Installation und Konfiguration von MetroCluster Tiebreaker

ONTAP MetroCluster

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap-metrocluster/tiebreaker/whats_new.html on April 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

Installation und Konfiguration von MetroCluster Tiebreaker . . . 1
Was ist neu . . . 1
Überblick über die Tiebreaker Software . . . 1
Installation der Tiebreaker Software . . . 5
Aktualisieren Sie den Host, auf dem der Tiebreaker Monitor ausgeführt wird . . . 56
Konfigurieren der Tiebreaker Software . . . 56
Konfigurieren von SNMP-Einstellungen für Tiebreaker Software . . . 59
Monitoring der MetroCluster-Konfiguration . . . 60
Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus . . . 66
Firewall-Anforderungen für MetroCluster Tiebreaker . . . 66
Ereignisprotokolldateien für MetroCluster Tiebreaker . . . 67
Wo Sie weitere Informationen finden . . . 68

Installation und Konfiguration von MetroCluster Tiebreaker

Was ist neu

Jede Version enthält Erweiterungen der MetroCluster Tiebreaker Software. Die aktuellen Versionen von MetroCluster Tiebreak enthalten alle Neuigkeiten.

Vorgestellt Werden

ONTAP Tiebreaker Version	Vorgestellt Werden
1.6	• Einfachere Installation • Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.5	• Aktualisierung der unterstützenden Bibliotheken • Verbesserte Sicherheit
1.4	• Aktualisierung der unterstützenden Bibliotheken

OS Support-Matrix

Tiebreaker Version	CentOS 7 - 7.9	Red Hat 7 - 7.9	Red Hat 8.1 - 8.7	Red Hat 8.8 -9,2	Rocky Linux 9.0
1.6	Nein	Nein	Ja.	Ja.	Ja.
1.5	Nein	Nein	Ja.	Nein	Nein
1.4	Ja.	Ja.	Ja.	Nein	Nein

Überblick über die Tiebreaker Software

Es ist hilfreich zu verstehen, was die NetApp MetroCluster Tiebreaker Software ist und wie sie zwischen verschiedenen Arten von Fehlern unterscheidet, sodass Sie Ihre MetroCluster Konfigurationen effizient überwachen können. Mit der Tiebreaker CLI können Einstellungen gemanagt und der Status und der Betrieb der MetroCluster Konfigurationen überwacht werden.

Erkennen von Ausfällen mit der NetApp MetroCluster Tiebreaker Software

Sie benötigen die Tiebreaker Software nur, wenn zwei Cluster und der Konnektivitätsstatus zwischen ihnen

von einem dritten Standort aus überwacht werden soll. Die Tiebreaker Software befindet sich auf einem Linux Host am dritten Standort, sodass jeder Partner in einem Cluster bei einem Standortausfall zwischen einem ISL-Ausfall und einem Standortausfall unterscheiden kann.

Nachdem Sie die Tiebreaker Software auf einem Linux-Host installiert haben, können Sie die Cluster in einer MetroCluster-Konfiguration konfigurieren, um auf Notfälle zu überwachen.

Die Tiebreaker Software überwacht bis zu 15 MetroCluster Konfigurationen gleichzeitig. Die Lösung unterstützt eine Kombination aus MetroCluster IP, MetroCluster FC und Stretch MetroCluster Konfigurationen.

Wie die Tiebreaker Software Standortausfällen erkennt

Die NetApp MetroCluster Tiebreaker Software überprüft die Erreichbarkeit der Nodes in einer MetroCluster Konfiguration und des Clusters, um zu ermitteln, ob ein Standortausfall aufgetreten ist. Über die Tiebreaker Software wird auch unter bestimmten Bedingungen eine Warnmeldung ausgelöst.

Komponenten, die über die Tiebreaker Software überwacht werden

Die Tiebreaker Software überwacht jeden Controller in der MetroCluster-Konfiguration, indem redundante Verbindungen über mehrere Pfade zu einer Node-Management-LIF und zur Cluster-Management-LIF erstellt werden, die beide im IP-Netzwerk gehostet werden.

Die Tiebreaker Software überwacht folgende Komponenten in der MetroCluster Konfiguration:

- Nodes über lokale Node-Schnittstellen
- Ein Cluster über die vom Cluster vorgegebenen Schnittstellen durchführen
- Überlebendes Cluster, um zu ermitteln, ob Verbindung zum Disaster-Standort vorhanden ist (NV Interconnect, Storage und Cluster-Peering)

Wenn es einen Verlust der Verbindung zwischen der Tiebreaker Software und allen Nodes im Cluster und dem Cluster selbst gibt, wird das Cluster durch die Tiebreaker Software als „`nicht erreichbar`“ deklariert. Es dauert etwa drei bis fünf Sekunden, einen Verbindungsfehler zu erkennen. Wenn ein Cluster über die Tiebreaker Software nicht erreichbar ist, muss das verbleibende Cluster (das Cluster, das noch erreichbar ist) angeben, dass alle Links zum Partner-Cluster getrennt werden, bevor die Tiebreaker Software eine Meldung auslöst.

> Alle Links werden getrennt, wenn das verbliebene Cluster nicht mehr über FC (NV Interconnect und Storage) und Intercluster-Peering mit dem Cluster am Disaster-Standort kommunizieren kann.

Ausfallszenarien, während denen Tiebreaker Software eine Warnmeldung auslöst

Die Tiebreaker Software löst eine Warnmeldung aus, wenn das Cluster (alle Nodes) an der Disaster-Site ausgefallen ist oder nicht erreichbar ist und das Cluster auf der überlebenden Site den Status „`AllLinksSevered`“ anzeigt.

Die Tiebreaker Software löst keine Warnmeldung (oder der Alarm wird über ein Vetos ausgelöst) in den folgenden Szenarien aus:

- Wenn in einer MetroCluster Konfiguration mit acht Nodes ein HA-Paar am Disaster-Standort ausfällt
- In einem Cluster, in dem alle Knoten am Katastrophenstandort ausgefallen sind, ein HA-Paar an der überlebenden Site unten und das Cluster auf der überlebenden Site zeigt den Status „`AllLinksSevered`“ an

Die Tiebreaker Software löst eine Warnmeldung aus, jedoch vetoes ONTAP diese Warnmeldung aus. In dieser Situation ist auch ein manuelles Switchover vetoed vetoed

- In jedem Szenario, in dem die Tiebreaker Software mindestens einen Node oder die Cluster-Schnittstelle am Disaster-Standort erreichen kann, kann der verbleibende Standort über FC (NV Interconnect und Storage) oder Intercluster Peering einen Node am Disaster-Standort erreichen

Verwandte Informationen

"Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus"

So erkennt die Tiebreaker Software Konnektivitätsausfälle zwischen Standorten

Die MetroCluster Tiebreaker Software benachrichtigt Sie, wenn alle Verbindungen zwischen den Standorten verloren gehen.

Arten von Netzwerkpfaden

Je nach Konfiguration gibt es drei Typen von Netzwerkpfaden zwischen den beiden Clustern in einer MetroCluster Konfiguration:

- **FC-Netzwerk (in Fabric-Attached MetroCluster-Konfigurationen vorhanden)**

  Dieser Netzwerktyp besteht aus zwei redundanten FC Switch Fabrics. Jede Switch-Fabric verfügt über zwei FC-Switches, wobei sich jeweils ein Switch jedes Switch-Fabric mit einem Cluster befindet. Jedes Cluster verfügt über zwei FC-Switches, eine von jedem Switch-Fabric. Alle Nodes sind mit jedem der zusammengehörige FC-Switches (NV Interconnect und FCP Initiator) verbunden. Die Daten werden über ISL vom Cluster zum Cluster repliziert.

- **Intercluster Peering-Netzwerk**

  Dieser Netzwerktyp besteht aus einem redundanten IP-Netzwerkpfad zwischen den beiden Clustern. Das Cluster-Peering-Netzwerk bietet die Konnektivität, die zur Spiegelung der Konfiguration der Storage Virtual Machine (SVM) erforderlich ist. Die Konfiguration aller SVMs auf einem Cluster wird vom Partner-Cluster gespiegelt.

- **IP-Netzwerk (in MetroCluster IP-Konfigurationen vorhanden)**

  Dieser Netzwerktyp besteht aus zwei redundanten IP Switch-Netzwerken. Jedes Netzwerk verfügt über zwei IP-Switches, wobei sich jeweils ein Switch jedes Switch-Fabric mit einem Cluster befindet. Jedes Cluster verfügt über zwei IP-Switches, einer von jedem Switch-Fabric. Alle Nodes sind mit jedem der zusammengehörige FC-Switches verbunden. Die Daten werden über ISL vom Cluster zum Cluster repliziert.

Monitoring der Konnektivität zwischen Standorten

Die Tiebreaker Software ruft regelmäßig den Status der Konnektivität zwischen Standorten von den Nodes ab. Wenn die NV-Interconnect-Konnektivität verloren geht und das Intercluster-Peering nicht auf Pings reagiert, gehen die Cluster davon aus, dass die Sites isoliert sind und die Tiebreaker Software eine Warnung mit „`AllLinksSevered`“ auslöst. Wenn ein Cluster den Status „`AllLinksSevered`“ identifiziert und der andere Cluster nicht über das Netzwerk erreichbar ist, löst die Tiebreaker Software eine Warnung mit dem Namen „`disaster`“ aus.

Auswirkungen verschiedener Ausfalltypen auf die Tiebreaker Software-Erkennungszeit

Für eine bessere Disaster Recovery-Planung benötigt die MetroCluster Tiebreaker Software einige Zeit, um einen Ausfall zu erkennen. Diese Zeit ist die “disaster detection time”. Die MetroCluster Tiebreaker Software erkennt den Standortausfall innerhalb von 30 Sekunden nach dem Zwischenfall und löst den Disaster Recovery-Vorgang aus, sodass Sie über den Notfall benachrichtigt werden.

Die Erkennungszeit hängt auch von der Art des Ausfalls ab und kann in einigen Szenarien 30 Sekunden überschreiten, die zumeist als „`Rolling Disasters`“ bekannt sind. Die wichtigsten Arten von Rolling Disaster sind:

- Stromausfall
- Panik
- Anhalten oder Neustarten
- Verlust von FC Switches am Disaster-Standort

Stromausfall

Die Tiebreaker Software löst sofort eine Warnmeldung aus, wenn der Node nicht mehr ausgeführt wird. Bei einem Stromausfall halten alle Verbindungen und Updates, wie Intercluster Peering, NV Interconnect und Mailbox-Festplatte, an. Die Zeit, die zwischen dem Cluster nicht mehr erreichbar war, die Erkennung des Ausfalls und der Auslöser, einschließlich der standardmäßigen Silent Time von 5 Sekunden, sollten 30 Sekunden nicht überschreiten.

Panik

In MetroCluster FC-Konfigurationen löst die Tiebreaker Software eine Warnmeldung aus, wenn die NV-Interconnect-Verbindung zwischen den Standorten ausfällt und der verbleibende Standort den Status „`AllLinksSevered`“ anzeigt. Dies geschieht nur, nachdem der Cordump-Prozess abgeschlossen ist. In diesem Szenario könnte die Zeit, die zwischen dem Cluster nicht mehr erreichbar wurde und der Erkennung eines Ausfalls mehr oder ungefähr der Zeit entsprechen, die für den Cordump-Prozess benötigt wurde. In vielen Fällen beträgt die Erkennungszeit mehr als 30 Sekunden.

Wenn ein Knoten nicht mehr funktioniert, aber keine Datei für den coredump-Prozess generiert, sollte die Erkennungszeit nicht länger als 30 Sekunden sein. In MetroCluster-IP-Konfigurationen stoppt der NV die Kommunikation, und der verbleibende Standort erkennt den coredump-Prozess nicht.

Anhalten oder Neustarten

Die Tiebreaker Software löst eine Warnmeldung nur aus, wenn der Knoten nicht verfügbar ist und die überlebende Seite den Status „`AllLinksSevered`“ anzeigt. Die Zeit, die zwischen dem Cluster, das nicht mehr erreichbar ist, und dem Erkennen eines Ausfalls dauert, könnte länger als 30 Sekunden sein. In diesem Szenario hängt die für die Erkennung eines Notfall benötigte Zeit davon ab, wie lange es dauert, bis die Nodes am Disaster-Standort heruntergefahren werden.

