CONTENTS

Chapter 1 Introduction 7
System requirements .................................................................................................................. 8
Limitations ................................................................................................................................ 8
Considerations ............................................................................................................................ 8
Cautions ....................................................................................................................................... 9
User interface choices ............................................................................................................... 9
Terminology .................................................................................................................................. 9
Related information ..................................................................................................................... 10

Chapter 2 Planned powerdown of the VNX 11
VNX VG10 and VNX VG50 planned powerdown ........................................................................ 12
VNX5200/VNX5400/VNX5600 and VNX-F5000 planned powerdown ........................................... 15
VNX5200/VNX5400/VNX5600/VNX-F5000 Block planned powerdown .................................................. 15
VNX5200/VNX5400/VNX5600 File/Unified planned powerdown .................................................... 18
VNX5800/VNX7600 and VNX-F7000 planned powerdown .............................................................. 23
VNX5800/VNX7600/VNX-F7000 Block planned powerdown ........................................................... 23
VNX5800/VNX7600 File/Unified planned powerdown ........................................................................ 26
VNX8000 planned powerdown ...................................................................................................... 30
VNX8000 Block planned powerdown ............................................................................................ 30
VNX8000 File/Unified planned powerdown ................................................................................... 33

Chapter 3 Power up the VNX 37
VNX VG10 and VNX VG50 powerup ............................................................................................. 38
VNX5200/VNX5400/VNX5600 and VNX-F5000 powerup ................................................................. 40
VNX5200/VNX5400/VNX5600/VNX-F5000 Block powerup .............................................................. 40
VNX5200/VNX5400/VNX5600 File/Unified powerup ........................................................................ 42
VNX5800/VNX7600 and VNX-F7000 powerup .................................................................................. 45
VNX5800/VNX7600/VNX-F7000 Block powerup .............................................................................. 45
VNX5800/VNX7600 for File/Unified powerup .................................................................................. 47
VNX8000 powerup ....................................................................................................................... 50
VNX8000 Block powerup .............................................................................................................. 50
VNX8000 File/Unified powerup ..................................................................................................... 52

Chapter 4 Shut down the VNX in an emergency 57
VNX series emergency shutdown ............................................................................................... 58
Power up after an emergency shutdown ..................................................................................... 58

Chapter 5 Halt and/or restart Control Stations and Data Movers 59
Halt the Control Station ................................................................................................................ 60
Halt one Control Station, locally or remotely ............................................................................. 60
Halt dual Control Station, locally or remotely ............................................................................ 60
Restart the Control Station ........................................................................................................... 61
Restart one Control Station, locally or remotely .......................................................................... 61
Restart two Control Station, locally or remotely .......................................................................... 61
Halt and/or restart Data Movers ................................................................................................... 62
Halt the Data Movers ................................................................................. 62
Restart a Data Mover .................................................................................. 63

Chapter 6  View and manage system details  65
Identify the software versions ...................................................................... 66
View Control Station software version ......................................................... 66
View Data Mover software version .............................................................. 66
Audit the VNX .............................................................................................. 66
Check the system status ................................................................................ 67
Change the Control Station hostname ......................................................... 67
Install Control Station Linux security alerts ............................................... 68
Verify the daemons ..................................................................................... 69
Back up the VNX database ........................................................................ 70
Manual VNX database backup .................................................................... 70
Query VNX for SCSI details ...................................................................... 72

Chapter 7  Manage VNX time and date settings  75
Set the date and time of the VNX ................................................................. 76
Set Control Station date and time .............................................................. 76
Set Data Mover date and time .................................................................. 76
Configure NTP service using the CLI ....................................................... 77
Set the time zone of the VNX ................................................................. 77
Change Control Station time zone manually using the CLI .................. 77
Set Data Mover time zone manually ......................................................... 78

Chapter 8  Manage networking  79
Configure IPv6 on the Control Station ...................................................... 80
Configure SNMP ....................................................................................... 80
Add DNS Server ....................................................................................... 81
Avoid private LAN IP address conflicts .................................................. 82
Configure IP aliasing ................................................................................ 82
Create an IP alias .................................................................................... 83
Delete an IP alias .................................................................................... 83
Change VNX management port IP address values .................................. 84

Chapter 9  Manage logging and alerting capabilities  85
Change the ConnectHome settings ............................................................ 86
Configure Connect Home ......................................................................... 86
Provision ESRS ......................................................................................... 88
Re-provision ESRS ................................................................................... 90
International toll-free numbers ............................................................... 90
Set the country code on the MT5634ZBA modem ................................... 92
Manual instructions for setting the country code ................................... 93
Interpret log files ..................................................................................... 95
Location of VNX logs .............................................................................. 96
Read log messages .................................................................................. 97
VNX and RSA Envision ........................................................................... 101
NAS or SAN environment rules ............................................................. 101
VNX for file problem information ........................................................... 103
Automatically collect and transfer logs .................................................... 103
Configuration file .................................................................................... 104
Enable Automatic Log Transfer from Unisphere.............................. 105
Run Log Collection from the CLI...................................................... 105
Disable Automatic Collection and Transfer tool.............................. 106
Use CLI options to perform script operations................................. 106

Chapter 10  Troubleshooting  109
EMC E-Lab Interoperability Navigator.................................................. 110
Error messages...................................................................................... 110
Error messages for Data Mover............................................................. 110
EMC Training and Professional Services................................................. 111
Recovery after an VNX SP failure......................................................... 111
Monitor system activity.......................................................................... 111
System activity output........................................................................... 112

Index  117
CHAPTER 1

Introduction

System operations are common operation tasks that include powering up or powering down a server, halting or restarting a Control Station or a Data Mover or setting the server time, date, and time zone.

This document is part of the EMC® VNX™ Series documentation set and is intended for use by system administrators responsible for performing day-to-day operations of a VNX File and for monitoring the server or resolving simple operation problems.

- System requirements .............................................................. 8
- Limitations .............................................................................. 8
- Considerations ....................................................................... 8
- Cautions ............................................................................... 9
- User interface choices .......................................................... 9
- Terminology ......................................................................... 9
- Related information ............................................................ 10
System requirements

System requirements on page 8 describes the VNX software, hardware, network, and storage configuration requirements.

Table 1 System requirements

<table>
<thead>
<tr>
<th>Software</th>
<th>EMC VNX OE for File version 8.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>VNX Series system</td>
</tr>
<tr>
<td>Network</td>
<td>No specific network requirements</td>
</tr>
<tr>
<td>Storage</td>
<td>No specific storage requirements</td>
</tr>
</tbody>
</table>

Limitations

When you change Data Mover names by using the command line interface (CLI), the new names do not appear in the EMC Unisphere™ software until you refresh the browser.

The *EMC VNX Operating Environment for File Release Notes* and *VNX Operating Environment for Block Release Notes* contain additional, late-breaking information about VNX and its OEs.

Considerations

This document covers the operation of the following servers:

Table 2 Supported VNX2 Series models and storage types

<table>
<thead>
<tr>
<th>Storage type</th>
<th>VNX model name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNX Gateway</td>
<td>• VNX VG10</td>
</tr>
<tr>
<td></td>
<td>• VNX VG50</td>
</tr>
<tr>
<td>VNX for Block, VNX for File, or VNX Unified</td>
<td>• VNX5200</td>
</tr>
<tr>
<td></td>
<td>• VNX5400</td>
</tr>
<tr>
<td></td>
<td>• VNX5600</td>
</tr>
<tr>
<td></td>
<td>• VNX5800</td>
</tr>
<tr>
<td></td>
<td>• VNX7600</td>
</tr>
<tr>
<td></td>
<td>• VNX8000</td>
</tr>
</tbody>
</table>

Table 3 Supported VNX-F Series models and storage types

<table>
<thead>
<tr>
<th>Storage type</th>
<th>VNX model name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNX-F (Block)</td>
<td>• VNX-F5000</td>
</tr>
<tr>
<td></td>
<td>• VNX-F7000</td>
</tr>
</tbody>
</table>
Cautions

⚠️ CAUTION

- To prevent data loss, never power down the VNX by simply turning off the red Emergency Power Off (EPO) switch.
- To avoid service disruption to other clients, do not turn off the two cabinet circuit breaker switches when the cabinet contains other equipment powered by these switches that either services other clients or is not part of the server.
- EMC strongly recommends that you regularly copy the VNX database backup file from the Control Station and save it to a remote location for safe keeping. Always copy the VNX database backup file when hardware or software upgrades are planned.
- Only EMC qualified support personnel should restore the VNX database by using the VNX database backup file.
- Do not manually edit the nas_db database without consulting Customer Service. Any changes you make might disrupt services.
- If you use the CLI to change the Control Station hostname and use the Unisphere software to manage the server, ensure that you follow this procedure carefully. Otherwise, file systems cannot be created using the Unisphere software.

User interface choices

The VNX offers flexibility in managing networked storage based on interface preferences and support environment. This document describes the system operations of the VNX by using the CLI. You can also perform some of these tasks by using one of the VNX management applications:

- EMC Unisphere software
- Microsoft Management Console (MMC) snap-ins
- Active Directory Users and Computers (ADUC) extensions

The following provide additional information about managing your VNX Unified/File:

- Unisphere online help
- *Installing Management Applications on VNX for File* includes instructions on launching Unisphere software, and on installing MMC snap-ins and ADUC extensions.

**Note**

Unless otherwise directed, log in as nasadmin when executing CLI commands.

Terminology

The VNX Glossary provides a complete list of VNX terminology.
Related information

Specific information related to the features and functionality described in this document is included in:

- *EMC VNX Command Line Interface Reference for File*
- *Parameters Guide for VNX for File*
- Online VNX for File man pages

EMC VNX Documentation on the EMC Online Support website:

The complete set of EMC VNX series customer publications is available on the EMC Online Support website. To search for technical documentation, go to [http://Support.EMC.com](http://Support.EMC.com). After logging in to the website, click the VNX Support by Product page to locate information for the specific feature required.

VNX wizards:

Unisphere software provides wizards for performing setup and configuration tasks. The Unisphere online help provides more details on the wizards.
CHAPTER 2

Planned powerdown of the VNX

You should perform a planned power down to remove power from the VNX in an orderly way to protect data.

**NOTICE**

Incorrectly powering down the VNX can cause data loss or service disruption.

**Note**

For instructions on powering up a DC-powered VNX, refer to the *EMC DC-Powered VNX Series Enclosures Installation and Operation Guide* (P/N: 300-012-880) for instructions.

- VNX VG10 and VNX VG50 planned powerdown
- VNX5200/VNX5400/VNX5600 and VNX-F5000 planned powerdown
- VNX5800/VNX7600 and VNX-F7000 planned powerdown
- VNX8000 planned powerdown
VNX VG10 and VNX VG50 planned powerdown

The VG10 can be configured with either one or two Data Movers and one or two Control Stations. The VG50 has either two to eight Data Movers and one or two Control Stations. These instructions cover all configurations.

Power down your VNX VG10/VG50 Gateway:

Procedure

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.

2. Log into Unisphere on the primary Control Station of the system being powered down and check the system status.
   a. From a browser, type the IP address of the primary Control Station.
   b. Log in to the Unisphere software as Root and define the scope as Local.
   c. On the Unisphere Dashboard locate the Systems by Severity quadrant.
   d. Verify that the Status fields for the VNX system to be powered down show no current Critical alerts.

3. Power down the entire VNX system from Unisphere.
   a. Select System List from the top navigation bar.

Note

At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

Note

Optionally, confirm the status of the Control Station and Data Mover components by selecting the VNX_system\System Run Command option in Unisphere under Control Station CLI on the right-hand side of the page:
/nasmcd/sbin/getreason

Expected Reason Code values for booted VNX with a single Control Station and two Data Movers:

10 - slot_0 primary control station
5 - slot_2 contacted
5 - slot_3 contacted

After confirming the system status, close the CLI Command pop-up and navigate back to the Dashboard.
If System List is not shown in the navigation bar, select All Systems in the system list drop-down menu.

b. Select the system to be powered down from the system list.

c. Click the Power Off button and follow the prompts that appear to power off the system.

Note

If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

Ensure that you read and follow the recommendations that appear in Unisphere as you power off the VNX system.

4. Your VNX should power down within five minutes.

5. If you want to power down the boot storage array for the VNX Gateway, follow the powerdown instructions in the array documentation at this time.

6. Follow the steps below to completely remove power from each Data Mover enclosure and Control Station.

   a. Confirm that each Data Mover enclosure (DME) has successfully powered down.
      
      – From the front of the DME, verify that the green CPU power LED on each Data Mover is OFF (unlit).
      
      – From the rear of the DME, verify that the green power LED on the right of the latch handle of each Data Mover I/O module is OFF.
      
      – Additionally, on the rear of a successfully powered down DME, the amber fault LED on the latch handle of each DME management module is ON.

   b. After verifying that each DME has successfully powered down, disconnect all DME power cables from the PDUs. There are two rear power cables per DME.

   c. Check the front LEDs of each Control Station.
Only the networking indication LEDs (green numbers shown in the illustration) may be lit on a successfully powered down Control Station. All other LEDs on the front of the Control Station are off.

d. After verifying the successful power down of each CS, disconnect the rear power cords on the rear of CS 0 and CS 1, if present, from the PDUs. There is one rear power cable per CS.

7. Does the VNX Gateway server cabinet contain other equipment that is connected to the cabinet PDPs and shared with other systems (such as Fibre Channel switches, storage arrays, and so forth)?
   - If yes, stop here. The VNX Gateway server is powered down.
   - If no, go to the next step.

8. Turn off (0 position) the left and right cabinet circuit-breaker switches located at the back of the cabinet near the bottom to complete the powerdown of the server.

**Note**

If the server is installed in a non-EMC cabinet, the switches are probably in a different location.
Note

To avoid service disruption to other clients, do not turn off the two cabinet circuit breaker switches when the cabinet contains other equipment powered by these switches that either services other clients or is not part of the VNX Gateway server.

VNX5200/VNX5400/VNX5600 and VNX-F5000 planned powerdown

The VNX5200/VNX5400/VNX5600 are each available in three configurations: Block, File, and Unified. Follow the instructions for your system configuration. The VNX-F5000 is available only in Block.

- VNX5200/VNX5400/VNX5600/VNX-F5000 Block planned powerdown on page 15
- VNX5200/VNX5400/VNX5600 Block planned powerdown on page 18

VNX5200/VNX5400/VNX5600/VNX-F5000 Block planned powerdown

The tasks to power down the VNX5200, VNX5400, VNX5600, and VNX-F5000 Block include stopping I/O, halting the storage processors, and powering down the system through Unisphere.

Follow the procedure below to perform a planned powerdown for your VNX5200, VNX5400, VNX5600 or VNX-F5000 Block:

Procedure

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.
At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

2. Log into Unisphere on one of the storage processors of the system being powered down and check the system status.
   a. From a browser, type the IP address of the storage processor.
   b. Log in to the Unisphere software as sysadmin and define the scope as **Global**.
   c. On the Unisphere **Dashboard** locate the **Systems by Severity** quadrant.
   d. Verify that the **Status** fields for the VNX system to be powered down show no current **Critical** alerts.

3. Power down the entire VNX system from Unisphere.
   a. Select **System List** from the top navigation bar.

   **Note**
   If **System List** is not shown in the navigation bar, select **All Systems** in the system list drop-down menu.

   b. Select the system to be powered down from the system list.
   c. Click the **Power Off** button and follow the prompts that appear to power off the system.

   **Note**
   If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

4. Your VNX should power down within five minutes.

5. Confirm SP and DPE power down and then completely remove all power from the disk processor enclosure:

   **Note**
   DO NOT remove power from a storage processor with a lit unsafe to remove LED. The unsafe to remove LED indicates the occurrence of essential system caching. Removing power from the storage processor prematurely can result in corrupted data.

   a. Ping the management IP address of each Storage Processor to verify that each SP is unresponsive and/or confirm that the state of SP and DPE LEDs.

   For VNX Operating Environment (OE) versions at or before VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

   **Table 4** DPE and SP LED state

   | DPE Fault LED | OFF |

---

**EMC VNX Series 8.1 System Operations**
Table 4 DPE and SP LED state (continued)

<table>
<thead>
<tr>
<th>SP Fault LED</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>ON (Green)</td>
</tr>
</tbody>
</table>

For VNX OE versions later than VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

Table 5 DPE and SP LED state

<table>
<thead>
<tr>
<th>SP Fault LED</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>OFF</td>
</tr>
</tbody>
</table>

b. After verifying the SP and DPE front LEDs, disconnect DPE power supply power cords. Locations shown below.

c. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, remove each BBU from the rear of the DPE by pushing the BBU’s orange release tab to the right, while grasping the handle, and pulling the BBU slightly.
d. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, with the power supply power cords disconnected, re-insert the BBUs by pushing each BBU into its slot until it clicks in place.

6. If there are additional optional DAEs and you intend to power off the entire array, disconnect the power cables from each DAE to the PDUs. This powers down the additional DAEs.

