NexentaStor 5.1 MetroHA Admin Guide

Date: June, 2018
Part Number: nxs-5.1-metroHAadminguide-RevA
Copyright © 2018 Nexenta Systems™, ALL RIGHTS RESERVED

Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose, without the express written permission of Nexenta Systems (hereinafter referred to as “Nexenta”).

Nexenta reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Nexenta products and services only can be ordered under the terms and conditions of Nexenta Systems’ applicable agreements. All of the features described in this document may not be available currently. Refer to the latest product announcement or contact your local Nexenta Systems sales office for information on feature and product availability. This document includes the latest information available at the time of publication.

Nexenta, NexentaStor, NexentaEdge, and NexentaConnect are registered trademarks of Nexenta Systems in the United States and other countries. All other trademarks, service marks, and company names in this document are properties of their respective owners.

This document applies to the following product versions:

<table>
<thead>
<tr>
<th>Product</th>
<th>Versions supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NexentaStor</td>
<td>5.1.1 or later</td>
</tr>
<tr>
<td>ATTO FibreBridge 7500</td>
<td>1.18 or later</td>
</tr>
</tbody>
</table>
# Contents

1 MetroHA Overview ................................................................. 1  
   What is MetroHA? ......................................................... 1  
   Components of a MetroHA Configuration .......................... 2  
      NexentaStor Head Nodes ........................................... 3  
      FC-to-SAS Bridges ................................................ 3  
      SAS-Connected Storage Enclosures ............................. 4  
      Stretched Fibre Link ............................................... 5  
   Fault Tolerance for MetroHA Solution Components ............... 5  

2 MetroHA Failover Scenarios .................................................. 7  
   Overview ................................................................. 7  
   Example MetroHA Configuration .................................... 7  
   Node Power Loss Scenario .......................................... 8  
   Site Partition Scenario .............................................. 10  
   Site Failure Scenario ................................................ 13  
   Stale Submirror Scenario ........................................... 16  

3 Administering MetroHA ........................................................ 17  
   Overview ................................................................. 17  
   Verifying the MetroHA Feature License ............................ 18  
   Assigning Site Labels to Nodes .................................... 18  
   Associating Storage Enclosures with Sites ....................... 19  
   Manually Overriding Broken-Site-Safe State ...................... 20  

4 Displaying MetroHA Information ............................................ 23  
   Overview ................................................................. 23  
   Output From Normal Operation ..................................... 23  
   Site Partition Example .............................................. 25  
      Repairing the MetroHA Service .................................. 27  
   Site Failure Example ................................................ 28  
   Overriding Broken-Site-Safe State ................................. 29
## 5 SAS Cable Connections for MetroHA

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>32</td>
</tr>
<tr>
<td>Two FibreBridges With Four Storage Enclosures Each (Eight Total)</td>
<td>32</td>
</tr>
<tr>
<td>Two FibreBridges With Eight Storage Enclosures Each (Sixteen Total)</td>
<td>33</td>
</tr>
<tr>
<td>Two FibreBridges With Sixteen Storage Enclosures Each (Thirty-Two Total)</td>
<td>34</td>
</tr>
</tbody>
</table>

## 6 Troubleshooting MetroHA

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>35</td>
</tr>
<tr>
<td>Verifying the MetroHA Path</td>
<td>35</td>
</tr>
<tr>
<td>Verifying Storage Enclosure Visibility</td>
<td>37</td>
</tr>
<tr>
<td>Troubleshooting the ATTO FibreBridges</td>
<td>38</td>
</tr>
<tr>
<td>Verifying Network Connectivity</td>
<td>38</td>
</tr>
<tr>
<td>Confirming ATTO FibreBridge SAS Port Connectivity</td>
<td>39</td>
</tr>
<tr>
<td>Checking SES Inventory</td>
<td>39</td>
</tr>
<tr>
<td>Checking SAS Target Visibility</td>
<td>40</td>
</tr>
<tr>
<td>Checking SAS-to-FC Mappings</td>
<td>41</td>
</tr>
<tr>
<td>Gathering Diagnostics From ATTO FibreBridges</td>
<td>42</td>
</tr>
</tbody>
</table>
Preface

This documentation presents information specific to Nexenta products. The information is for reference purposes and is subject to change.

About this Administration Guide

This guide is intended for Nexenta partners or end-users who may need to administer an existing MetroHA configuration. Administrative tasks for MetroHA include pool failover/failback, device replacement, and troubleshooting.

Typically, the initial installation and configuration of MetroHA is done by Nexenta personnel. Consequently, installation and configuration procedures are not covered in this document. For information on MetroHA installation and deployment, contact Nexenta Systems.

This documentation assumes that you have a working knowledge of UNIX. It also assumes that you have experience with data storage concepts, such as object storage, ZFS, iSCSI, NFS, CIFS, and so on.

Documentation History

The following table lists the released revisions of this documentation.

Table 1: Documentation Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3000-nxsmetro-000001-A</td>
<td>May, 2016</td>
<td>4.0.4-FP5 GA version</td>
</tr>
<tr>
<td>3000-nxsmetro-000002-A</td>
<td>December, 2016</td>
<td>4.0.5 GA version</td>
</tr>
<tr>
<td>3000-nxsmetro-000003-A</td>
<td>December, 2017</td>
<td>5.1.1 GA version</td>
</tr>
<tr>
<td>nxs-5.1-metroHAadminguide-RevA</td>
<td>June, 2018</td>
<td>Changes to document naming/numbering conventions</td>
</tr>
</tbody>
</table>

Comments

Your comments and suggestions to improve this documentation are greatly appreciated. Send any feedback to doc.comments@nexenta.com and include the documentation title, number, and revision. Refer to specific pages, sections, and paragraphs whenever possible.
MetroHA Overview

This chapter includes the following topics:

- What is MetroHA?
- Components of a MetroHA Configuration
- Fault Tolerance for MetroHA Solution Components

What is MetroHA?

Nexenta Systems’ Metro High Availability (MetroHA) is a solution that builds upon the NexentaStor HA Cluster feature to provide synchronous mirroring of data between two geographically remote sites.

This solution provides for single-instance mirroring of a data pool, with the mirrors separated by metro-wide distances (depending on inter-site latency, up to 50 miles / 80 kilometers) for storage redundancy, high availability, and disaster recovery, with minimal RTO/RPO. Since the data is mirrored across remote sites, it remains accessible to mission-critical applications even in the event of a data center failure or regional disruption.

MetroHA delivers this functionality through a combination of Nexenta products, including NexentaStor Enterprise Edition and the Cluster/HA plug-in. The MetroHA solution relies on a stretched HA cluster of NexentaStor head nodes (one per site) connected via Fibre Channel (FC) to an ATTO FibreBridge that bridges the FC to Serial Attached SCSI (SAS). The ATTO FibreBridge is connected via SAS to storage enclosures at each site.

Figure 1-1 shows a high-level illustration of the components in a MetroHA configuration. At a basic level, a MetroHA configuration consists of a set of NexentaStor head nodes, storage units, and FC-to-SAS bridges, deployed at sites connected via a stretched FC link.
Key features of MetroHA include the following:

- **Disk-level synchronous mirroring** – Data at each site in a MetroHA configuration is constantly and seamlessly mirrored across the Fibre link. MetroHA makes use of four-way mirrors to provide data protection. Two devices from each four-way mirror are located in each data center, in separate storage enclosures, allowing for both local data center and complete data center disk component or chassis failure. All I/Os are checksummed, and the mirrors are self-healing.

- **Automatic failover for high availability (HA)** – MetroHA ensures continuity in the presence of service-level exceptional events, such as power outages or link failures. When MetroHA detects that the NexentaStor node is not functioning on one of the sites, it can automatically fail over storage services to the alternate node. This is made possible by the four-way synchronous disk mirroring layout for all storage pools.

- **Disaster recovery (DR)** – In the event of a major failure at one of the sites, such as the site going offline entirely, MetroHA makes it possible to make the storage services available from the other site. Unlike HA, DR is a manually triggered process; however, the actual data recovery process is fully automated.

**Components of a MetroHA Configuration**

_Figure 1-1_ above shows a high-level illustration of the components in a MetroHA configuration. At a basic level, a MetroHA configuration consists of a set of NexentaStor head nodes, SAS-connected storage enclosures, and FC-to-SAS bridges, deployed at sites connected via a stretched Fibre Channel link.
Contact Nexenta Systems for specific hardware that has been certified to work in a MetroHA configuration.

