Tiebreaker Software 1.21 Installation and Configuration Guide
Contents

Deciding whether to use this guide ............................................................. 4

Overview of the Tiebreaker software .......................................................... 5
  Detecting failures with NetApp MetroCluster Tiebreaker software .................. 5
  How the Tiebreaker software detects site failures ........................................ 5
  How the Tiebreaker software detects intersite connectivity failures ................. 6
  How different disaster types affect Tiebreaker software detection time .......... 7
  About the Tiebreaker CLI and man pages .................................................. 8

Installing the Tiebreaker software ............................................................. 9
  System requirements for installing or upgrading Tiebreaker software .............. 9
  Installing MetroCluster Tiebreaker dependencies ......................................... 10
    Installing Java Runtime Environment 1.8 .................................................. 10
    Installing MySQL Server 5.5.30 or later and 5.6.x versions on Red Hat
      Enterprise Linux 6 or CentOS 6 .......................................................... 11
    Installing MariaDB server on Red Hat Enterprise Linux 7 or CentOS 7 ... 15
  Installing or upgrading the software package ............................................. 16
  Selecting the NTP source for the Tiebreaker software .................................. 18

Configuring the Tiebreaker software ....................................................... 19
  Launching the Tiebreaker software CLI .................................................... 19
  Adding MetroCluster configurations ......................................................... 19
  Commands for modifying MetroCluster Tiebreaker configurations .................. 20
  Removing MetroCluster configurations ...................................................... 21

Configuring SNMP settings for Tiebreaker software ............................. 22

Monitoring the MetroCluster configuration ............................................ 23
  Configuring AutoSupport ......................................................................... 23
  SNMP events and traps ........................................................................... 24
  Displaying the status of monitoring operations ......................................... 25
  Displaying MetroCluster configuration information .................................... 26
  Creating dump files ................................................................................. 27

Risks and limitations of using MetroCluster Tiebreaker in active
  mode ....................................................................................................... 28

Firewall requirements for MetroCluster Tiebreaker .................................. 29

Where to find additional information ..................................................... 30

Copyright ................................................................................................. 32

Trademark ............................................................................................... 33

How to send comments about documentation and receive update
  notifications .......................................................................................... 34

Index ....................................................................................................... 35
Deciding whether to use the MetroCluster Tiebreaker Software Installation and Configuration Guide

This guide describes how to install and configure the MetroCluster Tiebreaker software.

You should use this guide for installing the MetroCluster Tiebreaker software.

You can find other MetroCluster documentation in the following location:

ONTAP 9 Documentation Center
Overview of the Tiebreaker software

It is helpful to understand what the NetApp MetroCluster Tiebreaker software is and how it distinguishes between types of failures so that you can monitor your MetroCluster configurations efficiently. You use the Tiebreaker CLI to manage settings and monitor the status and operations of MetroCluster configurations.

Detecting failures with NetApp MetroCluster Tiebreaker software

The Tiebreaker software resides on a Linux host. You need the Tiebreaker software only if you want to monitor two clusters and the connectivity status between them from a third site. Doing so enables each partner in a cluster to distinguish between an ISL failure, when inter-site links are down, from a site failure.

After you install the Tiebreaker software on a Linux host, you can configure the clusters in a MetroCluster configuration to monitor for disaster conditions.

How the Tiebreaker software detects site failures

The NetApp MetroCluster Tiebreaker software checks the reachability of the nodes in a MetroCluster configuration and the cluster to determine whether a site failure has occurred. The Tiebreaker software also triggers an alert under certain conditions.

Components monitored by the Tiebreaker software

The Tiebreaker software monitors each controller in the MetroCluster configuration by establishing redundant connections through multiple paths to a node management LIF and to the cluster management LIF, both hosted on the IP network.

The Tiebreaker software monitors the following components in the MetroCluster configuration:

- Nodes through local node interfaces
- Cluster through the cluster-designated interfaces
- Surviving cluster to evaluate whether it has connectivity to the disaster site (NV interconnect, storage, and intercluster peering)

When there is a loss of connection between the Tiebreaker software and all of the nodes in the cluster and to the cluster itself, the cluster will be declared as “not reachable” by the Tiebreaker software. It takes around three to five seconds to detect a connection failure. If a cluster is unreachable from the Tiebreaker software, the surviving cluster (the cluster that is still reachable) must indicate that all of the links to the partner cluster are severed before the Tiebreaker software triggers an alert.

Note: All of the links are severed if the surviving cluster can no longer communicate with the cluster at the disaster site through FC (NV interconnect and storage) and intercluster peering.

Failure scenarios during which Tiebreaker software triggers an alert

The Tiebreaker software triggers an alert when the cluster (all of the nodes) at the disaster site is down or unreachable and the cluster at the surviving site indicates the “AllLinksSevered” status.