### VNX5200/VNX5400/VNX5600 File/Unified planned powerdown

The VNX5200 File/Unified can be configured with between one and three Data Movers and one or two Control Stations. The VNX5400 and VNX5600 (File/Unified) can be configured with between one and four Data Movers and one or two Control Stations.

Power down your VNX5200/VNX5400/VNX5600 system:

**Procedure**

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.

   **Note**
   At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

2. Log into Unisphere on the primary Control Station of the system being powered down and check the system status.
   a. From a browser, type the IP address of the primary Control Station.
   b. Log in to the Unisphere software as sysadmin and define the scope as **Global**.
   c. On the Unisphere **Dashboard** locate the **Systems by Severity** quadrant.
   d. Verify that the **Status** fields for the VNX system to be powered down show no current **Critical** alerts.
Note
Optionally, confirm the status of the Control Station and Data Mover components by selecting the **Run Command** option in Unisphere under **Control Station CLI** on the right-hand side of the page:

```
/nasmcd/sbin/getreason
```

Expected Reason Code values for booted VNX with a single Control Station and two Data Movers:

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>slot_0 primary control station</td>
</tr>
<tr>
<td>5</td>
<td>slot_2 contacted</td>
</tr>
<tr>
<td>5</td>
<td>slot_3 contacted</td>
</tr>
</tbody>
</table>

After confirming the system status, close the CLI Command pop-up and navigate back to the **Dashboard**.

3. Power down the entire VNX system from Unisphere

**Note**
In certain cases you may wish only to power down the File OE components (Data Movers and Control Stations), leaving the storage processors and additional DAEs powered to provide I/O to connected hosts, use the **Run Command** dialog box to issue:

```
#/nas/sbin/nas_halt now
```

Follow the prompts that appear.

After halting the Control Stations and Data Movers, follow the process in step 5 on page 19 to completely remove all power from the Control Stations and Data Movers.

- **Select System List** from the top navigation bar.

  **Note**
  If **System List** is not shown in the navigation bar, select **All Systems** in the system list drop-down menu.

- **Select** the system to be powered down from the system list.

- **Click** the **Power Off** button and follow the prompts that appear to power off the system.

  **Note**
  If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

  Ensure that you read and follow the recommendations that appear in Unisphere as you power off the VNX system.

4. Your VNX should power down within five minutes.

5. Follow the steps below to completely remove power from each Data Mover enclosure and Control Station.

- **Confirm** that each Data Mover enclosure (DME) has successfully powered down.
  - From the front of the DME, verify that the green CPU power LED on each Data Mover is OFF (unlit).
Planned powerdown of the VNX

*From the rear of the DME, verify that the green power LED on the right of the latch handle of each Data Mover I/O module is OFF.*

*Additionally, on the rear of a successfully powered down DME, the amber fault LED on the latch handle of each DME management module is ON.*

b. After verifying that each DME has successfully powered down, disconnect all DME power cables from the PDUs. There are two rear power cables per DME.

c. Check the front LEDs of each Control Station.
Only the networking indication LEDs (green numbers shown in the illustration) may be lit on a successfully powered down Control Station. All other LEDs on the front of the Control Station are off.

d. After verifying the successful power down of each CS, disconnect the rear power cords on the rear of CS 0 and CS 1, if present, from the PDUs. There is one rear power cable per CS.

6. Confirm SP and DPE power down and then completely remove all power from the disk processor enclosure:

Note

DO NOT remove power from a storage processor with a lit unsafe to remove LED. The unsafe to remove LED indicates the occurrence of essential system caching. Removing power from the storage processor prematurely can result in corrupted data.

a. Ping the management IP address of each Storage Processor to verify that each SP is unresponsive and/or confirm that the state of SP and DPE LEDs.

For VNX Operating Environment (OE) versions at or before VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

Table 6 DPE and SP LED state

<table>
<thead>
<tr>
<th>DPE Fault LED</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>ON (Green)</td>
</tr>
</tbody>
</table>

For VNX OE versions later than VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

Table 7 DPE and SP LED state

<table>
<thead>
<tr>
<th>SP Fault LED</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>OFF</td>
</tr>
</tbody>
</table>
b. After verifying the SP and DPE front LEDs, disconnect DPE power supply power cords. Locations shown below.

c. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, remove each BBU from the rear of the DPE by pushing the BBU's orange release tab to the right, while grasping the handle, and pulling the BBU slightly.

d. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, with the power supply power cords disconnected, re-insert the BBUs by pushing each BBU into its slot until it clicks in place.

7. If there are additional optional DAEs and you intend to power off the entire array, disconnect the power cables from each DAE to the PDUs. This powers down the additional DAEs.
VNX5800/VNX7600 and VNX-F7000 planned powerdown

The VNX5800 and VNX7600 are each available in three configurations: Block, File, and Unified. Follow the instructions for your system configuration. The VNX-F7000 is available only in Block.

- VNX5800/VNX7600/VNX-F7000 Block planned powerdown on page 23
- VNX5800/VNX7600 File/Unified planned powerdown on page 26

VNX5800/VNX7600/VNX-F7000 Block planned powerdown

The tasks to power down the VNX5800, VNX7600, and VNX-F7000 Block include stopping I/O, halting the storage processors, and powering down the system through Unisphere.

Follow the procedure below to perform a planned powerdown for your VNX5800, VNX7600, or VNX-F7000 Block:

**Procedure**

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.

   **Note**

   At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

2. Log into Unisphere on one of the storage processors of the system being powered down and check the system status.
   a. From a browser, type the IP address of the storage processor.
   b. Log in to the Unisphere software as sysadmin and define the scope as **Global**.
   c. On the Unisphere **Dashboard** locate the **Systems by Severity** quadrant.
   d. Verify that the **Status** fields for the VNX system to be powered down show no current **Critical** alerts.

3. Power down the entire VNX system from Unisphere.
   a. Select **System List** from the top navigation bar.

   **Note**

   If **System List** is not shown in the navigation bar, select **All Systems** in the system list drop-down menu.

   b. Select the system to be powered down from the system list.
   c. Click the **Power Off** button and follow the prompts that appear to power off the system.
If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

Ensure that you read and follow the recommendations that appear in Unisphere as you power off the VNX system.

4. Your VNX should power down within five minutes.

5. Confirm SP and DPE power down and then completely remove all power from the disk processor enclosure:

Note

DO NOT remove power from a storage processor with a lit unsafe to remove LED. The unsafe to remove LED indicates the occurrence of essential system caching. Removing power from the storage processor prematurely can result in corrupted data.

a. Ping the management IP address of each Storage Processor to verify that each SP is unresponsive and/or confirm that the state of SP and DPE LEDs.

For VNX Operating Environment (OE) versions at or before VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

Table 8 DPE and SP LED state

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DPE Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>ON (Green)</td>
</tr>
</tbody>
</table>

For VNX OE versions later than VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

Table 9 DPE and SP LED state

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SP Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>OFF</td>
</tr>
</tbody>
</table>
b. After verifying the SP and DPE front LEDs, disconnect DPE power supply power cords. Locations shown below.

c. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, remove each BBU from the rear of the DPE by pushing the BBU's orange release tab to the right, while grasping the handle, and pulling the BBU slightly.

d. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, with the power supply power cords disconnected, re-insert the BBUs by pushing each BBU into its slot until it clicks in place.

6. If there are additional optional DAEs and you intend to power off the entire array, disconnect the power cables from each DAE to the PDUs. This powers down the additional DAEs.
VNX5800/VNX7600 File/Unified planned powerdown

The VNX5800 for File and VNX5800 Unified can be configured with up to four Data Movers and one or two Control Stations. The VNX7600 for File and VNX7600 Unified can be configured with between two to six Data Movers and one or two Control Stations.

Power down your VNX5800/VNX7600 system:

Procedure

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.

   **Note**
   At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

2. Log into Unisphere on the primary Control Station of the system being powered down and check the system status.
   a. From a browser, type the IP address of the primary Control Station.
   b. Log in to the Unisphere software as sysadmin and define the scope as Global.
   c. On the Unisphere Dashboard locate the Systems by Severity quadrant.
   d. Verify that the Status fields for the VNX system to be powered down show no current Critical alerts.

   **Note**
   Optionally, confirm the status of the Control Station and Data Mover components by selecting the <<VNX_system>>System Run Command option in Unisphere under Control Station CLI on the right-hand side of the page:
   /nasmcd/sbin/getreason

   Expected Reason Code values for booted VNX with a single Control Station and two Data Movers:

   10 - slot_0 primary control station
   5 - slot_2 contacted
   5 - slot_3 contacted

   After confirming the system status, close the CLI Command pop-up and navigate back to the Dashboard.

3. Power down the entire VNX system from Unisphere
In certain cases you may wish only to power down the File OE components (Data Movers and Control Stations), leaving the storage processors and additional DAEs powered to provide I/O to connected hosts, use the Run Command dialog box to issue:

```
#/nas/sbin/nas_halt now
```

Follow the prompts that appear.

After halting the Control Stations and Data Movers, follow the process in step 5 on page 27 to completely remove all power from the Control Stations and Data Movers.

a. Select System List from the top navigation bar.

**Note**
If System List is not shown in the navigation bar, select All Systems in the system list drop-down menu.

b. Select the system to be powered down from the system list.

c. Click the Power Off button and follow the prompts that appear to power off the system.

**Note**
If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

Ensure that you read and follow the recommendations that appear in Unisphere as you power off the VNX system.

4. Your VNX should power down within five minutes.

5. Follow the steps below to completely remove power from each Data Mover enclosure and Control Station.

a. Confirm that each Data Mover enclosure (DME) has successfully powered down.

- From the front of the DME, verify that the green CPU power LED on each Data Mover is OFF (unlit).

- From the rear of the DME, verify that the green power LED on the right of the latch handle of each Data Mover I/O module is OFF.
Additionally, on the rear of a successfully powered down DME, the amber fault LED on the latch handle of each DME management module is ON.

b. After verifying that each DME has successfully powered down, disconnect all DME power cables from the PDUs. There are two rear power cables per DME.

c. Check the front LEDs of each Control Station.

d. After verifying the successful power down of each CS, disconnect the rear power cords on the rear of CS 0 and CS 1, if present, from the PDUs. There is one rear power cable per CS.

6. Confirm SP and DPE power down and then completely remove all power from the disk processor enclosure:
**Note**

DO NOT remove power from a storage processor with a lit unsafe to remove LED. The unsafe to remove LED indicates the occurrence of essential system caching. Removing power from the storage processor prematurely can result in corrupted data.

a. Ping the management IP address of each Storage Processor to verify that each SP is unresponsive and/or confirm that the state of SP and DPE LEDs.

For VNX Operating Environment (OE) versions at or before VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

**Table 10** DPE and SP LED state

<table>
<thead>
<tr>
<th>LED Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPE Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>ON (Green)</td>
</tr>
</tbody>
</table>

For VNX OE versions later than VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

**Table 11** DPE and SP LED state

<table>
<thead>
<tr>
<th>LED Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>(Unsafe to remove) LED</td>
<td>OFF</td>
</tr>
<tr>
<td>SP Power LED</td>
<td>OFF</td>
</tr>
</tbody>
</table>

b. After verifying the SP and DPE front LEDs, disconnect DPE power supply power cords. Locations shown below.
c. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, remove each BBU from the rear of the DPE by pushing the BBU’s orange release tab to the right, while grasping the handle, and pulling the BBU slightly.

d. If the VNX OE is VNX Operating Environment for Block 05.33.000.5.51/VNX Operating Environment for File 8.1.2.51 and earlier, with the power supply power cords disconnected, re-insert the BBUs by pushing each BBU into its slot until it clicks in place.

7. If there are additional optional DAEs and you intend to power off the entire array, disconnect the power cables from each DAE to the PDUs. This powers down the additional DAEs.

VNX8000 planned powerdown

The VNX8000 is available in three configurations: Block, File, and Unified. Follow the instructions for your system configuration.

- VNX8000 Block planned powerdown on page 30
- VNX8000 File/Unified planned powerdown on page 33

VNX8000 Block planned powerdown

The tasks to power down the VNX8000 Block include stopping I/O, halting the storage processors, and powering down the system through Unisphere.

Follow the procedure below to perform a planned powerdown for your VNX8000 Block:

Procedure

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.
At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

2. Log into Unisphere on one of the storage processors of the system being powered down and check the system status.
   a. From a browser, type the IP address of the storage processor.
   b. Log in to the Unisphere software as sysadmin and define the scope as Global.
   c. On the Unisphere Dashboard locate the Systems by Severity quadrant.
   d. Verify that the Status fields for the VNX system to be powered down show no current Critical alerts.

3. Power down the entire VNX system from Unisphere.
   a. Select System List from the top navigation bar.

   **Note**
   
   If System List is not shown in the navigation bar, select All Systems in the system list drop-down menu.

   b. Select the system to be powered down from the system list.
   c. Click the Power Off button and follow the prompts that appear to power off the system.

   **Note**
   
   If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

   Ensure that you read and follow the recommendations that appear in Unisphere as you power off the VNX system.

4. Your VNX should power down within five minutes.

5. Confirm SP and SPE power down and then completely remove all power from the storage processor enclosure using the SPS power switches.

**WARNING**

DO NOT remove power from a storage processor with a lit unsafe to remove LED. The unsafe to remove LED indicates the occurrence of essential system caching. Removing power from the storage processor prematurely can result in corrupted data.

   a. Ping the management IP address of each Storage Processor to verify that each SP is unresponsive and/or confirm that the state of SP and SPE LEDs.

For VNX Operating Environment (OE) versions at or before VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51
Table 12 SPE and SP LED state

<table>
<thead>
<tr>
<th>LED Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPE Fault LED</td>
<td>ON (Amber)</td>
</tr>
<tr>
<td>CPU Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>Unsafe to remove LED</td>
<td>OFF</td>
</tr>
<tr>
<td>CPU Power LED</td>
<td>ON (Blue)</td>
</tr>
</tbody>
</table>

For VNX OE versions later than VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

Table 13 SPE and SP LED state

<table>
<thead>
<tr>
<th>LED Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPE Fault LED</td>
<td>ON (Amber)</td>
</tr>
<tr>
<td>CPU Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>Unsafe to remove LED</td>
<td>OFF</td>
</tr>
<tr>
<td>CPU Power LED</td>
<td>OFF</td>
</tr>
</tbody>
</table>

b. After verifying the successful power down of the SPE and storage processors, turn OFF (0 position) all four rear SPS power switches, both on the SPE SPS and Bus 0 Enclosure 0 SPS.

6. If there are additional optional DAEs and you intend to power off the entire array, disconnect the power cables from each DAE to the PDUs. This powers down the additional DAEs.
VNX8000 File/Unified planned powerdown

The VNX8000 for File and VNX8000 Unified can be configured with between two to eight Data Movers and one or two Control Stations.

Perform a planned powerdown for your VNX8000 File/Unified:

Procedure

1. When possible, before you power down the system:
   a. Notify all users of the planned powerdown several days in advance when possible.
   b. Prevent all logins and notify all users several minutes in advance of the impending powerdown.
   c. Log out all users.

   **Note**

   At times in this procedure you will be directed to view status (power and/or fault) LEDs on certain system components. For an unobstructed view of a component’s status LEDs, be prepared to remove its protective front bezel. After completing the powering down the VNX, reattach any removed front bezels.

2. Log into Unisphere on the primary Control Station of the system being powered down and check the system status.
   a. From a browser, type the IP address of the primary Control Station.
   b. Log in to the Unisphere software as sysadmin and define the scope as Global.
   c. On the Unisphere **Dashboard** locate the **Systems by Severity** quadrant.
   d. Verify that the **Status** fields for the VNX system to be powered down show no current **Critical** alerts.

   **Note**

   Optionally, confirm the status of the Control Station and Data Mover components by selecting the **<VNX_system>** **System** → **Run Command** option in Unisphere under **Control Station CLI** on the right-hand side of the page:

   `/nasmcd/sbin/getreason`

   Expected Reason Code values for booted VNX with a single Control Station and two Data Movers:

   - 10 - slot_0 primary control station
   - 5 - slot_2 contacted
   - 5 - slot_3 contacted

   After confirming the system status, close the CLI Command pop-up and navigate back to the **Dashboard**.

3. Power down the entire VNX system from Unisphere
Planned powerdown of the VNX

**Note**

In certain cases you may wish only to power down the File OE components (Data Movers and Control Stations), leaving the storage processors and additional DAEs powered to provide I/O to connected hosts, use the Run Command dialog box to issue:

```bash
#/nas/sbin/nas_halt now
```

Follow the prompts that appear.

After halting the Control Stations and Data Movers, follow the process in step 5 on page 34 to completely remove all power from the Control Stations and Data Movers.

a. Select **System List** from the top navigation bar.

**Note**

If **System List** is not shown in the navigation bar, select **All Systems** in the system list drop-down menu.

b. Select the system to be powered down from the system list.

c. Click the **Power Off** button and follow the prompts that appear to power off the system.

**Note**

If you experience any issues or uncertainties during this planned powerdown activity, contact your authorized support provider. Do NOT remove external power from the VNX until you resolve the situation.