Verlust von FC Switches am Disaster-Standort (Fabric-Attached MetroCluster-Konfiguration)

Die Tiebreaker Software löst eine Warnmeldung aus, wenn ein Node nicht mehr ausgeführt wird. Wenn FC-Switches verloren gehen, versucht der Node, den Pfad zu einer Festplatte für ca. 30 Sekunden wiederherzustellen. Während dieser Zeit reagiert der Node auf das Peering-Netzwerk. Wenn beide FC-Switches ausgefallen sind und der Pfad zu einer Festplatte nicht wiederhergestellt werden kann, verursacht der Node einen MultiDiskFailure-Fehler und stoppt. Die zwischen dem FC-Switch-Ausfall und der Anzahl der

Male, die die Nodes MultiDiskFailure-Fehler produzierten, beträgt ca. 30 Sekunden länger. Diese zusätzlichen 30 Sekunden müssen zur Notfallerkennungszeit hinzugefügt werden.

Über die Tiebreaker CLI und die man-Pages

Über die Tiebreaker CLI können Sie die Tiebreaker Software per Remote konfigurieren und die MetroCluster Konfigurationen überwachen.

Die CLI-Eingabeaufforderung wird als NetApp MetroCluster Tiebreaker dargestellt::.

Die man-Pages sind in der CLI verfügbar. Geben Sie dazu den entsprechenden Befehlsnamen an der Eingabeaufforderung ein.

Installation der Tiebreaker Software

Tiebraker Installations-Workflow

Die Tiebreaker Software bietet Monitoring-Funktionen für eine Clustered Storage-Umgebung. Außerdem sendet er SNMP-Benachrichtigungen, wenn Probleme mit der Node-Konnektivität oder im Falle eines Standortnotfalls auftreten.

Informationen zu diesem Workflow

Sie können über diesen Workflow die Tiebreaker Software installieren oder aktualisieren.

1. **"Bereiten Sie sich auf die Installation der Tiebreaker Software vor"**

Vergewissern Sie sich vor der Installation und Konfiguration der Tiebreaker Software, dass Ihr System bestimmte Anforderungen erfüllt.

2. **"Sichern Sie die Installation"**

Bei Konfigurationen mit MetroCluster Tiebreaker 1.5 und höher können Sie das Host-Betriebssystem und die Datenbank sichern und absichern.

3. **"Installieren Sie das Tiebreaker Softwarepaket"**

Führen Sie eine Neuinstallation oder ein Upgrade der Tiebreaker Software durch. Der Installationsvorgang hängt von der Version von Tiebreaker ab, die Sie installieren möchten.

Bereiten Sie sich auf die Installation der Tiebreaker Software vor

Vor der Installation und Konfiguration der Tiebreaker Software sollten Sie überprüfen, ob Ihr System bestimmte Anforderungen erfüllt.

Softwareanforderungen

Je nach der zu installierenden Version von Tiebreaker müssen Sie die folgenden Software-Anforderungen erfüllen.

ONTAP Tiebreaker Version	Unterstützte ONTAP-Versionen	Unterstützte Linux-Versionen	Java/MariaDB-Anforderungen
1.6	ONTAP 9.12.1 und höher	Siehe "OS Support Matrix" Entsprechende Details.	Keine. Die Abhängigkeiten werden mit der Installation gebündelt.
1.5	ONTAP 9.13.1 und frühere Versionen	• Red hat Enterprise Linux 8.1 bis 8.7	Mit Red hat Enterprise Linux 8.1 bis 8.7: • MariaDB 10.x (verwenden Sie die Standardversion, die mit "yum install mariadb-Server.x86_64" installiert wird) • OpenJDK 17, 18 oder 19
1.4	ONTAP 9.11.1 und früher	• Red hat Enterprise Linux 8.1 bis 8.7 • Red hat Enterprise Linux 7 bis 7.9 • CentOS 7 auf 7.9 64 Bit	Mit CentOS: • MariaDB 5.5.52.x/MySQL Server 5.6x • 4 GB RAM • Öffnen Sie JRE 8 Mit Red hat Enterprise Linux 8.1 bis 8.7: *MariaDB 10.x (verwenden Sie die Standardversion, die mit "yum install mariadb-Server.x86_64" installiert ist) *JRE 8
1.3	ONTAP 9.10.1 und frühere Versionen	• Red hat Enterprise Linux 8.1 bis 8.7 • Red hat Enterprise Linux 7 bis 7.9 • CentOS 7 auf 7.9 64 Bit	Mit CentOS: • MariaDB 5.5.52.x/MySQL Server 5.6x • 4 GB RAM • Öffnen Sie JRE 8 Mit Red hat Enterprise Linux 8.1 bis 8.7: • MariaDB 10.x (verwenden Sie die Standardversion, die mit "yum install mariadb-Server.x86_64" installiert wird) • JRE 8

1.21 Px	ONTAP 9.9.1 und frühere Versionen	• Red hat Enterprise Linux 8.1 bis 8.7 • Red hat Enterprise Linux 7 bis 7.9 • CentOS 7 auf 7.9 64 Bit	Mit CentOS: • MariaDB 5.5.52.x/MySQL Server 5.6x • 4 GB RAM • Öffnen Sie JRE 8 Mit Red hat Enterprise Linux 8.1 bis 8.7: • MariaDB 10.x (verwenden Sie die Standardversion, die mit "yum install mariadb-Server.x86_64" installiert wird) • JRE 8

Zusätzlichen Anforderungen

Sie müssen die folgenden zusätzlichen Anforderungen kennen:

- Die Tiebreaker Software wird auf einem dritten Standort installiert, wodurch die Software zwischen einem Switch-Link- (ISL)-Fehler (wenn Verbindungen zwischen den Standorten ausgefallen sind) und einem Standortausfall unterscheiden kann. Ihr Hostsystem muss bestimmte Anforderungen erfüllen, bevor Sie die Tiebreaker Software auf Ihrem lokalen Computer installieren oder aktualisieren können, um die MetroCluster-Konfiguration zu überwachen.
- Sie müssen über „Root“-Berechtigungen verfügen, um die MetroCluster Tiebreaker Software und die abhängigen Pakete zu installieren.
- Sie können pro MetroCluster-Konfiguration nur einen MetroCluster Tiebreaker Monitor verwenden, um Konflikte mit mehreren Tiebreaker Monitoren zu vermeiden.
- Wenn Sie die NTP-Quelle (Network Time Protocol) für die Tiebreaker Software auswählen, müssen Sie eine lokale NTP-Quelle verwenden. Die Tiebreaker Software sollte nicht dieselbe Quelle wie die MetroCluster Standorte verwenden, die von der Tiebreaker Software überwacht werden.
- Festplattenkapazität: 8 GB
- Firewall:
  - Direkter Zugriff zum Einrichten von AutoSupport Meldungen
  - SSH (Port 22/TCP), HTTPS (Port 443/TCP) und Ping (ICMP)

Sicherung der Tiebreaker Host- und Datenbankinstallation

Bei Konfigurationen mit MetroCluster Tiebreaker 1.5 und höher können Sie das Host-Betriebssystem und die Datenbank sichern und absichern.

Sichern Sie den Host

Die folgenden Richtlinien zeigen Ihnen, wie Sie den Host sichern, auf dem die Tiebreaker Software installiert ist.

Empfehlungen für das Benutzermanagement

- Beschränken Sie den Zugriff des „root“-Benutzers.

    - Sie können Benutzer verwenden, die über Root-Zugriff verfügen, um die Tiebreaker Software zu installieren und zu verwalten.
    - Sie können Benutzer verwenden, die nicht in der Lage sind, den Root-Zugriff zu erhöhen, um Tiebreaker Software zu verwalten.
    - Während der Installation müssen Sie eine Gruppe namens „mcctbgrp“ erstellen. Der Host-Root-Benutzer und der Benutzer, der während der Installation erstellt wurde, müssen beide Mitglieder sein. Nur Mitglieder dieser Gruppe können die Tiebreaker Software vollständig verwalten.

> Benutzer, die nicht Mitglied dieser Gruppe sind, können nicht auf die Tiebreaker Software oder CLI zugreifen. Sie können zusätzliche Benutzer auf dem Host erstellen und sie zu Mitgliedern der Gruppe machen. Diese zusätzlichen Mitglieder können die Tiebreaker Software nicht vollständig verwalten. Sie haben Lesezugriff und können keine Monitore hinzufügen, ändern oder löschen.

    - Führen Sie Tiebreaker nicht als Root-Benutzer aus. Verwenden Sie ein dediziertes, nicht privilegiertes Servicekonto, um Tiebreaker auszuführen.
- Ändern Sie die Standard-Community-Zeichenfolge in der Datei „/etc/snmp/snmpd.conf“.
- Minimale Schreibberechtigungen zulassen. Das unprivilegierte Tiebreaker-Dienstkonto sollte keinen Zugriff haben, um seine ausführbare Binärdatei oder Konfigurationsdateien zu überschreiben. Nur Verzeichnisse und Dateien für lokalen Tiebreaker Storage (z. B. für integrierten Back-End Storage) oder Audit-Protokolle sollten vom Tiebreaker Benutzer beschreibbar sein.
- Erlauben Sie anonyme Benutzer nicht.
    - Setzen Sie AllowTcpForwarding auf „Nein“ oder verwenden Sie die Anweisung „Match“, um anonyme Benutzer zu beschränken.

Verwandte Informationen

- "Produktdokumentation zu Red hat Enterprise Linux 8"
- "Produktdokumentation zu Red hat Enterprise Linux 9"

Grundlegende Empfehlungen für die Host-Sicherheit

- Verwenden Sie Festplattenverschlüsselung
    - Sie können die Festplattenverschlüsselung aktivieren. Dabei kann es sich um FullDiskEncryption (Hardware) oder Verschlüsselung durch Hostos (Software) oder durch den SVM-Host handeln.
- Deaktivieren Sie nicht verwendete Dienste, die eingehende Verbindungen zulassen. Sie können jeden Dienst deaktivieren, der nicht verwendet wird. Die Tiebreaker Software erfordert keinen Service für eingehende Verbindungen, da alle Verbindungen aus der Tiebreaker Installation abgehend sind. Folgende Dienste können standardmäßig aktiviert und deaktiviert werden:
    - HTTP/HTTPS-Server
    - FTP-Server
    - Telnet, RSH, rlogin
    - NFS-, CIFS- und anderer Protokollzugriff
    - RDP (RemoteDesktopProtocol), X11 Server, VNC oder andere Remote-Service-Provider für Desktop-PCs.

> Sie müssen entweder den seriellen Konsolenzugriff (falls unterstützt) oder mindestens ein Protokoll aktivieren, um den Host Remote zu verwalten. Wenn Sie alle Protokolle deaktivieren, benötigen Sie physischen Zugriff auf den Host für die Administration.

- Sicherung des Hosts über FIPS
  - Sie können das Host-Betriebssystem im FIPS-konformen Modus installieren und dann Tiebreaker installieren.

    > OpenJDK 19 überprüft beim Start, ob der Host im FIPS-Modus installiert ist. Es sollten keine manuellen Änderungen erforderlich sein.

  - Wenn Sie den Host sichern, müssen Sie sicherstellen, dass der Host ohne Benutzereingriff starten kann. Wenn ein Benutzereingriff erforderlich ist, ist die Tiebreaker-Funktion möglicherweise nicht verfügbar, wenn der Host unerwartet neu startet. In diesem Fall ist die Tiebreaker-Funktion nur nach dem manuellen Eingriff und nach dem vollständigen Booten des Hosts verfügbar.
- Shell-Befehlsverlauf Deaktivieren.
- Aktualisieren Sie häufig. Tiebreaker wird aktiv weiterentwickelt. Regelmäßige Aktualisierungen sind wichtig, um Sicherheitfixes und alle Änderungen an Standardeinstellungen wie Schlüssellängen oder Chiffre Suites zu integrieren.
- Abonnieren Sie die HashiCorp Announcement Mailing-Liste, um Ankündigungen über neue Versionen zu erhalten, und besuchen Sie das Tiebreaker CHANGELOG, um weitere Informationen über aktuelle Updates für neue Versionen zu erhalten.
- Verwenden Sie die richtigen Dateiberechtigungen. Stellen Sie immer sicher, dass die erforderlichen Berechtigungen auf Dateien angewendet werden, bevor Sie die Tiebreaker Software starten, insbesondere auf Dateien mit vertraulichen Informationen.
- Die Multi-Faktor-Authentifizierung (MFA) erhöht die Sicherheit Ihres Unternehmens, da Administratoren mehr als nur einen Benutzernamen und ein Kennwort verwenden müssen, um sich selbst zu identifizieren. Obwohl wichtig, sind Benutzernamen und Passwörter anfällig für Brute-Force-Angriffe und können von Dritten gestohlen werden.
  - Red hat Enterprise Linux 8 bietet MFA, bei dem Benutzer mehr als eine Information bereitstellen müssen, um sich erfolgreich bei einem Konto oder Linux-Host zu authentifizieren. Die zusätzlichen Informationen können ein Einmalpasswort sein, das per SMS an Ihr Mobiltelefon gesendet wird, oder Anmeldedaten von einer App wie Google Authenticator, Twilio Authy oder FreeOTP.