The Tiebreaker software does not trigger an alert (or the alert is vetoed) in the following scenarios:
In an eight-node MetroCluster configuration, if one HA pair at the disaster site is down

In a cluster with all of the nodes at the disaster site down, one HA pair at the surviving site down, and the cluster at the surviving site indicates the “AllLinksSevered” status

The Tiebreaker software triggers an alert, but ONTAP vetoes that alert. In this situation, a manual switchover is also vetoed

Any scenario in which the Tiebreaker software can either reach at least one node or the cluster interface at the disaster site, or the surviving site still can reach either node at the disaster site through either FC (NV interconnect and storage) or intercluster peering

Related concepts

*Risks and limitations of using MetroCluster Tiebreaker in active mode* on page 28

How the Tiebreaker software detects intersite connectivity failures

The MetroCluster Tiebreaker software alerts you if all connectivity between the sites is lost.

Types of network paths

Depending on the configuration, there are three types of network paths between the two clusters in a MetroCluster configuration:

**FC network (present in fabric-attached MetroCluster configurations)**

This type of network is composed of two redundant FC switch fabrics. Each switch fabric has two FC switches, with one switch of each switch fabric co-located with a cluster. Each cluster has two FC switches, one from each switch fabric. All of the nodes have FC (NV interconnect and FCP initiator) connectivity to each of the co-located FC switches. Data is replicated from cluster to cluster over the ISL.

**Intercluster peering network**

This type of network is composed of a redundant IP network path between the two clusters. The cluster peering network provides the connectivity that is required to mirror the storage virtual machine (SVM) configuration. The configuration of all of the SVMs on one cluster is mirrored by the partner cluster.

**IP network (present in MetroCluster IP configurations)**

This type of network is composed of two redundant IP switch networks. Each network has two IP switches, with one switch of each switch fabric co-located with a cluster. Each cluster has two IP switches, one from each switch fabric. All of the nodes have connectivity to each of the co-located FC switches. Data is replicated from cluster to cluster over the ISL.

Monitoring intersite connectivity

The Tiebreaker software regularly retrieves the status of intersite connectivity from the nodes. If NV interconnect connectivity is lost and the intercluster peering does not respond to pings, then the clusters assume that the sites are isolated and the Tiebreaker software triggers an alert as “AllLinksSevered”. If a cluster identifies the “AllLinksSevered” status and the other cluster is not reachable through the network, then the Tiebreaker software triggers an alert as “disaster”.

Monitoring intersite connectivity
How different disaster types affect Tiebreaker software detection time

For better disaster recovery planning, the MetroCluster Tiebreaker software takes some time in detecting a disaster. This time spent is the “disaster detection time”. The MetroCluster Tiebreaker software detects the site disaster within 30 seconds from the time of occurrence of the disaster and triggers the disaster recovery operation to notify you about the disaster.

The detection time also depends on the type of disaster and might exceed 30 seconds in some scenarios, mostly known as “rolling disasters”. The main types of rolling disaster are as follows:

- Power loss
- Panic
- Halt or reboot
- Loss of FC switches at the disaster site

**Power loss**

The Tiebreaker software immediately triggers an alert when the node stops operating. When there is a power loss, all connections and updates, such as intercluster peering, NV interconnect, and MailBox disk, stop. The time taken between the cluster becoming unreachable, the detection of the disaster, and the trigger, including the default silent time of 5 seconds, should not exceed 30 seconds.

**Panic**

The Tiebreaker software triggers an alert when the NV interconnect connection between the sites is down and the surviving site indicates the “AllLinksSevered” status. This only happens after the coredump process is complete. In this scenario, the time taken between the cluster becoming unreachable and the detection of a disaster might be longer or approximately equal to the time taken for the coredump process. In many cases, the detection time is more than 30 seconds.

If a node stops operating but does not generate a file for the coredump process, then the detection time should not be longer than 30 seconds.

**Halt or reboot**

The Tiebreaker software triggers an alert only when the node is down and the surviving site indicates the “AllLinksSevered” status. The time taken between the cluster becoming unreachable and the detection of a disaster might be longer than 30 seconds. In this scenario, the time taken to detect a disaster depends on how long it takes for the nodes at the disaster site to be shut down.

**Loss of FC switches at the disaster site (fabric-attached MetroCluster configuration)**

The Tiebreaker software triggers an alert when a node stops operating. If FC switches are lost, then the node tries to recover the path to a disk for about 30 seconds. During this time, the node is up and responding on the peering network. When both of the FC switches are down and the path to a disk cannot be recovered, the node produces a MultiDiskFailure error and halts. The time taken between the FC switch failure and the number of times the nodes produced MultiDiskFailure errors is about 30 seconds longer. This additional 30 seconds must be added to the disaster detection time.
About the Tiebreaker CLI and man pages

The Tiebreaker CLI provides commands that enable you to remotely configure the Tiebreaker software and monitor the MetroCluster configurations.

The CLI command prompt is represented as `NetApp MetroCluster Tiebreaker::>.

The man pages are available in the CLI by entering the applicable command name at the prompt.
Installing the Tiebreaker software

The Tiebreaker software provides monitoring capabilities for a clustered storage environment. It also sends SNMP notifications in the event of node connectivity issues and site disasters.

Before you begin

The MetroCluster software must be installed and configured.

