs	ONTAP 9.16.1	Ab ONTAP 9.16.1 werden die folgenden MetroCluster SVM-Migrationen unterstützt: • Migration einer SVM zwischen einer Nicht-MetroCluster Konfiguration und einer MetroCluster IP Konfiguration • Migration einer SVM zwischen zwei MetroCluster IP-Konfigurationen • Migration einer SVM zwischen einer MetroCluster FC-Konfiguration und einer MetroCluster IP-Konfiguration Hinweis: Sowohl der Quell-Cluster als auch der Ziel-Cluster müssen ONTAP 9.16.1 oder höher ausführen, um die SVM-Migration zu unterstützen. Die folgenden MetroCluster SVM-Migrationen werden nicht von allen ONTAP Versionen unterstützt: • Migration einer SVM zwischen zwei MetroCluster FC-Konfigurationen • Migration einer SVM zwischen einer Nicht-MetroCluster Konfiguration und einer MetroCluster FC Konfiguration • Migration einer SVM zwischen dem lokalen Cluster und dem Partner-Cluster in derselben MetroCluster Konfiguration. Siehe die Voraussetzungen Anleitung zur Migration einer SVM in einer MetroCluster Konfiguration.
NetApp Aggregate Encryption (NAE)	ONTAP 9.11.1	NAE Volumes müssen auf einem NAE unterstützenden Ziel platziert werden. Wenn kein NAE Ziel verfügbar ist, schlägt der Migrationsvorgang fehl.
NDMP Konfigurationen	Nicht unterstützt	
NetApp Volume Encryption (NVE)	ONTAP 9.10.1	NVE Volumes werden als NVE Volumes auf dem Ziel migriert.
NFS v3, NFS v4.1 und NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.12.1	
NFSv4.1 mit pNFS	ONTAP 9.14.1	
NVMe over Fabric	Nicht unterstützt	
Onboard Key Manager (OKM) mit aktiviertem Common Criteria-Modus auf dem Quell-Cluster	Nicht unterstützt	

ONTAP Select	Nicht unterstützt	Die Migration von SVMs zu oder von ONTAP Select Instanzen wird nicht unterstützt.
Qtrees	ONTAP 9.14.1	
Kontingente	ONTAP 9.14.1	
S3	Nicht unterstützt	
S3 NAS-Buckets auf FlexVol Volumes	ONTAP 9.20.1	Die SVM-Migration kann fortgesetzt werden, wenn die Quell-SVM S3-NAS-Buckets enthält, die auf FlexVol Volumes gehostet sind.
SMB-Protokoll	ONTAP 9.12.1 Das SMB1-Protokoll wird jedoch nicht unterstützt.	SMB-Migrationen sind mit Unterbrechungen verbunden und erfordern nach der Migration eine Aktualisierung des Clients.
SnapMirror Cloud-Beziehungen	ONTAP 9.12.1	Ab ONTAP 9.12.1 muss beim Migrieren einer lokalen SVM mit SnapMirror Cloud-Beziehungen der Ziel-Cluster die "SnapMirror Cloud-Lizenz" installiert haben und über ausreichend Kapazität verfügen, um das Verschieben der Kapazität in den Volumes zu unterstützen, die in die Cloud gespiegelt werden.
SnapMirror asynchrones Ziel	ONTAP 9.12.1	

SnapMirror asynchrone Quelle	ONTAP 9.11.1	• Transfers können während des größten Teils der Migration in FlexVol SnapMirror Beziehungen wie gewohnt fortgesetzt werden. • Laufende Übertragungen werden während der Umstellung abgebrochen, und neue Übertragungen schlagen während der Umstellung fehl. Sie können erst nach Abschluss der Migration wieder aufgenommen werden. • Geplante Übertragungen, die während der Migration abgebrochen oder verpasst wurden, werden nach Abschluss der Migration nicht automatisch gestartet.  Wenn eine SnapMirror Quelle migriert wird, verhindert ONTAP das Löschen des Volumes nach der Migration erst, wenn das SnapMirror Update erfolgt ist. Dies geschieht, weil SnapMirror-bezogene Informationen für migrierte SnapMirror Quellvolumes erst nach Abschluss der Migration und nach dem ersten Update verfügbar sind.
SMTape Einstellungen	Nicht unterstützt	
SnapLock	Nicht unterstützt	
SnapMirror Active Sync	Nicht unterstützt	
SnapMirror SVM-Peer-Beziehungen	ONTAP 9.12.1	
SnapMirror SVM-Notfallwiederherstellung	Nicht unterstützt	
SnapMirror synchron	Nicht unterstützt	
Snapshots	ONTAP 9.10.1	
Manipulationssichere Schnappschussverriegelung	ONTAP 9.14.1	Manipulationssichere Snapshot-Sperrung ist nicht gleichzusetzen mit SnapLock. SnapLock Enterprise und SnapLock Compliance werden weiterhin nicht unterstützt.
Virtuelle IP LIFs/BGP	Nicht unterstützt	
ONTAP Tools for VMware vSphere	Nicht unterstützt	

Volumenklone	Nicht unterstützt	
Vscan	Nicht unterstützt	Die Migration von Vscan-fähigen SVMs wird nicht unterstützt.
vStorage	Nicht unterstützt	Eine Migration ist nicht zulässig, wenn vStorage aktiviert ist. Für eine Migration muss die vStorage Option deaktiviert und nach Abschluss der Migration wieder aktiviert werden.

Unterstützte Vorgänge während der Migration

Die folgende Tabelle zeigt die innerhalb des migrierenden SVM unterstützten Volumenoperationen basierend auf dem Migrationsstatus:

Volume-Betrieb	SVM Migrationsstatus		
	In Bearbeitung	**Pausiert**	**Umschaltung**
Erstellen	Nicht erlaubt	Erlaubt	Nicht unterstützt
Löschen	Nicht erlaubt	Erlaubt	Nicht unterstützt
Dateisystemanalyse deaktivieren	Erlaubt	Erlaubt	Nicht unterstützt
Dateisystemanalyse aktivieren	Nicht erlaubt	Erlaubt	Nicht unterstützt
Ändern	Erlaubt	Erlaubt	Nicht unterstützt
Offline/Online	Nicht erlaubt	Erlaubt	Nicht unterstützt
Verschieben/Neuhosting	Nicht erlaubt	Erlaubt	Nicht unterstützt
Qtree erstellen/ändern	Nicht erlaubt	Erlaubt	Nicht unterstützt
Kontingent erstellen/ändern	Nicht erlaubt	Erlaubt	Nicht unterstützt
Umbenennen	Nicht erlaubt	Erlaubt	Nicht unterstützt
Größe ändern	Erlaubt	Erlaubt	Nicht unterstützt
Beschränken	Nicht erlaubt	Erlaubt	Nicht unterstützt
Snapshot-Attribute ändern	Erlaubt	Erlaubt	Nicht unterstützt
Snapshot Autodelete ändern	Erlaubt	Erlaubt	Nicht unterstützt
Snapshot erstellen	Erlaubt	Erlaubt	Nicht unterstützt
Snapshot löschen	Erlaubt	Erlaubt	Nicht unterstützt
Datei aus Snapshot wiederherstellen	Erlaubt	Erlaubt	Nicht unterstützt

Informationen nach der Migration

- Nach der Migration haben lokale Snapshot-Richtlinien die Erweiterung -MIG, was einige Automatisierungen beeinträchtigen kann. Es empfiehlt sich, nach dieser Erweiterung zu suchen und die Richtlinien bei Bedarf umzubenennen.
- Migrierte Vault-Ziel-SnapMirror-Volumes müssen neu synchronisiert werden, um den Schutz wieder zu aktivieren. Die Vault-Neusynchronisierung ist erforderlich, da die Migration eine neue Baseline zwischen

den Migrations-SVMs erstellt, die aktueller ist als die vorherige Baseline des Vaults. Durch die Neusynchronisierung wird der Vault reaktiviert, wobei alle Daten gelöscht werden, die neuer als die aktuelle Vault-Baseline sind, insbesondere der während der Migration erstellte Snapshot.

Migration einer ONTAP SVM

Nach Abschluss einer SVM-Migration werden die Clients automatisch auf den Ziel-Cluster umgeschaltet und die nicht mehr benötigte SVM aus dem Quell-Cluster entfernt. Automatische Umschaltung und automatische Quellbereinigung sind standardmäßig aktiviert. Bei Bedarf kann die automatische Client-Umschaltung deaktiviert werden, um die Migration vor der Umschaltung zu unterbrechen, und auch die automatische Quell-SVM-Bereinigung kann deaktiviert werden.

Über diese Aufgabe

- Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Wenn Sie ein ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) besitzen:
  - Die Migration einer SVM von einem ASA Cluster zu einem ASA r2 Cluster erfolgt gemäß "diese Schritte"
  - Ab ONTAP 9.20.1 erfolgt die Migration einer SVM von einem ASA r2 Cluster zu einem ASA oder AFF Cluster gemäß "diese Schritte".
- Ab ONTAP 9.19.1 werden Direct-Attachment FC- und FC-NVMe-Konfigurationen für bestimmte AFF, ASA r2 und FAS Systeme unterstützt. Direct-Attachment Konfigurationen unterstützen keine SVM Migration.

Migrieren einer ONTAP SVM mit aktivierter automatischer Umschaltung

Standardmäßig werden die Clients nach Abschluss der Migration automatisch auf den Ziel-Cluster umgeschaltet, und die nicht mehr benötigte SVM wird aus dem Quell-Cluster entfernt.

Schritte

1. Vom Ziel-Cluster aus die Migrationsvorprüfungen ausführen:

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true
```

2. Von dem Ziel-Cluster aus die SVM-Migration starten:

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
```

3. Migrationsstatus prüfen:

```
vserver migrate show
```

   Der Status zeigt „migrate-complete“ an, wenn die SVM-Migration abgeschlossen ist.

Migrieren einer ONTAP SVM mit deaktivierter automatischer Client-Umstellung

Sie können die Option `-auto-cutover false` verwenden, um die Migration anzuhalten, wenn normalerweise eine automatische Client-Umstellung erfolgt, und die Umstellung später manuell durchführen. Siehe Manuelle Umstellung der Clients nach der SVM-Migration.

Schritte

1. Vom Ziel-Cluster aus die Migrationsvorprüfungen ausführen:

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true
```

2. Von dem Ziel-Cluster aus die SVM-Migration starten:

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-auto-cutover false`
```

3. Migrationsstatus prüfen:

```
vserver migrate show
```

Der Status wird als „bereit für die Umstellung“ angezeigt, wenn die SVM-Migration die asynchronen Datenübertragungen abgeschlossen hat und das System für den Umstellungsvorgang bereit ist.

Migration einer ONTAP SVM mit deaktivierter Quellbereinigung

Sie können die Option `-auto-source-cleanup false` der erweiterten Berechtigung verwenden, um die Entfernung der Quell-SVM nach der Umstellung zu deaktivieren und die Quellbereinigung anschließend nach der Umstellung manuell auszulösen. Siehe Quell-SVM manuell entfernen.

Schritte

1. Vom Ziel-Cluster aus die Migrationsvorprüfungen ausführen:

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true
```

2. Von dem Ziel-Cluster aus die SVM-Migration starten:

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-auto-source-cleanup false`
```

3. Migrationsstatus prüfen:

```
vserver migrate show
```

Der Status zeigt „bereit für die Quellbereinigung“ an, wenn der SVM-Migrationsübergang abgeschlossen ist und die SVM auf dem Quell-Cluster entfernt werden kann.