Verwandte Informationen

- "Produktdokumentation zu Red hat Enterprise Linux 8"
- "Produktdokumentation zu Red hat Enterprise Linux 9"

Sichern Sie die Datenbankinstallation

Die folgenden Richtlinien zeigen, wie Sie die MariaDB 10.x Datenbankinstallation sichern und absichern können.

- Beschränken Sie den Zugriff des „root“-Benutzers.
  - Tiebreaker verwendet ein dediziertes Konto. Das Konto und die Tabellen zum Speichern von (Konfigurations-)Daten werden während der Installation von Tiebreaker erstellt. Nur während der Installation ist ein erhöhter Zugriff auf die Datenbank erforderlich.
- Während der Installation sind folgende Zugriffsrechte und Berechtigungen erforderlich:

- Die Fähigkeit, eine Datenbank und Tabellen zu erstellen
- Die Fähigkeit, globale Optionen zu erstellen
- Die Möglichkeit, einen Datenbankbenutzer zu erstellen und das Kennwort festzulegen
- Die Möglichkeit, den Datenbankbenutzer mit der Datenbank und den Tabellen zu verknüpfen und Zugriffsrechte zuzuweisen

> Das Benutzerkonto, das Sie während der Tiebreaker-Installation angeben, muss über alle diese Berechtigungen verfügen. Die Verwendung mehrerer Benutzerkonten für die verschiedenen Aufgaben wird nicht unterstützt.

- Verwenden Sie die Verschlüsselung der Datenbank
  - Die Verschlüsselung ruhender Daten wird unterstützt. "Weitere Informationen zur Verschlüsselung ruhender Daten"
  - Die aktiven Daten sind nicht verschlüsselt. Die Daten im Flug verwenden eine lokale „SOCKS“-Dateiverbindung.
  - FIPS-Konformität für MariaDB — die FIPS-Konformität der Datenbank muss nicht aktiviert werden. Die Installation des Hosts im FIPS-konformen Modus reicht aus.

    "Weitere Informationen zu MySQL Enterprise Transparent Data Encryption (TDE)"

> Die Verschlüsselungseinstellungen müssen vor der Installation der Tiebreaker Software aktiviert sein.

Verwandte Informationen

- Benutzerverwaltung der Datenbank

  "Zugriffssteuerung und Account-Management"

- Sichern Sie die Datenbank

  "MySQL Secure gegen Angreifer"

  "Sicherung von MariaDB"

- Sichern Sie die Vault-Installation

  "Produktionshärtung"

Installieren Sie das Tiebreaker Softwarepaket

Wählen Sie den Installationsvorgang aus

Das Tiebreaker Installationsverfahren, das Sie durchführen, hängt von der Version von Tiebreaker ab, die Sie installieren.

Tiebreaker Version	Gehe zu…
Tiebreak 1.6	"Installieren Sie Tiebreaker 1.6"

Tiebreak 1.5 oder 1.4	"Installieren Sie Tiebreaker 1.5 oder 1.4"

Installieren Sie Tiebreaker 1.6

Führen Sie eine Neuinstallation oder ein Upgrade der Tiebreaker Software durch.

Über diese Aufgabe

- Auf Ihrem Storage-System muss ONTAP 9.12.1 oder höher ausgeführt werden.
- Sie können MetroCluster Tiebreaker als Benutzer ohne Root installieren, der über ausreichende Administratorrechte verfügt, um die Tiebreaker Installation durchzuführen, Tabellen und Benutzer zu erstellen und das Benutzerpasswort festzulegen.

Schritte

1. Laden Sie die Software MetroCluster Tiebreaker 1.6 herunter.

   "NetApp Support Website"

2. Melden Sie sich beim Host als Root-Benutzer an.
3. Wenn Sie ein Upgrade durchführen, überprüfen Sie die Version von Tiebreaker, die Sie ausführen:

   Das folgende Beispiel zeigt Tiebreaker 1.5.

   ```
   [root@mcctb ~] # netapp-metrocluster-tiebreaker-software-cli
   NetApp MetroCluster Tiebreaker :> version show
   NetApp MetroCluster Tiebreaker 1.5: Sun Mar 13 09:59:02 IST 2022
   NetApp MetroCluster Tiebreaker :> exit
   ```

4. Installieren oder aktualisieren Sie die Tiebreaker Software.

Installieren Sie Tiebreaker 1.6

Führen Sie die folgenden Schritte aus, um Tiebreaker 1.6 neu zu installieren.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Starten der Installation:

```
sh MetroClusterTiebreakerInstall-1.6
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Installation an:

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbadminuser
Unix user account "mcctbadminuser" doesn't exist. Do you wish to
create "mcctbadminuser" user account? [Y/N]: y
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
Unix account "mcctbadminuser" created.
Changing password for user mcctbadminuser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
MetroCluster Tiebreaker requires unix user account
"mcctbadminuser" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbadminuser" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
```

```
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE, HOME,
HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME, LS_COLORS, MAIL,
PATH, PWD, SHELL, SHLVL, SSH_CLIENT, SSH_CONNECTION, SSH_TTY,
STAF_TEMP_DIR, TERM, USER, VAULT_ADDR, VAULT_TOKEN,
XDG_RUNTIME_DIR, XDG_SESSION_ID, _, vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:14:28.532+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:14:28.577+0530 [INFO]  core: Initializing version
history cache for core
2023-11-23T15:14:38.552+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:14:38.552+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:14:38.554+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:14:38.555+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:14:38.556+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:38.577+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:14:38.577+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:38.577+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
```

```
2023-11-23T15:14:38.578+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:14:38.581+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:14:38.581+0530 [INFO]  core: restoring leases
2023-11-23T15:14:38.582+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:38.582+0530 [INFO]  identity: entities restored
2023-11-23T15:14:38.582+0530 [INFO]  identity: groups restored
2023-11-23T15:14:38.583+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
09:44:38.582881162 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:14:38.583+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:14:38.998+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:38.999+0530 [INFO]  core: root token generated
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:14:38.999+0530 [INFO]  rollback: stopping rollback
manager
2023-11-23T15:14:38.999+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:14:39.311+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:14:39.312+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:14:39.312+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:14:39.312+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:14:39.313+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
```

```
2023-11-23T15:14:39.314+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:14:39.314+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:14:39.314+0530 [INFO]  core: restoring leases
2023-11-23T15:14:39.314+0530 [INFO]  identity: entities restored
2023-11-23T15:14:39.314+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:14:39.314+0530 [INFO]  identity: groups restored
2023-11-23T15:14:39.315+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:14:39.316+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:14:39.316+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:14:39.795+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:14:39.885+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Installing the NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...                          #
################################# # [100%]

Updating / installing...

1:NetApp-MetroCluster-Tiebreaker-So#
################################# # [100%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-cli
is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.6.


IMPORTANT: Please ensure you store the following private key used
to decrypt audit logs securely in a safe location.
Consider the following recommendations:
- Save it to an encrypted storage device or file.
- Use strong, unique passwords to protect the storage device or
file.
- Restrict access to the private key file to authorized
individuals only.

The Private key is:

-----BEGIN PRIVATE KEY-----

<private_key_id>

-----END PRIVATE KEY-----
```

Upgrade von Tiebreaker 1.5 auf 1.6

Gehen Sie wie folgt vor, um die Tiebreaker 1.5 Softwareversion auf Tiebreaker 1.6 zu aktualisieren.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
==> Vault shutdown triggered
2023-07-21T00:30:22.335+0530 [INFO]  core: marked as sealed
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:22.335+0530 [INFO]  rollback: stopping rollback
manager
2023-07-21T00:30:22.335+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:22.335+0530 [INFO]  core: stopping cluster
listeners
2023-07-21T00:30:22.335+0530 [INFO]  core.cluster-listener:
forwarding rpc listeners stopped
2023-07-21T00:30:22.375+0530 [INFO]  core.cluster-listener: rpc
listeners successfully shut down
2023-07-21T00:30:22.375+0530 [INFO]  core: cluster listeners
successfully shut down
2023-07-21T00:30:22.376+0530 [INFO]  core: vault is sealed
```

```
Starting vault server...
==> Vault server configuration:

             Api Address: <api_address>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE, HOME,
HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME, LS_COLORS, MAIL,
PATH, PWD, SHELL, SHLVL, SSH_CLIENT, SSH_CONNECTION, SSH_TTY,
STAF_TEMP_DIR, TERM, USER, VAULT_ADDR, VAULT_TOKEN,
XDG_RUNTIME_DIR, XDG_SESSION_ID, _, vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-07-21T00:30:33.065+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-07-21T00:30:33.098+0530 [INFO]  core: Initializing version
history cache for core
2023-07-21T00:30:43.092+0530 [INFO]  core: security barrier not
initialized
2023-07-21T00:30:43.092+0530 [INFO]  core: seal configuration
missing, not initialized
2023-07-21T00:30:43.094+0530 [INFO]  core: security barrier not
initialized
2023-07-21T00:30:43.096+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-07-21T00:30:43.098+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.124+0530 [INFO]  core: loaded wrapping token
key
2023-07-21T00:30:43.124+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.124+0530 [INFO]  core: no mounts; adding
```

```
default mount table
2023-07-21T00:30:43.125+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-07-21T00:30:43.126+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-07-21T00:30:43.129+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-07-21T00:30:43.130+0530 [INFO]  rollback: starting rollback
manager
2023-07-21T00:30:43.130+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.130+0530 [INFO]  identity: entities restored
2023-07-21T00:30:43.130+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.131+0530 [INFO]  core: usage gauge collection
is disabled
2023-07-21T00:30:43.131+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.131+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-07-20
19:00:43.131158543 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-07-21T00:30:43.371+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.371+0530 [INFO]  core: root token generated
2023-07-21T00:30:43.371+0530 [INFO]  core: pre-seal teardown
starting
2023-07-21T00:30:43.371+0530 [INFO]  rollback: stopping rollback
manager
2023-07-21T00:30:43.372+0530 [INFO]  core: pre-seal teardown
complete
2023-07-21T00:30:43.694+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=0.0.0.0:8201
2023-07-21T00:30:43.695+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-07-21T00:30:43.695+0530 [INFO]  core: post-unseal setup
starting
2023-07-21T00:30:43.696+0530 [INFO]  core: loaded wrapping token
key
2023-07-21T00:30:43.696+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-07-21T00:30:43.697+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
```

```
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-07-21T00:30:43.698+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-07-21T00:30:43.701+0530 [INFO]  rollback: starting rollback
manager
2023-07-21T00:30:43.702+0530 [INFO]  core: restoring leases
2023-07-21T00:30:43.702+0530 [INFO]  identity: entities restored
2023-07-21T00:30:43.702+0530 [INFO]  expiration: lease restore
complete
2023-07-21T00:30:43.702+0530 [INFO]  identity: groups restored
2023-07-21T00:30:43.702+0530 [INFO]  core: usage gauge collection
is disabled
2023-07-21T00:30:43.703+0530 [INFO]  core: post-unseal setup
complete
2023-07-21T00:30:43.703+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-07-21T00:30:44.226+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-07-21T00:30:44.315+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
```

```
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
```

```
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-cli
is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]


IMPORTANT: Please ensure you store the following private key used
to decrypt audit logs securely in a safe location.
Consider the following recommendations:
- Save it to an encrypted storage device or file.
- Use strong, unique passwords to protect the storage device or
file.
- Restrict access to the private key file to authorized
individuals only.