**NexentaStor Head Nodes**

The head nodes are servers running NexentaStor Enterprise Edition. The head nodes present the storage services to clients. There is a head node at each site in a MetroHA configuration. The two head nodes exchange heartbeat information over both storage and IP links. An interruption in the heartbeat from one of the head nodes may indicate a failure condition and signal the other head node to take over from the failed node.

The NexentaStor nodes in a MetroHA configuration are running NexentaStor Enterprise edition version 5.1. The Cluster/HA plug-in is required on both nodes, along with the MetroHA feature license. Fibre Channel HBAs are installed on the nodes to connect to the FC fabric(s).

MetroHA uses a labelling mechanism, configured during initial setup, to identify the head nodes. Each node in the cluster is assigned a site label, which can indicate the geographical location of the site; for example, “London” or “Manchester”. Each shared storage enclosure in the pool is associated with the head node at its location. This allows MetroHA to keep track of which devices are local to a given site and which are remote.

**FC-to-SAS Bridges**

The FC-to-SAS bridges allow SAS-connected storage enclosures to be connected to an FC fabric, providing the connection between the head nodes and the storage enclosures.

ATTO FibreBridges are used as the FC-to-SAS bridges in a MetroHA configuration. MetroHA has been tested with ATTO FibreBridge models 6500 and 7500. A single ATTO FibreBridge can provide up to 75,000 IOPS. The ATTO FibreBridge functions as a bridge between SAS and FC topologies. It does so by taking SAS targets and presenting them as logical units (LUNs) behind a Fibre Channel (FCP) target port. NexentaStor is still aware of the devices and presents them in terms of their World Wide Name (WWN), but it accesses them in terms of LUN numbers and Fibre Channel ports rather than a SAS port WWN.

At least two ATTO FibreBridges are required in a MetroHA deployment, one at each site. **Figure 1-1** shows a two-FibreBridge deployment. For redundancy, MetroHA can also be deployed with four ATTO FibreBridges, two at each site (see **Figure 1-2** below).
SAS-Connected Storage Enclosures

The storage enclosures, connected via SAS to the FC-to-SAS bridges, provide the actual storage in the MetroHA configuration. Multiple storage enclosures may be multipath cascaded to provide expansion capability. Nexenta requires a minimum of two storage enclosures at each site to provide full data redundancy at a disk level.

In a MetroHA configuration, each storage enclosure has a label assigned to it. The label identifies at which site the enclosure is located, and associates the drives in the enclosure with the label applied to the enclosure.

See the Hardware Compatibility List for additional information about enclosures and devices supported for use with ATTO FibreBridges. See SAS Cable Connections for MetroHA for diagrams of how the SAS cables should be connected between the devices.

Four-Way Mirrors

The volume service in a MetroHA cluster is configured as a four-way mirror. The volume is constructed from four disk devices, with two devices each located in two separate storage enclosures at the local site and two separate storage enclosures at the remote site. In the event of a single storage enclosure failure, data remains available from the other local storage enclosure. In the event of a site failure, where both local storage enclosures are not available, clients can access data stored on the volume from the remaining mirrors on the remote site.
Stretched Fibre Link

To ensure synchronous mirroring of data, there must be a stretched fibre link between the remote sites for MetroHA traffic. The stretched fibre link ensures a reliable, predictable, low-latency connection between sites.

The primary requirement is that the link be sufficient to limit the round-trip delay (RTD) time between the sites to no more than 1 millisecond. Using the 1-millisecond RTD time as a guideline, this generally means that the maximum length of the stretched fibre link is approximately 80 kilometers. Lower latency between sites provides better overall performance.

The stretched fibre link can be described in terms of an Ethernet stretch and an FC stretch, as described below.

Ethernet Stretch

The Ethernet stretch applies to the IP-based data services (SMB, NFS, and iSCSI) and must be a contiguous segment with a VLAN spanning, not two subnets on different VLANs or segments. Heartbeat traffic can be routed, but Nexenta recommends using an isolated stretch VLAN dedicated to this purpose. Support for SSH binding between the nodes is required. This prevents data plane traffic from interfering with cluster communication at either level.

FC Stretch

The FC stretch between the sites in a MetroHA configuration (that is, the inter-site link or ISL) may be a series of fibre strands or DWDM channels.

Separate FC target ports are required for COMSTAR FC support. FC zoning should not allow visibility between target and initiator ports.

See the Hardware Compatibility List for specific requirements (zoning, buffer credits) for FC switches and fabrics.

Fault Tolerance for MetroHA Solution Components

MetroHA is designed to be a robust solution for both HA and DR. However, MetroHA works best when fault tolerance is taken into consideration for the components that make up the solution. Ideally there should be enough redundancy built in to the solution that a condition that requires failover is unlikely to occur.

To improve fault tolerance for individual MetroHA components, Nexenta recommends the following:

- Redundant links between NexentaStor nodes to ensure the flow of heartbeat traffic
  - LACP or IPMP can be used for link redundancy if Ethernet/IP is used to present data services to clients.
- Dual FC fabrics
- Full-path redundancy for inter-site links
Inter-site links be redundant and independent, such that they are truly separate failure domains. For example, having redundant fibres in the same cable conduits still means that these cables can be lost at the same time. Concurrent or cumulative loss of inter-site links creates a site partition, which disrupts MetroHA’s automatic failure capabilities and cross-site mirroring.
This chapter includes the following topics:

- Overview
- Example MetroHA Configuration
- Node Power Loss Scenario
- Site Partition Scenario
- Site Failure Scenario
- Stale Submirror Scenario

Overview

This chapter describes how MetroHA handles various scenarios to facilitate high availability, failover, and disaster recovery.

Note that these scenarios may combine with previous or subsequent faults or failures to create more complex problems, resulting in outcomes other than those described here. For example, if a standby node does not have Ethernet redundancy, a cable or switch failure may cause failover to abort, leaving the service in a broken/unsafe state.

Consequently, Nexenta advises following the recommendations in Fault Tolerance for MetroHA Solution Components and monitoring the MetroHA deployment for faults that may individually or cumulatively compromise failover and mirroring capabilities.

Example MetroHA Configuration

To illustrate various failure scenarios, Figure 2-1 shows an example MetroHA configuration consisting of two sites labelled “London” and “Manchester”. In the example, MetroHA is configured to protect a single storage pool, Pool A.
The physical setup for this configuration is similar to the one illustrated in Figure 1-1. There are NexentaStor head nodes, storage units, and FC-to-SAS bridges, deployed at geographically remote sites connected via a stretched Fibre Channel (FC) link. The London and Manchester nodes exchange heartbeat information across the network link.

Pool A is mirrored across both sites. Within the pool, heartbeat devices (indicated by “hb” in the illustration above) perform a constant periodic write of the heartbeat signature from each node (indicated by “L” or “M”). For each pool, there are two heartbeat devices, which can be physically located at one or both sites.

For each pool, there are two SCSI reservation devices (indicated by “R”) per site. MetroHA distinguishes between reservation devices on storage enclosures associated with the local node (known as local reservation devices) and reservation devices on storage enclosures associated with the other node in the cluster (known as remote reservation devices). In order to start a MetroHA service (without manual intervention) a node must be able to take ownership of both local and remote reservation devices.

The arrow extending from the pool through the London node indicates that a MetroHA service (haservice) is running on the node, and access to the pool is provided through the node.

### Node Power Loss Scenario

Figure 2-2 illustrates what happens when the NexentaStor head node providing service to clients suffers a loss of power.
In the illustration above, the following has occurred:

- The NexentaStor head node at the London site has lost power or failed in some fashion (although the London site itself remains operational).
- The network heartbeat between the London and Manchester nodes has stopped.
- The heartbeat device at the Manchester site no longer detects any heartbeats on local or remote devices.
- The MetroHA service on the London node stops, so clients cannot access storage in the pool through the London node.

*Figure 2-3* illustrates how MetroHA fails over service that was provided by the London node to the Manchester node.
Upon detection of the loss of heartbeats from the London site (both storage and network), the Manchester node takes ownership of both the local SCSI reservations and the remote SCSI reservations at the London site. A MetroHA service is started on the Manchester node that allows clients access to the storage in the pool, and client I/O can resume through the Manchester node.

When the London node becomes responsive again, it detects that it has lost SCSI reservations on the service’s storage and panics itself on the resulting reservation conflict. On reboot after panic, the London node rejoins the cluster and resumes normal operation as standby node for Pool A. Subsequent fail back of storage services to the London node must be done manually by an administrator.