Überwachung der ONTAP Volume Migration

Zusätzlich zur Überwachung der gesamten SVM-Migration mit dem `vserver migrate show` Befehl kann auch der Migrationsstatus der in der SVM enthaltenen Volumes überwacht werden.

Schritte

1. Im Ziel-Cluster den Status der Volume-Migration prüfen:

```
vserver migrate show-volume
```

ONTAP SVM Migration anhalten und fortsetzen

Möglicherweise möchten Sie eine SVM-Migration anhalten, bevor der Migrationsumstieg beginnt. Sie können eine SVM-Migration mit dem `vserver migrate pause` Befehl anhalten.

Migration pausieren

Sie können eine SVM-Migration pausieren, bevor der Client-Cutover beginnt, indem Sie den `vserver migrate pause` Befehl verwenden.

Einige Konfigurationsänderungen sind eingeschränkt, wenn ein Migrationsvorgang läuft; ab ONTAP 9.12.1 kann jedoch eine Migration angehalten werden, um bestimmte eingeschränkte Konfigurationen und einige Fehlerzustände zu beheben, sodass Konfigurationsprobleme korrigiert werden können, die möglicherweise den Fehler verursacht haben. Einige der Fehlerzustände, die beim Anhalten der SVM-Migration behoben werden können, umfassen Folgendes:

- `setup-configuration-failed`
- `migrate-failed`

Schritte

1. Vom Ziel-Cluster aus die Migration anhalten:

```
vserver migrate pause -vserver <vserver name>
```

Migrationen fortsetzen

Wenn eine pausierte SVM-Migration fortgesetzt werden soll oder wenn eine SVM-Migration fehlgeschlagen ist, kann der `vserver migrate resume` Befehl verwendet werden.

Schritte

1. Vom Ziel-Cluster aus die SVM-Migration fortsetzen:

```
vserver migrate resume
```

2. Es sollte überprüft werden, ob die SVM-Migration wieder aufgenommen wurde, und der Fortschritt kann überwacht werden:

```
vserver migrate show
```

Eine ONTAP SVM-Migration abbrechen

Wenn eine SVM-Migration vor deren Abschluss abgebrochen werden muss, kann der `vserver migrate abort` Befehl verwendet werden. Eine SVM-Migration kann nur abgebrochen werden, wenn sich der Vorgang im Status „Angehalten“ oder „Fehlgeschlagen“ befindet. Eine SVM-Migration kann nicht abgebrochen werden, wenn der Status „cutover-started“ ist oder nachdem der Cutover abgeschlossen wurde. Die `abort` Option kann nicht verwendet werden, wenn eine SVM-Migration im Gange ist.

Schritte

1. Im Ziel-Cluster den Migrationsstatus prüfen:

```
vserver migrate show -vserver <SVM_name>
```

2. Migration abbrechen:

```
vserver migrate abort -vserver <SVM_name>
```

3. Der Fortschritt des Abbruchvorgangs kann überprüft werden:

```
vserver migrate show
```

   Der Migrationsstatus zeigt „migrate-aborting“ an, solange der Abbruchvorgang läuft. Nach Abschluss des Abbruchvorgangs wird im Migrationsstatus nichts angezeigt.

Manuelle Umstellung der Clients nach einer ONTAP SVM Migration

Standardmäßig wird die Client-Umstellung auf den Ziel-Cluster automatisch durchgeführt, sobald die SVM-Migration den Status „ready-for-cutover“ erreicht hat. Wenn die automatische Client-Umstellung deaktiviert wird, ist die Client-Umstellung manuell durchzuführen.

Schritte

1. Manuelle Clientumstellung:

```
vserver migrate cutover -vserver <SVM_name>
```

2. Status des Umstellungsvorgangs prüfen:

```
vserver migrate show
```

Die Quell-ONTAP SVM wird nach der Clientumstellung manuell entfernt.

Wenn die SVM-Migration mit deaktivierter Quellbereinigung durchgeführt wurde, kann die Quell-SVM nach Abschluss der Clientumstellung manuell entfernt werden.

Schritte

1. Überprüfen, ob der Status für die Quellbereinigung bereit ist:

```
vserver migrate show
```

2. Quell-Cluster bereinigen:

```
vserver migrate source-cleanup -vserver <SVM_name>
```

HA Pair Verwaltung

Informationen zur Verwaltung von HA-Paaren in ONTAP Clustern

Clusterknoten sind in Hochverfügbarkeitspaaren (HA-Paaren) konfiguriert, um Fehlertoleranz und unterbrechungsfreie Vorgänge zu ermöglichen. Fällt ein Knoten aus oder muss ein Knoten für routinemäßige Wartungsarbeiten heruntergefahren werden, kann der Partner dessen Speicher übernehmen und weiterhin Daten daraus bereitstellen. Der Partner gibt den Speicher zurück, wenn der Knoten wieder online ist.

Die HA-Paar-Controller-Konfiguration besteht aus einem Paar übereinstimmender Speichercontroller (lokaler Node und Partner-Node). Jeder dieser Nodes ist mit den Festplatten-Shelfs des jeweils anderen verbunden. Wenn ein Node in einem HA-Paar einen Fehler feststellt und die Datenverarbeitung stoppt, erkennt der Partner den Ausfallstatus des Partners und übernimmt die gesamte Datenverarbeitung von diesem Controller.

Die Übernahme ist der Prozess, bei dem ein Node die Kontrolle über den Storage seines Partners übernimmt.

Giveback ist der Prozess, bei dem der Speicher an den Partner zurückgegeben wird.

Standardmäßig erfolgen Übernahmen automatisch in einer der folgenden Situationen:

- Auf einem Node tritt ein Software- oder Systemausfall auf, der zu einem Panic führt. Die HA Pair Controller übernehmen automatisch auf ihren Partner-Node. Nachdem sich der Partner vom Panic erholt und hochgefahren ist, führt der Node automatisch ein Giveback durch und versetzt den Partner wieder in den Normalbetrieb.
- Ein Systemausfall tritt auf einem Node auf, und der Node kann nicht neu gestartet werden. Beispielsweise übernehmen bei einem Ausfall eines Node aufgrund eines Stromausfalls die HA Pair Controller automatisch auf den Partner-Node und stellen Daten vom verbleibenden Storage Controller bereit.

> Wenn der Speicher eines Knotens gleichzeitig ebenfalls die Stromversorgung verliert, ist eine Standardübernahme nicht möglich.

- Heartbeat-Nachrichten werden vom Partner des Knotens nicht empfangen. Dies kann auftreten, wenn der Partner einen Hardware- oder Softwarefehler (zum Beispiel einen Interconnect-Fehler) hatte, der zwar keinen Panikzustand auslöste, aber dennoch die korrekte Funktion verhinderte.
- Sie halten einen der Knoten an, ohne den `-f` oder `-inhibit-takeover true` Parameter zu verwenden.

> In einem Zwei-Node-Cluster mit aktiviertem Cluster HA führt das Anhalten oder Neustarten eines Knotens mithilfe des `-inhibit-takeover true` Parameters dazu, dass beide Knoten keine Daten mehr liefern, es sei denn, zuerst wird Cluster HA deaktiviert und dann dem Knoten, der online bleiben soll, epsilon zugewiesen.

- Sie starten einen der Knoten neu, ohne den `-inhibit-takeover true` Parameter zu verwenden. (Der `-onboot` Parameter des `storage failover` Befehls ist standardmäßig aktiviert.)
- Das Fernverwaltungsgerät (Service Processor) erkennt einen Ausfall des Partnerknotens. Dies ist nicht zutreffend, wenn Hardware-unterstützt Takeover deaktiviert ist.

Übernahmen können auch manuell mit dem `storage failover takeover` Befehl initiiert werden.

Ab ONTAP 9.18.1 kann die verschlüsselte Kommunikation zwischen HA-Paar-Nodes konfiguriert werden. Weitere Informationen finden sich unter "Verschlüsselung für ONTAP HA Datenverkehr konfigurieren".

Resilienz von Clustern und diagnostische Verbesserungen

Ab ONTAP 9.9.1 verbessern die folgenden Erweiterungen hinsichtlich Ausfallsicherheit und Diagnose den Clusterbetrieb:

- **Portüberwachung und -vermeidung**: In Zwei-Knoten Cluster ohne Switches vermeidet das System Ports, bei denen es zu vollständigem Paketverlust (Verbindungsverlust) kommt. In ONTAP 9.8 und früher war diese Funktionalität nur in Konfigurationen mit Switches verfügbar.
- **Automatisches Node-Failover**: Kann ein Node keine Daten über sein Cluster-Netzwerk bereitstellen, sollte dieser Node keine Festplatten besitzen. Stattdessen sollte der HA-Partner übernehmen, sofern dieser funktionsfähig ist.
- **Befehle zur Analyse von Verbindungsproblemen**: Mit dem folgenden Befehl wird angezeigt, bei welchen Clusterpfaden Paketverluste auftreten: `network interface check cluster-connectivity show`

  Weitere Informationen zu `network interface check cluster-connectivity show` finden sich in der "ONTAP-Befehlsreferenz".

Wie Hardware-unterstütztes Takeover in ONTAP funktioniert

Die standardmäßig aktivierte Hardware-unterstützt Takeover-Funktion kann den Übernahmeprozess durch die Verwendung des Fernverwaltungsgeräts (Service Processor) eines Knotens beschleunigen.

Erkennt das Fernverwaltungsgerät einen Fehler, leitet es umgehend die Übernahme ein, anstatt darauf zu warten, dass ONTAP erkennt, dass der Heartbeat des Partners ausgefallen ist. Tritt ein Fehler auf, ohne dass diese Funktion aktiviert ist, wartet der Partner, bis er feststellt, dass der Knoten keinen Heartbeat mehr sendet, bestätigt den Ausfall und leitet dann die Übernahme ein.

Die Hardware-unterstützte Übernahmefunktion nutzt den folgenden Prozess, um diese Wartezeit zu vermeiden:

1. Das Fernverwaltungsgerät überwacht das lokale System auf bestimmte Fehlertypen.
2. Wird ein Fehler erkannt, sendet das Fernverwaltungsgerät umgehend eine Warnmeldung an den Partnerknoten.
3. Nach Erhalt der Benachrichtigung leitet der Partner die Übernahme ein.

Systemereignisse, die eine Hardware-unterstützte Übernahme auslösen

Der Partnerknoten kann abhängig von der Art der Warnung, die er vom Remote-Management-Gerät (Service Processor) erhält, eine Übernahme auslösen.