System requirements for installing or upgrading Tiebreaker software

The Tiebreaker software is installed on a third site, which allows the software to distinguish between an Inter-Switch Link (ISL) failure (when inter-site links are down) and a site failure. Your host system must meet certain requirements before you can install or upgrade the Tiebreaker software on your local computer to monitor the MetroCluster configuration.

The MetroCluster Tiebreaker software does not require any special configuration for the different MetroCluster configurations.

Note: You should have only one MetroCluster Tiebreaker monitor per MetroCluster configuration to avoid any conflict with multiple Tiebreaker monitors.

- Hardware and software:
  - ONTAP 8.3.x, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5
- Red Hat Enterprise Linux 7 to 7.5 or CentOS 7 to 7.5 64-bit (physical installation or virtual machine)
  - MariaDB 5.5.52.x
  - 4 GB RAM
  - Open Java Runtime Environment 8
- Red Hat Enterprise Linux 6.4 to 6.10 or CentOS 6.4 to 6.10 64-bit (physical installation or virtual machine)
  - MySQL Server 5.6.x
  - 2 GB RAM
  - Open Java Runtime Environment 8
- Disk capacity: 8 GB
- User: Root access.
- Firewall:
  - Direct access for setting up AutoSupport messages
  - SSH (port 22/TCP), HTTPS (port 443/TCP), and ping (ICMP)
Installing MetroCluster Tiebreaker dependencies

You must install a MySQL or MariaDB server depending on the Linux operating system that is your host before installing or upgrading the Tiebreaker software.

Steps

1. Install Java Runtime Environment.
   *Installing Java Runtime Environment 1.8* on page 10

2. Install MySQL or MariaDB server:

<table>
<thead>
<tr>
<th>If the Linux host is</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 6/</td>
<td>a. Install MySQL</td>
</tr>
<tr>
<td>CentOS 6</td>
<td><em>Installing MySQL Server 5.5.30 or later and 5.6.x versions on Red Hat Enterprise Linux 6 or CentOS 6</em> on page 11</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7/</td>
<td>a. Install MariaDB</td>
</tr>
<tr>
<td>CentOS 7</td>
<td><em>Installing MariaDB server on Red Hat Enterprise Linux 7 or CentOS 7</em> on page 15</td>
</tr>
</tbody>
</table>

Installing Java Runtime Environment 1.8

You must install Java Runtime Environment 1.8 on your host system before installing or upgrading the Tiebreaker software.

Steps

1. Log in as root to the host system.

   **Example**

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

2. Install Java Runtime Environment 1.8:

   ```
   [root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64  
   ```

   **Example**

   ```
   [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  
   ================  ===============  ===============  ===========  
   Installing:  
   java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4  
   updates  
   238 k  
   ```
Installing MySQL Server 5.5.30 or later and 5.6.x versions on Red Hat Enterprise Linux 6 or CentOS 6

You must install MySQL Server 5.5.30 or later and 5.6.x version on your host system before installing or upgrading the Tiebreaker software.

Steps

1. Log in as root to the host system.

   **Example**

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

2. Add the MySQL repository to your host system:

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

   **Example**

   ```bash
   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
   --> Finished Dependency Resolution
   Dependencies Resolved
   Transaction Summary
   Install 1 Package(s)
   Total size: 4.3 k
   Installed size: 4.3 k
   Is this ok [y/N]: y
   ```

3. Disable the mysql 57 repository:

   ```bash
   [root@mcctb ~]# yum-config-manager --disable mysql57-community
   ```
4. Enable the mysql 5.6 repository:

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

5. Enable the repository:

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

Example

<table>
<thead>
<tr>
<th>Package</th>
<th>Repository</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>mysql-connector-community</td>
<td>MySQL Connectors Community</td>
<td>21</td>
</tr>
<tr>
<td>mysql-tools-community</td>
<td>MySQL Tools Community</td>
<td>35</td>
</tr>
<tr>
<td>mysql56-community</td>
<td>MySQL 5.6 Community Server</td>
<td>231</td>
</tr>
</tbody>
</table>

6. Install the MySQL Community server:

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

Example

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-lib.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-lib-compat.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  
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID 5072e1f5: 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
    Installing: mysql-community-client-5.6.29-2.el6.x86_64
    Installing: mysql-community-libs-5.6.29-2.el6.x86_64
    Installing: mysql-community-libs-compat-5.6.29-2.el6.x86_64
    Installing: mysql-community-server-5.6.29-2.el6.x86_64
7/8
    Verifying: mysql-5.1.71-1.el6.x86_64
8/8
    Installed:
    mysql-community-client-5.6.29-2.el6.x86_64
    mysql-community-libs-5.6.29-2.el6.x86_64
    mysql-community-libs-compat-5.6.29-2.el6.x86_64
    mysql-community-server-5.6.29-2.el6.x86_64
    mysql-community-common-5.6.29-2.el6.x86_64
    Dependency Installed:
    mysql-community-common-5.6.29-2.el6.x86_64
    Replaced:
    mysql-5.1.71-1.el6.x86_64
    mysql-libs-5.1.71-1.el6.x86_64
    mysql-server-5.1.71-1.el6.x86_64
    mysql-community-client-5.6.29-2.el6.x86_64
    mysql-community-libs-5.6.29-2.el6.x86_64
    mysql-community-libs-compat-5.6.29-2.el6.x86_64
    mysql-community-server-5.6.29-2.el6.x86_64
    Complete!