Site Partition Scenario

Figure 2-4 illustrates what happens when the link between the London and Manchester sites goes down, but the nodes remain active. When the inter-site link fails, it results in a site partition.
Figure 2-4: MetroHA Site Partition

In this scenario, the following has occurred:

- The links between the London and Manchester sites have failed.
- The network heartbeat between the two nodes has stopped.
- The heartbeat device at the Manchester site no longer detects heartbeats from London.
- The Manchester site can see its local reservation drives, but cannot see the remote reservations.
- The MetroHA service on the London node continues, but mirroring to the Manchester site is disrupted.

Figure 2-5 illustrates how MetroHA functions when a site partition is encountered.
When the Manchester node loses contact with the London node, it attempts to take ownership of all the SCSI reservations on both sites and start a MetroHA service (haservice). However, since the inter-site link is down, it cannot access the remote reservation devices at the London site. This causes the Manchester node to place the MetroHA service in *broken-site-safe* state and notify the user that manual intervention is required.

In broken-site-safe state, the local node cannot take control of the remote reservations, and releases ownership of the local reservations. The remote node continues to provide service.

In *Figure 2-5* above, despite the lost link between the two sites, the London node continues to provide access to the pool. The Manchester node remains in broken-site-safe state until the link is restored, at which time the broken-site-safe state can be cleared by an administrator.

*Figure 2-6* illustrates what happens when the inter-site link is restored.
When the inter-site link is restored, heartbeats for the network and heartbeat devices resume. The London node assumes ownership of the remote SCSI reservations at Manchester. As mirroring between the two sites resumes, the pool is eventually synchronized and operates as it did before the site partition.

Site Failure Scenario

Figure 2-7 illustrates what happens when one of the sites in a MetroHA configuration fails entirely.

Figure 2-7: MetroHA Site Failure
In this scenario, the following has occurred:

- The London site has failed entirely.
- The network link between the London and Manchester sites has gone down.
- The network heartbeat between the two nodes has stopped.
- The heartbeat device at the Manchester site no longer detects heartbeats from London.
- The MetroHA service on the London node is stopped.
- I/O to the pool, including mirroring, is stopped.

Figure 2-8 illustrates how MetroHA functions in response to a failure of one of the sites.

**Figure 2-8: MetroHA Site Failure Broken-Site-Safe State**

![Diagram of MetroHA Site Failure Broken-Site-Safe State]

Similar to what happens during a site partition, the Manchester node attempts to take over the local and remote SCSI reservations and start a MetroHA service. Since the remote reservations are not visible, the MetroHA service goes into broken-site-safe state, and releases ownership of the local SCSI reservations.

Since the London site is not providing access to the pool, the broken-site-safe service at Manchester needs to be changed to running state. To change the service at Manchester to running state, you must override the broken-site-safe state; this must be done manually, using a CLI command. See [Manually Overriding Broken-Site-Safe State](#) for this procedure.

**Figure 2-9** illustrates the MetroHA configuration after the broken-site-safe state is manually overridden on the Manchester node.
After the broken-site-safe state is overridden, the Manchester node takes ownership of its local SCSI reservations, imports the pool, and starts the service, providing access to the pool.

When the London site is restored, the London node sees that the Manchester node is providing service and does not attempt to take over from the Manchester node. If you want to failback service to the London node, you can do this manually.

Once the London node restarts, mirroring between the two sites resumes, and the pool is eventually synchronized.
Stale Submirror Scenario

When a site partition occurs (see Site Partition Scenario), one node continues to provide service to clients, while the other node enters broken-site-safe state. Mirroring between the two nodes is disrupted, which means the submirror on the other node no longer has the most current version of the pool data. When the site partition is resolved, the broken-site-safe state is cleared, mirroring resumes, and the pool is eventually synchronized between the two sites.

When a site failure occurs at the site providing service (see Site Failure Scenario), it is necessary to override the broken-site-safe state on the node at the other site so that it can provide service using its submirror of the pool data. This override is done manually by an administrator using a CLI command (see Manually Overriding Broken-Site-Safe State).

It is possible that a site partition could occur, followed some time later by a site failure at the site providing service. At this point, you may want to fail over the MetroHA service to the node at the non-failed site. To do this, you would override the broken-site-safe state for the MetroHA service, which would cause the MetroHA service on the node at the non-failed site to enter the running state and provide service to clients.

However, since mirroring may have been disrupted at some point as a result of the site partition, the copy of the pool data on the node at the non-failed site may not be up-to-date (that is, stale). Consequently, you may not want to enable a service that provides clients access to this potentially out-of-date data.

When you enter the CLI command to override the broken-site-safe state for the MetroHA service, the system checks that the submirror at the local site has the most up-to-date copy of the pool data. If it does, then the override proceeds as requested. Otherwise, the system displays the date and time that the pool was last updated, and the date and time that contact was lost with the other node. Using this information, you can decide whether you want to proceed with overriding broken-site-safe state for the MetroHA service and provide clients access to pool data from this submirror.

Note: To prevent the London node from going to broken-site-safe state when it is restarted, you should ensure that the inter-site network link is working prior to restarting the node.
Administering MetroHA

This chapter includes the following topics:

- Overview
- Verifying the MetroHA Feature License
- Assigning Site Labels to Nodes
- Associating Storage Enclosures with Sites
- Manually Overriding Broken-Site-Safe State

Overview

This chapter contains procedures that are relevant to administering a MetroHA configuration. These tasks include those that may be performed by Nexenta Professional Services during initial MetroHA configuration, as well as those that are part of the day-to-day operation of a MetroHA cluster.

Installation and initial configuration of MetroHA are typically done by Nexenta Professional Services personnel. Following installation and configuration, there are administrative tasks related to MetroHA that you may need to undertake independently, including verifying the MetroHA feature license, assigning labels to nodes and enclosures, and overriding broken-site-safe state in the event of a site failure. This chapter describes how to perform these tasks.

Other administrative tasks that apply to HA and that also may apply to MetroHA are covered in the NexentaStor HA CLI QuickStart Guide and are not documented here. These tasks include:

- Creating / enabling / disabling services
- Failover / failback
- Repairing / recovering services
- Configuring the cluster
- Adding heartbeats
- Discovering pools
- Adding devices

You can obtain the NexentaStor HA CLI QuickStart Guide from your Nexenta representative, from the Nexenta customer portal, or from www.nexenta.com.
Verifying the MetroHA Feature License

MetroHA requires a four-way mirror configuration that includes two heartbeat devices and four reservation devices, distributed across both sites such that each site contains two reservation devices. The heartbeat devices can both be physically located on one of the sites, or can be distributed across the two sites.

Enabling the MetroHA license for a pool enforces these requirements. This means that you can verify that the heartbeat and reservation devices are correctly allocated by verifying the MetroHA license for the pool.

- To verify the MetroHA feature license, enter the following command:

  CLI@st-A> license show

  Check that metroHa, highAvailability, allFlash, continuousReplication, scheduledReplication, fibrechannel, and continuousReplication are listed for the features property. If they are not, contact Nexenta Systems for license information.

Assigning Site Labels to Nodes

MetroHA allocates resources and tracks ownership of storage devices based on a site label assigned on each node. The site label can indicate the geographical location of the site; for example, “London” or “Manchester”. Site labels are normally assigned during initial MetroHA configuration. In the examples in this chapter, node “st-A” is located at site “London”, and node “st-B” is located at site “Manchester”.

- To assign a site label to a node, enter the following command on each node:

  CLI@nexenta> config set ha.site=<site-label>

  For example:

  CLI@st-A> config set ha.site=London
  CLI@st-B> config set ha.site=Manchester
Associating Storage Enclosures with Sites

When a MetroHA service is started, it attempts to take ownership of the SCSI reservation devices on the node at the local site and the node at the remote site. To do this, it must be able to determine which storage enclosures are local to a given site and which are remote. As part of MetroHA configuration, you specify the enclosure(s) that are local to the site. The enclosures not specified as local are assumed to be remote.

To associate a storage enclosure with a site:

1. List the visible storage enclosures, local and remote, that are shared.

   CLI@st-A> hactl site
   
   System response:
   
   Shared enclosures:
   #1: 500304800111283f
   #2: 50030480091bda3f
   #3: 5003048000b127f7f
   #4: 5003048000b0547f
   
   Enter space-separated list of local enclosures:

2. At the prompt, enter the ID(s) of the storage enclosures local to the node. The specified enclosures are associated with the local site, and the remaining enclosures are associated with the remote site.