Alarm	Übernahme nach Erhalt eingeleitet?	Beschreibung
abnormaler_Neustart	Nein	Es kam zu einem abnormalen Neustart des Knotens.
l2_watchdog_reset	Ja	Die Systemüberwachungshardware erkannte einen L2-Reset. Das Fernverwaltungsgerät stellte fest, dass die System-CPU nicht reagierte und setzte das System zurück.
Verlust des Herzschlagsignals	Nein	Das Fernverwaltungsgerät empfängt keine Heartbeat-Nachricht mehr vom Knoten. Diese Warnung bezieht sich nicht auf die Heartbeat-Nachrichten zwischen den Knoten im HA-Paar, sondern auf die Heartbeat-Nachricht zwischen dem Knoten und seinem lokalen Fernverwaltungsgerät.
periodische Nachricht	Nein	Während eines normalen Hardware-unterstützten Übernahmevorgangs wird eine periodische Nachricht gesendet.
power_cycle_via_sp	Ja	Das Fernverwaltungsgerät hat die Systemstromversorgung aus- und wieder eingeschaltet.
Stromausfall	Ja	Auf dem Node ist ein Stromausfall aufgetreten. Das Remote-Management-Gerät verfügt über eine Stromversorgung, die nach einem Stromausfall für kurze Zeit aufrechterhalten wird, sodass der Stromausfall dem Partner gemeldet werden kann.

power_off_via_sp	Ja	Das Fernverwaltungsgerät hat das System ausgeschaltet.
reset_via_sp	Ja	Das Fernverwaltungsgerät hat das System zurückgesetzt.
prüfen	Nein	Eine Testnachricht wird gesendet, um eine Hardware-unterstützte Übernahme zu verifizieren.

Verwandte Informationen

"Hardware-unterstützte (HWassist) Übernahme, Leitfaden zur Fehlerbehebung"

Wie automatisches Takeover und Giveback in ONTAP funktionieren

Die automatischen Takeover- und Rückgabevorgänge können zusammenwirken, um Kundenausfälle zu reduzieren und zu vermeiden.

Standardmäßig übernimmt der Partnerknoten automatisch, wenn ein Knoten im HA-Paar abstürzt, neu startet oder anhält, und gibt den Speicher zurück, wenn der betroffene Knoten neu startet. Das HA-Paar setzt dann den normalen Betriebszustand fort.

Automatisches Takeover kann auch erfolgen, wenn einer der Knoten nicht mehr reagiert.

Die automatische Rückgabe erfolgt standardmäßig. Wenn Sie die Auswirkungen der Rückgabe auf Clients steuern möchten, kann die automatische Rückgabe deaktiviert und der `storage failover modify -auto -giveback false -node <node>` Befehl verwendet werden. Vor der automatischen Rückgabe (unabhängig vom Auslöser) wartet der Partnerknoten eine festgelegte Zeitspanne, die durch den `-delay-seconds` Parameter des `storage failover modify` Befehls gesteuert wird. Die Standardverzögerung beträgt 600 Sekunden.

Dieses Verfahren vermeidet einen einzelnen, längeren Ausfall, der die für Folgendes benötigte Zeit umfasst:

- Die Übernahmeoperation
- Der übernommene Knoten wird so weit hochgefahren, bis er bereit für die Rückgabe ist.
- Die Rückgabeaktion

Falls das automatische Giveback für eines der Nicht-Root-Aggregate fehlschlägt, unternimmt das System automatisch zwei weitere Versuche, das Giveback abzuschließen.

> Während des Takeover-Prozesses startet der automatische Giveback-Prozess, bevor der Partnerknoten für das Giveback bereit ist. Wenn das Zeitlimit des automatischen Giveback-Prozesses abläuft und der Partnerknoten weiterhin nicht bereit ist, wird der Timer neu gestartet. Daraus ergibt sich, dass die Zeit zwischen der Bereitschaft des Partnerknotens und der tatsächlichen Durchführung des Givebacks kürzer sein kann als die automatische Giveback-Zeit.

Was geschieht während eines Takeovers

Wenn ein Knoten die Funktion seines Partners übernimmt, werden weiterhin Daten in den Aggregaten und Volumes des Partners bereitgestellt und aktualisiert.

Im Rahmen des Takeover-Prozesses erfolgen folgende Schritte:

1. Wird das ausgehandelte Takeover vom Benutzer initiiert, werden die aggregierten Daten vom Partnerknoten auf den Knoten verschoben, der das Takeover durchführt. Es kommt zu einer kurzen Unterbrechung, da der aktuelle Eigentümer jedes Aggregats (mit Ausnahme des Root-Aggregat) auf den Takeover-Knoten wechselt. Diese Unterbrechung ist kürzer als eine Unterbrechung, die bei einem Takeover ohne Aggregatverschiebung auftritt.

   > Eine verhandelte Übernahme während einer Panik kann im Falle einer Panik nicht erfolgen. Eine Übernahme kann durch einen Fehler ausgelöst werden, der nicht mit einer Panik zusammenhängt. Ein Fehler tritt auf, wenn die Kommunikation zwischen einem Knoten und seinem Partner verloren geht, was auch als Heartbeat-Verlust bezeichnet wird. Wenn eine Übernahme aufgrund eines Fehlers erfolgt, kann der Ausfall länger dauern, da der Partnerknoten Zeit benötigt, um den Heartbeat-Verlust zu erkennen.

   - Sie können den Fortschritt mit dem `storage failover show-takeover` Befehl überwachen.
   - Die Aggregatverschiebung kann während dieser Takeover-Instanz vermieden werden, indem der `-bypass-optimization` Parameter mit dem `storage failover takeover` Befehl verwendet wird.

     Aggregate werden bei geplanten Takeover-Operationen nacheinander verlagert, um die Ausfallzeit für Clients zu reduzieren. Wenn die Aggregate-Verlagerung umgangen wird, tritt bei geplanten Takeover-Ereignissen eine längere Ausfallzeit für Clients auf.

2. Wenn die vom Benutzer initiierte Übernahme eine ausgehandelte Übernahme ist, fährt der Zielknoten ordnungsgemäß herunter, gefolgt von der Übernahme des Root-Aggregats und aller Aggregate, die im ersten Schritt nicht verschoben wurden.
3. Daten-LIFs (logische Schnittstellen) migrieren gemäß den LIF-Failover-Regeln vom Zielknoten auf den Übernahmeknoten oder auf einen anderen Knoten im Cluster. Die LIF-Migration kann vermieden werden, indem der `-skip-lif-migration` Parameter mit dem `storage failover takeover` Befehl verwendet wird. Im Fall einer benutzerinitiierten Übernahme werden die Daten-LIFs vor Beginn der Speicherübernahme migriert. Im Fall eines Systemabsturzes oder Ausfalls können die Daten-LIFs je nach Konfiguration zusammen mit dem Speicher oder nach Abschluss der Übernahme migriert werden.
4. Bestehende SMB-Sitzungen werden bei einem Takeover getrennt.

   > Aufgrund der Funktionsweise des SMB-Protokolls werden alle SMB-Sitzungen unterbrochen (mit Ausnahme von SMB 3.0-Sitzungen, die mit Freigaben verbunden sind, für die die Eigenschaft „Kontinuierliche Verfügbarkeit“ aktiviert ist). SMB 1.0- und SMB 2.x-Sitzungen können nach einem Takeover offene Dateihandles nicht wiederherstellen, daher ist das Takeover unterbrechend und es kann zu Datenverlust kommen.

5. SMB 3.0-Sitzungen, die zu Freigaben mit aktivierter Eigenschaft „Continuous Availability“ eingerichtet sind, können nach einem Takeover-Ereignis die Verbindung zu den getrennten Freigaben wiederherstellen. Wenn an Ihrem Standort SMB 3.0-Verbindungen zu Microsoft Hyper-V verwendet werden und die Eigenschaft „Continuous Availability“ auf den zugehörigen Freigaben aktiviert ist, sind Takeover-Ereignisse für diese Sitzungen unterbrechungsfrei.

Was passiert, wenn ein Knoten, der ein Takeover durchführt, einen Panic-Zustand erreicht?

Wenn der Knoten, der das Takeover durchführt, innerhalb von 60 Sekunden nach Einleitung des Takeovers in Panik gerät, treten die folgenden Ereignisse ein:

- Der Knoten, der einen Panic ausgelöst hat, wird neu gestartet.

- Nach dem Neustart führt der Knoten Selbstwiederherstellungsoperationen durch und befindet sich nicht mehr im Takeover-Modus.
- Failover ist deaktiviert.
- Falls der Knoten nach der Aktivierung des Storage-Failovers noch einige Aggregate des Partners besitzt, können diese Aggregate mit dem `storage failover giveback` Befehl an den Partner zurückgegeben werden.

Was geschieht während der Rückgabe

Der lokale Knoten gibt die Besitzrechte an den Partnerknoten zurück, wenn Probleme behoben sind, wenn der Partnerknoten hochfährt oder wenn die Rückgabe eingeleitet wird.

Der folgende Prozess läuft im Rahmen einer normalen Rückgabeoperation ab. In dieser Darstellung hat Node A die Kontrolle über Node B übernommen. Alle Probleme auf Node B wurden behoben und es ist bereit, die Datenbereitstellung wieder aufzunehmen.

1. Alle Probleme auf Knoten B wurden behoben und es wird die folgende Meldung angezeigt: `Waiting for giveback`
2. Die Rückgabe wird durch den `storage failover giveback`-Befehl oder durch automatisches Giveback eingeleitet, wenn das System entsprechend konfiguriert ist. Damit beginnt der Prozess, bei dem die Besitzrechte an den Aggregaten und Volumes von Node B von Node A zurück an Node B übertragen werden.
3. Knoten A gibt zuerst die Kontrolle über das Root-Aggregat zurück.
4. Knoten B schließt den Hochfahrvorgang bis zum Erreichen des normalen Betriebszustands ab.
5. Sobald Knoten B im Bootvorgang den Punkt erreicht hat, an dem er die Nicht-Root-Aggregate akzeptieren kann, gibt Knoten A die Besitzrechte an den übrigen Aggregaten nacheinander zurück, bis die Rückgabe abgeschlossen ist. Der Fortschritt der Rückgabe kann mit dem `storage failover show-giveback` Befehl überwacht werden.

> Der `storage failover show-giveback`Befehl zeigt keine Informationen über alle Vorgänge während des Storage Failover Giveback-Vorgangs an (und ist auch nicht dafür vorgesehen). Mit dem `storage failover show`Befehl lassen sich zusätzliche Details zum aktuellen Failover-Status des Knotens anzeigen, etwa ob der Knoten voll funktionsfähig ist, ein Takeover möglich ist und das Giveback abgeschlossen ist.

   Die E/A wird für jedes Aggregat wieder aufgenommen, nachdem die Rückgabe für dieses Aggregat abgeschlossen ist, was das gesamte Ausfallfenster verkürzt.

HA-Richtlinie und ihre Auswirkungen auf Takeover und Giveback

ONTAP weist einem Aggregat automatisch eine HA-Richtlinie mit CFO (Controller-Failover) und SFO (Storage-Failover) zu. Diese Richtlinie legt fest, wie Speicher-Failover-Operationen für das Aggregat und seine Volumes ablaufen.

Die beiden Optionen CFO und SFO bestimmen die Aggregat-Steuerungssequenz, die ONTAP während Storage-Failover- und Giveback-Vorgängen verwendet.

Obwohl die Begriffe CFO und SFO umgangssprachlich manchmal für Storage-Failover-Operationen (Takeover und Giveback) verwendet werden, bezeichnen sie tatsächlich die HA-Richtlinie, die den Aggregaten zugewiesen ist. Beispielsweise beziehen sich die Begriffe SFO Aggregate oder CFO Aggregate einfach auf die HA-Richtlinienzuweisung des Aggregats.