The Private key is:

-----BEGIN PRIVATE KEY-----
<private_key_id>
-----END PRIVATE KEY-----
```

Upgrade von Tiebreaker 1.4 auf 1.6

Gehen Sie wie folgt vor, um die Tiebreaker 1.4 Softwareversion auf Tiebreaker 1.6 zu aktualisieren.

Schritte

a. Führen Sie den folgenden Befehl auf der aus `[root@mcctb ~] #` Aufforderung zum Aktualisieren der Software:

```
sh MetroClusterTiebreakerInstall-1.6
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

```
Extracting the MetroCluster Tiebreaker installation/upgrade
archive
Install digest hash is Ok
Performing the MetroCluster Tiebreaker code signature check
Install code signature is Ok
Enter unix user account to use for the installation:
mcctbuseradmin1
Unix user account "mcctbuseradmin1" doesn't exist. Do you wish to
create "mcctbuseradmin1" user account? [Y/N]: y
Unix account "mcctbuseradmin1" created.
Changing password for user mcctbuseradmin1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.

Enter database user name : root

Please enter database password for root
Enter password:

Password updated successfully in the database.

MetroCluster Tiebreaker requires unix user account
"mcctbuseradmin1" to be added to the group "mcctbgrp" for admin
access.
Do you wish to add ? [Y/N]: y
Unix user account "mcctbuseradmin1" added to "mcctbgrp".
Do you wish to generate your own public-private key pair for
encrypting audit log? [Y/N]: y
Generating public-private key pair...
Configuring Vault...
Starting vault server...
==> Vault server configuration:
```

```
             Api Address: <api_addess>
                     Cgo: disabled
         Cluster Address: <cluster_address>
   Environment Variables: BASH_FUNC_which%%,
DBUS_SESSION_BUS_ADDRESS, GODEBUG, HISTCONTROL, HISTSIZE, HOME,
HOSTNAME, HOST_ACCOUNT, LANG, LESSOPEN, LOGNAME, LS_COLORS, MAIL,
PATH, PWD, SHELL, SHLVL, SSH_CLIENT, SSH_CONNECTION, SSH_TTY,
STAF_TEMP_DIR, TERM, USER, VAULT_ADDR, VAULT_TOKEN,
XDG_RUNTIME_DIR, XDG_SESSION_ID, _, vault_Addr, which_declare
              Go Version: go1.20.5
              Listener 1: tcp (addr: "0.0.0.0:8200", cluster
address: "0.0.0.0:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "enabled")
               Log Level:
                   Mlock: supported: true, enabled: true
           Recovery Mode: false
                 Storage: file
                 Version: Vault v1.14.0, built 2023-06-
19T11:40:23Z
             Version Sha:
13a649f860186dffe3f3a4459814d87191efc321

==> Vault server started! Log data will stream in below:

2023-11-23T15:58:10.400+0530 [INFO]  proxy environment:
http_proxy="" https_proxy="" no_proxy=""
2023-11-23T15:58:10.432+0530 [INFO]  core: Initializing version
history cache for core
2023-11-23T15:58:20.422+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:58:20.422+0530 [INFO]  core: seal configuration
missing, not initialized
2023-11-23T15:58:20.424+0530 [INFO]  core: security barrier not
initialized
2023-11-23T15:58:20.425+0530 [INFO]  core: security barrier
initialized: stored=1 shares=5 threshold=3
2023-11-23T15:58:20.427+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:20.448+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:58:20.448+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:20.448+0530 [INFO]  core: no mounts; adding
default mount table
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
```

```
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:20.449+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
namespace="ID: root. Path: "
2023-11-23T15:58:20.451+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:58:20.452+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:58:20.452+0530 [INFO]  core: restoring leases
2023-11-23T15:58:20.453+0530 [INFO]  identity: entities restored
2023-11-23T15:58:20.453+0530 [INFO]  identity: groups restored
2023-11-23T15:58:20.453+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:20.453+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:58:20.453+0530 [INFO]  core: Recorded vault
version: vault version=1.14.0 upgrade time="2023-11-23
10:28:20.453481904 +0000 UTC" build date=2023-06-19T11:40:23Z
2023-11-23T15:58:20.818+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:20.819+0530 [INFO]  core: root token generated
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
starting
2023-11-23T15:58:20.819+0530 [INFO]  rollback: stopping rollback
manager
2023-11-23T15:58:20.819+0530 [INFO]  core: pre-seal teardown
complete
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=0.0.0.0:8201
2023-11-23T15:58:21.116+0530 [INFO]  core.cluster-listener:
serving cluster requests: cluster_listen_address=[::]:8201
2023-11-23T15:58:21.117+0530 [INFO]  core: post-unseal setup
starting
2023-11-23T15:58:21.117+0530 [INFO]  core: loaded wrapping token
key
2023-11-23T15:58:21.117+0530 [INFO]  core: successfully setup
plugin catalog: plugin-directory=""
2023-11-23T15:58:21.119+0530 [INFO]  core: successfully mounted:
type=system version="v1.14.0+builtin.vault" path=sys/
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully mounted:
type=identity version="v1.14.0+builtin.vault" path=identity/
```

```
namespace="ID: root. Path: "
2023-11-23T15:58:21.120+0530 [INFO]  core: successfully mounted:
type=cubbyhole version="v1.14.0+builtin.vault" path=cubbyhole/
namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  core: successfully mounted:
type=token version="v1.14.0+builtin.vault" path=token/
namespace="ID: root. Path: "
2023-11-23T15:58:21.123+0530 [INFO]  rollback: starting rollback
manager
2023-11-23T15:58:21.124+0530 [INFO]  core: restoring leases
2023-11-23T15:58:21.124+0530 [INFO]  identity: entities restored
2023-11-23T15:58:21.124+0530 [INFO]  identity: groups restored
2023-11-23T15:58:21.124+0530 [INFO]  expiration: lease restore
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: usage gauge collection
is disabled
2023-11-23T15:58:21.125+0530 [INFO]  core: post-unseal setup
complete
2023-11-23T15:58:21.125+0530 [INFO]  core: vault is unsealed
Success! Uploaded policy: mcctb-policy
2023-11-23T15:58:21.600+0530 [INFO]  core: enabled credential
backend: path=approle/ type=approle version=""
Success! Enabled approle auth method at: approle/
2023-11-23T15:58:21.690+0530 [INFO]  core: successful mount:
namespace="" path=mcctb/ type=kv version=""
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Upgrading to NetApp-MetroCluster-Tiebreaker-Software-1.6-
1.x86_64.rpm
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]
Performing file integrity check
etc/cron.weekly/metrocluster-tiebreaker-support is Ok
etc/cron.weekly/metrocluster-tiebreaker-support-cov is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software is Ok
etc/init.d/netapp-metrocluster-tiebreaker-software-cov is Ok
etc/logrotate.d/mcctb is Ok
opt/netapp/mcctb/lib/common/activation-1.1.1.jar is Ok
opt/netapp/mcctb/lib/common/aopalliance.jar is Ok
opt/netapp/mcctb/lib/common/args4j.jar is Ok
opt/netapp/mcctb/lib/common/aspectjrt.jar is Ok
opt/netapp/mcctb/lib/common/aspectjweaver.jar is Ok
opt/netapp/mcctb/lib/common/asup.jar is Ok
```

```
opt/netapp/mcctb/lib/common/bcpkix-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk15on.jar is Ok
opt/netapp/mcctb/lib/common/bcprov-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bctls-fips-1.0.13.jar is Ok
opt/netapp/mcctb/lib/common/bctls-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/bcutil-jdk18on.jar is Ok
opt/netapp/mcctb/lib/common/cglib.jar is Ok
opt/netapp/mcctb/lib/common/commons-codec.jar is Ok
opt/netapp/mcctb/lib/common/commons-collections4.jar is Ok
opt/netapp/mcctb/lib/common/commons-compress.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.jar is Ok
opt/netapp/mcctb/lib/common/commons-daemon.src.jar is Ok
opt/netapp/mcctb/lib/common/commons-dbcp2.jar is Ok
opt/netapp/mcctb/lib/common/commons-io.jar is Ok
opt/netapp/mcctb/lib/common/commons-lang3.jar is Ok
opt/netapp/mcctb/lib/common/commons-logging.jar is Ok
opt/netapp/mcctb/lib/common/commons-pool2.jar is Ok
opt/netapp/mcctb/lib/common/guava.jar is Ok
opt/netapp/mcctb/lib/common/httpclient.jar is Ok
opt/netapp/mcctb/lib/common/httpcore.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.activation.jar is Ok
opt/netapp/mcctb/lib/common/jakarta.xml.bind-api.jar is Ok
opt/netapp/mcctb/lib/common/java-xmlbuilder.jar is Ok
opt/netapp/mcctb/lib/common/javax.inject.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-api-2.3.1.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-core.jar is Ok
opt/netapp/mcctb/lib/common/jaxb-impl.jar is Ok
opt/netapp/mcctb/lib/common/jline.jar is Ok
opt/netapp/mcctb/lib/common/jna.jar is Ok
opt/netapp/mcctb/lib/common/joda-time.jar is Ok
opt/netapp/mcctb/lib/common/jsch.jar is Ok
opt/netapp/mcctb/lib/common/json.jar is Ok
opt/netapp/mcctb/lib/common/jsvc.zip is Ok
opt/netapp/mcctb/lib/common/junixsocket-common.jar is Ok
opt/netapp/mcctb/lib/common/junixsocket-native-common.jar is Ok
opt/netapp/mcctb/lib/common/logback-classic.jar is Ok
opt/netapp/mcctb/lib/common/logback-core.jar is Ok
opt/netapp/mcctb/lib/common/mail-1.6.2.jar is Ok
opt/netapp/mcctb/lib/common/mariadb-java-client.jar is Ok
opt/netapp/mcctb/lib/common/mcctb-mib.jar is Ok
opt/netapp/mcctb/lib/common/mcctb.jar is Ok
opt/netapp/mcctb/lib/common/mockito-core.jar is Ok
opt/netapp/mcctb/lib/common/slf4j-api.jar is Ok
opt/netapp/mcctb/lib/common/snmp4j.jar is Ok
opt/netapp/mcctb/lib/common/spring-aop.jar is Ok
opt/netapp/mcctb/lib/common/spring-beans.jar is Ok
```

```
opt/netapp/mcctb/lib/common/spring-context-support.jar is Ok
opt/netapp/mcctb/lib/common/spring-context.jar is Ok
opt/netapp/mcctb/lib/common/spring-core.jar is Ok
opt/netapp/mcctb/lib/common/spring-expression.jar is Ok
opt/netapp/mcctb/lib/common/spring-web.jar is Ok
opt/netapp/mcctb/lib/common/vault-java-driver.jar is Ok
opt/netapp/mcctb/lib/common/xz.jar is Ok
opt/netapp/mcctb/lib/org.jacoco.agent-0.8.8-runtime.jar is Ok
opt/netapp/mcctb/bin/mcctb-asup-invoke is Ok
opt/netapp/mcctb/bin/mcctb_postrotate is Ok
opt/netapp/mcctb/bin/netapp-metrocluster-tiebreaker-software-cli
is Ok
/

Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software

Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.6.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]


 IMPORTANT: Please ensure you store the following private key
used to decrypt audit logs securely in a safe location.
Consider the following recommendations:
- Save it to an encrypted storage device or file.
- Use strong, unique passwords to protect the storage device or
file.
- Restrict access to the private key file to authorized
individuals only.

The Private key is:

-----BEGIN PRIVATE KEY-----
<private_key_id>
-----END PRIVATE KEY-----
```

Installieren Sie Tiebreaker 1.5 oder 1.4

Konfigurieren Sie den Administratorzugriff auf die ONTAP-API und SSH

Sie können den Administratorzugriff auf ONTAP-API und SSH konfigurieren.

Schritte

1. Erstellen Sie einen Admin-Benutzer mit ONTAP-API-Zugriff: `security login create -user-or -group-name mcctb -application ontapi -authentication-method password`
2. Erstellen Sie einen Admin-Benutzer mit SSH-Zugriff: `security login create -user-or-group -name mcctb -application ssh -authentication-method password`
3. Überprüfen Sie, ob die neuen Admin-Benutzer erstellt wurden: `security login show`
4. Wiederholen Sie diese Schritte auf dem Partner-Cluster.

> "Administratorauthentifizierung und RBAC" Ist implementiert.