   For example:

   Enter space-separated list of local enclosures: 500304800111283f 50030480091bda3f

   System response:

   Labelling enclosure 1 of 4: 500304800111283f
   Labelling enclosure 2 of 4: 50030480091bda3f
   Labelling enclosure 3 of 4: 5003048000b12f77f
   Labelling enclosure 4 of 4: 5003048000b0547f

   CHASSISID         SITE
   500304800111283f  London
   50030480091bda3f  London
   5003048000b12f77f  Manchester
   5003048000b0547f  Manchester

To display the site with which each storage enclosure is associated, enter the following command:

   CLI@st-A> hactl site --status

   System response:

   STATUS: OK

   CHASSISID         SITE
   500304800111283f  London
   50030480091bda3f  London
   5003048000b12f77f  Manchester
   5003048000b0547f  Manchester
To display information about the storage enclosures, enter the following command:

```
CLI@st-A> enclosure list -o chassisId,label,site,product,vendor,bays,used,serial
```

System response:

```
#  CHASSIS           LABEL  SITE        PRODUCT        VENDOR    BAYS  USED  SERIAL
0  5003048000b12f7f  -      Manchester  SAS2X36        LSI CORP  21    21    -
1  500304800111283f  -      London      SC216BE2CJBOD  SMCI      24    24    SMC0102030405060708090B
2  50030480091bda3f  -      London      SC216BE2CJBOD  SMCI      24    24    SMC0102030405060708090A
3  5003048000b0547f  -      Manchester  SAS2X36        LSI CORP  24    23    -
4  LEGACY_SAS        -      -           Onboard SAS    Nexenta   1     1     -
```

Manually Overriding Broken-Site-Safe State

During a site partition (see Site Partition Scenario), the standby node for a MetroHA service may go into broken-site-safe state. This can happen when the inter-site link between the nodes is disrupted, but the active node continues to provide service. In broken-site-safe state, the standby node does not attempt to provide access to the storage pool. When the inter-site link is restored, the active node takes ownership of the reservation devices at the remote site, and service continues as it had before the link disruption.

In the case of a site failure (see Site Failure Scenario) the other node is not able to provide service, and the standby node goes into broken-site-safe state. In order to restore access to the pool via the standby node, the broken-site-safe state must be overridden manually.

To override broken-site-safe state for a MetroHA service:

1. On the node at the non-failed site, list the name of the configured MetroHA service.

```
CLI@st-B> haservice list
```

System response:

```
NAME     GUID                    DESCRIPTION   VIPs   NODES      RUNNING   STOPPED   BROKEN
MetroHA  15165650219770712359    None                 st-A,st-B  -         st-A      st-B
```

2. Verify that the MetroHA service on the node is in broken-site-safe state.

```
CLI@st-B> haservice status
```

System response:

```
service: MetroHA
description: MetroHA service

status:
NODE     STATUS        MODE        UNBLOCKED   ERRORS
st-A   unknown        unknown     yes         -
st-B   broken_site_safe automatic yes     -
```

3. Override the broken-site-safe state.

```
CLI@st-B> haservice override broken-site-safe
```

System response:

```
Overridden broken-site-safe state for MetroHA
```

4. Verify that the MetroHA service on the node is no longer in broken-site-safe state.

```
CLI@st-B> haservice status
```

System response:

```
service: MetroHA
description: MetroHA service

status:
NODE     STATUS        MODE        UNBLOCKED   ERRORS
st-A   automatic      automatic   yes         -
st-B
```

pools:

```
NAME     GUID                 PRIMARY
PoolA   743969617085416734   yes
```

vips: not configured
init timeout:  20
run timeout:   0

disk heartbeats:
  DISK
c0t5000C50069009207d0
c0t5000C500893FBAD3d0

SCSI reservations:
  NODE   DISK                    TYPE
    st-A   c0t5000C50069010DA3d0   SCSI2
    st-A   c0t5000C50069010F17d0   SCSI2

3. Override the broken site safe state by entering the following command:

   CLI@st-B> haservice override --set <service-name>

   For example:

   CLI@st-B> haservice override --set MetroHA

   Pool last access time: Wed Jun 28 14:24:34 2017
   RSF lost contact time: Fri Jul 28 13:34:46 2017
   Pool TXG number: 5199066
   set broken-site-safe override for service 'MetroHA'? [y/N] y

   The system displays the date and time that the pool was last updated, and the date and time
   that contact was lost with the other node. Depending on the amount of time between the last
   pool update and when contact with the other node was lost, it could mean that the data in the
   local submirror is out of date. You should take this information into account when deciding
   whether to activate the MetroHA service and provide clients access to data from this submirror.
   See Stale Submirror Scenario.

4. Verify that the MetroHA service on the node is running.

   CLI@st-B> haservice status

   System response:

   service:      MetroHA
   description:  MetroHA service

   status:
   NODE   STATUS             MODE        UNBLOCKED   ERRORS
    st-A   unknown            unknown     yes         -
    st-B    running            automatic   yes         -

   pools:
   NAME    GUID                 PRIMARY
    PoolA   743969617085416734   yes

   vips: not configured

   init timeout:   20
   run timeout:    0

   disk heartbeats:
   DISK
When the broken-site-safe state is overridden, it starts a MetroHA service on the node that allows clients access to the storage pool (see Figure 2-10). When the node at the failed site is eventually restarted, to prevent it from going into broken-site-safe state, you should ensure that the inter-site network link is working prior to restarting the node.

Note that MetroHA re-establishes heartbeats and reservations, but does not attempt to re-create four-way mirrors and perform re-silvering. Depending on the circumstances of the recovery, such as whether the link is restored or new storage devices are installed, these tasks may be performed by ZFS, or you may need to do them manually.

<table>
<thead>
<tr>
<th>NODE</th>
<th>DISK</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>st-A</td>
<td>c0t5000c50069010da3d0</td>
<td>SCSI2</td>
</tr>
<tr>
<td>st-A</td>
<td>c0t5000c50069010f17d0</td>
<td>SCSI2</td>
</tr>
</tbody>
</table>
Displaying MetroHA Information

This chapter includes the following topics:

- Overview
- Output From Normal Operation
- Site Partition Example
- Site Failure Example

Overview

This chapter presents examples of output from NexentaStor CLI commands that display the status of a MetroHA configuration. Output is shown for normal operation, from when a site partition occurs, and from when a site failure occurs.

The example configuration consists of two nodes, st-A and st-B, located at sites geographically remote from each other. Under normal operation, the MetroHA service on node st-A protects pool mha01.

Output From Normal Operation

Under normal operation, the MetroHA pool is shown as ONLINE. For node st-A, the pool status command for the mha01 pool displays the following:

```
CLI@st-A> pool status mha01
pool     mha01
health   ONLINE
scan     resilver repaired 4.0K with 0 errors in 0s on Sep 21 10:08:54
trim     none requested

VDEV                       HEALTH  READ  WRITE  CKSUM  WHERE
mha01                    ONLINE  0     0      0      -
mirror-0                 ONLINE  0     0      0      -
c0t5000C50096F6830Bd0  ONLINE  0     0      0      500304800111283f/3
c0t5000C50088A91F6Fd0  ONLINE  0     0      0      50030480018da3f/3
```

4
Enter the `hacluster status` command on one of the nodes displays status for the MetroHA service on both nodes.

```
CLI@st-B> haservice status
service: mha01
description: MetroHA service

status:
NODE          STATUS    MODE       UNBLOCKED  ERRORS
st-B          stopped  automatic  yes        _
st-A          running   automatic  yes        _
pools:
NAME     GUID          PRIMARY
mha01     10403872400252891565  yes

vips:
NAME     ADDRESS                   IPv6  NODE  NIC   STATUS
mha01     10.3.53.28/255.255.252.0  no    st-B  igb0  down
           st-A  igb0  up

init timeout: 20
run timeout:  8

disk heartbeats:
DISK
c0t5000C500943D42Cb0
mirror-3
c0t5000C50096F688F0d0
mha01
vips:
NAME     ADDRESS                   IPv6  NODE  NIC   STATUS
mha01     10.3.53.28/255.255.252.0  no    st-B  igb0  down
           st-A  igb0  up

The `hacluster status -e` command displays additional cluster, node, and heartbeat information:

```
CLI@st-B> haservice status -e

== Cluster status ==
NAME       STATUS  NODES  SERVICES  DESCRIPTION
mha01      ok      2/2    2/2       metroHA ATTO7500

== Cluster configuration ==
FC MONITORING SERIAL HEARTBEATS ENABLED  NETWORK MONITORING
no            no                         yes