Die HA-Richtlinien wirken sich wie folgt auf Takeover- und Giveback-Vorgänge aus:

- Auf ONTAP-Systemen erstellte Aggregate (mit Ausnahme des Root-Aggregats, das das Root-Volume enthält) haben eine HA-Richtlinie von SFO. Eine manuell initiierte Übernahme ist hinsichtlich der Performance optimiert, indem SFO-Aggregate (Nicht-Root-Aggregate) vor der Übernahme seriell zum Partner verschoben werden. Während des Rückgabeprozesses werden Aggregate seriell zurückgegeben, nachdem das übernommene System gestartet ist und die Management-Anwendungen online sind, sodass der Node seine Aggregate empfangen kann.
- Da bei einer Aggregatverschiebung die Eigentumsrechte an der Aggregatfestplatte neu zugewiesen und die Kontrolle von einem Knoten auf seinen Partner übertragen werden, sind nur Aggregate mit einer HA-Richtlinie vom Typ SFO für eine Aggregatverschiebung geeignet.
- Das Root-Aggregat verfügt stets über die HA-Richtlinie CFO und wird zu Beginn des Rückgabevorgangs zurückgegeben. Dies ist erforderlich, damit das übernommene System starten kann. Alle anderen Aggregate werden nacheinander zurückgegeben, nachdem das übernommene System den Startvorgang abgeschlossen hat und die Managementanwendungen online sind, sodass der Knoten seine Aggregate empfangen kann.

> Die Änderung der HA-Richtlinie eines Aggregats von SFO auf CFO ist ein Wartungsmodus-Vorgang. Diese Einstellung sollte nur auf Anweisung eines Kundendienstmitarbeiters geändert werden.

Wie sich Hintergrundaktualisierungen auf Takeover und Giveback auswirken

Hintergrundaktualisierungen der Festplatten-Firmware wirken sich unterschiedlich auf HA-Paar-Takeover-, Giveback- und Aggregatverschiebungsoperationen aus, je nachdem, wie diese Operationen initiiert werden.

Die folgende Liste beschreibt, wie sich Hintergrund-Firmware-Updates der Festplatte auf Takeover, Giveback und Aggregatverschiebung auswirken:

- Wenn auf einer Festplatte eines der beiden Knoten ein Firmware-Update im Hintergrund durchgeführt wird, verzögern sich manuell initiierte Takeover-Vorgänge, bis das Firmware-Update auf dieser Festplatte abgeschlossen ist. Dauert das Firmware-Update im Hintergrund länger als 120 Sekunden, werden die Takeover-Vorgänge abgebrochen und müssen nach Abschluss des Firmware-Updates manuell neu gestartet werden. Wenn das Takeover mit dem `-bypass-optimization`-Parameter des `storage failover takeover`-Befehls auf `true` gesetzt initiiert wurde, hat das im Hintergrund laufende Firmware-Update auf dem Zielknoten keine Auswirkungen auf das Takeover.
- Wenn auf einer Festplatte des Quellknotens (oder Übernahmeknotens) ein Hintergrund-Firmware-Update stattfindet und die Übernahme manuell mit dem `-options` Parameter des `storage failover takeover` Befehls auf `immediate` gesetzt eingeleitet wurde, beginnen die Übernahmevorgänge sofort.
- Falls auf einer Festplatte eines Knotens im Hintergrund ein Firmware-Update durchgeführt wird und es zu einem Systemabsturz kommt, beginnt sofort die Übernahme des betroffenen Knotens.
- Wird auf einer Festplatte eines der beiden Knoten gerade ein Hintergrund-Firmware-Update durchgeführt, verzögert sich die Rückgabe der Datenaggregate, bis das Firmware-Update auf dieser Festplatte abgeschlossen ist.
- Dauert die Aktualisierung der Festplatten-Firmware im Hintergrund länger als 120 Sekunden, werden die Rückgabevorgänge abgebrochen und müssen nach Abschluss der Festplatten-Firmware-Aktualisierung manuell neu gestartet werden.
- Wird auf einem der beiden Knoten im Hintergrund ein Firmware-Update für eine Festplatte durchgeführt, werden die Aggregatverschiebungsvorgänge verzögert, bis das Firmware-Update auf dieser Festplatte abgeschlossen ist. Dauert das Firmware-Update im Hintergrund länger als 120 Sekunden, werden die Aggregatverschiebungsvorgänge abgebrochen und müssen nach Abschluss des Firmware-Updates

manuell neu gestartet werden. Wurde die Aggregatverschiebung mit dem `-override-destination-checks` des `storage aggregate relocation` Befehls auf `true` initiiert, hat das im Hintergrund laufende Firmware-Update auf dem Zielknoten keine Auswirkungen auf die Aggregatverschiebung.

Verwandte Informationen

- "Storage-Aggregat-Verlagerung"
- "Storage-Failover-Giveback"
- "storage failover modify"
- "storage failover show-giveback"
- "Storage-Failover-Takeover"

ONTAP automatische Takeover-Befehle

Automatisches Takeover ist auf allen unterstützten NetApp FAS, AFF und ASA Plattformen standardmäßig aktiviert. Es kann erforderlich sein, das Standardverhalten zu ändern und zu steuern, wann ein automatisches Takeover erfolgt, wenn der Partnerknoten neu startet, einen Systemabsturz hat oder angehalten wird.

Wenn das Takeover automatisch erfolgen soll, wenn der Partnerknoten…	Verwenden Sie diesen Befehl…
Neustarts oder Anhalten	`storage failover modify -node nodename -onreboot true`
Panics	`storage failover modify -node nodename -onpanic true`

E-Mail-Benachrichtigung aktivieren, wenn die Takeover-Funktion deaktiviert ist

Um umgehend benachrichtigt zu werden, falls die Takeover-Funktion deaktiviert wird, sollte das System so konfiguriert werden, dass automatische E-Mail-Benachrichtigungen für die EMS-Meldungen „`takeover impossible`“ aktiviert sind:

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

Verwandte Informationen

- "storage failover modify"

ONTAP automatische Rückgabebefehle

Standardmäßig gibt der übernehmende Partnerknoten den Speicher automatisch wieder zurück, wenn der offline gegangene Knoten wieder online ist, wodurch die High-Availability-Paarbeziehung wiederhergestellt wird. In den meisten Fällen ist dies das gewünschte Verhalten. Falls die automatische Rückgabe deaktiviert werden muss, zum Beispiel um die Ursache der Übernahme vor der Rückgabe zu untersuchen, ist auf die Wechselwirkung von abweichenden Einstellungen zu achten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Die automatische Rückgabe wird aktiviert, sodass die Rückgabe erfolgt, sobald der übernommene Knoten hochfährt, den Status „Warten auf Rückgabe“ erreicht und die Verzögerung vor automatischer Rückgabe abgelaufen ist. Die Standardeinstellung ist „true“.	`storage failover modify -node` *`nodename`* `-auto-giveback true`
Automatische Rückgabe deaktivieren. Die Standardeinstellung ist „true“. **Hinweis:** Wenn dieser Parameter auf „false“ gesetzt wird, wird die automatische Rückgabe nach einer Übernahme im Panikfall nicht deaktiviert; die automatische Rückgabe nach einer Übernahme im Panikfall muss durch Setzen des `-auto-giveback -after-panic` Parameters auf „false“ deaktiviert werden.	`storage failover modify -node` *`nodename`* `-auto-giveback false`
Die automatische Rückgabe nach Übernahme im Panikfall ist zu deaktivieren (diese Einstellung ist standardmäßig aktiviert).	`storage failover modify -node` *`nodename`* `-auto-giveback-after-panic false`
Die automatische Rückgabe wird um eine bestimmte Anzahl von Sekunden verzögert (Standardwert ist 600). Diese Option legt die Mindestzeit fest, die ein Knoten in der Übernahme verbleibt, bevor eine automatische Rückgabe durchgeführt wird.	`storage failover modify -node` *`nodename`* `-delay-seconds` *`seconds`*

Wie sich Variationen des Befehls storage failover modify auf die automatische Rückgabe auswirken

Die Funktionsweise der automatischen Rückführung hängt davon ab, wie die Parameter des Befehls storage failover modify konfiguriert werden.

Die folgende Tabelle listet die Standardeinstellungen für die `storage failover modify` Befehlsparameter auf, die für Übernahmeereignisse gelten, die nicht durch einen Panikzustand verursacht wurden.

Parameter	Standardeinstellung
`-auto-giveback` *`true`*	*`false`*
`true`	`-delay-seconds` *`integer`* `(seconds)`
600	`-onreboot` *`true`*

false`	*true*

Die folgende Tabelle beschreibt, wie Kombinationen der `-onreboot` und `-auto-giveback` Parameter die automatische Rückgabe bei Übernahmeereignissen beeinflussen, die nicht durch eine Panik verursacht wurden.

`storage failover modify` verwendete Parameter	Grund der Übernahme	Erfolgt ein automatisches Giveback?
`-onreboot` *true* `-auto-giveback` *true*	Neustartbefehl	Ja
Stoppbefehl oder Neustartvorgang, der vom Service Processor ausgelöst wird	Ja	`-onreboot` *true* `-auto-giveback` *false*
Neustartbefehl	Ja	Stoppbefehl oder Neustartvorgang, der vom Service Processor ausgelöst wird
Nein	`-onreboot` *false* `-auto-giveback` *true*	Neustartbefehl
Nicht zutreffend, in diesem Fall findet keine Übernahme statt	Stoppbefehl oder Neustartvorgang, der vom Service Processor ausgelöst wird	Ja
`-onreboot` *false* `-auto-giveback` *false*	Neustartbefehl	Nein

Der `-auto-giveback`Parameter steuert die Rückgabe nach einem Panic und allen anderen automatischen Takeovers. Wenn der `-onreboot`Parameter auf `true`gesetzt ist und eine Übernahme aufgrund eines Reboots erfolgt, wird die automatische Rückgabe immer durchgeführt, unabhängig davon, ob der `-auto-giveback`Parameter auf `true`gesetzt ist.

Der `-onreboot`Parameter gilt für Neustarts und Halt-Befehle, die von ONTAP ausgeführt werden. Wenn der `-onreboot`Parameter auf false gesetzt ist, findet im Fall eines Knotenneustarts keine Übernahme statt. Daher kann keine automatische Rückgabe erfolgen, unabhängig davon, ob der `-auto-giveback`Parameter auf true gesetzt ist. Eine Client-Unterbrechung tritt auf.

Die Auswirkungen automatischer Rückmeldeparameterkombinationen, die in Paniksituationen gelten.

Die folgende Tabelle listet die `storage failover modify` Befehlsparameter auf, die in Paniksituationen gelten:

Parameter	Standardeinstellung
`-onpanic _true	false_`
true	`-auto-giveback-after-panic _true

false_` (Berechtigung: Erweitert)	*true*
`-auto-giveback _true	false_`

Die folgende Tabelle beschreibt, wie sich Parameterkombinationen des `storage failover modify` Befehls auf die automatische Rückgabe in Paniksituationen auswirken.

`storage failover` verwendete Parameter	Erfolgt nach einem Panic eine automatische Rückgabe?