7. Start MySQL server:

[root@mcctb ~]# service mysqld start

Example

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

Starting mysqld: [ OK ]

8. Confirm that MySQL server is running:

[root@mcctb ~]# service mysqld status

Example

mysqld (pid 2739) is running...

9. Configure security and password settings:

[root@mcctb ~]# mysql_secure_installation

...Output truncated....
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):  
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL 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 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. Verify that the MySQL login is working:

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

Example

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>

If the MySQL login is working, the output will end at the mysql> prompt.
Enabling the MySQL autostart setting

You should ensure that the autostart feature is turned on for the MySQL daemon. Turning on the MySQL daemon automatically restarts MySQL if the system on which the MetroCluster Tiebreaker software resides reboots. If the MySQL daemon is not running, the Tiebreaker software continues running, but it cannot be restarted and configuration changes cannot be made.

See the MySQL documentation to enable autostart on your installation.

Installing MariaDB server on Red Hat Enterprise Linux 7 or CentOS 7

You must install MariaDB server on your host system before installing or upgrading the Tiebreaker software.

Before you begin

Your host system must be running on Red Hat Enterprise Linux (RHEL) 7 or CentOS 7.

Steps

1. Log in as root to the host system.

   **Example**

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

2. Install MariaDB server:

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

   **Example**

   ```
   [root@mcctb ~]# yum install mariadb-server.x86_64
   Loaded plugins: fastestmirror, langpacks
   ... ...
   Package   Arch     Version        Repository      Size
   mariadb-server.x86_64  x86_64  1:5.5.56-2.el7   base                   11 M
   Installing:
   mariadb-server.x86_64  x86_64  1:5.5.56-2.el7   base                   11 M
   Installing for dependencies:
   mariadb.x86_64 1:5.5.56-2.el7         mariadb-libs.x86_64 1:5.5.56-2.el7         mariadb-client.x86_64 1:5.5.56-2.el7         mariadb-server.x86_64 1:5.5.56-2.el7
   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-IO-Compress.noarch    | 51 kB | 00:00:01
   Installed: mariadb-server.x86_64 1:5.5.56-2.el7
   mariadb.x86_64 1:5.5.56-2.el7         mariadb-libs.x86_64 1:5.5.56-2.el7         mariadb-client.x86_64 1:5.5.56-2.el7         mariadb-server.x86_64 1:5.5.56-2.el7
   perl-Compress-Raw-Bzip2.x86_64 0:2.061-3.el7
   perl-Compress-Raw-Zip.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-Met-Daemon.noarch 0:0.48-5.el7 perl-P1RPC.noarch 0:0.2020-14.el7
   ```
3. Start MariaDB server:

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

Example

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

4. Verify MariaDB server has started:

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

Example

```
[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 scspr0523972001 systemd[1]: Started MariaDB database server.
```

Note: Ensure that the enable autostart setting is turned on for MariaDB.

5. Configure the security and password settings:

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

Example

```
[root@mcctb ~]# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
Set root password? [Y/n] y
New password: 
Re-enter new password: 
Password updated successfully!
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!
Remove test database and access to it? [Y/n] y 
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
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!
```

Installing or upgrading the software package

You must install or upgrade the MetroCluster Tiebreaker software on your local computer to monitor
MetroCluster configurations.

Before you begin

- Your storage system must be running ONTAP 8.3.x or later.
• You must have installed OpenJDK by using the `yum install java-1.8.0-openjdk` command.

**Steps**

1. **Download the NetApp-MetroCluster-Tiebreaker-Software-1.21P2-1.x86_64.rpm file.**

   **NetApp Support**

2. Log in to the host as the root user.

3. Install or upgrade the Tiebreaker software:

<table>
<thead>
<tr>
<th>If you are...</th>
<th>Issue this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performing a new installation</td>
<td><code>rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.21P2-1.x86_64.rpm</code></td>
</tr>
</tbody>
</table>

   The system displays the following output for a successful installation:

   ```bash
   [root@scspr0523972001 mcctb]# rpm -ivh NetApp-MetroCluster-
   Tiebreaker-Software-1.21P2-1.x86_64.rpm
   Preparing...
   #........................................... [100%]
   Updating / installing...
   1:NetApp-MetroCluster-Tiebreaker-
   Software-1.21P2-1.x86_64.rpm
   Post installation start Wed Sep 5 05:56:18 EDT 2018
   Enter MetroCluster Tiebreaker user password:
   Please enter mysql root password when prompted
   Enter password:
   Created symlink from /etc/systemd/system/multi-user.target.wants/netapp-metrocluster-tiebreaker-software.service to /etc/systemd/system/netapp-metrocluster-tiebreaker-software.service.
   Enabled autostart of NetApp MetroCluster Tiebreaker software daemon during boot
   Created symbolic link for NetApp MetroCluster Tiebreaker software CLI
   Post installation end Wed Sep 5 05:56:24 EDT 2018
   Successfully installed NetApp MetroCluster Tiebreaker software version 1.21P2
   ```

| Upgrading an existing installation | `rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-1.21P2-1.x86_64.rpm` |