== Nodes ==
NODE          STATUS SERVICES ADDRESS HostId    Release
st-B          up      1/2   10.3.53.114 1c080ceb  5.1.0.14
st-A          up      1/2   10.3.53.146 83b6a74e  5.1.0.14
```
-- Heartbeats --
<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>FROM</th>
<th>TO</th>
<th>PEER ADDRESS</th>
<th>STATUS</th>
<th>POOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>net</td>
<td>st-B</td>
<td>st-A</td>
<td>192.168.1.10</td>
<td>up</td>
<td>mha01</td>
</tr>
<tr>
<td>1</td>
<td>disc</td>
<td>st-B</td>
<td>st-A</td>
<td>c0t5000C50096F680Bd0</td>
<td>up</td>
<td>mha01</td>
</tr>
<tr>
<td>2</td>
<td>disc</td>
<td>st-B</td>
<td>st-A</td>
<td>c0t5000C5009439377d0</td>
<td>up</td>
<td>mha01</td>
</tr>
<tr>
<td>3</td>
<td>net</td>
<td>st-A</td>
<td>st-B</td>
<td>192.168.1.11</td>
<td>up</td>
<td>mha01</td>
</tr>
<tr>
<td>4</td>
<td>disc</td>
<td>st-A</td>
<td>st-B</td>
<td>c0t5000C50096F680Bd0</td>
<td>up</td>
<td>mha01</td>
</tr>
<tr>
<td>5</td>
<td>disc</td>
<td>st-A</td>
<td>st-B</td>
<td>c0t5000C5009439377d0</td>
<td>up</td>
<td>mha01</td>
</tr>
</tbody>
</table>

Site Partition Example

When the inter-site link fails, causing a site partition (see Site Partition Scenario), st-A continues to provide service to clients. However, the output of the pool status command indicates that the health of the pool is DEGRADED, and each node controls half of the pool.

On st-B, the pool status command shows that pool mha01 is in DEGRADED state. Half of the devices have a health status of ONLINE, and half have a health status of UNAVAIL or REMOVED.

CLI@st-B> pool status mha01
pool     mha01
health   DEGRADED
scan     resilver repaired 4.0K with 0 errors in 0s on Sep 21 10:08:54
trim     none requested

<table>
<thead>
<tr>
<th>DEVICES</th>
<th>HEALTH</th>
<th>READ</th>
<th>WRITE</th>
<th>CKSUM</th>
<th>WHERE</th>
</tr>
</thead>
<tbody>
<tr>
<td>mha01</td>
<td>DEGRADED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>mirror-0</td>
<td>DEGRADED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>mirror-1</td>
<td>DEGRADED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>mirror-2</td>
<td>DEGRADED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>mirror-3</td>
<td>DEGRADED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C50096F680Bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
<tr>
<td>c0t5000C5009439377d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480011243f/3</td>
</tr>
</tbody>
</table>

errors  no known data errors

Running the haservice status command on each node indicates that the other node is in broken-site-safe state.

CLI@st-A> haservice status
service:  mha01
description:  MetroHA service
status:
NODE  STATUS            MODE       UNBLOCKED  ERRORS
st-B  broken_site_safe  automatic  yes        st-B: Floating address(es) mha01 in use.
st-A  running           automatic  yes        

pools:
NAME       GUID                  PRIMARY
mha01      10403872400252891565  yes

vips:
NAME       ADDRESS                   IPv6  NODE        NIC   STATUS
mha01      10.3.53.28/255.255.252.0  no    st-B        igb0  down
st-A        igb0  up

init timeout: 20
run timeout: 8

disk heartbeats:
DISK
c0t5000C50088A91F6Fd0
c0t5000C50096F6830Bd0

SCSI reservations:
NODE  DISK                              TYPE
st-A  /dev/rdsk/c0t5000C500979CD593d0*  SCSI2
st-A  /dev/rdsk/c0t5000C50094395A73d0*  SCSI2
st-A  /dev/rdsk/c0t5000C500893FB93Fd0*  SCSI2
st-A  /dev/rdsk/c0t5000C500944FEFFd0*  SCSI2

The `hacluster status -e` command indicates that the heartbeat devices no longer detect heartbeats from the other site.

On st-A, the `hacluster status -e` command displays the following output:

CLI@st-A> hacluster status -e
== Cluster status ==
NAME       STATUS  NODES  SERVICES  DESCRIPTION
mha01      ok      2/2    2/2       metroHA ATTO7500

== Cluster configuration ==
FC MONITORING  SERIAL HEARTBEATS ENABLED  NETWORK MONITORING
no             no                         yes

== Nodes ==
NODE        STATUS  SERVICES  ADDRESS      HostId    Release
st-B        up      1/2       st-B         1c080ceb  5.1.0.14
st-A        up      1/2       st-A         83b6a74e  5.1.0.14

== Heartbeats ==
ID  TYPE  FROM  TO    PEER ADDRESS           STATUS  POOL
0   net  st-B  st-A  192.168.1.10           down    -
1   disc  st-B  st-A  c0t5000C50088A91F6Fd0  down    mha01
4   disc  st-B  st-A  c0t5000C50096F6830Bd0  down    mha01
5   net  st-A  st-B  192.168.1.11           down    -
6   disc  st-A  st-B  c0t5000C50096F6830Bd0  down    mha01
7   disc  st-A  st-B  c0t5000C50088A91F6Fd0  down    mha01

On st-B, the `hacluster status -e` command displays the following output:
CLI@st-B> hacluster status -e
-- Cluster status --
<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>NODES</th>
<th>SERVICES</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>mha01</td>
<td>ok</td>
<td>2/2</td>
<td>2/2</td>
<td>metroHA ATTO7500</td>
</tr>
</tbody>
</table>

-- FC MONITORING SERIAL HEARTBEATS ENABLED NETWORK MONITORING
no no yes

-- Nodes --
<table>
<thead>
<tr>
<th>NODE</th>
<th>STATUS</th>
<th>SERVICES</th>
<th>ADDRESS</th>
<th>HostId</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>st-B</td>
<td>up</td>
<td>1/2</td>
<td>st-B</td>
<td>1c080ceb</td>
<td>5.1.0.14</td>
</tr>
<tr>
<td>st-A</td>
<td>up</td>
<td>1/2</td>
<td>st-A</td>
<td>83b6a74e</td>
<td>5.1.0.14</td>
</tr>
</tbody>
</table>

-- Heartbeats --
<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>FROM</th>
<th>TO</th>
<th>PEER ADDRESS</th>
<th>STATUS</th>
<th>POOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>net</td>
<td>st-B</td>
<td>st-A</td>
<td>192.168.1.10</td>
<td>down</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>disc</td>
<td>st-B</td>
<td>st-A</td>
<td>c0t5000c50088a91f6fd0</td>
<td>down</td>
<td>mha01</td>
</tr>
<tr>
<td>4</td>
<td>disc</td>
<td>st-B</td>
<td>st-A</td>
<td>c0t5000c50096f6830bd0</td>
<td>down</td>
<td>mha01</td>
</tr>
<tr>
<td>5</td>
<td>net</td>
<td>st-A</td>
<td>st-B</td>
<td>192.168.1.11</td>
<td>down</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>disc</td>
<td>st-A</td>
<td>st-B</td>
<td>c0t5000c50096f6830bd0</td>
<td>down</td>
<td>mha01</td>
</tr>
<tr>
<td>7</td>
<td>disc</td>
<td>st-A</td>
<td>st-B</td>
<td>c0t5000c50088a91f6fd0</td>
<td>down</td>
<td>mha01</td>
</tr>
</tbody>
</table>

Repairing the MetroHA Service

When a site partition occurs, you must make the hardware and software changes necessary to correct whatever caused the link failure and restore communication between the nodes. Once the inter-site link is restored, you can clear the alert cases, rescan the disks, and repair the service.

For example:

CLI@st-A> pool clear mha01
Rediscover the disks with the following command:

CLI@st-A> disk rescan

When the pool is online again, you can check the status of the pool and repair the MetroHA service.

CLI@st-A> pool status mha01
pool mha01
health ONLINE
scan resilver repaired 128.0K with 0 errors in 1s on Sep 21 11:58:31
trim none requested
devices

<table>
<thead>
<tr>
<th>DEV</th>
<th>HEALTH</th>
<th>READ</th>
<th>WRITE</th>
<th>CKSUM</th>
<th>WHERE</th>
</tr>
</thead>
<tbody>
<tr>
<td>mha01</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>mirror-0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>c0t5000c500893fc48bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50030480091bda3f/7</td>
</tr>
<tr>
<td>c0t5000c50096f673af0d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>500304800111283f/6</td>
</tr>
<tr>
<td>mirror-1</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>c0t5000c50096f6830bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>500304801f279d3f/5</td>
</tr>
<tr>
<td>mirror-2</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>c0t5000c500979089c3d0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>500304800111283f/7</td>
</tr>
<tr>
<td>c0t5000c5009444a01fd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>500304801f279d3f/5</td>
</tr>
<tr>
<td>c0t5000c500944520e7bd0</td>
<td>ONLINE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>500304801f279d3f/2</td>
</tr>
</tbody>
</table>
Site Failure Example

When a failure of one of the sites occurs, the network heartbeat between the two nodes stops, as does mirroring of the pool between the nodes. (See Site Failure Scenario.)

In the example below, the site where node st-A is located has failed, causing node st-B to place mha01 into broken-site-safe state. To allow st-B to start providing service for pool mha01, the broken-site-safe state must be manually overriden.