`-onpanic true`
`-auto-giveback true`
`-auto-giveback-after-panic true`
	Ja

`-onpanic true`
`-auto-giveback true`
`-auto-giveback-after-panic false`
	Ja

`-onpanic true`
`-auto-giveback false`
`-auto-giveback-after-panic true`
	Ja

`-onpanic true`
`-auto-giveback false`
`-auto-giveback-after-panic false`
	Nein

`-onpanic false`Wenn `-onpanic`auf `false` gesetzt ist, findet keine Übernahme/Rückgabe statt, unabhängig vom Wert, der für `-auto-giveback` oder `-auto-giveback-after-panic` festgelegt ist.	Nein

Eine Übernahme kann durch einen Fehler ausgelöst werden, der nicht mit einer Panik zusammenhängt. Ein *Ausfall* tritt auf, wenn die Kommunikation zwischen einem Node und seinem Partner verloren geht, was auch als *Heartbeat-Verlust* bezeichnet wird. Wenn ein Takeover aufgrund eines Ausfalls erfolgt, wird der Giveback durch den Parameter `-onfailure` anstelle des Parameters `-auto-giveback-after-panic parameter` gesteuert.

Wenn ein Knoten in Panik gerät, sendet er ein Panikpaket an seinen Partnerknoten. Wird dieses Panikpaket aus irgendeinem Grund nicht vom Partnerknoten empfangen, kann die Panik fälschlicherweise als Fehler interpretiert werden. Ohne den Empfang des Panikpakets weiß der Partnerknoten lediglich, dass die Kommunikation unterbrochen wurde, und nicht, dass eine Panik aufgetreten ist. In diesem Fall behandelt der Partnerknoten den Kommunikationsverlust als Fehler anstatt als Panik, und die Rückgabe wird durch den `-onfailure` Parameter (und nicht durch den `-auto-giveback-after-panic parameter`) gesteuert.

Weitere Informationen zu `storage failover modify` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP manuelle Takeover-Befehle

Sie können eine Übernahme manuell durchführen, wenn beim Partner Wartungsarbeiten erforderlich sind und in anderen ähnlichen Situationen. Je nach Zustand des Partners

variiert der Befehl, den Sie zur Übernahme verwenden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Den Partnerknoten übernehmen	`storage failover takeover`
Der Fortschritt der Übernahme kann verfolgt werden, während die Aggregate des Partners auf den Knoten verschoben werden, der die Übernahme durchführt.	`storage failover show-takeover`
Der Storage-Failover-Status für alle Knoten im Cluster wird angezeigt.	`storage failover show`
Den Partnerknoten ohne Migration der LIFs übernehmen	`storage failover takeover -skip-lif -migration-before-takeover true`
Den Partnerknoten auch bei einer Festplatteninkompatibilität übernehmen	`storage failover takeover -allow-disk -inventory-mismatch true`
Den Partnerknoten auch bei einer ONTAP Versionsabweichung übernehmen. **Hinweis:** Diese Option wird nur während des unterbrechungsfreien ONTAP Upgrade-Prozesses verwendet.	`storage failover takeover -option allow -version-mismatch`
Den Partnerknoten übernehmen, ohne eine Aggregate-Umverteilung durchzuführen	`storage failover takeover -bypass -optimization true`
Den Partnerknoten übernehmen, bevor dieser seine Speicherressourcen ordnungsgemäß schließen kann	`storage failover takeover -option immediate`

Bevor Sie den storage failover-Befehl mit der Option "immediate" ausführen, müssen die Data-LIFs mithilfe des folgenden Befehls auf einen anderen Node migriert werden: `network interface migrate-all -node` *`node`*

Weitere Informationen zu `network interface migrate-all` finden sich in der "ONTAP-Befehlsreferenz".

Wenn Sie den `storage failover takeover -option immediate` Befehl angeben, ohne vorher die Daten-LIFs zu migrieren, wird die Daten-LIF-Migration vom Knoten erheblich verzögert, selbst wenn die `skip-lif-migration-before-takeover` Option nicht angegeben wird.

Wenn die Option „sofort“ angegeben wird, wird die ausgehandelte Übernahmeoptimierung umgangen, selbst wenn die Option „bypass-optimization“ auf *false* gesetzt ist.

Verschiebung von Epsilon für bestimmte manuell initiierte Takeovers

Sie sollten Epsilon verschieben, wenn Sie davon ausgehen, dass manuell eingeleitete Übernahmen dazu führen könnten, dass Ihr Speichersystem nur einen unerwarteten Knotenausfall von einem clusterweiten Quorumverlust entfernt ist.

Über diese Aufgabe

Für geplante Wartungsarbeiten muss einer der Knoten in einem HA-Paar übernommen werden. Das Cluster-weite Quorum muss aufrechterhalten werden, um ungeplante Unterbrechungen der Client-Daten für die verbleibenden Knoten zu verhindern. In einigen Fällen kann die Übernahme dazu führen, dass der Cluster nur noch einen unerwarteten Knotenausfall vom clusterweiten Verlust des Quorums entfernt ist.

Dies kann auftreten, wenn der zu übernehmende Knoten Epsilon enthält oder wenn der Knoten mit Epsilon nicht fehlerfrei ist. Zur Aufrechterhaltung eines widerstandsfähigeren Clusters kann Epsilon auf einen fehlerfreien Knoten übertragen werden, der nicht übernommen wird. Typischerweise wäre dies der HA Partner.

Nur gesunde und teilnahmeberechtigte Knoten nehmen an der Quorumsabstimmung teil. Um ein clusterweites Quorum aufrechtzuerhalten, sind mehr als N/2 Stimmen erforderlich (wobei N die Summe der gesunden, teilnahmeberechtigten, online befindlichen Knoten darstellt). In Clustern mit einer geraden Anzahl online befindlicher Knoten verleiht Epsilon dem Knoten, dem es zugeordnet ist, zusätzliches Stimmgewicht zur Aufrechterhaltung des Quorums.

> Obwohl die Abstimmung zur Clusterbildung mithilfe des `cluster modify -eligibility false` Befehls geändert werden kann, sollte dies nur in Situationen wie der Wiederherstellung der Knotenkonfiguration oder bei längerer Wartung eines Knotens erfolgen. Wenn ein Knoten als nicht berechtigt festgelegt wird, stellt er keine SAN-Daten mehr bereit, bis er wieder als berechtigt markiert und neu gestartet wird. Auch der NAS-Datenzugriff auf den Knoten kann beeinträchtigt sein, wenn der Knoten nicht berechtigt ist.

Schritte

1. Den Clusterstatus überprüfen und bestätigen, dass Epsilon von einem fehlerfreien Knoten gehalten wird, der nicht übernommen wird:

   a. Zur erweiterten Berechtigungsstufe wechseln und bestätigen, dass fortgefahren werden soll, wenn die Aufforderung für den erweiterten Modus erscheint (*>):

      ```
      set -privilege advanced
      ```

   b. Ermitteln Sie, welcher Knoten Epsilon enthält:

      ```
      cluster show
      ```

      Im folgenden Beispiel enthält Node1 das Epsilon:

Node	Systemzustand	Teilnahmeberechtigung	Epsilon
Node1 Node2	wahr wahr	wahr wahr	wahr falsch

      Falls der Knoten, den Sie übernehmen möchten, kein Epsilon enthält, ist mit Schritt 4 fortzufahren.

   Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".

2. Epsilon vom Knoten entfernen, der übernommen werden soll:

   ```
   cluster modify -node Node1 -epsilon false
   ```

3. Epsilon dem Partnerknoten (in diesem Beispiel Node2) zuweisen:

   ```
   cluster modify -node Node2 -epsilon true
   ```

4. Die Übernahme wird durchgeführt:

   ```
   storage failover takeover -ofnode node_name
   ```

5. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Verwandte Informationen

- "storage failover show"
- "Storage-Failover-Takeover"

ONTAP manuelle Rückgabebefehle

Es ist möglich, eine normale Rückgabe, eine Rückgabe mit Beendigung von Prozessen auf dem Partnerknoten oder eine erzwungene Rückgabe durchzuführen.

Vor der Durchführung einer Rückgabe müssen die defekten Laufwerke im übernommenen System wie in "Festplatten- und Aggregatverwaltung" beschrieben entfernt werden.

Wenn die Rückgabe unterbrochen wird

Wenn der Übernahmeknoten während des Rückgabeprozesses einen Ausfall oder einen Stromausfall erleidet, stoppt dieser Prozess und der Übernahmeknoten kehrt in den Übernahmemodus zurück, bis der Ausfall behoben oder die Stromversorgung wiederhergestellt ist.

Dies hängt jedoch von der Phase der Rückgabe ab, in der der Fehler aufgetreten ist. Wenn beim Knoten während des teilweisen Rückgabestatus (nachdem das Root-Aggregat zurückgegeben wurde) ein Fehler oder ein Stromausfall auftritt, kehrt er nicht in den Übernahmemodus zurück. Stattdessen kehrt der Knoten in den Modus der teilweisen Rückgabe zurück. Tritt dies auf, wird der Vorgang abgeschlossen, indem die Rückgabeoperation wiederholt wird.

Wenn das Giveback abgelehnt wird

Wird die Rückgabe abgelehnt, müssen die EMS-Meldungen geprüft werden, um die Ursache zu ermitteln. Abhängig vom Grund oder von den Gründen kann entschieden werden, ob die Ablehnungen gefahrlos außer Kraft gesetzt werden können.

Der `storage failover show-giveback` Befehl zeigt den Fortschritt der Rückgabe an und gibt an, welches Subsystem die Rückgabe gegebenenfalls abgelehnt hat. Weiche Vetos können überschrieben werden, harte Vetos hingegen nicht, selbst wenn sie erzwungen werden. Die folgenden Tabellen fassen die weichen Vetos zusammen, die nicht überschrieben werden sollten, sowie empfohlene Alternativen.

Die EMS-Details zu etwaigen Giveback-Vetos lassen sich mit dem folgenden Befehl anzeigen:

```
event log show -node * -event gb*
```

Weitere Informationen zu `event log show` finden sich in der "ONTAP-Befehlsreferenz".

Rückgabe des Root-Aggregats

Diese Vetos gelten nicht für Root-Aggregat-Umsiedlungsmaßnahmen:

Vetoing-Subsystemmodul	Problemumgehung

vfiler_low_level	Die SMB-Sitzungen, die das Veto verursachen, müssen beendet werden, oder die SMB-Anwendung, die die offenen Sitzungen hergestellt hat, muss heruntergefahren werden. Das Übergehen dieses Vetos könnte dazu führen, dass die Anwendung, die SMB verwendet, abrupt die Verbindung trennt und Daten verliert.
Datenträgerprüfung	Alle ausgefallenen oder umgangenen Datenträger sollten vor dem Rückgabeversuch entfernt werden. Wenn Datenträger bereinigt werden, sollte abgewartet werden, bis der Vorgang abgeschlossen ist. Das Aufheben dieses Vetos kann zu einem Ausfall führen, wenn Aggregate oder Volumes aufgrund von Reservierungskonflikten oder nicht zugänglichen Festplatten offline gehen.

Rückgabe der SFO Aggregate

Diese Vetos gelten nicht für Root-Aggregat-Umsiedlungsmaßnahmen:

Vetoing-Subsystemmodul	Problemumgehung
Lock Manager	Die SMB-Anwendungen, die geöffnete Dateien haben, sollten ordnungsgemäß heruntergefahren werden, oder diese Volumes in ein anderes Aggregat verschoben werden. Das Außerkraftsetzen dieses Vetos führt zum Verlust des SMB-Sperrstatus, was zu Unterbrechungen und Datenverlust führt.
Lock Manager NDO	Warten Sie, bis die Sperren gespiegelt sind. Das Übergehen dieses Vetos führt zu Unterbrechungen bei Microsoft Hyper-V-virtuellen Maschinen.
RAID	Die EMS-Meldungen geben Aufschluss über die Ursache des Vetos: Falls das Veto auf nvfile zurückzuführen ist, sollten die offline befindlichen Volumes und Aggregate online geschaltet werden. Wenn Datenträger-Hinzufügen- oder Datenträgereigentumsübertragungs-Operationen im Gange sind, abwarten, bis diese abgeschlossen sind. Falls das Veto auf einen Konflikt mit einem Aggregatnamen oder einer UUID zurückzuführen ist, sollte das Problem behoben werden. Wenn das Veto auf eine Spiegelsynchronisierung, eine Spiegelverifizierung oder Offline-Festplatten zurückzuführen ist, kann das Veto überschrieben werden und der Vorgang startet nach der Rückgabe erneut.