Installation der MetroCluster Tiebreaker Abhängigkeiten

Abhängig von Ihrem Linux-Host-Betriebssystem müssen Sie einen MySQL- oder MariaDB-Server installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren.

Schritte

1. Installieren Sie JRE.

   Installieren Sie JRE

2. Installieren und konfigurieren Sie Vault.

   Installieren und konfigurieren Sie Vault

3. MySQL oder MariaDB Server installieren:

Wenn der Linux-Host lautet	Dann…
Red hat Enterprise Linux 7/CentOS 7	Installieren Sie MySQL Installieren von MySQL Server 5.5.30 oder höher und 5.6.x Versionen unter Red hat Enterprise Linux 7 oder CentOS 7
Red Hat Enterprise Linux 8	Installieren Sie MariaDB Installation von MariaDB Server auf Red hat Enterprise Linux 8

Installieren Sie JRE

Sie müssen JRE auf Ihrem Host-System installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren. Führen Sie für Systeme mit Tiebreaker 1.4 und früheren Versionen JRE 8 aus. Führen Sie für Systeme mit Tiebreaker 1.5 und höher OpenJDK 17, 18 oder 19 aus.

Die Ausgaben im folgenden Beispiel zeigen JRE 1.8.0. (JRE 8).

Schritte

1. Melden Sie sich als „root“-Benutzer oder als sudo-Benutzer an, der in den erweiterten Berechtigungsmodus wechseln kann.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Prüfen Sie auf verfügbare JRE-Versionen:

```
yum search openjdk
```

3. Installieren Sie eine geeignete JRE-Version für die Version von Tiebreaker, die Sie installieren:

```
yum install java-<version>-openjdk.x86_64
```

```
[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
... shortened....
Dependencies Resolved

=========================================================================
Package               Arch   Version                 Repository    Size
=========================================================================
Installing:
 java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4 updates      238 k
 ..
 ..
Transaction Summary
=========================================================================
Install  1 Package  (+ 4 Dependent packages)

Total download size: 34 M
Is this ok [y/d/N]: y

Installed:
java-1.8.0-openjdk.x86_64 1:1.8.0.144-0.b01.el7_4
Complete!
```

Installieren und konfigurieren Sie Vault

Wenn Sie den lokalen Vault-Server nicht verwenden möchten oder haben, müssen Sie Vault installieren. Sie

können diese Standardanleitung für die Installation von Vault verwenden oder alternative Richtlinien in der Hashicorp-Installationsanleitung nachlesen.

> Wenn sich in Ihrem Netzwerk ein Vault-Server befindet, können Sie den MetroCluster Tiebreaker Host für die Verwendung dieser Vault-Installation konfigurieren. Wenn Sie dies tun, müssen Sie Vault nicht auf dem Host installieren.

Schritte

1. Navigieren Sie zum `/bin` Verzeichnis:

```
[root@mcctb] cd /bin
```

2. Laden Sie die Vault-ZIP-Datei herunter.

```
[root@mcctb /bin]#  curl -sO
https://releases.hashicorp.com/vault/1.12.2/vault_1.12.2_linux_amd64.zip
```

3. Entpacken Sie die Vault-Datei.

```
[root@mcctb /bin]# unzip vault_1.12.2_linux_amd64.zip
Archive:  vault_1.12.2_linux_amd64.zip
  inflating: vault
```

4. Überprüfen Sie die Installation.

```
[root@mcctb /bin]# vault -version
Vault v1.12.2 (415e1fe3118eebd5df6cb60d13defdc01aa17b03), built 2022-11-
23T12:53:46Z
```

5. Navigieren Sie zum `/root` Verzeichnis:

```
[root@mcctb /bin] cd /root
```

6. Erstellen Sie eine Vault-Konfigurationsdatei unter `/root` Verzeichnis.

   Am `[root@mcctb ~]` Um den zu erstellen, kopieren Sie den folgenden Befehl, und führen Sie ihn aus `config.hcl` Datei:

```
# cat > config.hcl << EOF
 storage "file" {
  address = "127.0.0.1:8500"
  path    = "/mcctb_vdata/data"
 }
 listener "tcp" {
   address     = "127.0.0.1:8200"
   tls_disable = 1
 }
EOF
```

7. Starten Sie den Vault-Server:

```
[root@mcctb ~] vault server -config config.hcl &
```

8. Exportieren Sie die Vault-Adresse.

```
[root@mcctb ~]# export VAULT_ADDR="http://127.0.0.1:8200"
```

9. Vault Initialisieren.

```
[root@mcctb ~]# vault operator init
2022-12-15T14:57:22.113+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.113+0530 [INFO]  core: seal configuration missing,
not initialized
2022-12-15T14:57:22.114+0530 [INFO]  core: security barrier not
initialized
2022-12-15T14:57:22.116+0530 [INFO]  core: security barrier initialized:
stored=1 shares=5 threshold=3
2022-12-15T14:57:22.118+0530 [INFO]  core: post-unseal setup starting
2022-12-15T14:57:22.137+0530 [INFO]  core: loaded wrapping token key
2022-12-15T14:57:22.137+0530 [INFO]  core: Recorded vault version: vault
version=1.12.2 upgrade time="2022-12-15 09:27:22.137200412 +0000 UTC"
build date=2022-11-23T12:53:46Z
2022-12-15T14:57:22.137+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T14:57:22.137+0530 [INFO]  core: no mounts; adding default
mount table
2022-12-15T14:57:22.143+0530 [INFO]  core: successfully mounted backend:
type=cubbyhole version="" path=cubbyhole/
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=system version="" path=sys/
```

```
2022-12-15T14:57:22.144+0530 [INFO]  core: successfully mounted backend:
type=identity version="" path=identity/
2022-12-15T14:57:22.148+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T14:57:22.149+0530 [INFO]  rollback: starting rollback manager
2022-12-15T14:57:22.149+0530 [INFO]  core: restoring leases
2022-12-15T14:57:22.150+0530 [INFO]  expiration: lease restore complete
2022-12-15T14:57:22.150+0530 [INFO]  identity: entities restored
2022-12-15T14:57:22.150+0530 [INFO]  identity: groups restored
2022-12-15T14:57:22.151+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T14:57:23.385+0530 [INFO]  core: post-unseal setup complete
2022-12-15T14:57:23.387+0530 [INFO]  core: root token generated
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown starting
2022-12-15T14:57:23.387+0530 [INFO]  rollback: stopping rollback manager
2022-12-15T14:57:23.387+0530 [INFO]  core: pre-seal teardown complete
Unseal Key 1: <unseal_key_1_id>
Unseal Key 2: <unseal_key_2_id>
Unseal Key 3: <unseal_key_3_id>
Unseal Key 4: <unseal_key_4_id>
Unseal Key 5: <unseal_key_5_id>

Initial Root Token: <initial_root_token_id>


Vault initialized with 5 key shares and a key threshold of 3. Please
securely
distribute the key shares printed above. When the Vault is re-sealed,
restarted, or stopped, you must supply at least 3 of these keys to
unseal it
before it can start servicing requests.

Vault does not store the generated root key. Without at least 3 keys to
reconstruct the root key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum
of
existing unseal keys shares. See "vault operator rekey" for more
information.
```

Sie müssen die Schlüssel-IDs und das erste Root-Token an einem sicheren Ort aufzeichnen und speichern, um es später in dem Verfahren verwenden zu können.

10. Exportieren Sie das Vault-Root-Token.

```
[root@mcctb ~]#  export VAULT_TOKEN="<initial_root_token_id>"
```

11. Heben Sie die Versiegelung des Tresors auf, indem Sie drei der fünf erstellten Schlüssel verwenden.

    Sie müssen den ausführen `vault operator unseal` Befehl für jeden der drei Tasten:

    a. Lösen Sie den Tresor mit dem ersten Schlüssel:

    ```
    [root@mcctb ~]# vault operator unseal
    Unseal Key (will be hidden):
    Key                Value
    ---                -----
    Seal Type          shamir
    Initialized        true
    Sealed             true
    Total Shares       5
    Threshold          3
    Unseal Progress    1/3
    Unseal Nonce       <unseal_key_1_id>
    Version            1.12.2
    Build Date         2022-11-23T12:53:46Z
    Storage Type       file
    HA Enabled         false
    ```

    b. Lösen Sie den Tresor mit dem zweiten Schlüssel:

    ```
    [root@mcctb ~]# vault operator unseal
    Unseal Key (will be hidden):
    Key                Value
    ---                -----
    Seal Type          shamir
    Initialized        true
    Sealed             true
    Total Shares       5
    Threshold          3
    Unseal Progress    2/3
    Unseal Nonce       <unseal_key_2_id>
    Version            1.12.2
    Build Date         2022-11-23T12:53:46Z
    Storage Type       file
    HA Enabled         false
    ```

    c. Lösen Sie den Tresor mit dem dritten Schlüssel:

```
[root@mcctb ~]# vault operator unseal
Unseal Key (will be hidden):
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener.tcp:
starting listener: listener_address=127.0.0.1:8201
2022-12-15T15:15:00.980+0530 [INFO]  core.cluster-listener: serving
cluster requests: cluster_listen_address=127.0.0.1:8201
2022-12-15T15:15:00.981+0530 [INFO]  core: post-unseal setup starting
2022-12-15T15:15:00.981+0530 [INFO]  core: loaded wrapping token key
2022-12-15T15:15:00.982+0530 [INFO]  core: successfully setup plugin
catalog: plugin-directory=""
2022-12-15T15:15:00.983+0530 [INFO]  core: successfully mounted
backend: type=system version="" path=sys/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=identity version="" path=identity/
2022-12-15T15:15:00.984+0530 [INFO]  core: successfully mounted
backend: type=cubbyhole version="" path=cubbyhole/
2022-12-15T15:15:00.986+0530 [INFO]  core: successfully enabled
credential backend: type=token version="" path=token/ namespace="ID:
root. Path: "
2022-12-15T15:15:00.986+0530 [INFO]  rollback: starting rollback
manager
2022-12-15T15:15:00.987+0530 [INFO]  core: restoring leases
2022-12-15T15:15:00.987+0530 [INFO]  expiration: lease restore
complete
2022-12-15T15:15:00.987+0530 [INFO]  identity: entities restored
2022-12-15T15:15:00.987+0530 [INFO]  identity: groups restored
2022-12-15T15:15:00.988+0530 [INFO]  core: usage gauge collection is
disabled
2022-12-15T15:15:00.989+0530 [INFO]  core: post-unseal setup complete
2022-12-15T15:15:00.989+0530 [INFO]  core: vault is unsealed
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

12. Vergewissern Sie sich, dass der Status „Vault Sealed“ falsch ist.

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault-cluster
Cluster ID      <cluster_id>
HA Enabled      false
```

13. Konfigurieren Sie den Vault-Dienst für den Start beim Booten.
    a. Führen Sie den folgenden Befehl aus: `cd /etc/systemd/system`

    ```
    [root@mcctb ~]#  cd /etc/systemd/system
    ```

    b. Am `[root@mcctb system]` Um die Vault-Dienstdatei zu erstellen, kopieren Sie den folgenden Befehl, und führen Sie ihn aus.

    ```
    # cat > vault.service << EOF
    [Unit]
    Description=Vault Service
    After=mariadb.service

    [Service]
    Type=forking
    ExecStart=/usr/bin/vault server -config /root/config.hcl &
    Restart=on-failure

    [Install]
    WantedBy=multi-user.target
    EOF
    ```

    c. Führen Sie den folgenden Befehl aus: `systemctl daemon-reload`

    ```
    [root@mcctb system]#  systemctl daemon-reload
    ```

    d. Führen Sie den folgenden Befehl aus: `systemctl enable vault.service`

```
[root@mcctb system]#  systemctl enable vault.service
Created symlink /etc/systemd/system/multi-
user.target.wants/vault.service → /etc/systemd/system/vault.service.
```

Sie werden während der Installation von MetroCluster Tiebreaker aufgefordert, diese Funktion zu verwenden. Wenn Sie die Methode zum Entsiegeln von Tresor ändern möchten, müssen Sie die MetroCluster Tiebreaker Software deinstallieren und neu installieren.

Installieren von MySQL Server 5.5.30 oder höher und 5.6.x Versionen unter Red hat Enterprise Linux 7 oder CentOS 7

Sie müssen MySQL Server 5.5.30 oder höher und 5.6.x-Version auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker-Software installieren oder aktualisieren.