```
cli@st-A> haservice repair mha01 st-A
```

Entering the pool status command on st-A indicates that the health of the mha01 pool is in DEGRADED state.
CLI@st-A> pool status mha01
pool     mha01
health   DEGRADED
scan     resilver repaired 16.02G with 0 errors in 7m 10s on Sep 21 12:20:54
trim     none requested

devices

VDEV                       HEALTH    READ  WRITE  CKSUM  WHERE
mha01                      DEGRADED  0     0      0      -
mirror-0                   DEGRADED  0     0      0      -
c0t5000C50096F6830Bd0      ONLINE  0     0      0      500304800111283f/3
c0t5000C50088BA91F6Ffd0    UNAVAIL  0     11     0      50030480091bda3f/3
c0t5000C50094943737d0      UNAVAIL  0     0      0      500304801f27843f/3

c0t5000C50094415D5Fd0      ONLINE  0     0      0      500304801f279d3f/3
mirror-1                   DEGRADED  0     0      0      -
c0t5000C500979CD593d0      ONLINE  0     0      0      500304800111283f/1

c0t5000C50094415433d0      UNAVAIL  0     0      0      50030480091bda3f/2

c0t5000C5009444FEEFd0      UNAVAIL  0     0      0      500304801f27843f/0

c0t5000C50094396A73d0      ONLINE  0     0      0      500304801f279d3f/0
mirror-2                   DEGRADED  0     0      0      -
c0t5000C50096F6793Bd0      ONLINE  0     0      0      500304800111283f/5

c0t5000C500893FBBB3d0      UNAVAIL  0     0      0      50030480091bda3f/5

c0t5000C50094395C7d0      UNAVAIL  0     0      0      500304801f27843f/1

c0t5000C500943D42CBd0      ONLINE  0     0      0      500304801f279d3f/1
mirror-3                   DEGRADED  0     0      0      -
c0t5000C50096F6880Fd0      ONLINE  0     0      0      500304800111283f/4

c0t5000C50094179DF3d0      UNAVAIL  0     0      0      50030480091bda3f/6

c0t5000C500941932Bd0      ONLINE  0     0      0      500304801f279d3f/4

errors  no known data errors

On st-A, the hacluster status -e command displays the following output:

CLI@st-A> hacluster status -e
hacluster status -e
-- Cluster status --
NAME     STATUS    NODES  SERVICES  DESCRIPTION
mha01    degraded  1/2    1/2       metroHA ATTO7500

-- Cluster configuration --
FC MONITORING  SERIAL HEARTBEATS ENABLED  NETWORK MONITORING
no             no                         yes

-- Nodes --
NODE  STATUS  SERVICES  ADDRESS      HostId    Release
st-B  down    0/2       10.3.53.114  -         5.1.0.14
st-A  up      1/2       10.3.53.146  83b6a74e  5.1.0.14

-- Heartbeats --
ID  TYPE  FROM  TO  PEER ADDRESS  STATUS  POOL
0 net st-B st-A  192.168.1.10  down  -
1 disc st-B st-A c0t5000C50096F6830Bd0 down mha01
4 disc st-B st-A c0t5000C50096F6830Bd0 down mha01

Overriding Broken-Site-Safe State

The following command, entered on node st-B, overrides broken-site-safe state for pool mha01, which allows st-B to start providing service for the pool.
CLI@st-B> haservice override --set mha01
Pool last access time: Wed Jun 28 14:24:34 2017
RSF lost contact time: Fri Jul 28 13:34:46 2017
Pool TXG number: 5199066
set broken-site-safe override for service 'mha01' ? [y/N] y

The system displays the date and time that the pool was last updated, and the date and time that contact was lost with the other node. Depending on the amount of time between the last pool update and when contact with st-A, it could mean that the data in the submirror on st-B is out of date. You should take this information into account when deciding whether to activate the MetroHA service and provide clients access to data from this submirror. See Stale Submirror Scenario.

Subsequently running the haservice status command on st-B indicates the node is running and providing service for pool mha01.

CLI@st-B> haservice status
service: mha01
description: MetroHA service

status:
NODE  STATUS   MODE       UNBLOCKED  ERRORS
st-B  running  automatic  yes        _
st-A  unknown  unknown    yes        _

pools:
NAME   GUID                  PRIMARY
mha01  10403872400252891565  yes

vips:
NAME   ADDRESS                   IPv6  NODE  NIC   STATUS
mha01  10.3.53.28/255.255.252.0  no    st-B  igb0  up

init timeout:  20
run timeout:   8

disk heartbeats:
DISK
c0t5000C50088A91F6Fd0
c0t5000C50096F6BD03Dd0

SCSI reservations:
NODE  DISK                              TYPE
st-B  /dev/rdsk/c0t5000C500979CD593d0*  SCSI2
st-B  /dev/rdsk/c0t5000C50094395A73d0*  SCSI2
st-B  /dev/rdsk/c0t5000C500893FB93Fd0*  SCSI2
st-B  /dev/rdsk/c0t5000C5009444FEFFd0*  SCSI2

Entering the pool status command on st-B indicates that the health of the mha01 pool is in DEGRADED state.

CLI@st-B> pool status mha01
pool    mha01
health  DEGRADED
scan    resilver repaired 16.02G with 0 errors in 7m 10s on Sep 21 12:20:54
trim    none requested
devices

VDEV HEALTH READ WRITE CKSUM WHERE
mha01    DEGRADED  0  0  0   -
mirror-0 DEGRADED  0  0  0   -
On st-B, the `hacluster status -e` command displays the following output:

```plaintext
CLI@st-B> hacluster status -e
-- Cluster status --
  NAME  STATUS  NODES  SERVICES  DESCRIPTION
  mha01  degraded  1/2    1/2       metroHA ATTO7500

-- Cluster configuration --
  FC MONITORING  SERIAL HEARTBEATS ENABLED  NETWORK MONITORING
   no             no                         yes

-- Nodes --
  NODE  STATUS  SERVICES  ADDRESS      HostId    Release
  st-A  down    0/2       10.3.53.114  -         5.1.0.14
  st-B  up      1/2       10.3.53.146  83b6a74e  5.1.0.14