Datenträgerinventar	Fehlerbehebung zur Identifizierung und Behebung der Problemursache. Der Zielknoten kann möglicherweise die zu einem migrierten Aggregat gehörenden Datenträger nicht sehen. Nicht zugängliche Datenträger können zu nicht zugänglichen Aggregaten oder Volumes führen.
Volume-Move-Vorgang	Fehlerbehebung zur Identifizierung und Behebung der Problemursache. Dieses Veto verhindert, dass der Vorgang zum Verschieben des Volumes während der wichtigen Umstellungsphase abgebrochen wird. Wenn der Vorgang während der Umstellungsphase abgebrochen wird, könnte das Volume nicht mehr erreichbar sein.

Befehle zur Durchführung einer manuellen Rückgabe

Sie können auf einem Node in einem HA-Paar manuell eine Rückgabe initiieren, um den Speicher nach Abschluss der Wartung oder der Behebung von Problemen, die die Übernahme verursacht haben, an den ursprünglichen Eigentümer zurückzugeben.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Speicher an einen Partnerknoten zurückgeben	`storage failover giveback -ofnode` *`nodename`*
Speicherplatz kann auch dann zurückgegeben werden, wenn sich der Partner nicht im Modus „Warten auf Rückgabe“ befindet.	`storage failover giveback -ofnode` *`nodename`* `-require-partner-waiting false` Diese Option sollte nur verwendet werden, wenn ein längerer Clientausfall akzeptabel ist.
Speicher auch dann zurückgeben, wenn Prozesse den Giveback-Vorgang verhindern (Giveback erzwingen)	`storage failover giveback -ofnode` *`nodename`* `-override-vetoes true` Die Nutzung dieser Option kann unter Umständen zu längeren Client-Ausfällen führen oder dazu, dass Aggregate und Volumes nach der Rückmeldung nicht online gehen.
Nur die CFO-Aggregate (das Root-Aggregat) zurückgeben	`storage failover giveback -ofnode` *`nodename`* `-only-cfo-aggregates true`
Der Fortschritt der Rückgabe kann nach Ausführung des Befehls „giveback“ überwacht werden.	`storage failover show-giveback`

Verwandte Informationen

- "Storage-Failover-Giveback"
- "storage failover show-giveback"

Test von Takeover und Giveback in ONTAP

Nachdem alle Aspekte Ihres HA-Paares konfiguriert wurden, sollte überprüft werden, ob es wie erwartet arbeitet und während Übernahme- und Rückgabevorgängen den unterbrechungsfreien Zugriff auf den Speicher beider Knoten aufrechterhält. Während des Übernahmevorgangs sollte der lokale (oder übernehmende) Knoten weiterhin die Daten bereitstellen, die normalerweise vom Partnerknoten bereitgestellt werden. Während der Rückgabe sollten Kontrolle und Bereitstellung des Speichers des Partners wieder an den Partnerknoten zurückkehren.

Schritte

1. Die Verkabelung der HA Interconnect-Kabel sollte überprüft werden, um sicherzustellen, dass sie fest sitzt.
2. Es sollte möglich sein, auf beiden Knoten für jedes lizenzierte Protokoll Dateien zu erstellen und abzurufen.
3. Führen Sie den folgenden Befehl aus:

   ```
   storage failover takeover -ofnode partnernode
   ```

   Weitere Informationen zu `storage failover takeover` finden sich in der "ONTAP-Befehlsreferenz".

4. Einer der folgenden Befehle bestätigt, dass die Übernahme erfolgt ist:

   ```
   storage failover show-takeover
   ```

   ```
   storage failover show
   ```

   Wenn Sie die `storage failover` Option des `-auto-giveback` Befehls aktiviert haben:

Node	Partner	Übernahme möglich	Statusbeschreibung
Knoten 1	Knoten 2	-	Warten auf Giveback
Knoten 2	Knoten 1	false	Bei einer Übernahme wird die automatische Rückgabe nach einer bestimmten Anzahl von Sekunden eingeleitet.

   Wenn Sie die `storage failover` Option des `-auto-giveback` Befehls deaktiviert haben:

Node	Partner	Übernahme möglich	Statusbeschreibung
Knoten 1	Knoten 2	-	Warten auf Giveback
Knoten 2	Knoten 1	false	Bei der Übernahme

5. Alle Datenträger, die zum Partnerknoten (Node2) gehören und vom Übernahmeknoten (Node1) erkannt werden können, werden angezeigt:

   ```
   storage disk show -home node2 -ownership
   ```

   Der folgende Befehl zeigt alle zu Node2 gehörenden Datenträger an, die von Node1 erkannt werden können:

```
cluster::> storage disk show -home node2 -ownership
```

Festplatte	Aggregat	Start	Eigentümer	DR-Startseite	Home-ID	Owner-ID	DR Home ID	Reserver	Pool
1.0.2	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0

6. Bestätigen Sie, dass der Übernahmeknoten (Node1) die Aggregate des Partnerknotens (Node2) kontrolliert:

```
aggr show -fields home-id,home-name,is-home
```

Aggregat	Heim-ID	home-nameh	ist Zuhause
aggr0_1	2014942045	node1	true
aggr0_2	4078312453	node2	false
aggr1_1	2014942045	node1	true
aggr1_2	4078312453	node2	false

Während der Übernahme ist der Wert “is-home” der Aggregate des Partner-Node falsch.

7. Den Datendienst des Partnerknotens zurückgeben, nachdem die Meldung „`Warten auf Rückgabe`“ angezeigt wird:

```
storage failover giveback -ofnode partnernode
```

8. Einer der folgenden Befehle zeigt den Fortschritt der Rückgabeoperation an:

```
storage failover show-giveback
```

```
storage failover show
```

9. Fahren Sie je nachdem fort, ob die Meldung angezeigt wurde, dass das Giveback erfolgreich abgeschlossen wurde:

Wenn Übernahme und Rückgabe…	Dann…
Wurden erfolgreich abgeschlossen	Schritt 2 bis Schritt 8 werden auf dem Partnerknoten wiederholt.
Fehler	Den Fehler bei der Übernahme oder Rückgabe beheben und anschließend dieses Verfahren erneut ausführen.

Verwandte Informationen

- "Speicherdatenträger anzeigen"
- "Storage-Failover-Giveback"
- "storage failover show"

- "storage failover show-giveback"

ONTAP Befehle zur Überwachung eines HA-Paares

Sie können ONTAP Befehle verwenden, um den Status des HA Paars zu überwachen. Wenn eine Übernahme erfolgt, lässt sich auch die Ursache der Übernahme feststellen.

Wenn Sie überprüfen möchten	Verwenden Sie diesen Befehl
Ob ein Failover aktiviert ist oder bereits stattgefunden hat oder Gründe, warum ein Failover derzeit nicht möglich ist	`storage failover show`
Die Knoten, auf denen die Einstellung „Storage Failover HA-Modus“ aktiviert ist, werden angezeigt. Der Wert muss auf „ha“ gesetzt werden, damit der Knoten an einer Storage Failover (HA-Paar) Konfiguration teilnimmt.	`storage failover show -fields mode`
Ob Hardware-unterstützte Übernahme aktiviert ist	`storage failover hwassist show`
Die Historie der Hardware-unterstützt Übernahmeereignisse, die aufgetreten sind	`storage failover hwassist stats show`
Der Fortschritt einer Übernahmeoperation, während die Aggregate des Partners auf den Knoten übertragen werden, der die Übernahme durchführt	`storage failover show-takeover`
Der Fortschritt einer Rückgabeoperation bei der Rückgabe von Aggregaten an den Partnerknoten	`storage failover show-giveback`
Ob ein Aggregat während einer Übernahme oder Rückgabe seinen Home-Status hat	`aggregate show -fields home-id,owner-id,home-name,owner-name,is-home`
Ob Cluster HA aktiviert ist (gilt nur für Cluster mit zwei Knoten)	`cluster ha show`
Der HA-Zustand der Komponenten eines HA-Paares (auf Systemen, die den HA-Zustand verwenden)	`ha-config show`Dies ist ein Befehl im Wartungsmodus.

Von den Befehlen „storage failover show-type“ angezeigte Knotenzustände

Die folgende Liste beschreibt die Knotenzustände, die der `storage failover show` Befehl anzeigt.

Knotenstatus	Beschreibung
Verbindung zu partner_name hergestellt, automatische Übernahme deaktiviert.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Die automatische Übernahme des Partnerknotens ist deaktiviert.

Warten auf partner_name, Rückgabe der Partner-Ersatzfestplatten ausstehend.	Der lokale Knoten kann keine Informationen mit dem Partnerknoten über die HA-Verbindung austauschen. Die Rückgabe der SFO Aggregate an den Partner ist abgeschlossen, aber die Ersatzfestplatten des Partners sind weiterhin im Besitz des lokalen Knotens. • Der `storage failover show-giveback`Befehl liefert weitere Informationen.
Warten auf partner_name. Warten auf Synchronisierung der Partnersperre.	Der lokale Knoten kann über die HA Interconnect keine Informationen mit dem Partnerknoten austauschen und wartet auf die Partner-Sperrsynchronisierung.
Warten auf partner_name. Warten auf die Verfügbarkeit der Clusteranwendungen auf dem lokalen Node.	Der lokale Knoten kann über die HA Interconnect keine Informationen mit dem Partnerknoten austauschen und wartet darauf, dass die Clusteranwendungen online gehen.
Übernahme geplant. Der Zielknoten verlagert seine SFO-Aggregate zur Vorbereitung der Übernahme.	Die Übernahmeverarbeitung wurde gestartet. Der Zielknoten verlegt die Eigentumsrechte an seinen SFO-Aggregaten im Vorfeld der Übernahme.
Übernahme geplant. Der Zielknoten hat seine SFO-Aggregate zur Vorbereitung der Übernahme verlegt.	Die Übernahmeverarbeitung wurde gestartet. Der Zielknoten hat die Eigentumsverhältnisse seiner SFO-Aggregate im Vorfeld der Übernahme verlagert.
Übernahme geplant. Warten auf Deaktivierung von Hintergrund-Firmware-Updates auf dem lokalen Knoten. Ein Firmware-Update wird derzeit auf dem Node durchgeführt.	Die Übernahmeverarbeitung wurde gestartet. Das System wartet darauf, dass die Hintergrund-Firmware-Aktualisierungsvorgänge auf dem lokalen Knoten abgeschlossen werden.
Verlagerung der SFO Aggregate zum übernehmenden Node in Vorbereitung auf die Übernahme.	Der lokale Knoten verlagert die Eigentumsrechte an seinen SFO Aggregaten auf den übernehmenden Knoten im Vorfeld der Übernahme.
SFO Aggregate wurden auf den übernehmenden Node verschoben. Warten darauf, dass der übernehmende Node übernimmt.	Die Übertragung der Eigentumsrechte an den SFO Aggregaten vom lokalen Knoten auf den übernehmenden Knoten ist abgeschlossen. Das System wartet auf die Übernahme durch den übernehmenden Knoten.
SFO Aggregate werden zu partner_name verschoben. Warten auf die Deaktivierung von Hintergrund-Firmware-Updates auf dem lokalen Knoten. Ein Firmware-Update wird derzeit auf dem Node durchgeführt.	Die Übertragung der Zuständigkeit für SFO Aggregate vom lokalen Knoten auf den übernehmenden Knoten ist im Gange. Das System wartet darauf, dass die Hintergrund-Firmware-Aktualisierungsvorgänge auf dem lokalen Knoten abgeschlossen werden.
SFO Aggregate werden zu partner_name verschoben. Es wird darauf gewartet, die Hintergrund-Firmware-Updates für Festplatten auf partner_name zu deaktivieren. Ein Firmware-Update wird derzeit auf dem Node durchgeführt.	Die Übertragung der Zuständigkeit für SFO Aggregate vom lokalen Knoten auf den übernehmenden Knoten ist im Gange. Das System wartet auf den Abschluss von Hintergrund-Firmware-Aktualisierungsvorgängen auf dem Partnerknoten.