Ensure that you read and follow the recommendations that appear in Unisphere as you power off the VNX system.

4. Your VNX should power down within five minutes.

5. Follow the steps below to completely remove power from each Data Mover enclosure and Control Station.

a. Confirm that each Data Mover enclosure (DME) has successfully powered down.

   – From the front of the DME, verify that the green CPU power LED on each Data Mover is OFF (unlit).

   – From the rear of the DME, verify that the green power LED on the right of the latch handle of each Data Mover I/O module is OFF.
Additionally, on the rear of a successfully powered down DME, the amber fault LED on the latch handle of each DME management module is ON.

b. After verifying that each DME has successfully powered down, disconnect all DME power cables from the PDUs. There are two rear power cables per DME.

c. Check the front LEDs of each Control Station.

Only the networking indication LEDs (green numbers shown in the illustration) may be lit on a successfully powered down Control Station. All other LEDs on the front of the Control Station are off.

d. After verifying the successful power down of each CS, disconnect the rear power cords on the rear of CS 0 and CS 1, if present, from the PDUs. There is one rear power cable per CS.

6. Confirm SP and SPE power down and then completely remove all power from the storage processor enclosure using the SPS power switches.

**WARNING**

DO NOT remove power from a storage processor with a lit unsafe to remove LED. The unsafe to remove LED indicates the occurrence of essential system caching. Removing power from the storage processor prematurely can result in corrupted data.
a. Ping the management IP address of each Storage Processor to verify that each SP is unresponsive and/or confirm that the state of SP and SPE LEDs.

For VNX Operating Environment (OE) versions at or before VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

**Table 14** SPE and SP LED state

<table>
<thead>
<tr>
<th>LED Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPE Fault LED</td>
<td>ON (Amber)</td>
</tr>
<tr>
<td>CPU Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>Unsafe to remove LED</td>
<td>OFF</td>
</tr>
<tr>
<td>CPU Power LED</td>
<td>ON (Blue)</td>
</tr>
</tbody>
</table>

For VNX OE versions later than VNX OE for Block 05.33.000.5.51/VNX OE for File 8.1.2.51

**Table 15** SPE and SP LED state

<table>
<thead>
<tr>
<th>LED Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPE Fault LED</td>
<td>ON (Amber)</td>
</tr>
<tr>
<td>CPU Fault LED</td>
<td>OFF</td>
</tr>
<tr>
<td>Unsafe to remove LED</td>
<td>OFF</td>
</tr>
<tr>
<td>CPU Power LED</td>
<td>OFF</td>
</tr>
</tbody>
</table>

b. After verifying the successful power down of the SPE and storage processors, turn OFF (0 position) all four rear SPS power switches, both on the SPE SPS and Bus 0 Enclosure 0 SPS.

7. If there are additional optional DAEs and you intend to power off the entire array, disconnect the power cables from each DAE to the PDUs. This powers down the additional DAEs.
CHAPTER 3

Power up the VNX

Follow the appropriate task below to power up the VNX after a planned power down or after an emergency shutdown:

Note

For instructions on powering up a DC-powered VNX, refer to the *EMC DC-Powered VNX Series Enclosures Installation and Operation Guide* (P/N: 300-012-880) for instructions.

- VNX VG10 and VNX VG50 powerup ................................................................. 38
- VNX5200/VNX5400/VNX5600 and VNX-F5000 powerup .............................. 40
- VNX5800/VNX7600 and VNX-F7000 powerup ................................................. 45
- VNX8000 powerup ....................................................................................... 50
VNX VG10 and VNX VG50 powerup

The VG10 can be configured with either one or two Data Movers and one or two Control Stations. The VG50 has either two to eight Data Movers and one or two Control Stations. These instructions cover all configurations.

Before you begin

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

Note

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

Power up your VNX VG10/VNX VG50 Gateway:

Procedure

1. If the powered down VNX Gateway is in a cabinet by itself (that is, the storage array is not in the same cabinet), then turn off the cabinet circuit-breakers to remove all power from the cabinet.
2. Ensure that the power cables for the Data Mover enclosures (two cables per enclosure) and Control Stations (one cable per CS) are not connected to the PDUs. You will connect these power cables later.
3. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.
4. Turn ON (I position) the left and right cabinet circuit-breaker switches at the back of the cabinet near the bottom.
   If the server is installed in a cabinet not manufactured by EMC, the circuit-breaker switches might be in a different location.
5. If the boot storage array is off, power it up. Follow the instructions in the array documentation.
6. Power on the Data Mover enclosure and boot the VNX OE for File by connecting all Data Mover enclosure power cables to the PDUs in a manner ensuring high availability and wait for the Data Movers to power up.
   The blue power LED on the front of the Data Mover enclosure will light when the Data Movers have powered up, and each Data Mover will display a steady green power LED.
7. Wait 4-5 minutes as the Data Movers power up to ensure that the Data Movers have booted and that they are ready. Then, connect the power cable for the Control Station 0 to the PDU.

**Note**

Do not plug in the power cable for CS 1, if present, at this time. CS 1 will be booted later in this process.

8. Check the CS power LED (labeled in the following figure) on the front of the Control Station verify that the CS is booting. This green LED will blink as the CS boots and be on when complete.

**Note**

The front bezel must be removed to for a clear view of the CS LEDs and to access the power button of the Control Station.

**Note**

If, after 5 minutes, this LED indicates that the Control Station is off, turn on the Control Station by pressing the front reset button.
Ensure that the Control Station is powered up before continuing.

9. Check the system and hardware status as follows:
   a. From a browser, type the IP address of the primary Control Station.
   b. Log in to the Unisphere software.
   c. Use the drop-down list at the top-left **Dashboard** to select the system name and view its **System Information**.
   d. On this page, verify that the **Status** fields for the VNX display OK.
   e. Next, locate the **Run Command** option in Unisphere under **Control Station CLI** on the right-hand side of the **System** page and verify that CS 0 and the Data Movers booted successfully by running a Control Station CLI command:

   ```
   /nasmcd/sbin/getreason
   ```

   **Expected Reason Code values for booted VNX for File components:**

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>slot_0 primary control station</td>
</tr>
<tr>
<td>5</td>
<td>slot_2 contacted</td>
</tr>
<tr>
<td>5</td>
<td>slot_3 contacted</td>
</tr>
</tbody>
</table>

10. For dual Control Station systems only, once you have confirmed that CS 0 is up and healthy, power up CS 1 by connecting the power cable for the CS 1 to a PDU on a different circuit from CS 0 to ensure high availability.

11. After completing the power up of the system, return to the **Run Command** option in Unisphere and perform a system checkup:

   ```
   nas_checkup
   ```

   Fix issues discovered by the `nas_checkup` command in the manner indicated in its output.

**VNX5200/VNX5400/VNX5600 and VNX-F5000 powerup**

The VNX5200/VNX5400/VNX5600 are each available in three configurations: Block, File, and Unified. Follow the instructions for your system configuration. The VNX-F5000 is available only in Block.

- [VNX5200/VNX5400/VNX5600/VNX-F5000 Block powerup on page 40](#)
- [VNX5200/VNX5400/VNX5600 File/Unified powerup on page 42](#)

**VNX5200/VNX5400/VNX5600/VNX-F5000 Block powerup**

**Before you begin**

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

**Note**

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

Power up your VNX5200, VNX5400, VNX5600, or VNX-F5000 for Block:
Procedure

1. Verify that the master switch/circuit breakers for each cabinet power strip are ON.

2. Verify that the power cable for each DPE power supply (PS A and PS B) is not connected to the cabinet power strips.

3. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.

4. Power on the disk processor enclosure (DPE) and boot the VNX OE for Block by connecting the power supply power cords for PS A and PS B to the cabinet power strips in a manner ensuring high availability and the ensure the power cable retention bails are in place.

5. Wait 10 minutes for the storage processors to boot. Use the front LEDs to verify the boot status of the DPE.

   When booted, the
   - power LED on each SP will be lit steady green
   - enclosure power LED will be lit steady blue

   The storage system can take 10-12 minutes to complete a typical power up. Fault LEDs flash amber during BIOS and the power on self-test (POST), flash blue as the operating system boots, then turn off. The front fault LED and other storage array LEDs commonly stay on for several minutes while the system batteries are charging.
VNX5200/VNX5400/VNX5600 File/Unified powerup

The VNX5200 File/Unified can be configured with between one and three Data Movers and one or two Control Stations. The VNX5400 and VNX5600 (File/Unified) can be configured with between one and four Data Movers and one or two Control Stations.

Before you begin

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

Note

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

Power up your VNX5200/VNX5400/VNX5600 File/Unified:

Procedure

1. Verify that the master switch/circuit breakers for each cabinet power strip are ON.
2. Ensure that the power cables for the Data Mover enclosures (two cables per enclosure) and Control Stations (one cable per CS) are not connected to the PDUs. You will connect these power cables later.
3. Verify that the power cable for each DPE power supply (PS A and PS B) is not connected to the cabinet power strips.
4. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.
5. Power on the disk processor enclosure (DPE) and boot the VNX OE for Block by connecting the power supply power cords for PS A and PS B to the cabinet power strips in a manner ensuring high availability and the ensure the power cable retention bails are in place.
6. Wait 10 minutes for the storage processors to boot. Use the front LEDs to verify the boot status of the DPE.

When booted, the
- power LED on each SP will be lit steady green
- enclosure power LED will be lit steady blue

The storage system can take 10-12 minutes to complete a typical power up. Fault LEDs flash amber during BIOS and the power on self-test (POST), flash blue as the operating system boots, then turn off. The front fault LED and other storage array LEDs commonly stay on for several minutes while the system batteries are charging.

**Note**

If amber LEDs on the front or back of the storage system remain on for more than 10 minutes, ensure that the system is correctly cabled, and then refer to the Troubleshooting Trees on the EMC Support page for the storage system. If you cannot determine any reasons for the fault, contact your authorized service provider.

7. Power on the Data Mover enclosure and boot the VNX OE for File by connecting all Data Mover enclosure power cables to the PDUs in a manner ensuring high availability and wait for the Data Movers to power up.

The blue power LED on the front of the Data Mover enclosure will light when the Data Movers have powered up, and each Data Mover will display a steady green power LED.

8. Wait 4-5 minutes as the Data Movers power up to ensure that the Data Movers have booted and that they are ready. Then, connect the power cable for the Control Station 0 to the PDU.
9. Check the CS power LED (labeled in the following figure) on the front of the Control Station verify that the CS is booting. This green LED will blink as the CS boots and be on when complete.

Note
The front bezel must be removed to for a clear view of the CS LEDs and to access the power button of the Control Station.

Note
Do not plug in the power cable for CS 1, if present, at this time. CS 1 will be booted later in this process.

Note
If, after 5 minutes, this LED indicates that the Control Station is off, turn on the Control Station by pressing the front reset button.

Ensure that the Control Station is powered up before continuing.

10. Check the system and hardware status as follows:
a. From a browser, type the IP address of the primary Control Station.
b. Log in to the Unisphere software.
c. Use the drop-down list at the top-left Dashboard to select the system name and view its System Information.
d. On this page, verify that the Status fields for the VNX display OK.
e. Next, locate the Run Command option in Unisphere under Control Station CLI on the right-hand side of the System page and verify that CS 0 and the Data Movers booted successfully by running a Control Station CLI command:

```
/nasmcd/sbin/getreason
```

Expected Reason Code values for booted VNX for File components:

- 10 - slot_0 primary control station
- 5 - slot_2 contacted
- 5 - slot_3 contacted

11. For dual Control Station systems only, once you have confirmed that CS 0 is up and healthy, power up CS 1 by connecting the power cable for the CS 1 to a PDU on a different circuit from CS 0 to ensure high availability.

12. After completing the power up of the system, return to the Run Command option in Unisphere and perform a system checkup:

```
nas_checkup
```

Fix issues discovered by the nas_checkup command in the manner indicated in its output.

VNX5800/VNX7600 and VNX-F7000 powerup

The VNX5800 and VNX7600 are each available in three configurations: Block, File, and Unified. Follow the instructions for your system configuration. The VNX-F7000 is available only in Block.

- VNX5800/VNX7600/VNX-F7000 Block powerup on page 45
- VNX5800/VNX7600 for File/Unified powerup on page 47

VNX5800/VNX7600/VNX-F7000 Block powerup

Before you begin

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

**Note**

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

Power up your VNX5800, VNX7600, or VNX-F7000 for Block:

**Procedure**

1. Verify that the master switch/circuit breakers for each cabinet power strip are ON.
2. Verify that the power cable for each DPE power supply (PS A and PS B) is not connected to the cabinet power strips.
3. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.

4. Power on the disk processor enclosure (DPE) and boot the VNX OE for Block by connecting the power supply power cords for PS A and PS B to the cabinet power strips in a manner ensuring high availability and the ensure the power cable retention bails are in place.

5. Wait 10 minutes for the storage processors to boot. Use the front LEDs to verify the boot status of the DPE.

When booted, the
- power LED on each SP will be lit steady green
- enclosure power LED will be lit steady blue

The storage system can take 10-12 minutes to complete a typical power up. Fault LEDs flash amber during BIOS and the power on self-test (POST), flash blue as the operating system boots, then turn off. The front fault LED and other storage array LEDs commonly stay on for several minutes while the system batteries are charging.

**Note**

If amber LEDs on the front or back of the storage system remain on for more than 10 minutes, ensure that the system is correctly cabled, and then refer to the Troubleshooting Trees on the EMC Support page for the storage system. If you cannot determine any reasons for the fault, contact your authorized service provider.
VNX5800/VNX7600 for File/Unified powerup

The VNX5800 for File and VNX5800 Unified can be configured with up to four Data Movers and one or two Control Stations. The VNX7600 for File and VNX7600 Unified can be configured with between two to six Data Movers and one or two Control Stations.

**Before you begin**

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

---

**Note**

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

---

Power up your VNX5800/VNX7600 File/Unified:

**Procedure**

1. Verify that the master switch/circuit breakers for each cabinet power strip are ON.

2. Ensure that the power cables for the Data Mover enclosures (two cables per enclosure) and Control Stations (one cable per CS) are not connected to the PDUs. You will connect these power cables later.

3. Verify that the power cable for each DPE power supply (PS A and PS B) is not connected to the cabinet power strips.

4. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.

5. Power on the disk processor enclosure (DPE) and boot the VNX OE for Block by connecting the power supply power cords for PS A and PS B to the cabinet power strips in a manner ensuring high availability and the ensure the power cable retention bails are in place.

6. Wait 10 minutes for the storage processors to boot. Use the front LEDs to verify the boot status of the DPE.

   When booted, the

   - power LED on each SP will be lit steady green
   - enclosure power LED will be lit steady blue
The storage system can take 10-12 minutes to complete a typical power up. Fault LEDs flash amber during BIOS and the power on self-test (POST), flash blue as the operating system boots, then turn off. The front fault LED and other storage array LEDs commonly stay on for several minutes while the system batteries are charging.

**Note**

If amber LEDs on the front or back of the storage system remain on for more than 10 minutes, ensure that the system is correctly cabled, and then refer to the Troubleshooting Trees on the EMC Support page for the storage system. If you cannot determine any reasons for the fault, contact your authorized service provider.

7. Power on the Data Mover enclosure and boot the VNX OE for File by connecting all Data Mover enclosure power cables to the PDUs in a manner ensuring high availability and wait for the Data Movers to power up.

   The blue power LED on the front of the Data Mover enclosure will light when the Data Movers have powered up, and each Data Mover will display a steady green power LED.

8. Wait 4-5 minutes as the Data Movers power up to ensure that the Data Movers have booted and that they are ready. Then, connect the power cable for the Control Station 0 to the PDU.
Note

Do not plug in the power cable for CS 1, if present, at this time. CS 1 will be booted later in this process.

9. Check the CS power LED (labeled in the following figure) on the front of the Control Station verify that the CS is booting. This green LED will blink as the CS boots and be on when complete.

Note

The front bezel must be removed to for a clear view of the CS LEDs and to access the power button of the Control Station.

Note

If, after 5 minutes, this LED indicates that the Control Station is off, turn on the Control Station by pressing the front reset button.

Ensure that the Control Station is powered up before continuing.

10. Check the system and hardware status as follows:
a. From a browser, type the IP address of the primary Control Station.
b. Log in to the Unisphere software.
c. Use the drop-down list at the top-left Dashboard to select the system name and view its System Information.
d. On this page, verify that the Status fields for the VNX display OK.
e. Next, locate the Run Command option in Unisphere under Control Station CLI on the right-hand side of the System page and verify that CS 0 and the Data Movers booted successfully by running a Control Station CLI command:

```
/nasmcd/sbin/getreason
```

Expected Reason Code values for booted VNX for File components:

<table>
<thead>
<tr>
<th>Reason Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>slot_0 primary control station</td>
</tr>
<tr>
<td>5</td>
<td>slot_2 contacted</td>
</tr>
<tr>
<td>5</td>
<td>slot_3 contacted</td>
</tr>
</tbody>
</table>

11. For dual Control Station systems only, once you have confirmed that CS 0 is up and healthy, power up CS 1 by connecting the power cable for the CS 1 to a PDU on a different circuit from CS 0 to ensure high availability.