   The system displays the following output for a successful upgrade:

   ```bash
   [root@scspr0523972001 mcctb]# rpm -Uvh NetApp-MetroCluster-
   Tiebreaker-Software-1.21P2-1.x86_64.rpm
   Preparing...
   #........................................... [100%]
   Upgrading NetApp MetroCluster Tiebreaker software....
   Stopping NetApp MetroCluster Tiebreaker software services before upgrade.
   Stopping NetApp MetroCluster Tiebreaker software daemon [ OK ]
   Upgrading / installing...
   1:NetApp-MetroCluster-Tiebreaker-
   Software-1.21P2-1.x86_64.rpm
   Post installation start Wed Sep 5 05:59:13 EDT 2018
   Enabled autostart of NetApp MetroCluster Tiebreaker software daemon during boot
   Created symbolic link for NetApp MetroCluster Tiebreaker software CLI
   Post installation end Wed Sep 5 05:59:24 EDT 2018
   Successfully installed NetApp MetroCluster Tiebreaker software version 1.21P2
   Cleaning up / removing...
   2:NetApp-MetroCluster-Tiebreaker-
   So........................................... [100%]
   ```

If you enter the wrong MySQL root password, the Tiebreaker software indicates that it was installed successfully, but displays `Access denied` messages. To resolve the issue, you must uninstall the Tiebreaker software by using the `rpm -e` command, and then reinstall the software by using the correct MySQL root password.
4. Verify the Tiebreaker connectivity to the MetroCluster software by opening an SSH connection from the Tiebreaker host to each of the node management LIFs and cluster management LIFs.

Related information

NetApp Support

Selecting the NTP source for the Tiebreaker software

You should use a local Network Time Protocol (NTP) source for the Tiebreaker software. It should not use the same source as the MetroCluster sites that the Tiebreaker software monitors.
Configuring the Tiebreaker software

After installation of the Tiebreaker software, you can add or modify MetroCluster configurations, or remove them from the Tiebreaker software.

Launching the Tiebreaker software CLI

After installing the Tiebreaker software you must launch its CLI to configure the software.

Step

1. Launch the CLI from the prompt of the host on which you installed the software:
   ```
   netapp-metrocluster-tiebreaker-software-cli
   ```

Adding MetroCluster configurations

After installing the NetApp MetroCluster Tiebreaker software, you can add more MetroCluster configurations, one at a time.

Before you begin

You must have installed the MetroCluster configuration in an ONTAP environment and enabled the settings in the software.

Steps

1. Use the Tiebreaker command-line interface (CLI) `monitor add` command to add MetroCluster configurations.
   
   If you are using the host name, it must be the fully qualified domain name (FQDN).

   Example
   
   The following example shows the configuration of cluster_A:
   
   ```
   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. Confirm that the MetroCluster configuration was added properly by using the Tiebreaker CLI `monitor show -status` command.

   Example
   
   ```
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```
3. Optional: Disable the observer mode for the Tiebreaker software to automatically initiate a switchover after it detects a site failure:

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

Example

```
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 Guide.
Are you sure you want to enable automatic switchover capability for monitor "8pack"? [Y/N]: y
```

Related concepts

*Risks and limitations of using MetroCluster Tiebreaker in active mode* on page 28

Commands for modifying MetroCluster Tiebreaker configurations

You can modify the MetroCluster configuration whenever you need to change the settings.

The Tiebreaker CLI `monitor modify` command can be used with any of the following options. You can confirm your changes with the `monitor show -status` command.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-monitor-name</code></td>
<td>Name of the MetroCluster configuration</td>
</tr>
<tr>
<td><code>-enable-monitor</code></td>
<td>Enables and disables monitoring of the MetroCluster configuration</td>
</tr>
<tr>
<td><code>-silent-period</code></td>
<td>Period in seconds for which the MetroCluster Tiebreaker software waits to confirm a site failure after detection</td>
</tr>
</tbody>
</table>
| `-observer-mode`        | Observer mode *(true)* provides monitoring only, and does not trigger a switchover if a site disaster occurs. Online mode *(false)* triggers a switchover if a site disaster occurs.  
  - *How the Tiebreaker software detects site failure* on page 5
  - *Risks and limitations of using MetroCluster Tiebreaker in active mode* on page 28 |

The following example changes the silent period for the configuration.

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

The Tiebreaker CLI debug command can be used to change the logging mode.
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug status</td>
<td>Displays the status of the debug mode</td>
</tr>
<tr>
<td>debug enable</td>
<td>Enables the debug mode for logging</td>
</tr>
<tr>
<td>debug disable</td>
<td>Disables the debug mode for logging</td>
</tr>
</tbody>
</table>

The Tiebreaker CLI `update-mcctb-password` command can be used to update the user password.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>update-mcctb-password</td>
<td>The user password is successfully updated</td>
</tr>
</tbody>
</table>

### Removing MetroCluster configurations

You can remove the MetroCluster configuration that is being monitored by the Tiebreaker software when you no longer want to monitor a MetroCluster configuration.