Verbindung zu partner_name hergestellt. Vorheriger Übernahmeversuch wurde abgebrochen, da reason. Der lokale Node besitzt einige SFO Aggregate des Partners. Eine erneute Übernahme des Partners mit dem `-bypass-optimization` Parameter auf true übernimmt die verbleibenden Aggregate, alternativ gibt eine Rückgabe des Partners die verlagerten Aggregate zurück.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der vorherige Übernahmeversuch wurde aufgrund des unter „Grund“ angezeigten Grundes abgebrochen. Der lokale Knoten besitzt einige SFO Aggregate seines Partners. • Entweder eine erneute Übernahme des Partnerknotens durchführen, wobei der Parameter „-bypass-optimization“ auf „true“ gesetzt wird, um die verbleibenden SFO-Aggregate zu übernehmen, oder eine Rückgabe des Partners durchführen, um die verschobenen Aggregate zurückzugeben.
Verbindung zu partner_name hergestellt. Der vorherige Übernahmeversuch wurde abgebrochen. Der lokale Node besitzt einige SFO Aggregate des Partners. Eine erneute Übernahme des Partners mit dem `-bypass-optimization` Parameter auf true übernimmt die verbleibenden Aggregate, alternativ gibt eine Rückgabe des Partners die verlagerten Aggregate zurück.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der vorherige Übernahmeversuch wurde abgebrochen. Der lokale Knoten besitzt einige SFO Aggregate seines Partners. • Entweder eine erneute Übernahme des Partnerknotens durchführen, wobei der Parameter „-bypass-optimization“ auf „true“ gesetzt wird, um die verbleibenden SFO-Aggregate zu übernehmen, oder eine Rückgabe des Partners durchführen, um die verschobenen Aggregate zurückzugeben.
Warten auf partner_name. Vorheriger Übernahmeversuch wurde abgebrochen, da reason. Der lokale Node besitzt einige SFO Aggregate des Partners. Eine erneute Übernahme des Partners mit dem Parameter „-bypass-optimization“ auf „true“ übernimmt die verbleibenden Aggregate, alternativ gibt ein Giveback des Partners die verlagerten Aggregate zurück.	Der lokale Knoten kann keine Informationen mit dem Partnerknoten über die HA-Verbindung austauschen. Der vorherige Übernahmeversuch wurde aufgrund des unter „Grund“ angezeigten Grundes abgebrochen. Der lokale Knoten besitzt einige SFO Aggregate seines Partners. • Entweder eine erneute Übernahme des Partnerknotens durchführen, wobei der Parameter „-bypass-optimization“ auf „true“ gesetzt wird, um die verbleibenden SFO-Aggregate zu übernehmen, oder eine Rückgabe des Partners durchführen, um die verschobenen Aggregate zurückzugeben.

Warten auf partner_name. Der vorherige Übernahmeversuch wurde abgebrochen. Der lokale Node besitzt einige SFO Aggregate des Partners. Eine erneute Übernahme des Partners mit dem Parameter „-bypass-optimization“ auf „true“ übernimmt die verbleibenden Aggregate, alternativ gibt ein Giveback des Partners die verlagerten Aggregate zurück.	Der lokale Knoten kann keine Informationen mit dem Partnerknoten über die HA-Verbindung austauschen. Der vorherige Übernahmeversuch wurde abgebrochen. Der lokale Knoten besitzt einige SFO Aggregate seines Partners. • Entweder eine erneute Übernahme des Partnerknotens durchführen, wobei der Parameter „-bypass-optimization“ auf „true“ gesetzt wird, um die verbleibenden SFO-Aggregate zu übernehmen, oder eine Rückgabe des Partners durchführen, um die verschobenen Aggregate zurückzugeben.
Verbindung zu partner_name hergestellt. Der vorherige Übernahmeversuch wurde abgebrochen, da die Deaktivierung der Hintergrund-Disk-Firmware-Aktualisierung (BDFU) auf dem lokalen Node fehlgeschlagen ist.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der vorherige Übernahmeversuch wurde abgebrochen, da das Hintergrund-Firmware-Update der Festplatte auf dem lokalen Knoten nicht deaktiviert war.
Verbindung zu partner_name hergestellt. Vorheriger Übernahmeversuch wurde abgebrochen, da reason.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der vorherige Übernahmeversuch wurde aufgrund des unter „Grund“ angezeigten Grundes abgebrochen.
Warten auf partner_name. Vorheriger Übernahmeversuch wurde abgebrochen, da reason.	Der lokale Knoten kann keine Informationen mit dem Partnerknoten über die HA-Verbindung austauschen. Der vorherige Übernahmeversuch wurde aufgrund des unter „Grund“ angezeigten Grundes abgebrochen.
Verbindung zu partner_name hergestellt. Der vorherige Übernahmeversuch von partner_name wurde abgebrochen, weil reason.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der vorherige Übernahmeversuch durch den Partnerknoten wurde aufgrund des unter „Grund“ angezeigten Grundes abgebrochen.
Verbindung zu partner_name hergestellt. Vorheriger Übernahmeversuch von partner_name wurde abgebrochen.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der vorherige Übernahmeversuch des Partnerknotens wurde abgebrochen.
Warten auf partner_name. Der vorherige Übernahmeversuch von partner_name wurde abgebrochen, weil reason.	Der lokale Knoten kann keine Informationen mit dem Partnerknoten über die HA-Verbindung austauschen. Der vorherige Übernahmeversuch durch den Partnerknoten wurde aufgrund des unter „Grund“ angezeigten Grundes abgebrochen.
Der vorherige Rückgabevorgang ist im Modul: Modulname fehlgeschlagen. Die automatische Rückgabe wird in number of seconds Sekunden eingeleitet.	Der vorherige Rückgabeversuch ist im Modul module_name fehlgeschlagen. Die automatische Rückgabe wird in number of seconds Sekunden eingeleitet. • Der `storage failover show-giveback`Befehl liefert weitere Informationen.

Node besitzt die Aggregate des Partners im Rahmen des unterbrechungsfreien Controller-Upgrade-Verfahrens.	Der Knoten besitzt die Aggregate seines Partners aufgrund des derzeit laufenden nicht unterbrechenden Controller Upgrade Verfahrens.
Verbindung zu partner_name hergestellt. Der Knoten besitzt Aggregate, die zu einem anderen Knoten im Cluster gehören.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Der Knoten besitzt Aggregate, die zu einem anderen Knoten im Cluster gehören.
Verbindung zu partner_name hergestellt. Warten auf Synchronisierung der Partnersperre.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Das System wartet auf den Abschluss der Partner-Lock-Synchronisierung.
Verbindung zu partner_name hergestellt. Warten auf die Verfügbarkeit der Clusteranwendungen auf dem lokalen Node.	Die HA-Verbindung ist aktiv und kann Daten an den Partnerknoten übertragen. Das System wartet darauf, dass die Clusteranwendungen auf dem lokalen Knoten online sind.
Im Nicht-HA-Modus ist ein Neustart erforderlich, um den gesamten NVRAM zu nutzen.	Storage-Failover ist nicht möglich. Die HA-Mode-Option ist auf non_ha konfiguriert. • Der Knoten muss neu gestartet werden, damit der gesamte NVRAM genutzt werden kann.
Nicht-HA-Modus. Der Node muss neu gestartet werden, um HA zu aktivieren.	Storage-Failover ist nicht möglich. • Der Knoten muss neu gestartet werden, um die HA-Funktionalität zu aktivieren.
Nicht-HA-Modus.	Storage-Failover ist nicht möglich. Die HA-Mode-Option ist auf non_ha konfiguriert. • Sie müssen den `storage failover modify -mode ha -node nodename` Befehl auf beiden Nodes im HA-Paar ausführen und anschließend die Nodes neu starten, um die HA-Fähigkeit zu aktivieren.

Verwandte Informationen

- "ONTAP-Befehlsreferenz"
- "cluster ha show"
- "Storage Failover Hardware-unterstützt"
- "storage failover modify"
- "storage failover show"
- "storage failover show-giveback"

ONTAP Befehle zum Aktivieren und Deaktivieren von Storage Failover

Die folgenden Befehle dienen zum Aktivieren und Deaktivieren der Storage-Failover-Funktionalität.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…

Takeover aktivieren	`storage failover modify -enabled true -node` *nodename*
Takeover deaktivieren	`storage failover modify -enabled false -node` *nodename*

Die Speicherausfallsicherung sollte nur dann deaktiviert werden, wenn dies im Rahmen einer Wartungsmaßnahme erforderlich ist.

Verwandte Informationen

- "storage failover modify"

ONTAP Knoten in Zwei-Node-Clustern anhalten oder neu starten, ohne eine Übernahme einzuleiten

Ein Halt oder Neustart eines Knotens in einem Zwei-Node-Cluster ohne Einleitung einer Übernahme erfolgt, wenn bestimmte Hardware-Wartungsarbeiten an einem Knoten oder einem Shelf durchgeführt werden und die Ausfallzeit durch das Weiterbetreiben des Partnerknotens begrenzt werden soll oder wenn Probleme eine manuelle Übernahme verhindern und die Aggregate des Partnerknotens weiterhin in Betrieb bleiben und Daten bereitstellen sollen. Zusätzlich kann es vorkommen, dass der technische Support im Rahmen der Fehlerbehebung diese Vorgehensweise empfiehlt.

Über diese Aufgabe

- Bevor Sie die Übernahme verhindern (mithilfe des `-inhibit-takeover true` Parameters), deaktivieren Sie die Cluster HA.

- In einem Zwei-Node-Cluster stellt Cluster HA sicher, dass der Ausfall eines Knotens den Cluster nicht deaktiviert. Wenn Cluster HA jedoch nicht deaktiviert wird, bevor der `-inhibit-takeover true` Parameter verwendet wird, stellen beide Knoten die Datenbereitstellung ein.
- Wenn versucht wird, einen Node anzuhalten oder neu zu starten, bevor Cluster HA deaktiviert wird, gibt ONTAP eine Warnung aus und weist darauf hin, dass Cluster HA deaktiviert werden muss.