12. After completing the power up of the system, return to the Run Command option in Unisphere and perform a system checkup:

```
nas_checkup
```

Fix issues discovered by the nas_checkup command in the manner indicated in its output.

---

### VNX8000 powerup

The VNX8000 is available in three configurations: Block, File, and Unified. Follow the instructions for your system configuration.

- VNX8000 Block powerup on page 50
- VNX8000 File/Unified powerup on page 52

### VNX8000 Block powerup

#### Before you begin

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

---

**Note**

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

---

Power up your VNX8000 for Block:

#### Procedure

1. Verify that the master switch/circuit breakers for each cabinet power strip are ON.
2. Verify that the all SPS power switches on the SPE SPS unit and DAE SPS unit are in the OFF position.
3. Verify that the power cables for the SPE SPS unit and DAE SPS unit are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and that the power cable retention bails are in place.

4. Verify that the four SPE power cables are plugged into the SPS unit dedicated to the storage processors and that the power cable retention bails are in place.
   a. SP A to SPS A
   b. SP A to SPS B
   c. SP B to SPS A
   d. SP B to SPS B

5. At the front of the enclosure, ensure that the four SPE power supply power cables are connected and the retention clips are in place.

6. Verify that the power cables for vault DAE are plugged into the SPS unit dedicated to the first DAE and that the power cable retention bails are in place.
   a. DAE PS A to SPS A
   b. DAE PS B to SPS B

7. Verify that the following sense cable connections are in place:
   a. Serial sense cable connections between SPE and SPE SPS:
      – SP A to SPE SPS A
      – SP B to SPE SPS B
   b. RJ12 sense cable connections between DAE 0 and DAE 0 SPS:
      – DAE LCC A to DAE SPS A
      – DAE LCC B to DAE SPS B

8. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.

9. Toggle all four SPS power switches to the | (ON) position.

10. Wait 10 minutes for the storage processors boot and the power LED on each SP to be lit blue and unblinking.
The storage system can take 10-12 minutes to complete a typical power up. Fault LEDs flash amber during BIOS and the power on self-test (POST), flash blue as the operating system boots, then turn off. The front fault LED and other storage array LEDs commonly stay on for several minutes while the system batteries are charging.

**Note**

If amber LEDs on the front or back of the storage system remain on for more than 10 minutes, ensure that the system is correctly cabled, and then refer to the Troubleshooting Trees on the EMC Support page for the storage system. If you cannot determine any reasons for the fault, contact your authorized service provider.

**VNX8000 File/Unified powerup**

The VNX8000 for File and VNX8000 Unified can be configured with between two to eight Data Movers and one or two Control Stations.

**Before you begin**

Ensure the powered down VNX storage system and component power cabling are in the state described in the planned power down procedure for your VNX model.

**Note**

If you performed an emergency power down of your VNX system, review the planned power down procedure and ensure that you prepare the VNX for power up by disconnecting the necessary VNX components from rack power, as described in the planned power down procedure for your VNX model, before beginning this power up procedure.

**Power up your VNX8000 File/Unified:**

**Procedure**

1. Verify that the master switch/circuit breakers for each cabinet power strip are ON.
2. Ensure that the power cables for the Data Mover enclosures (two cables per enclosure) and Control Stations (one cable per CS) are not connected to the PDUs. You will connect these power cables later.
3. Verify that the all SPS power switches on the SPE SPS unit and DAE SPS unit are in the OFF position.
4. Verify that the power cables for the SPE SPS unit and DAE SPS unit are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and that the power cable retention bails are in place.
5. Verify that the four SPE power cables are plugged into the SPS unit dedicated to the storage processors and that the power cable retention bails are in place.
   a. SP A to SPS A
   b. SP A to SPS B
   c. SP B to SPS A
   d. SP B to SPS B
6. At the front of the enclosure, ensure that the four SPE power supply power cables are connected and the retention clips are in place.
7. Verify that the power cables for vault DAE are plugged into the SPS unit dedicated to the first DAE and that the power cable retention bails are in place.
8. Verify that the following sense cable connections are in place:
   a. Serial sense cable connections between SPE and SPE SPS:
      - SP A to SPE SPS A
      - SP B to SPE SPS B
   b. RJ12 sense cable connections between DAE 0 and DAE 0 SPS:
      - DAE LCC A to DAE SPS A
      - DAE LCC B to DAE SPS B

9. Verify that the power cables for any additional DAEs are plugged into the appropriate cabinet power strips on either side of the rack in a manner ensuring high availability and the power cable retention bails are in place.

10. Toggle all four SPS power switches to the | (ON) position.

11. Wait 10 minutes for the storage processors boot and the power LED on each SP to be lit blue and unblinking.

The storage system can take 10-12 minutes to complete a typical power up. Fault LEDs flash amber during BIOS and the power on self-test (POST), flash blue as the operating system boots, then turn off. The front fault LED and other storage array LEDs commonly stay on for several minutes while the system batteries are charging.

**Note**

If amber LEDs on the front or back of the storage system remain on for more than 10 minutes, ensure that the system is correctly cabled, and then refer to the Troubleshooting Trees on the EMC Support page for the storage system. If you cannot determine any reasons for the fault, contact your authorized service provider.
12. Power on the Data Mover enclosure and boot the VNX OE for File by connecting all Data Mover enclosure power cables to the PDUs in a manner ensuring high availability and wait for the Data Movers to power up.

The blue power LED on the front of the Data Mover enclosure will light when the Data Movers have powered up, and each Data Mover will display a steady green power LED.

13. Wait 4-5 minutes as the Data Movers power up to ensure that the Data Movers have booted and that they are ready. Then, connect the power cable for the Control Station 0 to the PDU.

**Note**

Do not plug in the power cable for CS 1, if present, at this time. CS 1 will be booted later in this process.

14. Check the CS power LED (labeled in the following figure) on the front of the Control Station verify that the CS is booting. This green LED will blink as the CS boots and be on when complete.

**Note**

The front bezel must be removed to for a clear view of the CS LEDs and to access the power button of the Control Station.
Note

If, after 5 minutes, this LED indicates that the Control Station is off, turn on the Control Station by pressing the front reset button.

Ensure that the Control Station is powered up before continuing.

15. Check the system and hardware status as follows:

a. From a browser, type the IP address of the primary Control Station.

b. Log in to the Unisphere software.

c. Use the drop-down list at the top-left Dashboard to select the system name and view its System Information.

d. On this page, verify that the Status fields for the VNX display OK.

e. Next, locate the Run Command option in Unisphere under Control Station CLI on the right-hand side of the System page and verify that CS 0 and the Data Movers booted successfully by running a Control Station CLI command:

/nasmcd/sbin/getreason

Expected Reason Code values for booted VNX for File components:
16. For dual Control Station systems only, once you have confirmed that CS 0 is up and healthy, power up CS 1 by connecting the power cable for the CS 1 to a PDU on a different circuit from CS 0 to ensure high availability.

17. After completing the power up of the system, return to the Run Command option in Unisphere and perform a system checkup:

```
nas_checkup
```

Fix issues discovered by the nas_checkup command in the manner indicated in its output.
Chapter 4
Shut down the VNX in an emergency

This section explains how to shut down the VNX in case of an emergency. Power down the VNX on page 57 provides more specifics on normal (planned) powerdown procedures.

Perform the following tasks to shut down the VNX in an emergency:

⚠️ **CAUTION**

These procedures can cause data loss or disrupt service to other clients. Use these procedures only when faced with personal hazard or possible property damage.

- VNX series emergency shutdown ................................................................. 58
- Power up after an emergency shutdown ..................................................... 58
VNX series emergency shutdown

To shut down VNX systems in an emergency, turn off the two cabinet circuit-breaker switches.

⚠️ CAUTION

Turning off the cabinet circuit-breakers immediately removes power from Data Movers, Control Station, storage array system, standby power supplies (SPSs), and any other equipment connected to the cabinet’s PDU. No other action is required.

Power up after an emergency shutdown

After you use the emergency shutdown procedure, you might encounter errors or problems when you try to restart the VNX server. If this occurs, record any error messages and contact the EMC Customer Service immediately.

To power up a server after an emergency shutdown, follow Power up the VNX on page 58.
CHAPTER 5

Halt and/or restart Control Stations and Data Movers

Follow the tasks below to perform routine Control Station and Data Mover power management tasks.

- Halt the Control Station .......................................................................................... 60
- Restart the Control Station ..................................................................................... 61
- Halt and/or restart Data Movers .............................................................................. 62
Halt the Control Station

This section explains how to perform an orderly halt of Control Stations in Unified, Integrated, and Gateway servers. You can halt a Control Station either locally or remotely.

Perform these tasks to halt Control Stations either locally or remotely:

- Halt one Control Station, locally or remotely on page 60
- Halt dual Control Station, locally or remotely on page 60

Halt one Control Station, locally or remotely

This procedure applies to all VNX Unified and VNX File systems with a single Control Station.

Procedure

1. Log in to the server as root.

   Note
   If logging in remotely, use a secure, encrypted, remote login application to log in to the server as root.

2. Halt the Control Station by typing:

   # /sbin/halt

   The Control Station halts.

Halt dual Control Station, locally or remotely

This procedure applies to all VNX Unified and VNX File systems with two Control Stations.

Note
Always halt the secondary Control Station before the primary.

Procedure

1. Log in to the server as root.

   Note
   If logging in remotely, use a secure, encrypted, remote login application to log in to the server as root.

2. Determine which Control Station (CS 0 or CS 1) is primary and which is secondary by typing:

   # /nasmdc/getreason

   The primary Control Station returns a reason code of 10; the secondary Control Station returns a reason code of 11.

3. If logged in to the primary CS, log in to the secondary Control Station as root.

   Note
   If logging in remotely, use a secure, encrypted, remote login application to log in to the secondary CS as root.
4. Halt the secondary CS by typing:
   `
   # /sbin/halt
   ` The secondary CS halts.
5. Log in to the primary Control Station as root.

   **Note**
   If logging in remotely, use a secure, encrypted, remote login application to log in to the primary CS as root.
6. Halt the primary CS by typing:
   `
   # /sbin/halt
   ` The primary CS halts.

### Restart the Control Station

This section explains how to perform an orderly restart of Control Station(s) in a VNX Unified and VNX File systems. Control Stations restart either locally or remotely.

Perform these tasks to restart Control Stations either locally or remotely:
- Restart one Control Station, locally or remotely on page 61
- Restart two Control Station, locally or remotely on page 61

### Restart one Control Station, locally or remotely

This restart procedure applies to all VNX Unified and VNX File systems with a single Control Station.

**Procedure**

1. Log in to the server as root.

   **Note**
   If logging in remotely, use a secure, encrypted, remote login application to log in to the server as root.

2. Restart the CS by typing:
   `
   # reboot
   ` The CS reboots.

   **Note**
   To continue working remotely, establish another remote connection.

### Restart two Control Station, locally or remotely

This restart procedure applies to all VNX Unified and VNX File systems with a two Control Stations.

**Procedure**

1. Log in to the server as root.
### Halt and/or restart Data Movers

This section explains how to perform an orderly halt or reboot of Data Movers in Unified, Integrated, and Gateway servers. You can halt or reboot a Data Mover either locally or remotely.

- **Halt the Data Movers on page 62**
- **Restart a Data Mover on page 63**

### Halt the Data Movers

The following procedure explains how to perform an orderly, timed, or immediate halt of a network server’s Data Mover. This procedure applies to all VNX Unified and VNX File systems.

---

**Note**

If logging in remotely, use a secure, encrypted, remote login application to log in to the server as root.

2. Determine which Control Station (CS 0 or CS 1) is primary and which is secondary by typing:

   ```
   # /nasmcd/getreason
   ```

   The primary Control Station returns a reason code of 10; the secondary Control Station returns a reason code of 11.

3. If not already, log in to the primary Control Station as root.

**Note**

If logging in remotely, use a secure, encrypted, remote login application to log in to the primary CS as root.

4. Restart the primary CS by typing:

   ```
   # reboot
   ```

   The primary Control Station restarts and fails over to the secondary Control Station (making it the new primary Control Station).

   Do not go to the next step until the Control Station has finished restarting.

5. Log in to the new primary Control Station as root.

**Note**

If logging in remotely, use a secure, encrypted, remote login application to log in to the new primary CS as root.

6. Restart the new primary CS by typing:

   ```
   # reboot
   ```

   The new primary Control Station restarts and fails over to the original primary Control Station (returning it the primary Control Station).

**Note**

To continue working remotely, establish another remote connection.
A Data Mover is also called a blade. There is no functional difference between a Data Mover and a blade.

To immediately halt a Data Mover, use this command syntax:
```
server_cpu <movername> -halt <time>
```
where:
- `<movername>` = name of the Data Mover
- `<time>` = when the Data Mover is to be halted, specified as one of the following:
  - `now`
  - `+<min>`
  - `<hour>:<min>`

**Example:**
To halt server_5 immediately, type:
```
server_cpu server_5 -halt now
```

---

**Restart a Data Mover**

The following procedure explains how to perform an orderly, timed or immediate restart of the network server's Data Movers. The procedure applies to all VNX Unified and VNX File systems.

To immediately restart and monitor a Data Mover, use this command syntax:
```
server_cpu <movername> -reboot [cold|warm] -monitor <time>
```
where:
- `<movername>` = name of the Data Mover
- `[cold|warm]` = defines the degree to which the Data Mover is reset.
  - A cold reboot or a hardware reset shuts down the Data Mover completely before restarting, including a Power on Self Test (POST).
  - A warm reboot or a software reset performs a partial shutdown of the Data Mover, and skips the POST after restarting. A software reset is faster than the hardware reset.
- `<time>` = when the Data Mover is to be restarted, specified as one of the following:
  - `now`
  - `+<min>`
  - `<hour>:<min>`

**Note**
The default parameter of the `-reboot` option will be the warm parameter. In case the warm rebooting fails, the `-reboot` option will use the cold parameter to reboot the Data Mover.

**Example 1:**
To monitor an immediate cold restart of server_5, type:
```
server_cpu server_5 -reboot cold -monitor now
```

**Example 2:**
To monitor an immediate warm restart of server_5, type:
```
server_cpu server_5 -reboot -monitor now
```

Note

You can verify when the system is back online by using /nas/sbin/getreason. Code 5 indicates the Data Mover is available.

You might also see the following codes as the Data Mover restarts:

- 0 - (reset) - Data Mover performing BIOS check, then begins boot sequence
- 1 - (POST pass) - Data Mover passes POST
- 3 - (loaded) - Operating system loaded and initializing
- 4 - (ready) - Operating system initialized
- 5 - (contacted) - Data Mover available
CHAPTER 6

View and manage system details

Find details about viewing and managing general system settings.

- Identify the software versions ................................................................. 66
- Audit the VNX ....................................................................................... 66
- Check the system status ....................................................................... 67
- Change the Control Station hostname ................................................ 67
- Install Control Station Linux security alerts ........................................ 68
- Verify the daemons ............................................................................... 69
- Back up the VNX database .................................................................... 70
- Query VNX for SCSI details ................................................................. 72
Identify the software versions

To determine the software versions on the Control Station or Data Mover, use the following:

- View Control Station software version on page 66
- View Data Mover software version on page 66

View Control Station software version

Procedure

- To view the software version running on the Control Station, type:

```bash
$ nas_version -l
```

Output:

<table>
<thead>
<tr>
<th>Name</th>
<th>emcnas</th>
<th>Relocations: /nas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>8.1.30</td>
<td>Vendor: EMC</td>
</tr>
<tr>
<td>Release</td>
<td>1</td>
<td>Build Date: Wed 10 Dec 2013 06:54:59 PM EST</td>
</tr>
<tr>
<td>Size</td>
<td>753358063</td>
<td>License: EMC</td>
</tr>
<tr>
<td>Copyright</td>
<td></td>
<td>Packager: EMC Corporation</td>
</tr>
<tr>
<td>Signature</td>
<td>(none)</td>
<td>URL: <a href="http://www.emc.com">http://www.emc.com</a></td>
</tr>
<tr>
<td>Description</td>
<td>EMC nfs base install</td>
<td></td>
</tr>
</tbody>
</table>

View Data Mover software version

Procedure

- To view the software version running on a Data Mover, type:

```bash
$ server_version <movername>
```

where `<movername>` = name of the Data Mover

For example:

```bash
$ server_version server_3
```

Audit the VNX

The Control Station provides powerful system auditing capabilities. VNX auditing provides a method to audit/detect access to the Data Mover file systems from the Control Station.

Auditing is enabled by default on the Control Station after a fresh install and a Control Station recovery.