**Steps**

1. Use the Tiebreaker CLI `monitor remove` command to remove the MetroCluster configuration.

   **Example**
   
   In the following example, cluster_A is removed from the software:
   
   ```bash
   NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
   Successfully removed monitor from NetApp MetroCluster Tiebreaker software.
   ```

2. Confirm that the MetroCluster configuration is removed properly by using the Tiebreaker CLI `monitor show -status` command.

   **Example**
   
   ```bash
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```
Configuring SNMP settings for Tiebreaker software

To use SNMP with the Tiebreaker software, you must configure SNMP settings.

Steps

1. Use the Tiebreaker CLI `snmp config wizard` command to add MetroCluster configurations.

   Example
   The following example shows the configuration of an SNMP receiver that supports SNMP V1 with an IP address of 10.222.210.234, port number 162 for trap messages, and the community string set to `public`:

   ```
   NetApp MetroCluster Tiebreaker :> snmp config wizard
   Enter SNMP Version [V1/V3]: V1
   Enter SNMP Host: 10.222.210.234
   Enter SNMP Port: 162
   Enter SNMP V1 Community: public
   Successfully added SNMP properties to NetApp MetroCluster Tiebreaker software.
   NetApp MetroCluster Tiebreaker :
   ```

   The Tiebreaker software is ready to send traps to the SNMP receiver that you specified.

2. Verify that the SNMP settings are configured:

   `snmp config test`

   Example
   The following example shows that the Tiebreaker software can send an SNMP trap for the event TEST_SNMP_CONFIG:

   ```
   NetApp MetroCluster Tiebreaker :> snmp config test
   Successfully sent SNMP trap for event TEST_SNMP_CONFIG
   NetApp MetroCluster Tiebreaker :
   ```
Monitoring the MetroCluster configuration

MetroCluster Tiebreaker software automates the recovery process by enabling you to monitor the MetroCluster configuration status, evaluate SNMP events and traps that are sent to NetApp customer support, and view the status of monitoring operations.

Configuring AutoSupport

By default, AutoSupport messages are sent to NetApp a week after installation of the Tiebreaker software. Events that trigger AutoSupport notification include Tiebreaker software panics, detection of disaster conditions on MetroCluster configurations, or an unknown MetroCluster configuration status.

Before you begin

You must have a direct access for setting up AutoSupport messages.

Step

1. Use the Tiebreaker CLI `autosupport` command with any of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--invoke</td>
<td>Sends an AutoSupport message to customer support</td>
</tr>
<tr>
<td>--configure wizard</td>
<td>Wizard to configure proxy server credentials</td>
</tr>
<tr>
<td>--delete configuration</td>
<td>Deletes the proxy server credentials</td>
</tr>
<tr>
<td>--enable</td>
<td>Enables AutoSupport notification (This is the default.)</td>
</tr>
<tr>
<td>--disable</td>
<td>Disables AutoSupport notification</td>
</tr>
<tr>
<td>--show</td>
<td>Displays AutoSupport status</td>
</tr>
</tbody>
</table>

Example

The following example shows that AutoSupport is enabled or disabled and the destination to which the AutoSupport content is posted:

```
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

Example
The following example shows AutoSupport configured by means of an authenticated proxy server, using an IP address and port number:

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.

Example
The following example shows the deletion of an AutoSupport configuration:

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

SNMP events and traps
NetApp MetroCluster Tiebreaker software uses SNMP traps to notify you of significant events. These traps are part of the NetApp MIB file. Each trap contains the following information: trap name, severity, impact level, timestamp, and message.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Event detail</th>
<th>Trap number</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetroCluster Tie-Breaker is unable to reach the MetroCluster configuration</td>
<td>Warns the administrator that the software cannot detect a disaster. This event occurs when both clusters are not reachable.</td>
<td>25000</td>
</tr>
<tr>
<td>MetroCluster Tie-Breaker is unable to reach cluster</td>
<td>Warns the administrator that the software cannot reach one of the clusters.</td>
<td>25001</td>
</tr>
<tr>
<td>MetroCluster Tie-Breaker detected disaster at cluster</td>
<td>Notifies the administrator that the software detects a site failure. A notification will be delivered.</td>
<td>25002</td>
</tr>
<tr>
<td>Event name</td>
<td>Event detail</td>
<td>Trap number</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>All links between partner cluster are severed.</td>
<td>The software detects that both clusters are reachable, but all the network paths between the two clusters are down, and the clusters cannot communicate with each other.</td>
<td>25005</td>
</tr>
<tr>
<td>SNMP Test Trap</td>
<td>SNMP configuration can now be tested by running the <code>snmp config test</code> command.</td>
<td>25006</td>
</tr>
</tbody>
</table>

## Displaying the status of monitoring operations

You can display the overall status of monitoring operations for a MetroCluster configuration.