- Sie migrieren LIFs (logische Schnittstellen) zu dem Partner-Node, der online bleiben soll.
- Wenn sich auf dem Knoten, den Sie anhalten oder neu starten, Aggregate befinden, die Sie behalten möchten, werden diese auf den Knoten verschoben, der online bleiben soll.

Schritte

1. Überprüfen Sie, ob beide Knoten fehlerfrei sind:

```
cluster show
```

Für beide Knoten `true` erscheint es in der `Health` Spalte.

```
cluster::> cluster show
```

```
Node         Health  Eligibility
------------ ------- ------------
node1        true     true
node2        true     true
```

Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".

2. Migrieren Sie alle LIFs von dem Knoten, den Sie anhalten oder neu starten möchten, auf den Partnerknoten:

```
network interface migrate-all -node <node_name>
```

Weitere Informationen zu `network interface migrate-all` finden sich in der "ONTAP-Befehlsreferenz".

3. Wenn sich auf dem Knoten Aggregate befinden, die Sie beim Anhalten oder Neustarten des Knotens online halten möchten, verschieben Sie diese auf den Partnerknoten.

   a. Zeigen Sie die Aggregate auf dem Knoten, den Sie anhalten oder neu starten werden, an:

```
storage aggregates show -node <node_name>
```

Beispielsweise ist node1 der Knoten, der angehalten oder neu gestartet wird:

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1       2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
            4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

b. Verschieben Sie die Aggregate auf den Partnerknoten:

```
storage aggregate relocation start -node <node_name> -destination
<node_name> -aggregate-list <aggregate_name>
```

Beispielsweise werden die Aggregate aggr1, aggr2 und test2_aggr von node1 auf node2 verschoben:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr
```

4. Cluster-HA deaktivieren:

```
cluster ha modify -configured false
```

Wenn Cluster-HA deaktiviert ist, wird Epsilon automatisch auf Knoten 1 verschoben. Die Rückgabe bestätigt, dass HA deaktiviert ist: `Notice: HA is disabled`

Dieser Vorgang deaktiviert das Storage-Failover nicht.

5. Wenn der anzuhaltende oder neu zu startende Knoten Knoten 1 ist, verschieben Sie Epsilon zu Knoten 2:
   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

   b. Überprüfen Sie, ob Knoten 2 intakt und für Epsilon geeignet ist:

```
cluster show
```

   c. Entfernen Sie Epsilon von Knoten 1:

```
cluster modify -node <node1_name> -epsilon false
```

   d. Weisen Sie Knoten 2 Epsilon zu:

```
cluster modify -node <node2_name> -epsilon true
```

   e. Überprüfen Sie, ob Epsilon auf Knoten 2 ist:

```
cluster show
```

6. Anhalten oder Neustarten und Übernahme des Zielknotens verhindern:

Den Node anhalten, ohne eine Übernahme einzuleiten:	`system node halt -node _node_name_ -inhibit-takeover true`
Starten Sie den Knoten neu, ohne die Übernahme einzuleiten:	`system node reboot -node _node_name_ -inhibit-takeover true`

In der Befehlsausgabe erscheint eine Warnung, ob Sie fortfahren möchten, geben Sie `y` ein.

7. Überprüfen Sie, ob sich der noch online befindliche Knoten in einem fehlerfreien Zustand befindet (während der Partner ausgefallen ist):

```
cluster show
```

Für den Online-Knoten, `true` erscheint in der `Health` Spalte.

In der Ausgabe des Befehls wird eine Warnung angezeigt, dass Cluster-HA nicht konfiguriert ist. Sie können die Warnung ignorieren.

8. Führen Sie die Aktionen aus, die ein Anhalten oder einen Neustart des Knotens erfordern.
9. Starten Sie den offline geschalteten Node über die LOADER-Eingabeaufforderung:

```
boot_ontap
```

10. Überprüfen Sie, ob beide Knoten fehlerfrei sind:

```
cluster show
```

Für beide Knoten `true` erscheint es in der `Health` Spalte.

In der Ausgabe des Befehls wird eine Warnung angezeigt, dass Cluster-HA nicht konfiguriert ist. Die Warnung kann zu diesem Zeitpunkt ignoriert werden.

11. Cluster-HA wieder aktivieren:

```
cluster ha modify -configured true
```

12. Wenn Sie zuvor in diesem Verfahren Aggregate auf den Partnerknoten verschoben haben, verschieben Sie sie zurück auf ihren Heimatknoten.

```
storage aggregate relocation start -node <node_name> -destination
<node_name> -aggregate-list <aggregate_name>
```

Beispielsweise werden die Aggregate aggr1, aggr2 und test2_aggr vom Knoten node2 zum Knoten node1 verschoben:
`storage aggregate relocation start -node node2 -destination node1 -aggregate -list aggr1,aggr2,test2_aggr`

13. LIFs auf ihre Home-Ports zurückführen:
    a. LIFs anzeigen, die nicht zu Hause sind:

    ```
    network interface show -is-home false
    ```

    Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

    b. Falls es nicht-Home-LIFs gibt, die nicht vom ausgefallenen Node migriert wurden, sollte vor dem Zurücksetzen überprüft werden, ob eine sichere Verschiebung möglich ist.
    c. Wenn es sicher ist, tun Sie dies und setzen Sie alle LIFs auf ihre Ausgangsposition zurück.

    ```
    network interface revert *
    ```

    Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "cluster ha modify"
- "Start der Verlagerung des Storage Aggregats"

Verschlüsselung für ONTAP HA Datenverkehr konfigurieren

Ab ONTAP 9.18.1 ist die Verschlüsselung des Netzwerkverkehrs zwischen den Knoten eines Hochverfügbarkeitspaars (HA-Paar) konfigurierbar. Diese Verschlüsselung schützt Kundendaten und Metadaten, die zwischen den Knoten eines HA-Paars übertragen werden.

Über diese Aufgabe

- Die Verschlüsselung des HA-Datenverkehrs ist standardmäßig deaktiviert.
- Das Aktivieren oder Deaktivieren der HA-Datenverkehrsverschlüsselung wirkt sich auf alle HA-Paare im Cluster aus. Die Verschlüsselung kann nicht für einzelne Knoten aktiviert oder deaktiviert werden.
- Wenn die HA-Datenverkehrsverschlüsselung aktiviert ist, werden alle Kundendaten und Metadaten, die zwischen den Knoten des HA-Paares übertragen werden, verschlüsselt. Ein Teil des HA-Datenverkehrs, wie Dateisystemmetadaten und Heartbeat-Nachrichten, wird nicht verschlüsselt.
- Wenn die HA-Datenverkehrsverschlüsselung aktiviert ist und neue HA-Paare zum Cluster hinzugefügt werden, muss die HA-Datenverkehrsverschlüsselung für die neuen Knoten manuell aktiviert werden, indem der `security ha-network modify -enabled true` Befehl erneut ausgeführt wird.

Bevor Sie beginnen

- Sie müssen ONTAP Administrator auf der `admin`-Privilegstufe sein, um das folgende Verfahren auszuführen.
- Bevor die HA-Datenverkehrsverschlüsselung aktiviert wird, muss "Externe Schlüsselverwaltung konfigurieren".
- Alle Knoten im Cluster müssen ONTAP 9.18.1 oder höher ausführen, damit die HA-Verkehrsverschlüsselung aktiviert werden kann.

Schritte

1. Aktueller Verschlüsselungsstatus für HA-Datenverkehr:

```
security ha-network show
```

Dieser Befehl zeigt den aktuellen Status der HA-Datenverkehrsverschlüsselung für jeden Knoten an:

```
security ha-network show
Node                  Enabled
--------------------- --------------------
node1                 true
node2                 true
node3                 true
node4                 true
4 entries were displayed.
```

2. Verschlüsselung für HA-Datenverkehr aktivieren oder deaktivieren:

```
security ha-network modify -enabled <true|false>
```

Dieser Befehl aktiviert oder deaktiviert den verschlüsselten HA-Datenverkehr für alle Knoten im Cluster. Wenn dem Cluster neue HA-Paare hinzugefügt werden, ist dieser Befehl erneut auszuführen, um die Verschlüsselung des HA-Datenverkehrs für die neuen Knoten zu aktivieren.

REST API-Verwaltung mit System Manager

REST API-Verwaltung mit ONTAP System Manager

Das REST-API-Protokoll erfasst die API-Aufrufe, die der System Manager an ONTAP sendet. Das Protokoll ermöglicht ein Verständnis der Art und Reihenfolge der Aufrufe, die für die Durchführung der verschiedenen ONTAP administrativen Aufgaben erforderlich sind.

Wie System Manager die REST API und das API-Protokoll verwendet

Es gibt mehrere Möglichkeiten, wie der System Manager REST-API-Aufrufe an ONTAP sendet.

Wann sendet der System Manager API-Aufrufe?

Hier sind die wichtigsten Beispiele dafür, wann der System Manager ONTAP REST API-Aufrufe ausführt.

Automatische Seitenaktualisierung

System Manager gibt im Hintergrund automatisch API-Aufrufe aus, um die angezeigten Informationen, wie auf der Dashboard-Seite, zu aktualisieren.

Anzeigeaktion des Benutzers

Beim Anzeigen einer bestimmten Speicherressource oder einer Sammlung von Ressourcen über die System Manager Benutzeroberfläche werden ein oder mehrere API-Aufrufe ausgelöst.

Aktualisierungsaktion des Benutzers

Ein API-Aufruf wird ausgelöst, wenn Sie eine ONTAP-Ressource über die System Manager-Benutzeroberfläche hinzufügen, ändern oder löschen.

Erneutes Auslösen eines API-Aufrufs

Sie können einen API-Aufruf auch manuell erneut auslösen, indem Sie auf einen Protokolleintrag klicken. Dadurch wird die unformatierte JSON-Ausgabe des Aufrufs angezeigt.

Weitere Informationen

- "ONTAP 9 Automatisierungsdokumente"

Zugriff auf das ONTAP REST API-Protokoll

Sie können auf das Protokoll zugreifen, das eine Aufzeichnung der vom System Manager durchgeführten ONTAP REST API-Aufrufe enthält. Beim Anzeigen des Protokolls besteht außerdem die Möglichkeit, API-Aufrufe erneut auszuführen und die Ausgabe zu überprüfen.

Schritte

1. Oben auf der Seite  wird das REST-API-Protokoll angezeigt.

   Die aktuellsten Einträge werden am unteren Ende der Seite angezeigt.

2. Links auf **DASHBOARD** klicken und die neuen Einträge beobachten, die für die zum Aktualisieren der Seite ausgegebenen API-Aufrufe erstellt werden.
3. Auf **SPEICHER** und dann auf **Qtrees** klicken.

   Dies veranlasst System Manager, einen spezifischen API-Aufruf durchzuführen, um eine Liste der Qtrees abzurufen.

4. Den Logeintrag finden, der den API-Aufruf beschreibt und folgendes Format hat:

   ```
   GET /api/storage/qtrees
   ```

   Sie werden zusätzliche HTTP-Abfrageparameter im Eintrag sehen, wie `max_records`.

5. Klicken Sie auf den Protokolleintrag, um den GET API-Aufruf erneut auszuführen und die unformatierte JSON-Ausgabe anzuzeigen.

   Beispiel


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
00a0986abd71/1"
        }
```

```
      }
    },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.