Verify if auditing is enabled, by:

Procedure

1. Log in to the server as root.
2. To check if auditing is running on the Control Station, type:

```bash
#/sbin/service auditd status
```

Output:
Check the system status

Use the nas_checkup command to perform a health checkup for the VNX.
nas_checkup runs scheduled and unscheduled health checks on the VNX and reports problems that are found, and the actions needed to fix the problem and acts as a system health monitor.
The scheduled run time for the nas_checkup command is every 2 weeks by default. If a warning or error is discovered during this time, an alert is posted on the Unisphere software.

Set up email notification for warnings or errors in the Unisphere software Notifications page, or modify and load the sample nas_checkup event configuration file.
nas_checkup returns one of the following exit statuses for system diagnostics:

- 0 — No problems found
- 1 — nas_checkup posted information
- 2 — nas_checkup discovered a warning
- 3 — nas_checkup discovered an error
- 255 — Any other error

Examples of errors that could cause a 255 exit status include, but are not limited to:

- If nas_checkup is run when another instance of nas_checkup is running
- If nas_checkup is run by someone other than root or the administrator group (generally nasadmin)
- If nas_checkup is run on the standby Control Station

If a problem is discovered that requires EMC Service Personnel assistance, nas_checkup will notify EMC.

To perform a checkup of the VNX File, use this command syntax:

```
$ nas_checkup
```

Change the Control Station hostname

You can change a VNX server's Control Station hostname. The following procedure uses the CLI. However, if you use the Unisphere software to manage the server, use it to make the hostname change instead.

In the following procedure, the Control Station hostname was changed from Eng_1 to cs100.
CAUTION

If you use the CLI to change the Control Station hostname and use the Unisphere software to manage the server, ensure that you follow this procedure carefully. Otherwise, you will not be able to create file systems by using the Unisphere software.

Add the new hostname to either DNS or the VNX system. To make changes to DNS, check the DNS documentation. This procedure adds the new hostname to the VNX system only.

Procedure

1. Log in to the Control Station as root.
2. To verify the current environment, type:
   
   ```
   # hostname
   Output:
   Eng_1
   ```

3. To display information about the Control Station, including its hostname and ID, type:

   ```
   #/nas/bin/nas_cel -list
   ```

   Output:

   ```
   id name owner mount_dev channel net_path CMU
   0 Eng_1 0                               172.24.101.100
   APM04490091900
   ```

4. To change the hostname of the Control Station, type:

   ```
   #/nas/bin/nas_cs -set -hostname <new_hostname>
   ```

   Output:

   ```
   OK
   ```

5. To confirm the hostname of the Control Station, type:

   ```
   #/nas/bin/nas_cel -list
   ```

   Output:

   ```
   id name owner mount_dev channel net_path CMU
   0 cs100 0                               172.24.101.100
   APM04490091900
   ```

6. To change the SSL certificate for Apache, type:

   ```
   #/nas/sbin/nas_config -ssl
   ```

   Output:

   ```
   Installing a new SSL certificate requires restarting the Apache web server.
   Do you want to proceed? [y/n]: y
   New SSL certificate has been generated and installed successfully.
   ```

Install Control Station Linux security alerts

EMC monitors Linux security alerts and carefully evaluates how the associated errata apply to Control Station Linux. Be sure to install only EMC-approved security updates on the VNX. You can have them installed anytime either during the installation of a new VNX software release or between the installation of new software releases.

New software release installations

EMC-approved Linux security updates are automatically installed on the VNX each time a new VNX software release is installed.
Between software release installations
If you want to install a current Linux security update before installing a new VNX software release, contact the EMC Customer Service. Only EMC-approved security updates should be installed on the VNX.

Verify the daemons

After installation, daemons begin running on the Control Station at all times. If for some reason the daemons become disabled, certain server facilities might fail.

Perform these tasks to verify whether VNX daemons are enabled:

- View VNX daemons on page 69
- View HTTPD daemons on page 69

View VNX daemons
To view the VNX daemons enabled at the Control Station, type:

```
$ ps -e|grep nas | awk ' { print $4 } ' | sort | uniq
```

The following appears:

- nas_boxmonitor
- nas_eventcollec
- nas_eventlog
- nas_mcd
- nas_watchdog

**Note**

The complete list of daemons is displayed in the output above, but the output list for your server might be different.

If the daemons are not running, restart them by typing:

```
/etc/rc.d/init.d/nas stop
/etc/rc.d/init.d/nas start
```

View HTTPD daemons
It is essential that the HTTPD daemons run on the Control Station at all times, so the Unisphere software can manage the VNX.

To view whether the HTTPD daemons are enabled at the Control Station and to reenable them if necessary, type:

```
$ ps -e|grep httpd
```

The following appears:

- 15937 ? 00:00:10 httpd
- 15949 ? 00:00:00 httpd
- 15950 ? 00:00:00 httpd
- 15951 ? 00:00:00 httpd
- 15964 ? 00:00:00 httpd
- 15965 ? 00:00:00 httpd
- 15966 ? 00:00:00 httpd
- 15995 ? 00:00:00 httpd
- 16008 ? 00:00:00 httpd
Back up the VNX database

VNX database created by the VNX software during installation is stored on disk in the Control Station. The VNX database maintains vital information required for each Data Mover. The VNX File software automatically creates a VNX database backup file 1 minute after each hour. You can manually create a VNX database backup file at any time.

Perform these tasks to back up the VNX database:

- Automatic VNX database backup on page 70
- Manual VNX database backup on page 70

CAUTION

- EMC strongly recommends that you regularly copy the VNX database backup file from the Control Station and save it to a remote location for safe keeping. Always copy the VNX database backup file when hardware or software upgrades are planned.
- Only EMC qualified support personnel should restore the VNX database by using the VNX database backup file.
- Do not manually edit the nas_db database without consulting Customer Service. Any changes you make might disrupt services.

Automatic VNX database backup

The VNX automatically backs up the entire database and saves it to a file named nasdb_backup.1.tar.gz in the /nas/var/backup directory. It does this 1 minute after each hour. It also maintains the last 12 backup files.

To copy a VNX database backup file to a remote location, use FTP as described in Using FTP, TFTP and SFTP on VNX.

Manual VNX database backup

Use this procedure to back up and save a copy of the VNX database without waiting for an hourly automatic backup.

Procedure

1. Log in to the primary Control Station as nasadmin.
2. List the VNX database backup files by typing:

   $ ls -l nasdb*

   A display similar to the following appears:

   -rw-r--r-- 1 nasadmin nasadmin 1920308 May 4 12:03 nasdb_backup.1.tar.gz
   -rw-r--r-- 1 nasadmin root 1022219 Mar 23 19:32 nasdb_backup.b.tar.gz
Ensure that a version of nasdb_backup.1.tar is listed with the current date and time. If a current version is not present, ensure that nasadmin is the group and owner of nasdb_backup.1.tar.gz and _nasbkup.

3. To ensure that the VNX database backup does not fill the root file system, check the root file system free space by typing:

   $ df -k /

   The system returns the amount of space in the root directory in kilobytes (KB). Ensure that the free space is more than the size of the most recent VNX database backup.

4. Create a backup file of the VNX database by using this command syntax:

   $ /nas/sbin/nasdb_backup /nas /celerra/backup <yymmdd>

   where <yymmdd> is the last two digits of the current year, the two-digit month, and the two-digit day.

   The following appears:

   NAS_DB backup in progress .....NAS_DB checkpoint in progress.....done

5. Examine the date and time to verify that a new version of nasdb_backup.<yymmdd>.tar.gz was created by typing:

   $ ls -l celerra/backup*

   A display similar to the following appears:

   total 46208
   -rw-r--r-- 1 nasadmin nasadmin 2700 Feb 5 13:01 _dbms_backup.01.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 2702 Feb 5 14:01 _dbms_backup.02.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 2702 Feb 5 14:01 _dbms_backup.OK.tar.gz
   drwx------ 2 root root 16384 Feb 1 11:27 lost+found
   -rw-r--r-- 1 nasadmin nasadmin 3163954 Feb 5 13:01 _nasbkup.01.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163960 Feb 5 14:01 _nasbkup.02.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163941 Feb 5 03:01 _nasbkup.03.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163965 Feb 5 04:01 _nasbkup.04.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163959 Feb 5 05:01 _nasbkup.05.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163934 Feb 5 06:01 _nasbkup.06.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163945 Feb 5 07:01 _nasbkup.07.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163957 Feb 5 08:01 _nasbkup.08.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163964 Feb 5 09:01 _nasbkup.09.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163922 Feb 5 10:01 _nasbkup.10.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163960 Feb 5 11:01 _nasbkup.11.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 3163954 Feb 5 12:01 _nasbkup.12.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 4407468 Feb 5 14:01 nasdb_backup.1.tar.gz
   -rw-r--r-- 1 nasadmin nasadmin 4268888 Feb 1 11:33 nasdb_backup.b.tar.gz
   drwxrwxr-x 2 root root 4096 Feb 1 12:01 SCCS
   -rw-r--r-- 1 root root 528384 Feb 1 12:01 wpart

6. Using secure FTP, copy the VNX database file nasdb_backup.<yymmdd>.tar.gz and nasdb_backup.b.tar.gz to a remote location.
Note
The backup file should not be copied to the Data Mover because Data Movers might not be functional if VNX database gets corrupted.

Query VNX for SCSI details

The Control Station database maintains a list of all SCSI devices. When required, you can probe the storage system to discover and save the present SCSI devices for a specific Data Mover.

Discover SCSI devices
To discover all SCSI devices for the specified Data Mover, use this command syntax:

```
$ server_devconfig <movername> -probe -scsi -all
```

where `<movername>` = name of the Data Mover

For example, the following command and output pair discovers all SCSI devices for DM 2, named server_2:

```
$ server_devconfig server_2 -probe -scsi -all
server_2:
SCSI disk devices:
chain= 0, scsi-0
symm_id= 0 symm_type= 0
tid/lun= 0/0 type= disk sz= 4153 val= 1 info= 526691000051
tid/lun= 0/1 type= disk sz= 4153 val= 2 info= 526691001051
tid/lun= 1/0 type= disk sz= 8631 val= 3 info= 52669100C051
tid/lun= 1/1 type= disk sz= 8631 val= 4 info= 52669100D051
tid/lun= 1/2 type= disk sz= 8631 val= 5 info= 52669100E051
tid/lun= 1/3 type= disk sz= 8631 val= 6 info= 52669100F051
tid/lun= 1/4 type= disk sz= 8631 val= 7 info= 526691010051
tid/lun= 1/5 type= disk sz= 8631 val= 8 info= 526691011051
tid/lun= 1/6 type= disk sz= 8631 val= 9 info= 526691012051
tid/lun= 1/7 type= disk sz= 8631 val= 10 info= 526691013051
tid/lun= 1/8 type= disk sz= 8631 val= 11 info= 526691014051
tid/lun= 1/9 type= disk sz= 8631 val= 12 info= 526691015051
```

Note
If you attempt to view SCSI devices and the system stops responding, the storage system might be offline. To solve this, verify that the storage system is online and then retry the procedure.

CAUTION
Discovering or saving SCSI devices is time-consuming for the server, so it is better to do it during nonpeak times when resources are available. Discovering and saving SCSI devices might cause temporary service disruption to the VNX.

Save SCSI devices
You can save SCSI devices to the device table. Before using the `-create` option, ensure that you back up the existing camdisk file located in the `/nas/server/slot_#` directory.

To discover and save all SCSI devices for a Data Mover, use this command syntax:

```
$ server_devconfig <movername> -create -scsi -all
```

where `<movername>` = name of the Data Mover
For example, the following command and output pair discovers and saves all SCSI devices for DM 2, named server_2:

```
$ server_devconfig server_2 -create -scsi -all
server_2 : done
```
View and manage system details
CHAPTER 7

Manage VNX time and date settings

Find details about setting timezone values, managing NTP service, and setting the time and date for the VNX system in the sections that follow.

- Set the date and time of the VNX................................................................. 76
- Configure NTP service using the CLI......................................................... 77
- Set the time zone of the VNX................................................................. 77
Set the date and time of the VNX

To set the date and time of a Control Station or a Data Mover:
- Set Control Station date and time on page 76
- Set Data Mover date and time on page 76

Set Control Station date and time

Before you begin
You must log in as root on the primary Control Station to perform this operation.
To set the date and time for a primary Control Station, use this command syntax:
```
# nas_cs -set -time <yyyymmddhhmm [ss]>
```
where `<yyyymmddhhmm [ss]>` = date and time (seconds, optional) format

**Note**
Additionally, you can define the timezone and NTP servers, using the `-timezone` and `-ntp_servers nas_cs` switches, respectively. For more information review your system Command Reference Manual.

Example:
To set the date and time to 2:40 P.M. on July 2, 2012, type:
```
# nas_cs -set -time 201207021440
```
OK

**Note**
To view the output, type `date` at the command prompt.

Set Data Mover date and time

You can customize the display of the date and time on a Data Mover by using the `server_date` command. Configuring Time Services on VNX provides additional information on time services.
To set the current date and time for a Data Mover, use this command syntax:
```
$ server_date <movername> <yyymmmddhhmm> [ss]
```
where:
- `<movername>` = name of the Data Mover
- `<yyymmmddhhmm> [ss]` = where `<yy>` is the year; the first `<mm>` is the month; `<dd>` is the day; `<hh>` is the hour (in 24-hour system); and the second `<mm>` is the minute, and `<ss>` is the second.

Example:
To set the date and time on server_2 to July 4, 2005, 10:30 A.M., type:
```
$ server_date server_2 0507041030
server_2 : done
Configure NTP service using the CLI

Note
For more information about the configuring NTP, refer to the Configuring Time Services on VNX technical module.

Procedure
1. Log in to the primary Control Station as root.
2. View the current time, date, NTP settings on the primary Control Station:
   
   \# nas\_cs -info

3. Add or remove NTP servers from the Control Station:
   
   - To add an NTP server:
     \# nas\_cs -set -ntp\_servers \textit{ntp\_server\_IP\_address}
   
   \textbf{Note}
   When adding multiple NTP servers at one time, type the IP addresses for each NTP server to be added in a comma-separated list.

   - To clear all NTP servers:
     \# nas\_cs -clear -ntp\_servers

4. View the updated time, date, NTP settings on the primary Control Station:
   
   \# nas\_cs -info

Set the time zone of the VNX
You can update the time zone information on the Data Mover by using simple and decipherable strings that correspond to the time zones available in the Control Station. You can also update the daylight savings time on the Data Mover for the specified time zone.

- Change Control Station time zone manually using the CLI on page 77
- Set Data Mover time zone manually on page 78

Change Control Station time zone manually using the CLI

Procedure
1. Log in to the primary Control Station as root.
2. To verify the current environment, type:
   
   \# date
   Output:
   
   Mon Feb 27 16:42:52 EST 2012

3. Change the timezone:
Note

To view a list of the supported timezones, at the command prompt, type:
# nas_cs -info -timezone

# nas_cs -set -timezone <supported_timezone>
Example:
# nas_cs -set -timezone America/Denver
Warning 17985699848: The time zone has been set successfully.
Reboot the Control Station.

4. Reboot the primary CS:

Note

If the system is configured with two Control Stations, you will need to power down the secondary Control Station prior to rebooting the primary CS.

# nas_cs -reboot

5. To verify the current environment, type:
   # date
   Output:
   Mon Feb 27 14:42:52 MTN 2012

6. If you powered down the secondary CS earlier, power on CS 1 at this time.

Results

The time zone of the Control Station is changed to the new location specified.

Set Data Mover time zone manually

Procedure

1. Log in to the Control Station as root.

2. To set the time zone on a Data Mover using the Linux time zone method, use this command syntax:

$ server_date <movername> timezone -name <timezonename>

where:

- `<movername>` = name of the Data Mover
- `<timezonename>` = a Linux style time zone specification

Example:
To set the time zone to Central Time and adjust the daylight savings time for a Data Mover by using the Linux method, type:

$ server_date server_2 timezone -name America/Chicago

Output:
server_2 : done
CHAPTER 8

Manage networking

Manage the VNX networking settings and values using the following sections:

- Configure IPv6 on the Control Station ............................................................... 80
- Configure SNMP ................................................................................................. 80
- Add DNS Server ............................................................................................... 81
- Avoid private LAN IP address conflicts ........................................................... 82
- Configure IP aliasing ......................................................................................... 82
- Change VNX management port IP address values ........................................... 84
Configure IPv6 on the Control Station

The Control Station supports IPv6 through a dual-stacking implementation of IPv4 and IPv6 network addresses. To implement and manage this feature, a new CLI command, nas_cs, has been introduced to manage the configuration properties of the Control Station.

**Note**

For more information about nas_cs and configuring IPv6 on the Control Station, refer to *VNX Command Line Interface Reference for File*.

To set the IPv6 address of a primary Control Station, it must be implemented alongside IPv4. To implement dual-stacking of IPv4 and IPv6 addresses through the CLI follow the process below.