**Step**

1. Use the Tiebreaker CLI `monitor show` command to display the status of a MetroCluster operation with any of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-monitor-name</code></td>
<td>Displays the status for the specified monitor name</td>
</tr>
<tr>
<td><code>-operation-history</code></td>
<td>Displays up to 10 monitoring operations that were last performed on a cluster</td>
</tr>
<tr>
<td><code>-stats</code></td>
<td>Displays the statistics related to the specified cluster</td>
</tr>
<tr>
<td><code>-status</code></td>
<td>Displays the status of the specified cluster</td>
</tr>
</tbody>
</table>

**Note:** The MetroCluster Tiebreaker software might take up to 10 minutes to reflect the completion status of operations such as heal aggregates, heal roots, or switchback.

### Example

The following example shows that the clusters `cluster_A` and `cluster_B` are connected and healthy:

```bash
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
  Reachable: true
  State: normal
  Node: mcc5-a2 (UUID: 9a8b1059-0809-11e4-9f5e-8d97cdec7102)
    Reachable: true
```
Example

In the following example, the last seven operations that were run on cluster_B are displayed:

NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
[ 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 04:48:35.308 ] 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"

Displaying MetroCluster configuration information

You can display the monitor name and IP address of all instances of MetroCluster configurations in the Tiebreaker software.

Step

1. Use the Tiebreaker CLI `configuration show` command to display the MetroCluster configuration information.

Example

The following example shows the information for clusters cluster_A and cluster_B:

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
Creating dump files

You save the overall status the Tiebreaker software to a dump file for debugging purposes.

**Step**

1. Use the Tiebreaker CLI `monitor dump -status` command to create a dump file of the overall status of all MetroCluster configurations.

**Example**

The following example shows the successful creation of the `/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml` dump file:

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MCCTB status successfully dumped in file /var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```
Risks and limitations of using MetroCluster Tiebreaker in active mode

Switchover upon detection of a site failure happens automatically, with MetroCluster Tiebreaker in active mode. This mode can be used to supplement the ONTAP/FAS automatic switchover capability.

When you implement MetroCluster Tiebreaker in active mode, the following known issues might lead to data loss:

- When the inter-site link fails, the controllers on each site continue to serve the clients. However, the controllers will not be mirrored. Failure of a controller in one site is identified as a site failure and the MetroCluster Tiebreaker initiates a switchover. The data which is not mirrored after the inter-site link failure with the remote site will be lost.
- A switchover occurs when the aggregates in remote site are in degraded state. The data will not be replicated if the switchover has occurred before aggregate resync.
- A remote storage failure occurs when switchover is in progress.
- The nonvolatile memory (NVRAM or NVMEM, depending on the platform model) in the storage controllers is not mirrored to the remote disaster recovery (DR) partner on the partner site.
- Metadata is lost if the cluster peering network is down for an extended period and the metadata volumes are not online after a switchover.

Note: You might encounter scenarios that are not mentioned. NetApp is not responsible for any damages that may arise out of use of MetroCluster Tiebreaker in active mode. Do not use MetroCluster Tiebreaker in active mode if the risks and limitations are not acceptable to you.
Firewall requirements for MetroCluster Tiebreaker

MetroCluster Tiebreaker uses a number of ports to communicate with specific services.

The following table lists the ports that you must allow in your firewall:

<table>
<thead>
<tr>
<th>Port/services</th>
<th>Source</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>443 / TCP</td>
<td>Tiebreaker</td>
<td>Internet</td>
<td>Sending AutoSupport messages to NetApp</td>
</tr>
<tr>
<td>22 / TCP</td>
<td>Management host</td>
<td>Tiebreaker</td>
<td>Tiebreaker Management</td>
</tr>
<tr>
<td>443 / TCP</td>
<td>Tiebreaker</td>
<td>MetroCluster management LIFs</td>
<td>Secure communications via HTTP (SSL)</td>
</tr>
<tr>
<td>22 / TCP</td>
<td>Tiebreaker</td>
<td>MetroCluster management LIFs</td>
<td>Secure communications via SSH</td>
</tr>
<tr>
<td>443 / TCP</td>
<td>Tiebreaker</td>
<td>MetroCluster management LIFs</td>
<td>Secure communications via HTTP (SSL)</td>
</tr>
<tr>
<td>22 / TCP</td>
<td>Tiebreaker</td>
<td>MetroCluster management LIFs</td>
<td>Secure communications via SSH</td>
</tr>
<tr>
<td>162 / UDP</td>
<td>Tiebreaker</td>
<td>SNMP trap host</td>
<td>Used to send alert notification SNMP traps</td>
</tr>
<tr>
<td>ICMP (ping)</td>
<td>Tiebreaker</td>
<td>MetroCluster management LIFs</td>
<td>Check if cluster IP is reachable</td>
</tr>
<tr>
<td>ICMP (ping)</td>
<td>Tiebreaker</td>
<td>MetroCluster management LIFs</td>
<td>Check if node IP is reachable</td>
</tr>
</tbody>
</table>
Where to find additional information

You can learn more about MetroCluster configuration and operation in from the NetApp documentation library.