-- Heartbeats --
  ID  TYPE  FROM  TO  PEER ADDRESS     STATUS  POOL
  0  net  st-A  st-B  192.168.1.10   down   -
  1  disc st-A  st-B  c0t5000c50088a91f6fd0 down  mha01
  2  disc st-A  st-B  c0t5000c50096f6830bd0 down  mha01
```
This chapter includes the following topics:

- **Overview**
- **Two FibreBridges With Four Storage Enclosures Each (Eight Total)**
- **Two FibreBridges With Eight Storage Enclosures Each (Sixteen Total)**
- **Two FibreBridges With Sixteen Storage Enclosures Each (Thirty-Two Total)**

**Overview**

In a MetroHA configuration, ATTO FibreBridges provide the connectivity between the FC fabric(s) and the SAS storage enclosures. MetroHA supports using either one or two FibreBridges per site.

For redundancy, multiple storage enclosures can be connected to each FibreBridge. The illustrations in this section show how the SAS cables are connected between the SAS ports on the FibreBridges and the SAS ports on the SAS shelves containing the storage enclosures.

**Two FibreBridges With Four Storage Enclosures Each (Eight Total)**

If MetroHA is deployed in a four-FibreBridge configuration, with two FibreBridges at each site, a given storage enclosure within a SAS shelf must connect through only one FibreBridge, not through both FibreBridges. **Figure 5-1** shows a configuration where two FibreBridges are deployed at a site, with four storage enclosures connected to each FibreBridge.
Figure 5-1: SAS Port Connections for Two FibreBridges and Eight Storage Enclosures

Two FibreBridges With Eight Storage Enclosures Each (Sixteen Total)

Figure 5-2 shows a configuration where two FibreBridges are deployed at a site with eight storage enclosures connected to each FibreBridge.

Figure 5-2: SAS Port Connections for Two FibreBridges and Sixteen Storage Enclosures
Two FibreBridges With Sixteen Storage Enclosures Each (Thirty-Two Total)

*Figure 5-3* shows a configuration where the storage enclosures are cascaded further. Two FibreBridges are deployed at a site with 16 storage enclosures connected to each FibreBridge, 32 storage enclosures total.

*Figure 5-3: SAS Port Connections for Two FibreBridges and Sixteen SAS Shelves*
Troubleshooting MetroHA

This chapter includes the following topics:

- Overview
- Verifying the MetroHA Path
- Verifying Storage Enclosure Visibility
- Troubleshooting the ATTO FibreBridges

Overview

This chapter contains procedures you can use to troubleshoot a MetroHA topology. When troubleshooting MetroHA, Nexenta recommends using an inside-out approach, which can minimize errors and reduce diagnostic time in localizing storage problems in terms of the device topology. For MetroHA, the inside-out approach means that you start with the device’s immediate connection point in the SAS storage enclosure and move further out, one layer at a time, so that you are certain of the previous layer’s state when diagnosing the next layer. For MetroHA, the layers are:

1. Storage devices
2. SAS enclosures
3. ATTO FibreBridges
4. FC switches
5. NexentaStor head nodes

Some steps may require assistance from Nexenta support or whoever operates your FC switch environment.

You can access an ATTO FibreBridge for remote management using a Web browser or a Telnet client. NexentaStor does not ship with a Telnet client by default, so you should install one from your desktop if you do not wish to use a Web browser.

Verifying the MetroHA Path

Using the NexentaStor CLI, check the status of the FC ports to ensure that the end-to-end connection from the NexentaStor head nodes to the ATTO FibreBridges is operational.

You can use the `fcinitiator` CLI command to list the FC initiators, then display hardware details and status for a specific FC initiator:

For example:
CLI@nexenta> fcinitiator list
NAME                  NODEWWN           CURRSPEED  STATE
wwn.10000000c9ea9f68  2000001b320c463f  4Gb        online
wwn.2101001b322c463f  2001001b322c463f  4Gb        online

CLI@nexenta> fcinitiator get all wwn.10000000c9ea9f68
NAME                  PROPERTY      VALUE
wwn.10000000c9ea9f68  model         LPe12002-M8
wwn.10000000c9ea9f68  serialNumber  BK21833103
wwn.10000000c9ea9f68  vendor        Emulex
wwn.10000000c9ea9f68  name          wwn.10000000c9ea9f68
wwn.10000000c9ea9f68  nodeWwn       20000000c9ea9f68
wwn.10000000c9ea9f68  currSpeed     4Gb
wwn.10000000c9ea9f68  state         online
wwn.10000000c9ea9f68  suppSpeeds    2Gb 4Gb 8Gb
wwn.10000000c9ea9f68  topoType      N-port
wwn.10000000c9ea9f68  physPortWwn   10000000c9ea9f68
wwn.10000000c9ea9f68  portType      physical

You can use the NexentaStor fcinitiator CLI command to display information about the remote port that is connected to a specified local initiator.

For example:

CLI@nexenta> fcinitiator scan wwn.10000090fa498c2e
NAME                  NODEWWN           SCSI  STATE   SYMBOLICNAME
wwn.2100001086702540  2000001086702540  yes   online  ATTO XstreamCORE FC 7500 2.10, FC Port Number 1
wwn.21000010867001d0  20000010867001d0  yes   online  -

CLI@nexenta> fcinitiator scan wwn.10000090fa498c2f
NAME                  NODEWWN           SCSI  STATE   SYMBOLICNAME
wwn.2200001086702540  2000001086702540  yes   online  ATTO XstreamCORE FC 7500 2.10, FC Port Number 2
wwn.22000010867001d0  20000010867001d0  yes   online  -

Use the NexentaStor inventory lu CLI command to display the inventory of logical-path-to-FC-connected backend devices that are used in the MetroHA configuration.

In a MetroHA configuration, absent a path failure, there are two FC paths between the NexentaStor node and an ATTO FibreBridge, and two SAS connections between the ATTO FibreBridge and the storage enclosure. The ATTO FibreBridge provides a full mesh connection between the frontend FC paths and the backend SAS connections, so each device in a storage enclosure actually has four logical paths.

For example, the following command displays information for a specified LU:

CLI@nexenta> inventory lu | grep -i 5000C50028D412B3
5000c50028d412b3  disk         c0t5000c50028d412b3d0  Emulex-42D0494-0  20   21000010867001d0  ONLINE
5000c50028d412b3  disk         c0t5000c50028d412b3d0  Emulex-42D0494-0  6    21000010867001d0  ONLINE
5000c50028d412b3  disk         c0t5000c50028d412b3d0  Emulex-42D0494-0  20   22000010867001d0  ONLINE
5000c50028d412b3  disk         c0t5000c50028d412b3d0  Emulex-42D0494-0  6    22000010867001d0  ONLINE

The output of the inventory lu example above indicates that LU 5000C50028D412B3 has four paths. This LU is shared using LUN IDs 20 and 6 by the ATTO FibreBridge. Each LUN ID is presented over both FC target ports on the ATTO FibreBridge (21000010867001d0 and 22000010867001d0).

In the event of an FC failure, the FC path count drops from four to two, which you can verify with the following command:

CLI@nexenta> disk list -o*,pathcount
#   NAME                   LABEL  SIZE     MEDIATYPE  SED  STATE     WHERE                USAGE                 PATHCOUNT
0   c0t50014e002339d  -      232.89G  hdd        no   ONLINE   LEGACY_SATA:0        -                     1
1   c0t50014e157af2b  -      233.82G  hdd        no   ONLINE    LEGACY_SATA:1        rpool (active)        1
2   c0t5000c50030253e  -      186.31G  ssd        no   ONLINE    5000c50028d412b3d0 ONLINE
3   c0t5000c50094446d  -      1.09T    hdd        no   ONLINE    5000c50028d412b3d0 ONLINE
After restoring the FC link, use the following command to recover the FC paths:

CLI@nexenta> disk rescan

After the disk rescan, the FC path count should be back to four:

CLI@nexenta> disk list -o*,pathcount

Verifying Storage Enclosure Visibility

At the ATTO FibreBridge CLI, use the command SASEnclosures to verify enclosure visibility.

Ready.

SASEnclosures

<table>
<thead>
<tr>
<th>Idx Enclosure Addr</th>
<th># Devs</th>
<th>Start LUN</th>
<th># Vendor</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 500304800111283f</td>
<td>45</td>
<td>1</td>
<td>SMCI</td>
<td>SC216BE2CJBOD</td>
</tr>
<tr>
<td>1 50030480091bdaf</td>
<td>45</td>
<td>91</td>
<td>SMCI</td>
<td>SC216BE2CJBOD</td>
</tr>
<tr>
<td>2 50030480011128bf</td>
<td>45</td>
<td>136</td>
<td>SMCI</td>
<td>SC216BE2CJBOD</td>
</tr>
<tr>
<td>3 50030480091bdaf</td>
<td>45</td>
<td>46</td>
<td>SMCI</td>
<td>SC216BE2CJBOD</td>
</tr>
</tbody>
</table>

The command shows redundant SAS expanders in an enclosure separately. In this example 500304800111283f and 50030480091bdaf are the two expanders in the first storage enclosure, and 50030480091bdaf and 50030480091bdabf are the two in the second. Although these are twenty-four bay expanders, SES reports 45 bays; thus the FibreBridge allocates LUN numbers for 44 bays on each expander, plus a LUN number for the expander so that SES data can be bridged.
Troubleshooting the ATTO FibreBridges

Use the procedures in this section to check the following:

- The FibreBridge has FC connectivity
- The links to the ATTO FibreBridges are up
- The storage enclosures are visible from the FibreBridge
- All SAS targets are visible
- The SAS-to-FC mappings are correct

If necessary, you can gather diagnostic information from the FibreBridge and submit it to Nexenta Support for analysis.

Verifying Network Connectivity

Use the following FibreBridge CLI commands to check FibreBridge FC connectivity.

Ready.
```
FCPortList
4 ; Port Status ;===============
1   Up
2   Up
```

Ready.
```
get FCConnMode all
4 ; Port Conn Mode ;=================
1   ptp-loop
2   ptp-loop
```

Ready.
```
get FCDataRate all
4 ; Port Data Rate ;=================
1   auto
2   auto
```

The FCPortList command shows the ports as up or down; the FCConnMode command shows what the ports are configured to do, which may include negotiations with outcomes that aren’t displayed.

To confirm that the switch sees the bridges as connected, enter the command `switchshow output on the bridge`, which displays the WWPN and the port state. You should see online FC F-Ports for edge devices. Anything else, and it may be that the FCConnMode setting on the bridge is set to something other than ptp-loop, such that it prefers or exclusively accepts loop mode.
Confirming ATTO FibreBridge SAS Port Connectivity

Use the FibreBridge CLI command `SASPortList` to verify the SAS connections are up. There should be redundant SAS and FC connections throughout the deployment. Therefore, you should see two online SAS ports negotiated up to 6 Gb.

For example:

```
Ready.
SASPortList
10
;Connector   PHY   Link  Speed   SAS Address
;===============================================
Device A    1     Up    6Gb    500108600618fc6
Device A    2     Up    6Gb    500108600618fc6
Device A    3     Up    6Gb    500108600618fc6
Device A    4     Up    6Gb    500108600618fc6
Device B    1     Up    6Gb    500108600618fc6
Device B    2     Up    6Gb    500108600618fc6
Device B    3     Up    6Gb    500108600618fc6
Device B    4     Up    6Gb    500108600618fc6
...```

Checking SES Inventory

The FibreBridge maps devices in terms of slot population using SES data, so you need to confirm that all slots are properly reported. You can see this data for individual expanders by entering the `SASEnclosures` command on the FibreBridge with an index specified.

For example:

```
Ready.
SASEnclosures 0
47
;Slot #  Device Description
-----------------------------------------------
  1  5000c50069009205  0 SEAGATE ST800FM0043 P3G1113700000T0000000
  2  5000c50069010f15  0 SEAGATE ST800FM0043 P3G1111800000T0000000
  3  5000c50069010f1d  0 SEAGATE ST800FM0043 P3G1111700000T0000000
  4  5000c50069011ca5  0 SEAGATE ST800FM0043 P3G1134600000T0000000
  5  5000c50069010da5  0 SEAGATE ST800FM0043 P3G1301C00000T0000000
  6  5000c50069010ee5  0 SEAGATE ST800FM0043 P3G11115E00000T0000000
  7  5000c50069010f31  0 SEAGATE ST800FM0043 P3G11112800000T0000000
  8  5000c50069011bcd  0 SEAGATE ST800FM0043 P3G11126400000T0000000
  9  5000c50069011f49  0 SEAGATE ST800FM0043 P3G1112700000T0000000
 10 5000c50069011da9  0 SEAGATE ST800FM0043 P3G1300500000T0000000
 11 5000c50069010db5  0 SEAGATE ST800FM0043 P3G1300900000T0000000
 12 5000c50069010d91  0 SEAGATE ST800FM0043 P3G1303000000T0000000
 13 5000c50069010d61  0 SEAGATE ST800FM0043 P3G1301900000T0000000
 14 5000c50069003339  0 SEAGATE ST800FM0043 P3G1023300000T0000000
 15 5000c50069010f49  0 SEAGATE ST800FM0043 P3G11112700000T0000000
 16 5000c5003012e239  0 SEAGATE ST800FM0043 Z3G013BS0000Z3G013BS
 17 5000c50069012e24d  0 SEAGATE ST800FM0043 Z3G013JC0000Z3G013JC
```
In this example, the command shows output for a fully populated 24-bay SuperMicro SC216BE2CJBOD. For the enclosure, the expander is at the bottom, which does not have a slot index (slot UNK). The enclosure indicates it has 44 bays, but the FibreBridge believes its first slot is 1 rather than 0, so the device in slot 0 appears second from bottom in an unknown slot.

### Checking SAS Target Visibility

There are two separate items to look at when checking device visibility via the FibreBridge:

- Is the device in a working slot and properly reported by SES? See "Checking SES Inventory" above.
- Is the device connected to the FibreBridge via SAS?

Use the FibreBridge CLI command SASTargets to check target visibility. Since the ATTO FibreBridge does not reduce multipathed entities to a single instance, redundantly connected SAS devices appear as the same serial number twice. Note that the command does not show through which SAS port the target is visible, so if a target is not visible, you should check whether both FibreBridge ports are online and connected (see Confirming ATTO FibreBridge SAS Port Connectivity.)

Ready.

**SASTargets**

101

<table>
<thead>
<tr>
<th>Tgt VendorID ProductID</th>
<th>Type</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 TOSHIBA AL13SEB900</td>
<td>Disk</td>
<td>X2U0A01HFR6</td>
</tr>
<tr>
<td>1 TOSHIBA AL13SEB900</td>
<td>Disk</td>
<td>X2U0A01HFR6</td>
</tr>
</tbody>
</table>
Checking SAS-to-FC Mappings

Use the FibreBridge CLI command `RouteDisplay FC` to display the mappings of SAS targets to FC LUNs. In a MetroHA configuration, each SAS port is presented out of each FC port, so the host sees the devices four times but knows to present a device only once per path. On the FibreBridge side, everything is seen twice from the SAS side, which is then doubled when presented by redundant FC ports.

The following example shows a working set of mappings:

```
Ready.
RouteDisplay FC
103
; FL Device Address LUN VendorID ProductID SerialNumber
;=================================================================
  0 Controller
1  5000c50069009205 0 SEAGATE ST800FM0043 P3G111370000T0000000
2  5000c50069010f15 0 SEAGATE ST800FM0043 P3G111180000T0000000
3  5000c50069010f1d 0 SEAGATE ST800FM0043 P3G111700000T0000000
4  5000c50069011ca5 0 SEAGATE ST800FM0043 P3G113460000T0000000
5  5000c50069010dal0 0 SEAGATE ST800FM0043 P3G1301c0000T0000000
6  5000c50069010eaf 0 SEAGATE ST800FM0043 P3G111280000T0000000
7  5000c50069010ee5 0 SEAGATE ST800FM0043 P3G1115e0000T0000000
8  5000c50069010ef31 0 SEAGATE ST800FM0043 P3G110F60000T0000000
9  5000c50069011b0d0 0 SEAGATE ST800FM0043 P3G131090000T0000000
10 5000c50069010ada9 0 SEAGATE ST800FM0043 P3G130050000T0000000
11 5000c50069010d6b5 0 SEAGATE ST800FM0043 P3G130090000T0000000
12 5000c50069010d691 0 SEAGATE ST800FM0043 P3G130300000T0000000
13 5000c50069010d6d1 0 SEAGATE ST800FM0043 P3G130190000T0000000
14 5000c50069003339 0 SEAGATE ST800FM0043 P3G102330000T0000000
15 5000c50069010f49 0 SEAGATE ST800FM0043 P3G111270000T0000000
16 5000c50069010e239 0 SEAGATE ST800FM0043 Z3G013BS0000Z3G013BS
17 5000c50069010e24d 0 SEAGATE ST800FM0043 Z3G013JC0000Z3G013JC
18 5000c50069010d0ad 0 SEAGATE ST800FM0043 P3G1300C0000T0000000
19 5000c50069008a95 0 SEAGATE ST800FM0043 P3G1110B0000T0000000
20 5000c50069011b59 0 SEAGATE ST800FM0043 P3G1126F0000T0000000
```
In this example, the expander itself is mapped as LUN 45, which allows the appliance to see the JBOD device census.

The FC mappings from the `RouteDisplay FC` command show 15 SAS attachments each per FC port (that is, the same 30 target attachments, accounting for everything in the `SASTargets` output) plus two bridge mappings, which means the full SAS inventory is mapped.

### Gathering Diagnostics From ATTO FibreBridges

Nexenta Support may request diagnostics from the ATTO FibreBridges. You should retain records of the IP addresses and root passwords for the FibreBridges so that you can log in to them as directed.

- **To gather diagnostic information for an ATTO FibreBridge:**

  1. Using a Web browser, log into the FibreBridge by entering its IP address or host name and then entering root’s login credentials.
  2. Once logged in, navigate to the **Advanced** item in the list on the left-hand side, which presents the Advanced CLI configuration page.
  3. Use the **DumpConfiguration** command.

     The DumpConfiguration command generally produces more output than can be buffered by a Telnet client or the browser interface, but it also generates a file that can be retrieved via FTP.
  4. After running the DumpConfiguration command, log into the FibreBridge via FTP with the same address or name and credentials. Note that the ATTO FibreBridge only supports one concurrent login, and the previous login session may need to expire before another login can succeed.
  5. Once connected by FTP, retrieve the `dumpcfg.txt` file, which contains the diagnostic information.