Schritte

1. Melden Sie sich als Root-Benutzer oder sudo-Benutzer an, der in den erweiterten Berechtigungsmodus wechseln kann.

   ```
   login as: root
   root@mcctb's password:
   Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
   ```

2. Fügen Sie das MySQL-Repository zum Host-System hinzu:

   ```
   [root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-
   release-el6-11.noarch.rpm
   ```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
=============================================================================
========
Package               Arch   Version
                                     Repository
Size
=============================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
=============================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Deaktivieren Sie das MySQL 57-Repository:

```
[root@mcctb ~]# yum-config-manager --disable mysql57-community
```

4. Aktivieren Sie das MySQL 56-Repository:

```
[root@mcctb ~]# yum-config-manager --enable mysql56-community
```

5. Repository aktivieren:

```
[root@mcctb ~]# yum repolist enabled | grep "mysql.-community."
```

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Installieren Sie den MySQL Community Server:

```
[root@mcctb ~]# yum install mysql-community-server
```

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
 .....Output truncated.....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
=================================================================================
Package                          Arch   Version       Repository
Size
=================================================================================
Installing:
 mysql-community-client         x86_64  5.6.29-2.el6  mysql56-community
18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs           x86_64  5.6.29-2.el6  mysql56-community
1.9 M
```

```
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat    x86_64  5.6.29-2.el6  mysql56-community
1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server         x86_64  5.6.29-2.el6  mysql56-community
53  M
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common          x86_64  5.6.29-2.el6  mysql56-community
308 k

Transaction Summary
=================================================================================
=======
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm       |  18 MB
00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm       | 308 kB
00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm         | 1.9 MB
00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm  | 1.6 MB
00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm       |  53 MB
03:42
 ---------------------------------------------------------------------------
--------
Total                                               289 kB/s |  74 MB
04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
<key_id> NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch
         (@/mysql-community-release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
```

```
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
  mysql-community-client.x86_64 0:5.6.29-2.el6
  mysql-community-libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6
  mysql-community-server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6
  mysql-server.x86_64 0:5.1.71-1.el6
Complete!
```

7. MySQL-Server starten:

```
[root@mcctb ~]# service mysqld start
```

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT value is deprecated. Please use
--explicit_defaults_for_timestamp server option (see documentation
for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29)
        starting as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
        buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
       number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
.....Output truncated.....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Bestätigen Sie, dass MySQL-Server ausgeführt wird:

```
[root@mcctb ~]# service mysqld status
```

```
mysqld (pid  2739) is running...
```

9. Konfigurieren Sie die Sicherheits- und Kennworteinstellungen:

```
[root@mcctb ~]# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
       SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install
                                                          hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorization.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test';
```

```
database doesn't exist
 ... Failed!  Not critical, keep moving...
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Überprüfen Sie, ob die MySQL-Anmeldung funktioniert:

```
[root@mcctb ~]# mysql -u root -p
```

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

Wenn der MySQL-Login funktioniert, endet die Ausgabe am `mysql>` Eingabeaufforderung:

Aktivieren der Einstellung Autostart von MySQL

Sie sollten überprüfen, ob die Autostart-Funktion für den MySQL-Daemon aktiviert ist. Durch Aktivieren des MySQL-Daemon wird MySQL automatisch neu gestartet, wenn das System, auf dem die MetroCluster Tiebreaker Software ausgeführt wird, neu gestartet wird. Wenn der MySQL-Daemon nicht ausgeführt wird, wird die Tiebreaker-Software weiterhin ausgeführt, kann aber nicht neu gestartet werden und

Konfigurationsänderungen können nicht vorgenommen werden.

Schritt

1. Vergewissern Sie sich, dass MySQL beim Starten automatisch gestartet wird:

   ```
   [root@mcctb ~]# systemctl list-unit-files mysqld.service
   ```

   ```
   UNIT FILE          State
   ------------------ ----------
   mysqld.service     enabled
   ```

   Wenn MySQL beim Starten nicht aktiviert ist, lesen Sie die MySQL-Dokumentation, um die Autostart-Funktion für Ihre Installation zu aktivieren.

Installation von MariaDB Server auf Red hat Enterprise Linux 8

Sie müssen MariaDB Server auf Ihrem Hostsystem installieren, bevor Sie die Tiebreaker Software installieren oder aktualisieren.

Bevor Sie beginnen

Ihr Hostsystem muss unter Red hat Enterprise Linux (RHEL) 8 ausgeführt werden.

Schritte

1. Melden Sie sich als an `root` Benutzer oder ein Benutzer, der in den erweiterten Berechtigungsmodus wechseln kann.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

1. Installieren Sie den MariaDB-Server:

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   ```

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   Loaded plugins: fastestmirror, langpacks
    ...
    ...

   ================================================================================
    Package                      Arch   Version         Repository
   Size
   ================================================================================
   Installing:
   ```

```
mariadb-server               x86_64   1:5.5.56-2.el7   base
11 M
Installing for dependencies:

Transaction Summary
=========================================================================
===
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y

Downloading packages:
No Presto metadata available for base warning:
/var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature,
key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3 MB  00:00:13 ETA
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
-------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7
perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7
perl-DBD-MySQL.x86_64 0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7
perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7
perl-PlRPC.noarch 0:0.2020-14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

2. MariaDB-Server starten:

```
[root@mcctb ~]# systemctl start mariadb
```

3. Überprüfen Sie, ob der MariaDB-Server gestartet wurde:

```
[root@mcctb ~]# systemctl status mariadb
```

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 mcctb systemd[1]: Started MariaDB database server.
```

4. Konfigurieren Sie die Sicherheits- und Kennworteinstellungen:

> Wenn Sie zur Eingabe des Root-Passworts aufgefordert werden, lassen Sie es leer, und drücken Sie die EINGABETASTE, um mit der Konfiguration der Sicherheits- und Kennworteinstellungen fortzufahren.

```
[root@mcctb ~]# mysql_secure_installation
```

```
root@localhost systemd]# mysql_secure_installation

 NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing
anyone
to log into MariaDB without having to have a user account created for
```

```
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
  ... Success!
 - Removing privileges on test database...
   ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]

 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Aktivieren der Autostart-Einstellung für den MariaDB-Server

Überprüfen Sie, ob die Autostart-Funktion für den MariaDB-Server aktiviert ist. Wenn Sie die Autostart-Funktion nicht aktivieren und das System, auf dem sich die MetroCluster Tiebreaker Software befindet, neu gestartet werden muss, wird die Tiebreaker Software ausgeführt, der MariaDB-Service kann jedoch nicht neu gestartet werden und Konfigurationsänderungen können nicht vorgenommen werden.

Schritte

1. Aktivieren des Autostart-Dienstes:

```
[root@mcctb ~]# systemctl enable mariadb.service
```

2. Vergewissern Sie sich, dass MariaDB beim Starten automatisch gestartet wird:

```
[root@mcctb ~]# systemctl list-unit-files mariadb.service
```

```
UNIT FILE          State
------------------ ----------
mariadb.service    enabled
```

Installieren oder Aktualisieren des Softwarepakets

Sie müssen die MetroCluster Tiebreaker Software auf Ihrem lokalen Computer installieren oder aktualisieren, um MetroCluster Konfigurationen zu überwachen.

Über diese Aufgabe

- Ihr Storage-System muss ONTAP 8.3.x oder höher ausgeführt werden.
- Sie müssen OpenJDK mithilfe der installiert haben `yum install java-x.x.x-openjdk` Befehl. Führen Sie für Systeme mit Tiebreaker 1.4 und früheren Versionen JRE 8 aus. Führen Sie für Systeme mit Tiebreaker 1.5 und höher OpenJDK 17, 18 oder 19 aus. Die Ausgaben im Beispiel zeigen JRE 1.8.0. (JRE 8).
- Sie können MetroCluster Tiebreaker als Benutzer ohne Root installieren, der über ausreichende Administratorrechte verfügt, um die Tiebreaker Installation durchzuführen, Tabellen und Benutzer zu erstellen und das Benutzerpasswort festzulegen.

Schritte

1. Laden Sie die MetroCluster Tiebreaker Software herunter. In diesem Beispiel wird Version 1.5 verwendet.

   "NetApp Support Website"

2. Laden Sie die herunter `MetroCluster_Tiebreaker_RPM_GPG` Schlüssel:

   "NetApp Support Website"

3. Melden Sie sich beim Host als Root-Benutzer an.
4. Erstellen Sie einen Benutzer, der kein Root-Benutzer ist, und den `mcctbgrp` Gruppieren.

   a. Erstellen Sie einen Benutzer, der kein Root-Benutzer ist, und legen Sie das Passwort fest.

      Mit den folgenden Beispielbefehlen wird ein nicht-root-Benutzer mit dem Namen erstellt `mcctbuser1`:

```
[root@mcctb ~]# useradd mcctbuser1
[root@mcctb ~]# passwd mcctbuser1
Changing password for user mcctbuser1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

b. Erstellen Sie eine Gruppe mit dem Namen `mcctbgrp`:

```
[root@mcctb ~~]# groupadd mcctbgrp
```

c. Fügen Sie den nicht-Root-Benutzer, den Sie erstellt haben, zum hinzu `mcctbgrp` Gruppieren.

Mit dem folgenden Befehl wird hinzugefügt `mcctbuser1` Bis zum `mcctbgrp` Gruppe:

```
[root@mcctb ~]# usermod -a -G mcctbgrp mcctbuser1
```

5. Überprüfen Sie die RPM-Datei.

Führen Sie die folgenden Teilschritte aus dem Verzeichnis mit dem RPM-Schlüssel aus.

a. Laden Sie die RPM-Schlüsseldatei herunter, und importieren Sie sie:

```
[root@mcctb ~]# rpm --import MetroCluster_Tiebreaker_RPM_GPG.key
```

b. Überprüfen Sie, ob der richtige Schlüssel importiert wurde, indem Sie den Fingerabdruck überprüfen.

Das folgende Beispiel zeigt einen korrekten Schlüsselfinger:

```
root@mcctb:~/signing/mcctb-rpms# gpg --show-keys --with-fingerprint
MetroCluster_Tiebreaker_RPM_GPG.key
pub   rsa3072 2022-11-17 [SCEA] [expires: 2025-11-16]
      65AC 1562 E28A 1497 7BBD  7251 2855 EB02 3E77 FAE5
uid                      MCCTB-RPM (mcctb RPM production signing)
<mcctb-rpm@netapp.com>
```

a. Überprüfen Sie die Signatur: `rpm --checksig NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

```
NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm: digests OK
```

> Sie dürfen mit der Installation erst fortfahren, nachdem Sie die Signatur erfolgreich verifiziert haben.

6. Installieren oder aktualisieren Sie die Tiebreaker Software:

> Ein Upgrade auf Tiebreaker Version 1.5 ist nur möglich, wenn Sie ein Upgrade von Tiebreaker Version 1.4 durchführen. Ein Upgrade von früheren Versionen auf Tiebreaker 1.5 wird nicht unterstützt.

Wählen Sie das richtige Verfahren aus der folgenden Liste aus, je nachdem, ob Sie eine neue Installation durchführen oder eine vorhandene Installation aktualisieren.

Führen Sie eine neue Installation durch

a. Abrufen und Aufzeichnen des absoluten Pfads für Java:

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Führen Sie den folgenden Befehl aus: `rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.5-1.x86_64.rpm`

   Das System zeigt die folgende Ausgabe für eine erfolgreiche Installation an:

> Wenn Sie während der Installation dazu aufgefordert werden, geben Sie den nicht-Root-Benutzer an, den Sie zuvor erstellt und dem zugewiesen haben `mcctbgrp` Gruppieren.

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Enter database user name:
root
Please enter database password for root
Enter password:
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Created symlink /etc/systemd/system/multi-
user.target.wants/netapp-metrocluster-tiebreaker-software.service
→ /etc/systemd/system/netapp-metrocluster-tiebreaker-
software.service.
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully installed NetApp MetroCluster Tiebreaker software
version 1.5.
```

Aktualisierung einer vorhandenen Installation

a. Überprüfen Sie, ob eine unterstützte Version von OpenJDK installiert ist und die aktuelle Java-Version auf dem Host ist.