MetroCluster and miscellaneous guides

<table>
<thead>
<tr>
<th>Guide</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ONTAP 9 Documentation Center</strong></td>
<td>• All MetroCluster guides</td>
</tr>
<tr>
<td></td>
<td>• Best practices for MetroCluster configuration.</td>
</tr>
<tr>
<td><strong>ONTAP 9 Fabric-attached MetroCluster Installation and Configuration Guide</strong></td>
<td>• Fabric-attached MetroCluster architecture</td>
</tr>
<tr>
<td></td>
<td>• Cabling the configuration</td>
</tr>
<tr>
<td></td>
<td>• Configuring the FC-to-SAS bridges</td>
</tr>
<tr>
<td></td>
<td>• Configuring the FC switches</td>
</tr>
<tr>
<td></td>
<td>• Configuring the MetroCluster in ONTAP</td>
</tr>
<tr>
<td><strong>ONTAP 9 Stretch MetroCluster Installation and Configuration Guide</strong></td>
<td>• Stretch MetroCluster architecture</td>
</tr>
<tr>
<td></td>
<td>• Cabling the configuration</td>
</tr>
<tr>
<td></td>
<td>• Configuring the FC-to-SAS bridges</td>
</tr>
<tr>
<td></td>
<td>• Configuring the MetroCluster in ONTAP</td>
</tr>
<tr>
<td><strong>MetroCluster IP Installation and Configuration Guide</strong></td>
<td>• MetroCluster IP architecture</td>
</tr>
<tr>
<td></td>
<td>• Cabling the configuration</td>
</tr>
<tr>
<td></td>
<td>• Configuring the MetroCluster in ONTAP</td>
</tr>
<tr>
<td>Guide</td>
<td>Content</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>MetroCluster Service Guide</strong></td>
<td>• Guidelines for maintenance in a MetroCluster configuration</td>
</tr>
<tr>
<td></td>
<td>• Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches</td>
</tr>
<tr>
<td></td>
<td>• Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster configuration</td>
</tr>
<tr>
<td></td>
<td>• Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster configuration</td>
</tr>
<tr>
<td></td>
<td>• Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster configuration</td>
</tr>
<tr>
<td></td>
<td>• Expanding a two-node fabric-attached or stretch MetroCluster configuration to a four-node MetroCluster configuration</td>
</tr>
<tr>
<td></td>
<td>• Expanding a four-node fabric-attached or stretch MetroCluster configuration to an eight-node MetroCluster configuration</td>
</tr>
<tr>
<td>Active IQ Unified Manager documentation</td>
<td>• Monitoring the MetroCluster configuration and performance</td>
</tr>
<tr>
<td>NetApp Documentation: Product Guides and Resources</td>
<td></td>
</tr>
<tr>
<td>7-Mode Transition Tool 3.3.1 Copy-Based Transition Guide</td>
<td>• Transitioning data from 7-Mode storage systems to clustered storage systems</td>
</tr>
</tbody>
</table>
Copyright

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

A
about this guide
deciding whether to use the MetroCluster Tiebreaker Software Installation and Configuration Guide 4
Allow ports
in the firewall 29
autostart
setting in MySQL 15
AutoSupport
configuring for MetroCluster configurations 23

C
CLI for Tiebreaker software
launching 19
clusters
how Tiebreaker software monitors MetroCluster 5
comments
how to send feedback about documentation 34

D
detection time
how different disaster types affect Tiebreaker software 7
disaster types
how they affect Tiebreaker software disaster detection time 7
documentation
how to receive automatic notification of changes to 34
how to send feedback about 34
where to find MetroCluster configuration 30
dump files
creating 27

F
failures
detecting with NetApp MetroCluster Tiebreaker software 5
feedback
how to send comments about documentation 34
files, dump
creating 27
Firewall
for MetroCluster Tiebreaker 29

G
guides
requirements for using the MetroCluster Tiebreaker Software Installation and Configuration Guide 4

H
history
displaying for MetroCluster monitoring operations 25
host systems
installing Java Runtime Environment 1.8 on, before installing or upgrading the Tiebreaker software 10
installing MySQL Server 5.5.30 or later versions on, before installing or upgrading the Tiebreaker software 11

I
information
how to send feedback about improving documentation 34
installing
MySQL Server 5.5.30 or later and 5.6.x version before installing or upgrading the Tiebreaker software 11
intersite connectivity failures
how Tiebreaker software detects MetroCluster 6

J
Java Runtime Environment 1.8
installing on your host system before installing or upgrading the Tiebreaker software 10

M
MariaDB server
installing on your host system before installing or upgrading the Tiebreaker software 15
MetroCluster
in active mode 28
MetroCluster configurations
adding on both clusters after installing Tiebreaker software 19
configuring AutoSupport for Tiebreaker 23
displaying information about 26
displaying statistics 25
displaying status 25
how the MetroCluster Tiebreaker software detects site failures 5
introduction to monitoring 23
removing 21
where to find information about 30
MetroCluster in active mode
risks and limitations 28
MetroCluster Tiebreaker
dependency installation 10
MetroCluster Tiebreaker configurations
options for changing the settings 20
MetroCluster Tiebreaker dependencies
installing 10
MetroCluster Tiebreaker software
about the CLI and man pages 8
configuring SNMP settings 22
creating dump files 27