> Für Upgrades auf Tiebreaker 1.5 müssen Sie entweder OpenJDK Version 17, 18 oder 19 installieren.

```
[root@mcctb ~]# readlink -f /usr/bin/java
/usr/lib/jvm/java-19-openjdk-19.0.0.0.36-
2.rolling.el8.x86_64/bin/java
```

b. Überprüfen Sie, ob der Vault-Dienst entsiegelt ist und ausgeführt wird: `vault status`

```
[root@mcctb ~]# vault status
Key             Value
---             -----
Seal Type       shamir
Initialized     true
Sealed          false
Total Shares    5
Threshold       3
Version         1.12.2
Build Date      2022-11-23T12:53:46Z
Storage Type    file
Cluster Name    vault
Cluster ID      <cluster_id>
HA Enabled      false
```

c. Upgrade der Tiebreaker Software

```
[root@mcctb ~]# rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-
1.5-1.x86_64.rpm
```

Das System zeigt die folgende Ausgabe für eine erfolgreiche Aktualisierung an:

```
Verifying...
################################# [100%]
Preparing...
################################# [100%]
Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
So################################# [ 50%]

Enter the absolute path for Java : /usr/lib/jvm/java-19-openjdk-
19.0.0.0.36-2.rolling.el8.x86_64/bin/java
Verifying if Java exists...
Found Java. Proceeding with the installation.
Enter host user account to use for the installation:
mcctbuser1
User account mcctbuser1 found. Proceeding with the installation
Sealed          false
Do you wish to auto unseal vault(y/n)?y
Enter the key1:
Enter the key2:
Enter the key3:
Success! Uploaded policy: mcctb-policy
Error enabling approle auth: Error making API request.
URL: POST http://127.0.0.1:8200/v1/sys/auth/approle
Code: 400. Errors:
* path is already in use at approle/
Success! Enabled the kv secrets engine at: mcctb/
Success! Data written to: auth/approle/role/mcctb-app
Enter database user name : root
Please enter database password for root
Enter password:
Password updated successfully in the database.
Password updated successfully in the vault.
Synchronizing state of netapp-metrocluster-tiebreaker-
software.service with SysV service script with
/usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable netapp-
metrocluster-tiebreaker-software
Attempting to start NetApp MetroCluster Tiebreaker software
services
Started NetApp MetroCluster Tiebreaker software services
Successfully upgraded NetApp MetroCluster Tiebreaker software to
version 1.5.
Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
So################################# [100%]
```

> Wenn Sie das falsche MySQL-Root-Passwort eingeben, zeigt die Tiebreaker Software an, dass sie erfolgreich installiert wurde, zeigt aber „Access Denied“-Meldungen an. Um das Problem zu lösen, müssen Sie die Tiebreaker Software mit verwenden `rpm -e` Führen Sie einen Befehl aus, und installieren Sie dann die Software mit dem richtigen MySQL-Root-Passwort neu.

7. Prüfen Sie die Tiebreaker Konnektivität zur MetroCluster Software, indem Sie über den Tiebreaker Host eine SSH-Verbindung zu jedem Node-Management-LIFs und Cluster-Management-LIFs öffnen.

Verwandte Informationen

"NetApp Support"

Aktualisieren Sie den Host, auf dem der Tiebreaker Monitor ausgeführt wird

Unter Umständen müssen Sie den Host aktualisieren, auf dem der Tiebreaker Monitor ausgeführt wird.

Schritte

1. Deinstallieren Sie die Tiebreaker Software:

   ```
   rpm -e NetApp-MetroCluster-Tiebreaker-Software
   ```

2. Aktualisieren Sie den Host. Weitere Informationen finden Sie in der Dokumentation zum Host-Betriebssystem.
3. Installieren Sie die Tiebreaker Software neu.

   Führen Sie eine Neuinstallation von Tiebreaker durch, indem Sie die unter beschriebenen Schritte ausführen "Installation der Tiebreaker Software".

Konfigurieren der Tiebreaker Software

Nach der Installation der Tiebreaker Software können MetroCluster Konfigurationen hinzugefügt oder geändert oder aus der Tiebreaker Software entfernt werden.

Starten der Tiebreaker Software-CLI

Nach der Installation der Tiebreaker Software müssen Sie die CLI starten, um die Software zu konfigurieren.

1. Starten Sie die CLI von der Eingabeaufforderung des Hosts, auf dem Sie die Software installiert haben:

   ```
   netapp-metrocluster-tiebreaker-software-cli
   ```

2. Geben Sie nach der Installation und während des ersten Startvorgangs das Kennwort für den Tiebreaker-Benutzer ein, um auf die Datenbank zuzugreifen. Dies ist das Kennwort, das Sie während der Installation für den Datenbankbenutzer angegeben haben.

Hinzufügen von MetroCluster Konfigurationen

Nach der Installation der NetApp MetroCluster Tiebreaker Software können mehrere MetroCluster Konfigurationen gleichzeitig hinzugefügt werden.

Sie müssen die MetroCluster-Konfiguration in einer ONTAP-Umgebung installiert und die Einstellungen in der Software aktiviert haben.

1. Über die Tiebreaker Befehlszeilenschnittstelle (CLI) können Sie mit dem Hinzufügungs-Befehl MetroCluster-Konfigurationen hinzufügen.

   Wenn Sie den Hostnamen verwenden, muss dieser der vollständig qualifizierte Domänenname (FQDN) sein.

   Im folgenden Beispiel wird die Konfiguration von Cluster_A gezeigt:

   ```
   NetApp MetroCluster Tiebreaker :> monitor add wizard
   Enter monitor Name: cluster_A
   Enter Cluster IP Address: 10.222.196.130
   Enter Cluster Username: admin
   Enter Cluster Password:
   Enter Peer Cluster IP Address: 10.222.196.40
   Enter Peer Cluster Username: admin
   Enter Peer Cluster Password:
   Successfully added monitor to NetApp MetroCluster Tiebreaker software.
   ```

2. Überprüfen Sie, ob die MetroCluster-Konfiguration ordnungsgemäß mit der Tiebreaker CLI hinzugefügt wurde `monitor show -status` Befehl.

   ```
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```

3. Deaktivieren Sie den Observer-Modus für die Tiebreaker-Software, um eine Umschaltung automatisch zu starten, nachdem ein Standortfehler erkannt wurde:

   `monitor modify -monitor-name monitor_name -observer-mode false`

   ```
   NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
   -observer-mode false
   Warning: If you are turning observer-mode to false, make sure to review
   the 'risks and limitations'
   as described in the MetroCluster Tiebreaker installation and
   configuration.
   Are you sure you want to enable automatic switchover capability for
   monitor "8pack"? [Y/N]: y
   ```

Verwandte Informationen

"Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus"

Befehle zum Ändern von MetroCluster Tiebreaker Konfigurationen

Sie können die MetroCluster-Konfiguration jederzeit ändern, wenn Sie die Einstellungen ändern möchten.

Der Tiebreaker CLI-Monitor-Änderungsbefehl kann mit einer der folgenden Optionen verwendet werden. Mit dem Befehl Monitor show -Status können Sie Ihre Änderungen bestätigen.

Option	Beschreibung
-Monitor-Name	Name der MetroCluster-Konfiguration
-Monitor aktivieren	Aktiviert und deaktiviert die Überwachung der MetroCluster-Konfiguration
-Stumm-Periode	Zeitraum in Sekunden, für die die MetroCluster Tiebreaker Software nach der Erkennung einen Standortausfall bestätigt
-Observer-Modus	Der Observer-Modus (True) bietet nur Überwachung und löst bei einem Standortunfall keine Umschaltung aus. Der Online-Modus (false) löst bei einem Standortausfall eine Umschaltung aus. • "Wie die Tiebreaker Software Standortausfällen erkennt" • "Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus"

Im folgenden Beispiel wird der Silent Period für die Konfiguration geändert.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name cluster_A
-silent-period 15
Successfully modified monitor in NetApp MetroCluster Tiebreaker
software.
```

Über die Tiebreaker CLI `debug` Mit dem Befehl kann der Protokollierungsmodus geändert werden.

Befehl	Beschreibung
Debug-Status	Zeigt den Status des Debug-Modus an
Debug aktivieren	Aktiviert den Debug-Modus für die Protokollierung
Debug deaktivieren	Deaktiviert den Debug-Modus für die Protokollierung

Bei Systemen mit Tiebreaker 1.4 und älteren Versionen bietet die Tiebreaker CLI `update-mcctb-password` Mit dem Befehl kann das Benutzerpasswort aktualisiert werden. Dieser Befehl ist in Tiebreak 1.5 und höher veraltet.

Befehl	Beschreibung
Update-mcctb-password	Das Benutzerpasswort wurde erfolgreich aktualisiert

Entfernen von MetroCluster-Konfigurationen

Sie können die MetroCluster-Konfiguration entfernen, die von der Tiebreaker Software überwacht wird, wenn Sie keine MetroCluster-Konfiguration mehr überwachen möchten.

1. Verwenden Sie die Tiebreaker CLI `monitor remove` Befehl zum Entfernen der MetroCluster-Konfiguration.

   Im folgenden Beispiel wird „`Cluster_A`“ aus der Software entfernt:

   ```
   NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
   Successfully removed monitor from NetApp MetroCluster Tiebreaker
   software.
   ```

2. Überprüfen Sie, ob die MetroCluster-Konfiguration ordnungsgemäß mithilfe der Tiebreaker CLI entfernt wird `monitor show -status` Befehl.

   ```
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```

Konfigurieren von SNMP-Einstellungen für Tiebreaker Software

Um SNMP mit der Tiebreaker Software verwenden zu können, müssen Sie die SNMP-Einstellungen konfigurieren.

1. Verwenden Sie die Tiebreaker CLI `snmp config wizard` Befehl zum Hinzufügen von MetroCluster-Konfigurationen.

   > Derzeit wird nur ein SNMP-Trap-Host unterstützt.

   Das folgende Beispiel zeigt die Konfiguration eines SNMP-Empfängers, der SNMP V3 mit einer IP-Adresse 10.240.45.66 und der Portnummer 162 für Trap-Nachrichten unterstützt. Die Tiebreaker Software ist bereit, Traps an den von Ihnen angegebenen SNMP-Empfänger zu senden.

```
NetApp MetroCluster Tiebreaker :> snmp config wizard
Enter SNMP Version[V1/V3]: v3
Enter SNMP Host: 10.240.45.66
Enter SNMP Port: 162
Enter SNMP V3 Security Name: v3sec
Enter SNMP V3 Authentication password:
Enter SNMP V3 Privacy password:
Engine ID : 8000031504932eff571825192a6f1193b265e24593
Successfully added SNMP properties to NetApp MetroCluster Tiebreaker
software.
```

Sie sollten SNMPv3 konfigurieren, da SNMPv1 nicht sicher ist. Stellen Sie sicher, dass der Standard-Community-String **NOT** auf public gesetzt ist.

2. Vergewissern Sie sich, dass die SNMP-Einstellungen konfiguriert sind:

   ```
   snmp config test
   ```

   Das folgende Beispiel zeigt, dass die Tiebreaker Software einen SNMP Trap für den Event TEST_SNMP_CONFIG senden kann:

   ```
   NetApp MetroCluster Tiebreaker :> snmp config test
   Sending SNMP trap to localhost. Version : V1.
   Successfully sent SNMP trap for event TEST_SNMP_CONFIG
   NetApp MetroCluster Tiebreaker :>
   ```

Monitoring der MetroCluster-Konfiguration

Die MetroCluster Tiebreaker Software automatisiert den Recovery-Prozess, da Kunden damit den MetroCluster-Konfigurationsstatus überwachen, SNMP-Ereignisse und Traps bewerten, die an den NetApp Kunden-Support gesendet werden, und den Status von Monitoring-Vorgängen anzeigen können.

AutoSupport wird konfiguriert

Standardmäßig werden AutoSupport-Meldungen eine Woche nach der Installation der Tiebreaker Software an NetApp gesendet. Ereignisse, die die AutoSupport-Benachrichtigung auslösen, sind eine Panik der Tiebreaker Software, die Erkennung von Ausfallszenarien für MetroCluster-Konfigurationen oder ein unbekannter MetroCluster-Konfigurationsstatus.

Bevor Sie beginnen

Sie müssen über einen direkten Zugriff für das Einrichten von AutoSupport Meldungen verfügen.

Schritte

1. Verwenden Sie den Tiebreaker CLI-AutoSupport-Befehl mit einer der folgenden Optionen:

Option	Beschreibung
-Rufe	Sendet eine AutoSupport-Nachricht an den Kundensupport
-Configure Wizard	Assistent zum Konfigurieren der Anmeldeinformationen für den Proxyserver
-Delete-Konfiguration	Löscht die Anmeldeinformationen des Proxyservers
--aktivieren	Aktiviert die AutoSupport-Benachrichtigung (dies ist die Standardeinstellung).
-Disable	Deaktiviert die AutoSupport-Benachrichtigung
-Anzeigen	Zeigt den AutoSupport-Status an

Im folgenden Beispiel wird AutoSupport aktiviert oder deaktiviert und das Ziel, an das der AutoSupport Inhalt gesendet wird, angezeigt:

```
NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport already enabled.

NetApp MetroCluster Tiebreaker :> autosupport disable
AutoSupport status            : disabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport status            : enabled
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport invoke
AutoSupport transmission      : success
Proxy Server IP Address       : 10.234.168.79
Proxy Server Port Number      : 8090
Proxy Server Username         : admin
AutoSupport destination       :
https://support.netapp.com/asupprod/post/1.0/postAsup
```

Das folgende Beispiel zeigt AutoSupport, die über einen authentifizierten Proxy-Server mit einer IP-Adresse und Portnummer konfiguriert sind:

```
NetApp MetroCluster Tiebreaker :> autosupport configure wizard
Enter Proxy Server IP address :  10.234.168.79
Enter Proxy Server port number :  8090
Enter Proxy Server Username :  admin
Enter Proxy Server Password : 123abc
Autosupport configuration updated successfully.
```

Im folgenden Beispiel wird das Löschen einer AutoSupport-Konfiguration gezeigt:

```
NetApp MetroCluster Tiebreaker :> autosupport delete configuration
Autosupport configuration deleted successfully.
```

SNMP-Ereignisse und -Traps

Die NetApp MetroCluster Tiebreaker Software verwendet SNMP-Traps, um Sie über wichtige Ereignisse zu informieren. Diese Fallen sind Teil der NetApp MIB Datei. Jeder Köder enthält die folgenden Informationen: Trap-Name, Schweregrad, Impact-Level, Zeitstempel und Nachricht.

Ereignis-Name	Ereignisdetails	Fallnummer
MetroCluster Tie-Breaker kann die MetroCluster-Konfiguration nicht erreichen	Weist den Administrator darauf hin, dass die Software einen Notfall nicht erkennen kann. Dieses Ereignis tritt auf, wenn beide Cluster nicht erreichbar sind.	25000
MetroCluster Tie-Breaker kann den Cluster nicht erreichen	Warnt den Administrator, dass die Software keinen der Cluster erreichen kann.	25001
MetroCluster Tie-Breaker hat einen Notfall am Cluster erkannt	Benachrichtigt den Administrator, dass die Software einen Standortausfall erkennt. Es wird eine Benachrichtigung zugestellt.	25002
Alle Verbindungen zwischen dem Partner-Cluster werden getrennt.	Die Software erkennt, dass beide Cluster erreichbar sind, aber alle Netzwerkpfade zwischen den beiden Clustern sind ausgefallen, und die Cluster können nicht miteinander kommunizieren.	25005
SNMP-Test-Trap	Die SNMP-Konfiguration kann nun durch Ausführen des befehls snmp config Test getestet werden.	25006

Anzeigen des Status von Monitoring-Vorgängen

Sie können den Gesamtstatus der Überwachungsvorgänge für eine MetroCluster-Konfiguration anzeigen.

Schritt

1. Verwenden Sie den Tiebreaker CLI-Monitor-Befehl, um den Status eines MetroCluster-Vorgangs mit einer der folgenden Optionen anzuzeigen:

Option	Beschreibung
-Monitor-Name	Zeigt den Status des angegebenen Monitornamens an
-Operation-history	Zeigt bis zu 10 Überwachungsvorgänge an, die zuletzt auf einem Cluster durchgeführt wurden
-Stats	Zeigt die Statistiken zum angegebenen Cluster an
-Status	Zeigt den Status des angegebenen Clusters an **Hinweis:** die MetroCluster Tiebreaker Software kann bis zu 10 Minuten dauern, um den Status des Abschlusses von Vorgängen wie Heal Aggregates, Heal Roots oder Switchback zu reflektieren.

Im folgenden Beispiel wird gezeigt, dass die Cluster „Cluster_A“ und „Cluster_B“ verbunden und sich in einem ordnungsgemäßen Zustand befinden:

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

Im folgenden Beispiel werden die letzten sieben Vorgänge angezeigt, die auf Cluster_B ausgeführt wurden:

```
NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
 [ 2014-09-15 04:48:32.274 ] MetroCluster Monitor is initialized
 [ 2014-09-15 04:48:32.278 ] Started Discovery and validation of
MetroCluster Setup
 [ 2014-09-15 04:48:35.078 ] Discovery and validation of MetroCluster
Setup succeeded. Started monitoring.
 [ 2014-09-15 04:48:35.246 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5a"
 [ 2014-09-15 04:48:35.256 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5b"
 [ 2014-09-15 04:48:35.298 ] Link to remote DR cluster is up for cluster
"mcc5a"
 [ 2014-09-15 04:48:35.308 ] Link to remote DR cluster is up for cluster
"mcc5b"
```

Anzeigen von Informationen über die MetroCluster-Konfiguration

Sie können den Monitornamen und die IP-Adresse aller Instanzen von MetroCluster-Konfigurationen in der Tiebreaker Software anzeigen.

Schritt

1. Zeigen Sie mit dem Tiebreaker CLI-Konfigurationsbefehl die MetroCluster-Konfigurationsinformationen an.

   Im folgenden Beispiel werden die Informationen für Cluster „Cluster_A“ und „Cluster_B“ angezeigt:

```
MetroCluster: North America
    Monitor Enabled: true
    ClusterA name: cluster_A
    ClusterA IpAddress: 10.222.196.130
    ClusterB name: cluster_B
    ClusterB IpAddress: 10.222.196.140
```

Erstellen von Dump-Dateien

Sie speichern den Gesamtstatus der Tiebreaker Software in einer Dump-Datei für Debugging-Zwecke.

Schritt

1. Verwenden Sie den Tiebreaker CLI Monitor Dump -Status-Befehl, um eine Dump-Datei des Gesamtstatus aller MetroCluster-Konfigurationen zu erstellen.

   Das folgende Beispiel zeigt die erfolgreiche Erstellung der Dump-Datei /var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml:

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MetroCluster Tiebreaker status successfully dumped in file
/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```

Risiken und Einschränkungen bei der Verwendung von MetroCluster Tiebreaker im aktiven Modus

Umschaltung bei Erkennung eines Standortausfalls wird automatisch ausgeführt. MetroCluster Tiebreaker befindet sich im aktiven Modus. Dieser Modus kann zur Ergänzung der Funktion zur automatischen Umschaltung von ONTAP/FAS verwendet werden.

Wenn Sie MetroCluster Tiebreaker im aktiven Modus implementieren, können die folgenden bekannten Probleme zu Datenverlust führen:

- Wenn die Verbindung zwischen den Standorten fehlschlägt, werden die Controller auf jedem Standort weiterhin mit den Clients verbunden. Die Controller werden jedoch nicht gespiegelt. Der Ausfall eines Controllers an einem Standort wird als Standortausfall erkannt und der MetroCluster Tiebreaker initiiert eine Umschaltung. Die Daten, die nach dem Ausfall der Verbindung zwischen den Standorten mit dem Remote Standort nicht gespiegelt werden, gehen verloren.
- Eine Umschaltung findet statt, wenn die Aggregate am Remote-Standort eingeschränkt sind. Die Daten werden nicht repliziert, wenn die Umschaltung erfolgt ist, bevor die Aggregat-Resynchronisierung erfolgt ist.
- Wenn die Umschaltung abgeschlossen wird, tritt ein Remote-Storage-Ausfall auf.
- Nicht-flüchtiger Speicher (NVRAM oder NVMEM, je nach Plattformmodell) in den Storage-Controllern wird nicht vom Remote Disaster Recovery (DR)-Partner am Partnerstandort gespiegelt.
- Die Metadaten gehen verloren, wenn das Cluster-Peering-Netzwerk über einen längeren Zeitraum ausfällt und die Metadaten-Volumes nach einem Switchover nicht online sind.

> Möglicherweise treten Szenarien auf, die nicht erwähnt werden. NetApp ist nicht verantwortlich für jegliche Schäden, die sich aus der Verwendung von MetroCluster Tiebreaker im aktiven Modus ergeben können. Verwenden Sie MetroCluster Tiebreaker nicht im aktiven Modus, wenn die Risiken und Einschränkungen für Sie nicht akzeptabel sind.

Firewall-Anforderungen für MetroCluster Tiebreaker

MetroCluster Tiebreaker nutzt eine Reihe von Ports, um mit bestimmten Services zu kommunizieren.

In der folgenden Tabelle sind die Ports aufgeführt, die Sie in Ihrer Firewall zulassen müssen:

Port/Services	Quelle	Ziel	Zweck
443 / TCP	Tiebreaker	Internet	Senden von AutoSupport Meldungen an NetApp

22 / TCP	Management-Host	Tiebreaker	Tiebreaker Management
443 / TCP	Tiebreaker	Cluster-Management-LIFs	Sichere Kommunikation zum Cluster über HTTP (SSL)
22 / TCP	Tiebreaker	Cluster-Management-LIFs	Sichere Kommunikation zum Cluster über SSH
443 / TCP	Tiebreaker	Node-Management-LIFs	Sichere Kommunikation mit Knoten über HTTP (SSL)
22 / TCP	Tiebreaker	Node-Management-LIFs	Sichere Kommunikation mit Knoten über SSH
162 / UDP	Tiebreaker	SNMP-Trap-Host	Wird zum Senden von SNMP-Traps für Warnmeldungen verwendet
ICMP (Ping)	Tiebreaker	Cluster-Management-LIFs	Überprüfen, ob Cluster-IP erreichbar ist
ICMP (Ping)	Tiebreaker	Node-Management-LIFs	Überprüfen Sie, ob die Knoten-IP erreichbar ist

Ereignisprotokolldateien für MetroCluster Tiebreaker

Die Event-Log-Datei enthält ein Protokoll aller Aktionen, die von der MetroCluster Tiebreaker Software durchgeführt werden.

Die Tiebreaker Software führt folgende Aktionen durch:

- Erkennt Standortausfälle
- Erkennt Konfigurationsänderungen in Verbindung mit der Datenbank, anderen Tiebreaker Monitoren oder der MetroCluster Tiebreaker Software
- Erkennt SSH-Verbindungen und -Verbindungen
- Erkennung von MetroCluster-Konfigurationen

Diese Aktionen werden in der Ereignis-Log-Datei im folgenden Format protokolliert:

Zeitstempel der Schweregrad/des Thread-id-Moduls auf Protokollebene

```
2022-09-07 06:14:30,797 INFO  [MCCTBCommandServer-16] [SslSupport]
Successfully initiated SSL context. Protocol used is TLSv1.3.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16] [DataBase]
Successfully read MCCTB database.
2022-09-07 06:14:34,137 INFO  [MCCTBCommandServer-16]
[ConfigurationMonitor] Debug mode disabled.
```

Wo Sie weitere Informationen finden

Weitere Informationen zur Konfiguration und zum Betrieb von MetroCluster erhalten Sie hier.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff
"MetroCluster-Dokumentation"	• Alle MetroCluster-Informationen
"Technischer Bericht 4375 zu NetApp MetroCluster für ONTAP 9.3"	• Eine technische Übersicht über Konfiguration und Betrieb von MetroCluster • Best Practices für die Konfiguration von MetroCluster.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von MetroCluster IP"	• MetroCluster IP Architektur • Verkabelung der MetroCluster IP-Konfiguration • Konfigurieren der MetroCluster in ONTAP

"Warten der MetroCluster-Komponenten"	• Richtlinien für die Wartung in einer MetroCluster-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster Konfiguration • Entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweiterung einer Fabric-Attached oder Stretch MetroCluster Konfiguration mit vier Nodes auf eine MetroCluster Konfiguration mit acht Nodes
Active IQ Unified Manager-Dokumentation "NetApp Dokumentation: Produktleitfäden und Ressourcen"	• Monitoring der MetroCluster Konfiguration und Performance
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen

Copyright-Informationen

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

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

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