```
# nas_cs -set -ip6address <ipv6_address[/prefix_length]> -ip6gateway <ipv6_gateway>
```

where:

* `<ipv6_address[/prefix_length]>` = the IPv6 network address of the primary Control Station. The IPv6 address must be a valid address. The `/prefix_length` option sets the integer value, between 8 and 128, for the prefix length of the IPv6 address of the primary Control Station.

* `<ipv6_gateway>` = the IPv6 network address of the gateway machine for the primary Control Station on the network. The IPv6 address must be a valid address.

**Example:**

To set the IPv6 address and the IPv6 gateway for the primary Control Station, type:

```
```

OK

Configure SNMP

The SNMP collects and processes valuable network information. It gathers data by polling the devices on the network from a management station at fixed or random intervals. When the network is operating ideally, SNMP establishes a state that is called a baseline, which lists all of the operational parameters.

The SNMP protocol acts as a network safeguard against irregularities that might hamper the functioning of the network. The SNMP agent, the SNMP daemon (SNMPD), which runs on the Data Mover, supports SNMPv1, SNMPv2c, and SNMPv3. The SNMPD service is started, but unconfigured, by default.

For more information about SNMP and SNMPv3, refer to *Using SNMPv3 on VNX* and the server_snmpd man pages.

**View SNMP status**

To view the SNMP service status for all Data Movers, type:

```
$ server_snmpd ALL -service -status
```
Output:
server_2:
SNMP Running

server_3:
SNMP Stopped

Note
Only a single SNMPD runs on each Data Mover. In the event of a failover, the standby Data Mover runs the SNMPD.

Add DNS Server

Before you begin
Only a global user who has the privileges associated with the Administrator or Security Administrator role can configure DNS settings.

Note
The list of DNS Server IP addresses is an ordered list. Both IPv4 and IPv6 addresses are acceptable. The VNX for block OE will always prefer IPv6 addresses (if the addresses have been configured) over IPv4, even if the addresses are ordered differently at configuration time.

To add a DNS Server:

Procedure
1. Select All Systems > Domains, and from the Local Domain task list, click Configure DNS.

   Alternatively, select the system, and then select Settings, and from the Network Settings task list, click Configure DNS.

   DNS Configuration for Storage Domain appears.
2. In DNS Domain Suffix, if the displayed domain suffix is not correct for the DNS Server you are adding, type the valid domain suffix for the DNS Server.

   If the domain suffix has never been set, the field is empty.
3. In DNS Server IP Address, type the IP address of the server (either an IPv4 or IPv6 address is acceptable) in the box to the left of Add.
4. Click Add.

   The IP address entry appears at the bottom of the list.
5. If required, you can click an IP address and use Move Up or Move Down to position the IP address in the list.
6. If the domain suffix does not appear in Domain Search List, type the valid domain suffix for the DNS Server in the box to the left of Add.
7. Click Add.

   The domain suffix entry for the DNS Server appears at the bottom of the list.
8. If required, you can click a domain suffix and then use Move Up or Move Down to position the domain suffix in the list.
9. Click OK to save any changes.
Avoid private LAN IP address conflicts

VNX servers use a private LAN for communication between the Control Stations and Data Movers. This LAN is sometimes also called a local or internal LAN. By default, this private LAN uses IP addresses in the following three subnets:

- 128.221.252.nnn — This subnet is the primary private LAN. For the NS series servers, this LAN connects to the LAN switch on the Control Station 0 tray assembly.
- 128.221.253.nnn — This subnet is the secondary (or backup) private LAN. For the VNX server with two Control Stations, the secondary LAN connects to the LAN switch on the Control Station 1 tray assembly. For a single Control Station NS series server, it shares the same network as the primary private LAN, which uses the LAN switch on the Control Station 0 tray assembly.
- 128.221.254.nnn — This subnet is used for the Intelligent Platform Management Interface (IPMI) connection between two Control Stations. IPMI enables one Control Station to restart the other. The subnet consists of a crossover cable connected between ports on the two Control Stations. This subnet is not used for single Control Station servers.

Although the VNX private LAN does not connect to the public LAN, the Data Movers (or blades) and Control Stations do connect to both the private and public. If you are using these default subnet addresses in the public network, the VNX equipment installer gave the VNX private LAN new addresses at installation time. Ensure that you have these new addresses.

**Note**

To prevent server disruption, do not connect the private LAN Ethernet switch to any other network, network device, or host.

If you have more than one VNX server, each server can have the same set of private LAN addresses. A conflict occurs only when the same subnet exists in both the public and private LANs.

If you change the network configuration after the VNX server is installed, avoid using the VNX private LAN subnets. If you must use them, reconfigure the VNX private LAN to use different subnet addresses.

If you still have questions after reading this section, contact the EMC Customer Service for assistance to avoid creating conflicting subnets.

Configure IP aliasing

IP aliasing allows different IP addresses to point to the same network device. The VNX allows you to configure IP aliasing for a Control Station. This enables communication with the primary Control Station by using a single IP address regardless of whether the primary Control Station is running in slot 0 or slot 1.

To create or delete an IP alias:

**Note**

Any IP address entered is checked to ensure that it is valid and not used by another network device.

- [Create an IP alias on page 83](#)
Create an IP alias

Procedure
1. Log in to the server as root.
2. To create an IP alias for the Control Station, use one of the following scripts:
   - For an IPv4 IP alias, use:
     ```bash
     #/nas/sbin/nas_config -IPalias -create 0
     ```
   - For an IPv6 IP alias, use:
     ```bash
     #/nas/sbin/nas_config -IPalias -create6 0
     ```
3. To use a new IP address as the IP alias, answer no to the question and then type the new IP address to use as an IP alias within the same network.
   For example, when the script prompts:
   ```
   Do you want slot_0 IP address <1.2.3.4> as your alias [yes or no]: no
   Please enter an IP address to use as an alias: 1.2.3.6
   ```
4. To use the current IP address as the IP alias, answer yes to the question, and then type a new IP address to replace the current IP address.
   For example, when the script prompts:
   ```
   Do you want slot_0 IP address <1.2.3.4> as your alias [yes or no]: yes
   Please enter an IP address to use as an alias: 1.2.3.6
   ```
5. To view the IP alias you created:
   - For an IPv4 IP alias, use:
     ```bash
     #/nas/sbin/nas_config -IPalias -list
     ```
   - For an IPv6 IP alias, use:
     ```bash
     #/nas/sbin/nas_config -IPalias -list6
     ```

Delete an IP alias

Procedure
1. To delete an IP alias using the script, type:
   - For an IPv4 IP alias, use:
     ```bash
     #/nas/sbin/nas_config -IPalias -delete 0
     ```
   - For an IPv6 IP alias, use:
     ```bash
     #/nas/sbin/nas_config -IPalias -delete6 0
     ```
2. Type yes to delete the IP alias at the prompt shown below:
   ```
   All current sessions using alias eth2:0 will terminate
   Do you want to continue [yes or no]: yes
done
   ```
3. To view the result, type:
For an IPv4 IP alias, use:

```
# /nas/sbin/nas_config -IPalias -list 0
```

For an IPv6 IP alias, use:

```
# /nas/sbin/nas_config -IPalias -list6 0
```

**Change VNX management port IP address values**

The network properties are initially set by EMC service personnel to work at your site. We strongly recommend that you do not change any value unless you are moving the SP to another LAN or subnet.

**Change the IP addresses for VNX for File/Unified management ports**

---

**Note**

Do not attempt to change the IP addresses of a VNX system using Unisphere, you will lose management access to this storage system.

---

To properly change the IP addresses of this system, refer to the *Changing VNX File/Unified IP Addresses* procedure located in the **Related Documents** on [https://mydocs.emc.com/VNX](https://mydocs.emc.com/VNX) for instructions on changing management ports IP addresses.
CHAPTER 9

Manage logging and alerting capabilities

Configure VNX logging and alert capabilities using the following sections.

- Change the ConnectHome settings .................................................. 86
- Set the country code on the MT5634ZBA modem .......................... 92
- Interpret log files ........................................................................... 95
- VNX and RSA Envision ................................................................. 101
- NAS or SAN environment rules ...................................................... 101
- VNX for file problem information .................................................. 103
Change the ConnectHome settings

The VNX ConnectHome function automatically notifies the EMC service center or other service provider if the VNX system detects a serious problem. ConnectHome sends messages by using email, FTP server, or the VNX modem and a customer supplied analog telephone line.

Configure Connect Home

EMC recommends that ESRS transport be configured as the primary transport.

If necessary, EMC recommends that Email transport be configured as the secondary transport and that you keep the default EMC recipient address, emailalert@emc.com, unless otherwise specified by your authorized service provider. Be sure to update the settings if your Site ID or dial-in information changes.

Note

To pause and resume the Connect Home service, and to clear the pending Connect Home event files, use the nas_connecthome -service command. The online man page for nas_connecthome provides more information.

Configure the sender address of the email transport using the nas_connecthome command with the site administrator's email address to capture the email relay errors.

To change any of the properties, you must be logged in as root.

Procedure

1. Select System.

2. From the task list, under Service Tasks, select Manage Connect Home.

   If you access the ConnectHome page and every transport mechanism is disabled, an informational message appears on top of the ConnectHome page. The message instructs you to configure a transport mechanism and recommends the ESRS transport mechanism. If you access the ConnectHome page and the ESRS is disabled on the Control Station, an informational message appears on top of the ConnectHome page. The message notifies you that the ESRS is disabled and instructs you to enable it. In this case, the ESRS Priority drop-down list is disabled until ESRS is provisioned.

3. In the Your Site ID field, type the name of your site, if known.

4. The Enable dial-in is selected by default.

   This option allows support personnel to access your Control Station remotely; it is intended for modem dial in.

5. In the Number to Dial In (Modem) field, type the modem number of the VNX system. Be sure to include country and city codes, if applicable.

   If your VNX system has two modems, one for each Control Station, type both dial-in phone numbers.

   First, type the modem number for Control Station 0, followed by a slash (/), and then the modem number for Control Station 1. You cannot enter more than 31 characters.

   Examples:

   Numbers without extension: 912344356000/912344356001

   Numbers with extension: 911239549842x6095/x6096
6. Enable or disable encryption using the **Enable Encryption**.

   Encryption is used for ESRS, email and FTP only, and is enabled by default. This option allows encryption of all transport type payloads during transmission.

7. Use the **ESRS Priority** drop-down list to set or modify ESRS as a primary, secondary, or tertiary transport mechanism.

   If ESRS is disabled, **Disabled** appears in the **ESRS Priority** drop-down list and the list is disabled. You must click **Manage ESRS Settings** to open the **Manage ESRS** page and provision ESRS. See **Provision ESRS on page 88** for instructions. When ESRS provisioning is completed, the drop-down list is enabled. Also, if you need to re-provision the ESRS, click **Manage ESRS Settings** to open the **Manage ESRS** page and make any necessary changes to ESRS. See **Re-provision ESRS on page 90** for instructions.

   This selection refers to using the ESRS software on the Control Station which is included as part of the VNX Operating Environment (OE). The ESRS software on the Control Station should not be used in conjunction with the ESRS IP Client for VNX software which must be installed on a host or virtual machine.

8. Use the **Email Priority** drop-down list to set or modify email as a primary, secondary, or tertiary transport mechanism.

   Specifying **disabled** removes email as a transport mechanism.

9. In the **Email-SMTP** field, type the fully qualified domain name or IP address of the primary email server. You cannot enter more than 63 characters.

10. In the **Subject** field, set or modify the subject of the email message. You cannot enter more than 127 characters.

11. In the **Recipient Address (es)** field, set or modify the destination email addresses that receive event files. You cannot enter more than 255 characters.

   **Note**

   EMC recommends that you do not change the default EMC recipient address emailalert@emc.com unless otherwise specified by your authorized service provider.

12. In the **Sender Email Address** field, accept or modify the sender email address.

   It is important to note that email can be forwarded through your email server. In this case, the Email server will require a valid mail user.

13. Under FTP, use the **FTP Priority** drop-down list to set or modify FTP as a primary, secondary, or tertiary transport mechanism.

   Specifying **disabled** removes FTP as a transport mechanism.

14. In the **FTP Server** field, type the IP address of the ESRS Gateway FTP server. This is where event files will be transferred.

15. In the **FTP Port** field, set or modify the corresponding primary FTP port.

16. In the **User Name** field, set or modify the username of the login account on the primary FTP server. You cannot enter more than 15 characters.

17. In the **Password** field, set or modify the password of the login account on the primary FTP server. You cannot enter more than 15 characters.

18. In the **Remote Location** field, set or modify the remote directory path on the FTP server where event files will be deposited. You cannot enter more than 63 characters.

19. In the **Transfer Mode** field, set or modify the transfer mode of the primary FTP transport mechanism.
20. Use the **Modem Priority** drop-down list to set or modify the modem as a primary, secondary, or tertiary transport mechanism.

   If there is no modem, select **Disabled**.

21. By default, the modem uses a dialing prefix of 9 to get an outside line, and then dials a 1-800 number. You do not need to change the number in the **Number to Dial Out** field if you are configuring Connect Home on a system in the US or Canada.

   **Note**

   Review the list of International toll-free numbers on page 90 if you are configuring Connect Home on a system outside of the US or Canada.

22. Use the **Monitoring Station HTTPS Priority** drop-down list to set or modify the monitoring station server as a primary, secondary, or tertiary transport mechanism.

   This selection refers to using the ESRS IP Client for VNX software which is not included as part of the VNX OE. The ESRS IP Client for VNX software must be installed on a host or virtual machine and should not be used in conjunction with the ESRS software on the Control Station that is included as part of the VNX OE.

23. Use the **URL** to set or modify the URL of the monitoring station server. IPv4 and IPv6 addresses can be used in the URL.

   An IPv6 address must be in the following format:
   https://[<IPv6-address>]:<port>/<directory>

   where
   
   `<IPv6-address>` = IPv6 address
   `<port>` = port number
   `<directory>` = target directory

24. Click **Apply**.

**After you finish**

*Configuring Events and Notifications on VNX for File* provides more information about events that cause the VNX system to connect home.

---

**Provision ESRS**

**Before you begin**

EMC Secure Remote Support (ESRS) depends on the DNS setting on the Control Station. To function properly, the VNX system must be configured with at least one DNS Server.

To provision ESRS, you must be logged in with root privileges.

**Procedure**

1. Ensure that a DNS Server is configured.

   To view and, if necessary, add a DNS Server to the DNS configuration settings, select **All Systems** >Domains, and from the **Local Domain** task list, click **Configure DNS**. Alternatively, select the system, and then select **Settings**, and from the **Network Settings** task list, click **Configure DNS**. **DNS Configuration for Storage Domain** appears. See **Add DNS Server on page 81** for more information about adding a DNS Server.

2. Select **System**.

3. From the task list, under **Service Tasks**, select **Manage EMC Secure Remote Support**.

   For a VNX with two Control Stations, a dialog box for selecting the target Control Station (Primary or Standby) appears first. The Primary Control Station will be selected...
by default. If necessary, change the selection and click Continue to navigate to the Manage ESRS page for the corresponding Control Station.

As an alternate method to access the ESRS parameters, under Service Tasks, select Manage Connect Home and click Manage ESRS Settings in the ESRS Priority field. This link navigates directly to the Manage ESRS page for the primary Control Station. To manage the ESRS on a standby Control Station, you must select Manage EMC Secure Remote Support from the task list under Service Tasks.

4. Select either EMC Online Support (Powerlink) or RSA SecurID for the Type credential.

The EMC support credentials are required for ESRS.

If you select RSA SecurID, be aware that the SecurID is valid for only 60 seconds. The SecurID password may expire while you fill in the remaining fields.

5. Type the user name for the User Name credential.

6. Type the password for the Password credential.

7. If a Proxy Server will be used in the ESRS configuration, select the checkbox to the right of Use Proxy Server for ESRS.

The fields related to the Proxy Server appear.

8. Select either HTTP or SOCKS for the Protocol field.

9. Type the IP address of the Proxy Server in the Proxy Address field.

10. Type the port number to use for the Proxy Server in the Port field.

11. If credentials are required for the Proxy Server, select the checkbox to the right of Need Credentials.

When the credentials for the Proxy Server are required they must be provided; otherwise, the Proxy Server may fail to connect to the ESRS server.

12. Type the user name for the User Name credential.

13. Type the password for the Password credential.

14. If a Policy Manager will be used in the ESRS configuration, select the checkbox to the right of Use Policy Manager for ESRS.

The fields related to the Policy Manager appear.

15. If SSL protocol will be used for the Policy Manager, select the checkbox to the right of Is Secure.

16. Type the IP address of the Policy Manager in the Address field.

17. Type the port number to use for the Policy Manager in the Port field.

18. If a Proxy Server will be used for the Policy Manager, select the checkbox to the right of Use Proxy Server.

19. Select either HTTP or SOCKS for the Protocol field.

20. Type the IP address of the Proxy Server in the Proxy Address field.

21. Type the port number to use for the Proxy Server in the Proxy Port field.

22. If credentials are required for the Proxy Server, select the checkbox to the right of Need Credentials.

When the credentials for the Policy Manager Proxy Server are required they must be provided; otherwise, the Proxy Server may fail to connect to the Policy Manager.

23. Type the user name for the User Name credential.

24. Type the password for the Password credential.
25. Click OK to save the ESRS configuration.

**Re-provision ESRS**

**Before you begin**

EMC Secure Remote Support (ESRS) must be provisioned completely and enabled before you can re-provision the ESRS.

To re-provision ESRS, you must be logged in with root privileges.

**Procedure**

1. Select System.
2. From the task list, under Service Tasks, select Manage EMC Secure Remote Support.
   For a VNX with two Control Stations, a dialog box for selecting the target Control Station (Primary or Standby) appears first. The Primary Control Station will be selected by default. If necessary, change the selection and click Continue to navigate to the Manage ESRS page for the corresponding Control Station.
   As an alternate method to access the provisioned ESRS parameters, under Service Tasks, select Manage Connect Home and click Manage ESRS Settings in the ESRS Priority field. This link navigates directly to the Manage ESRS page for the primary Control Station. To manage the ESRS on a standby Control Station, you must select Manage EMC Secure Remote Support from the task list under Service Tasks.
3. Click the check box to the right of Re-provision.
4. Select either EMC Online Support (Powerlink) or RSA SecurID for the Type credential.
   The EMC support credentials are required for ESRS.
   If you select RSA SecurID, be aware that the SecurID is valid for only 60 seconds. The SecurID password may expire while you fill in the remaining fields.
5. Type the user name for the User Name credential.
6. Type the password for the Password credential.
7. Make any necessary changes to the Proxy Server or Policy Manager parameters.
   To add a Proxy Server, you must select the check box to the right of Use Proxy Server for ESRS and provision the related fields. To change existing Proxy Server information, you must unselect then select the check box to the right of Use Proxy Server for ESRS and re-provision the related fields.
8. Click OK to save the changes.

**International toll-free numbers**

The Connect Home dialing configuration must change if any of the following were to apply:

- If the customer is outside the U.S. or Canada, refer to the list of international toll-free numbers.
- If the customer-supplied telephone line does not use the prefix 9 to reach an outside line, change the dialing prefix.
- If the customer is located in a country that does not use the U.S.-style dial tone, such as Germany, disable dial tone detection on the modem.
- If the customer has an MT5634ZBA modem (check the label on the bottom of the modem or on the box that the modem shipped in), you might need to run a special utility to set the correct country/regional code.
<table>
<thead>
<tr>
<th>Country</th>
<th>AT&amp;T 1800</th>
<th>MCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>0800-444-0932</td>
<td>0-800-3330327</td>
</tr>
<tr>
<td>Australia (AU)</td>
<td>10800-150-072</td>
<td>1-800-148291</td>
</tr>
<tr>
<td>Austria</td>
<td>0800-200-288</td>
<td>0800-292575</td>
</tr>
<tr>
<td></td>
<td>866-285-3258</td>
<td></td>
</tr>
<tr>
<td>Bahamas</td>
<td>1-866-282-3258</td>
<td>1-8662216493</td>
</tr>
<tr>
<td>Bahrain</td>
<td>8000-960</td>
<td></td>
</tr>
<tr>
<td>Belgium (BG)</td>
<td>0800-7-2692</td>
<td>0800-78824</td>
</tr>
<tr>
<td>Brazil (BZ)</td>
<td>000811-005-9773</td>
<td>0800-891-0678</td>
</tr>
<tr>
<td>Chile (CH)</td>
<td>1230-020-0133</td>
<td>123-0-020-2855</td>
</tr>
<tr>
<td>China (Netcom Group) (CI)</td>
<td>10-800-711-0288</td>
<td>10-800-712-0654</td>
</tr>
<tr>
<td>China (Telecom South) (CI)</td>
<td>10-800-110-0288</td>
<td>10-800-120-0654</td>
</tr>
<tr>
<td>Colombia (CL)</td>
<td>980912-1659</td>
<td>01800-9-155034</td>
</tr>
<tr>
<td>Costa Rica (CR)</td>
<td>0-800-011-0794</td>
<td>0800-012-0994</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>800-142-409</td>
<td></td>
</tr>
<tr>
<td>Denmark (DK)</td>
<td>80-884824</td>
<td>80-883573</td>
</tr>
<tr>
<td>Dominican Republic (DR)</td>
<td>1-866-285-3258</td>
<td>1-888-156-1787</td>
</tr>
<tr>
<td>Finland (FI)</td>
<td>08001-1-7491</td>
<td>0-800-1-19810</td>
</tr>
<tr>
<td>France (FR)</td>
<td>0800-90-7131</td>
<td>0800-908817</td>
</tr>
<tr>
<td>Germany (GE)</td>
<td>0800-182-7792</td>
<td>0800-1009325</td>
</tr>
<tr>
<td>Greece (GR)</td>
<td>00-800-11-005-9773</td>
<td>00800-12-5546</td>
</tr>
<tr>
<td>Guam (U.S. Trust Territory)</td>
<td>1-866-285-3258</td>
<td></td>
</tr>
<tr>
<td>Guanya</td>
<td></td>
<td>1-866-820-7113</td>
</tr>
<tr>
<td>Hong Kong (HK)</td>
<td>800-96-6548</td>
<td>800-900982</td>
</tr>
<tr>
<td>Hungary (HU)</td>
<td>06-800-12-038</td>
<td>06-800-14445</td>
</tr>
<tr>
<td>Indonesia (ID)</td>
<td>001-803-1-005-9773</td>
<td>001-803-011-2869</td>
</tr>
<tr>
<td>Ireland (IR)</td>
<td>1-800-55-3878</td>
<td>1-800-55-7532</td>
</tr>
<tr>
<td>Israel (IS)</td>
<td>1-800-941-9773</td>
<td>1-800-930-3020</td>
</tr>
<tr>
<td>Italy (IT)</td>
<td>800-783283</td>
<td>800-782106</td>
</tr>
<tr>
<td>Japan (JP)</td>
<td>00531-11-5188</td>
<td>00531-1-20466</td>
</tr>
<tr>
<td>Korea (KO)</td>
<td>00798-1-1-005-9773</td>
<td>00798-14-800-5139</td>
</tr>
<tr>
<td>Latvia (LV)</td>
<td>800-0013</td>
<td></td>
</tr>
<tr>
<td>Luxembourg (LX)</td>
<td>800-23011</td>
<td>8002-9833</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1-800-80-5830</td>
<td>1-800-8-04295</td>
</tr>
</tbody>
</table>
### Table 16 International toll-free numbers (continued)

<table>
<thead>
<tr>
<th>Country</th>
<th>AT&amp;T 1800</th>
<th>MCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico (MX)</td>
<td>001-866-285-3258</td>
<td>001-8663644901</td>
</tr>
<tr>
<td>Netherlands (NL)</td>
<td>0800-023-2361</td>
<td>0800-0224963</td>
</tr>
<tr>
<td>New Zealand (NZ)</td>
<td>0800-103519</td>
<td>0800-446336</td>
</tr>
<tr>
<td>Nicaragua (NI)</td>
<td></td>
<td>001-800-2201512</td>
</tr>
<tr>
<td>Norway (NW)</td>
<td>800-15798</td>
<td>800-12660</td>
</tr>
<tr>
<td>Peru</td>
<td>0800-50997</td>
<td>0800-51592</td>
</tr>
<tr>
<td>Philippines (PH)</td>
<td>1-800-1-111-0841</td>
<td>1-800-1-114-1093</td>
</tr>
<tr>
<td>Poland (PD)</td>
<td>0-0-800-111-1422</td>
<td>00-800-1112812</td>
</tr>
<tr>
<td>Portugal (PO)</td>
<td>800-8-11028</td>
<td>800-8-12381</td>
</tr>
<tr>
<td>Russia (RU)</td>
<td></td>
<td>8-10-8002-3153011 or 8-10-8022-1523011</td>
</tr>
<tr>
<td>Singapore (SI)</td>
<td>800-110-1285</td>
<td>800-1203666</td>
</tr>
<tr>
<td>South Africa</td>
<td>0800-990-808</td>
<td>080-09-99955</td>
</tr>
<tr>
<td>Spain (SP)</td>
<td>900-95-1215</td>
<td>900-961845</td>
</tr>
<tr>
<td>Sweden (SW)</td>
<td>020-79-0950</td>
<td>020-79-6581</td>
</tr>
<tr>
<td>Switzerland (SZ)</td>
<td>0800-56-4581</td>
<td>0800-835421</td>
</tr>
<tr>
<td>Taiwan (TW)</td>
<td>0080-10-3965</td>
<td>00801-13-7087</td>
</tr>
<tr>
<td>Thailand (TH)</td>
<td>001800-11-005-9773</td>
<td>001-800-12-066-3916</td>
</tr>
<tr>
<td>Turkey (TU)</td>
<td>00-800-13-005-9773</td>
<td>00-800-151-0964</td>
</tr>
<tr>
<td>UK</td>
<td>0800-028-7702</td>
<td>08-001696651</td>
</tr>
<tr>
<td>Uruguay (UR)</td>
<td>000-411-005-9773</td>
<td>000-413-598-2665</td>
</tr>
<tr>
<td>United States</td>
<td>866-285-3258</td>
<td>800-527-0941</td>
</tr>
<tr>
<td>Venezuela</td>
<td>0800-1-00-2043</td>
<td>0800-1-00-2404</td>
</tr>
</tbody>
</table>

---

**Set the country code on the MT5634ZBA modem**

If the customer has a MT5634ZBA modem (check the label on the bottom of the modem or on the box that the modem shipped in) you might need to run a special utility to set the correct country or regional code. The modem ships with a default value for the country or regional code. The default value might not be appropriate for the location of the system.

*Manual instructions for setting the country code on page 92* provides more information if your service laptop is not a Microsoft Windows-based PC. If your service laptop is a Microsoft Windows-based PC, then the procedure explained in the Windows-based PC instructions that follow has more information.
Note

If you need to verify the country or regional code that is configured on the modem, you must use the manual instructions.

Procedure

1. Download the latest version of the ZBAWizard.exe utility:
   a. In a web browser on your service laptop go to the Global Services website: http://www.cs.isus.EMC.com/
   b. Click the Application Download Area hyperlink.
   c. Click the ZBA Global Modem Wizard hyperlink.
   d. Click the ZBAWizard.exe hyperlink to download the executable.
   e. Click Save and select a location on your service laptop to save the file. This application will be run at a later step in the procedure, so ensure that you know where the file is.

2. Connect the serial cable from the modem to your service laptop.

   Note

   Ensure that the modem is powered on.

4. Type EMC (case-sensitive) and click OK when prompted for the decryption password. The Global Wizard application appears, as displayed.
5. Click Next to begin the wizard. The wizard will now try to contact the modem. Wait for modem detection. If this does not occur, verify that the modem is powered on and the serial cable is securely connected at both ends.
6. Click Next when the modem is found.
7. If the following message appears, click OK to acknowledge the message.
8. Select or verify that the correct country or region is selected, as displayed. Click Next. A confirmation screen appears with your selection.
9. Click Next on the confirmation screen.
10. Click Finish to exit the wizard. This completes the procedure.

Manual instructions for setting the country code

To manually set the country or region code without ZBAWizard.exe:

Procedure

1. Connect the serial cable from the modem to your service laptop.

   Note

   Ensure that the modem is powered on.

2. Open a terminal emulator session by using the following settings:
   - 19200 bits per second
   - 8 data bits
3. Type the following command to check the current country or regional setting:
   
   ```
   ATI9
   9
   ```
   
   The decimal value associated with the country or region code is output to the terminal emulator session. **MT5634ZBA modem country/region codes on page 94** details the list of countries and their decimal values.

   For example:
   ```
   +++
   + ATI9
   952
   2(?$MT500C1\MODEM\TIA0602, TIA0578\MultiTech Systems
   MT5634ZBAV92A9)
   OK
   ```

4. If the country or region code needs to be changed, type the following command:
   
   ```
   AT%T19,0, <modem_hex_value>
   ```

   where `<modem_hex_value>` is the hex value for the country or region code. **MT5634ZBA modem country/region codes on page 94** provides more information.

   For example:
   ```
   AT%T19,0,1
   1OK
   ```

5. Type the following command to confirm that the current country or regional setting was changed correctly:
   
   ```
   ATI9
   ```

   The decimal value associated with the country or region code is output to the terminal emulator session. **MT5634ZBA modem country/region codes on page 94** details the list of countries and their decimal values.

   This completes the procedure.

   **Table 17 MT5634ZBA modem country/region codes**

<table>
<thead>
<tr>
<th>Country</th>
<th>Region config. command (Hex)</th>
<th>ATI9 result code (Decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>AT%T19,0,1</td>
<td>1</td>
</tr>
<tr>
<td>Hong Kong, Hungary, India, Indonesia, Israel, Korea, Malaysia, Republic of Korea, Philippines, Poland, Singapore, Slovenia, Vietnam</td>
<td>AT%T19,0,30</td>
<td>48</td>
</tr>
<tr>
<td>Japan</td>
<td>AT%T19,0,10</td>
<td>16</td>
</tr>
<tr>
<td>New Zealand</td>
<td>AT%T19,0,9</td>
<td>9</td>
</tr>
<tr>
<td>South Africa</td>
<td>AT%T19,0,35</td>
<td>53</td>
</tr>
<tr>
<td>Afghanistan, Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Antigua and Barbuda, Argentina, Armenia, Aruba,</td>
<td>AT%T19,0,34</td>
<td>52</td>
</tr>
</tbody>
</table>
### Table 17 MT5634ZBA modem country/region codes (continued)

<table>
<thead>
<tr>
<th>Country</th>
<th>Region config. command (Hex)</th>
<th>AT%T result code (Decimal)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria, Azerbaijan, Bahamas, Bahrain, Bangladesh, Barbados, Belarus,</td>
<td>AT%T19,0,34</td>
<td>52</td>
</tr>
<tr>
<td>Belgium, Belize, Benin, Bermuda, Bhutan, Bolivia, Bosnia and Herzegovina,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botswana, Brazil, Brunei Darussalam, Bulgaria, Burkina Faso, Burundi,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cambodia, Cameroon, Canada, Canary Islands, Cape Verde, Cayman Islands,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central African Republic, Chad, Chile, China, Colombia, Congo, The</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Democratic Republic of Congo, Cook Islands, Costa Rica, Côte D’Ivoire,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Croatia, Cyprus, Czech Republic, Denmark, Djibouti, Dominica,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dominican Republic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>East Timor, Ecuador, Egypt, El Salvador, Equatorial Guinea, Estonia,</td>
<td>AT%T19,0,34</td>
<td>52</td>
</tr>
<tr>
<td>Ethiopia, Faero Islands, Fiji, Finland, France, French Guiana, French</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guiana, French Polynesia, Gabon, Gambia, Georgia, Germany, Ghana,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gibraltar, Greece, Greenland, Grenada, Guadeloupe, Guam, Guatemala,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guernsey, C.I., Guinea, Guinea-Bissau, Guyana, Haiti, Holy See</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Vatican City State), Honduras, Iceland, Iran, Iraq, Ireland, Isle of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Man, Italy, Jamaica, Jersey C.I., Jordan, Kazakhstan, Kenya, Kiribati,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kuwait, Kyrgyzstan, Lao People’s Democratic Republic, Latvia, Lebanon,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liberia, Libya, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Former Yugoslav Republic of, Madagascar, Malawi, Maldives, Mali,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malta, Martinique, Mauritania, Mauritius, Mayotte, Mexico, Moldova,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Republic of Monaco, Mongolia, Montserrat, Morocco, Mozambique</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Namibia, Nauru, Nepal, Netherlands, Netherlands Antilles, New</td>
<td>AT%T19,0,34</td>
<td>52</td>
</tr>
<tr>
<td>Caledonia, Nicaragua, Niger, Nigeria, Norway, Oman, Pakistan, Palestine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Territory, Occupied, Panama, Papua New Guinea, Paraguay, Peru, Portugal,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Puerto Rico, Qatar, Reunion, Romania, Russian Federation, Rwanda,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samoa, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Slovakia,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solomon Islands, Spain, Sri Lanka, Sudan, Surinam, Swaziland, Sweden,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switzerland, Syrian Arab Republic, Taiwan, Tajikistan, Tanzania, United</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Republic of, Thailand, Tahiti, Togo, Tonga, Trinidad and Tobago,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunisia, Turkey, Turkmenistan, Turks and Caicos Islands, Uganda,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ukraine, United Arab Emirates, United Kingdom, Uruguay, USA, Uzbekistan,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vanuatu, Venezuela, Virgin Islands, British, Virgin Islands, Yemen,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yugoslavia, Zambia, Zimbabwe</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Interpret log files

Log files contain messages to assist you in determining what is happening with the VNX. Some logs have information about the state of the VNX, while others have information about errors. The system log (sys_log) must be viewed using the nas_logviewer command when viewing the log from the CLI.

- Location of VNX logs on page 96
Location of VNX logs

VNX log files on page 96 provides a complete list of VNX File logs.

**Note**

To view VNX logs located in the `/nas/log` directory, use the `nas_logviewer` command to format and view these log files.

For example, to view the last 50 entries to the `/nas/log/sys_log` file tersely formatted, use the logviewer command in the following manner:

```
$ /nas_logviewer -t /nas/log/sys_log|tail -50
```

<table>
<thead>
<tr>
<th>Log</th>
<th>Command line or log location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td><code>$ /nas/log/cmd_log</code></td>
<td>Displays a list of all successful commands executed for the VNX File.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Commands displaying information only and most commands in the /nas/sbin directory are not logged.</td>
</tr>
<tr>
<td>Command</td>
<td><code>$ /nas/log/cmd_log.err</code></td>
<td>Lists all the failed commands issued by the administrator. Commands</td>
</tr>
<tr>
<td></td>
<td></td>
<td>displaying information only and most commands in the /nas/sbin directory are not logged.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the <code>-s</code> option to display logs with a user-friendly timestamp.</td>
</tr>
<tr>
<td>Data Mover</td>
<td><code>$ server_log &lt;movename&gt;</code></td>
<td>Displays the current log updates from the most recent restart.</td>
</tr>
<tr>
<td></td>
<td><code>$ server_log &lt;movename&gt; -a</code></td>
<td>Displays the available history of logs for a Data Mover.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Use the <code>-s</code> option to display logs with a user-friendly timestamp.</td>
</tr>
<tr>
<td>System</td>
<td><code>$ /nas/log/sys_log</code></td>
<td>Displays a cumulative list of system event and log messages from the most recent Control Station restarts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use this command to format system logs: <code>nas_logviewer -f /nas/log/sys_log</code></td>
</tr>
<tr>
<td>OS system</td>
<td><code>$ /nas/log/osmlog</code></td>
<td>Lists events related to the Control Station operating-system operation.</td>
</tr>
<tr>
<td>ConnectHome</td>
<td><code>$ /nas/log/ConnectHome</code></td>
<td>Stores each CallHome pending in XML format.</td>
</tr>
<tr>
<td>SIB POST</td>
<td><code>$ /nas/log/sibpost_log</code></td>
<td>Displays results from Control Station hardware tests performed at boot time.</td>
</tr>
</tbody>
</table>
Table 18 VNX log files (continued)

<table>
<thead>
<tr>
<th>Log</th>
<th>Command line or log location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMC Symmetrix™ API</td>
<td>$/nas/log/symapi.log</td>
<td>Lists events from the SYMAPI layer generated as the VNX File interacts with an attached Symmetrix system. The Symmetrix documentation provides more information about these messages.</td>
</tr>
<tr>
<td>Installation and upgrade</td>
<td>$/nas/log/instcli.log</td>
<td>Stores log SYMCLI installation.</td>
</tr>
<tr>
<td></td>
<td>$/nas/log/install.&lt;NAS_Code_Version&gt;.log</td>
<td>NAS code installations and upgrades.</td>
</tr>
<tr>
<td></td>
<td>$/nas/log/upgrade.&lt;NAS_Code_Version&gt;.log</td>
<td></td>
</tr>
</tbody>
</table>

Read log messages

Each type of log has a slightly different format. This section explains the formats by displaying a line of the log with an explanation of the component parts.

Server log
Example:
2012-03-15 04:38:04: ADMIN: 4: Command succeeded: logsys add output> disk=root_log_2 bufsz=256

Server log components on page 97 provides a complete list of Server log components using the example shown above.

Table 19 Server log components

<table>
<thead>
<tr>
<th>Log component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Displays the date.</td>
<td>2012-03-15</td>
</tr>
<tr>
<td>Time</td>
<td>Displays the time.</td>
<td>04:38:04</td>
</tr>
<tr>
<td>Category</td>
<td>Lists the part of the VNX File where the error originates. Server log message category on page 98 provides a complete list of categories.</td>
<td>ADMIN</td>
</tr>
<tr>
<td>Severity level</td>
<td>Indicates the importance of the event. Values can be 0 through 7, with 0 indicating the highest level of importance. Server log and system log severity levels on page 98 describes these levels. The default severity for each module is set to 4. Whenever the Data Mover tries to generate a log message, it provides the log severity level and the module name. If the given severity is less than or equal to the current severity level for the given module, the message goes to server log; otherwise, it is ignored.</td>
<td>4</td>
</tr>
<tr>
<td>Message text</td>
<td>The log message.</td>
<td>Command succeeded:</td>
</tr>
</tbody>
</table>
Table 19  Server log components (continued)

<table>
<thead>
<tr>
<th>Log component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
|               |             | • logsys add output>
|               |             | • disk=root_log_2
|               |             | • bufsz=256 |

Server log and system log severity levels on page 98 provides a complete list of server log and system log severity levels.

Table 20  Server log and system log severity levels

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Meaning</th>
<th>Severity level</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency</td>
<td>4</td>
<td>Warning</td>
</tr>
<tr>
<td>1</td>
<td>Alert</td>
<td>5</td>
<td>Notice</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>6</td>
<td>Info</td>
</tr>
<tr>
<td>3</td>
<td>Error</td>
<td>7</td>
<td>Debug</td>
</tr>
</tbody>
</table>

Server log message category on page 98 provides a list of server message category types.

Table 21  Server log message category

<table>
<thead>
<tr>
<th>Category</th>
<th>Explanation</th>
<th>Category</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN</td>
<td>Status of commands issued to the VNX File</td>
<td>PAX</td>
<td>Portable Archive Exchange for backup</td>
</tr>
<tr>
<td>BOOT</td>
<td>CPU boot</td>
<td>RCPD</td>
<td>VNX Replicator remote copy daemon messages</td>
</tr>
<tr>
<td>CAM</td>
<td>Common Access Method layer, typically storage-system related</td>
<td>RPC</td>
<td>Remote Procedure Call</td>
</tr>
<tr>
<td>CFS</td>
<td>Common File System, generic file system information, not specific to UxFS</td>
<td>SECURITY</td>
<td>Security messages</td>
</tr>
<tr>
<td>CVFS</td>
<td>Checkpoint Virtual File System</td>
<td>SHADOW</td>
<td>Shadow directory messages</td>
</tr>
<tr>
<td>DRIVERS</td>
<td>Device driver messages (for example, SCSI, Fibre Channel, NIC)</td>
<td>SMB</td>
<td>CIFS services</td>
</tr>
<tr>
<td>FMP and MPFS</td>
<td>MPFS server and file system</td>
<td>STORAGE and CHAMII</td>
<td>Similar to CAM — messages related to the storage system storage devices</td>
</tr>
<tr>
<td>FSTOOLS</td>
<td>File system monitoring</td>
<td>SVFS</td>
<td>EMC SnapSure™ checkpoint activity</td>
</tr>
</tbody>
</table>
### Table 21 Server log message category (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Explanation</th>
<th>Category</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTPD</td>
<td>FTP daemon</td>
<td>SYSTEM</td>
<td>Environment monitor-related messages (for example, SIB attention status and bit errors)</td>
</tr>
<tr>
<td>HTTPD</td>
<td>HTTP daemon</td>
<td>TCP</td>
<td>TCP layer messages</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol (IP) layer messages (for example, address block allocation/release and route changes)</td>
<td>TIMESRVC</td>
<td>Time service activity messages (for example, NTP)</td>
</tr>
<tr>
<td>KERBEROS</td>
<td>Kerberos-related messages (for example, domain join)</td>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>KERNEL</td>
<td>Data Mover motherboard and BIOS messages</td>
<td>UFS</td>
<td>File system messages</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol-related messages</td>
<td>VC</td>
<td>Antivirus-checking related</td>
</tr>
<tr>
<td>LIB</td>
<td>Library-related messages</td>
<td>VERSION</td>
<td>Data Mover version</td>
</tr>
<tr>
<td>LOCK</td>
<td>Lock manager messages (for example, statd for NFS)</td>
<td>VMCAST</td>
<td>EMC VNX Replicator volume multicasting</td>
</tr>
<tr>
<td>MGFS</td>
<td>Migration File System</td>
<td>VRPL</td>
<td>VNX Replicator</td>
</tr>
<tr>
<td>NDMP</td>
<td>Network Data Management Protocol information</td>
<td>XLT</td>
<td>I18N or Unicode messages</td>
</tr>
<tr>
<td>NFS</td>
<td>NFS information (for example, exports and cache activity)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### System log

**System log components on page 99** provides a complete list of system log components.

**Example:**

Jun 24 10:39:46 2011 BoxMonitor:2:101 Slot 1 reason code of 0 is stale

### Table 22 System log components

<table>
<thead>
<tr>
<th>Log component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time</td>
<td>Displays the date and time.</td>
<td>Jun 24 10:39:46 2011</td>
</tr>
<tr>
<td>Facility</td>
<td>Identifies the part of the system generating the message text.</td>
<td>BoxMonitor</td>
</tr>
<tr>
<td>Severity level</td>
<td>Indicates the importance of the event. Values can be 0 through 7, with 0 indicating the highest level of importance. <strong>Server log and system log severity levels on page 98</strong> describes these levels.</td>
<td>2</td>
</tr>
</tbody>
</table>
### Table 22 System log components (continued)

<table>
<thead>
<tr>
<th>Log component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event ID</td>
<td>Identifies the event associated with the facility. <em>EMC VNX Command Line Interface Reference for File</em> provides more details on the nas_event command.</td>
<td>101</td>
</tr>
<tr>
<td>Event text</td>
<td>Displays the log message.</td>
<td>Slot 1 reason code of 0 is stale</td>
</tr>
</tbody>
</table>

Some of the facilities that generate messages are explained in *System log facilities on page 100*.

### Table 23 System log facilities

<table>
<thead>
<tr>
<th>Facility</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BoxMonitor</td>
<td>Monitors hardware components presence, interrupts, and alarms.</td>
</tr>
<tr>
<td>MasterControl</td>
<td>Monitors required system processes.</td>
</tr>
<tr>
<td>CallHome</td>
<td>Contains messages related to the CallHome feature.</td>
</tr>
</tbody>
</table>

### Command log and command error log

**Example:**

```
2005-03-15 09:52:36.075 db:0:9558:S: /nas/bin/nas_acl -n nasadmin -c -u
201 level=2
server_2
-get group /nas/server/slot_2/group.nbk: No such file or directory
```

*Command log components on page 100* lists the command log components using the example shown above.

### Table 24 Command log components

<table>
<thead>
<tr>
<th>Log component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Displays the date.</td>
<td>2005-03-15</td>
</tr>
<tr>
<td>Time</td>
<td>Displays the time.</td>
<td>09:52:36.075</td>
</tr>
<tr>
<td>Source</td>
<td>Indicates where the command or error originates.</td>
<td>db</td>
</tr>
<tr>
<td>User ID</td>
<td>Indicates the user who issued the command.</td>
<td>0</td>
</tr>
</tbody>
</table>
| Note          | - 0=root
               - 201=nasadmin |
| Process ID    | A system-generated identifier. | 9558 |
Table 24 Command log components (continued)

<table>
<thead>
<tr>
<th>Log component</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning and end</td>
<td>Displays the beginning (S) and end (E) of the command. If there is not an S</td>
<td>S</td>
</tr>
<tr>
<td>markers</td>
<td>and E pair, the command did not complete.</td>
<td></td>
</tr>
<tr>
<td>Message text</td>
<td>• The command log displays</td>
<td>/nas/bin/nas_acl -n nasadmin</td>
</tr>
<tr>
<td></td>
<td>commands.</td>
<td>-c -u 201</td>
</tr>
<tr>
<td></td>
<td>• The command error log displays</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the command and the error.</td>
<td></td>
</tr>
</tbody>
</table>

VNX and RSA Envision

To make VNX storage systems even more secure, they also leverage the continuous collecting, monitoring, and analyzing capabilities of RSA enVision. RSA enVision performs the following functions:

- **Collects logs** - Collects event log data from over 130 event sources - from firewalls to databases. RSA enVision can also collect data from custom, proprietary sources using standard transports such as Syslog, OBDC, SNMP, SFTP, OPSEC, or WMI.

- **Securely stores logs** - Compresses and encrypts log data so that it can be stored for later analysis, while maintaining log confidentiality and integrity.

- **Analyzes logs** - Analyzes data in real time to check for anomalous behavior that requires an immediate alert and response. The RSA enVision proprietary logs are also optimized for later reporting and forensic analysis. Built-in reports and alerts allow administrators and auditors quick and easy access to log data that is easy to understand.

RSA enVision collects and analyzes administrative events logged by VNX storage systems, and creates logs of this information that it stores on the VNX storage system. This gives auditors easy access to scheduled and unscheduled reports about administrative events that occurred on VNX storage systems; the auditor does not have to access the actual device itself or have knowledge of VNX administrative applications. Specific use cases include:

- Providing an audit trail for making copies of data
- Alerting and reporting when replication services malfunction
- Creating reports on daily device configuration changes
- Creating alerts and reports about user actions
- Creating alerts about disks that are removed

NAS or SAN environment rules

When you connect a SAN configuration to the VNX, you create a NAS or SAN configuration. A NAS or SAN configuration has rules for RAID types, LUN allocation, and array read or write cache settings that you must consider. VNX File/VNX for Block NAS and SAN environment considerations on page 102 lists these considerations.

If needed, contact the EMC Customer Support or your service provider for help with template selection. The EMC E-LabTM Interoperability Navigator explains how to
configure CLARiiON CX, CLARiiON CX3, CLARiiON CX4, VNX for Block storage arrays by using predefined templates and is available at http://Support.EMC.com.

After logging in, go to Support › Interoperability and Product Lifecycle Information › E-Lab Interoperability Navigator.

**Note**

The E-Lab Interoperability Navigator provides information on supported NAS or SAN environments.

### Table 25 VNX File/VNX for Block NAS and SAN environment considerations

<table>
<thead>
<tr>
<th>Category</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID types</td>
<td>• For detailed information about RAID types and LUN usages see the <em>EMC Unified Storage Best Practices for Performance and Availability Common Platform and Block Storage 31.0: Applied Best Practices</em> found on Powerlink.</td>
</tr>
<tr>
<td></td>
<td>• The Vault drives containing the VNX control LUNs uses about 192 GB of their per-drive capacity for system files. The portion of the drives not used for the system files is user configurable. A RAID group for traditional LUNs may be created there. To provision system drives for the highest usable capacity they can be configured as a four drive RAID level 5 (3+1) and used to host traditional LUNs.</td>
</tr>
<tr>
<td></td>
<td>• There are no RAID-type restrictions for LUNs on a SAN. RAID groups consisting of only SAN LUNs might be configured with any number of disks supported by the VNX for Block system.</td>
</tr>
<tr>
<td></td>
<td>• On a single shelf, you can configure mixed RAID types.</td>
</tr>
<tr>
<td>Allocation of LUNs</td>
<td>• The RAID group containing the VNX File control LUNs must be dedicated to NAS. No SAN LUNs might reside on this RAID group. LUN numbers 0 to 15 are dedicated to VNX File control LUNs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Any attempt to allocate storage in a LUN number between 0-15 will result in Error 3147: volume &lt;disk-id&gt; resides on a reserved disk. If a reserved disk is already used in an AVM storage pool, no additional storage will be allocated from the volume built on the reserved disk. This restriction affects only new space allocation. Existing file systems will continue to function normally. If you see this error, contact your EMC Customer Support representative so corrective action can be taken.</td>
</tr>
<tr>
<td></td>
<td>• All other RAID groups are not restricted to all SAN or all NAS. The RAID group can be sliced up into LUNs and distributed to either a SAN or NAS environment.</td>
</tr>
<tr>
<td></td>
<td>• RAID groups do not have to be split into two, four, or eight equal-size NAS LUNs, but they must be balanced across the array. This means an equal number of same-size NAS LUNs must be spread across storage processor (SP) A and SP B.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If you do not configure the LUNs across SP A and SP B properly, you will not be able to manage the LUNs by using the Unisphere software.</td>
</tr>
<tr>
<td>Array read/write</td>
<td>For the VNX File with a VNX for block integrated array, set the read or write caches with the following principle: the rule of the thumb is to allocate one third of memory for read cache and two thirds for write cache (remember that read cache is for prefetch and that if data is in the write cache, it is read from cache, not from disk).</td>
</tr>
<tr>
<td>cache settings</td>
<td></td>
</tr>
</tbody>
</table>
Table 25 VNX File/VNX for Block NAS and SAN environment considerations (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>For gateway servers, write cache is required. The VNX for Block documentation provides more details on settings.</td>
</tr>
<tr>
<td><strong>Standard parameters and settings when binding LUNs</strong></td>
<td>These parameters or settings must be enabled or disabled as follows:</td>
</tr>
<tr>
<td></td>
<td>• Enable write cache</td>
</tr>
<tr>
<td></td>
<td>• Enable read cache</td>
</tr>
<tr>
<td></td>
<td>• Disable auto-assign for each LUN</td>
</tr>
<tr>
<td></td>
<td>• Disable clariion no_tresspass</td>
</tr>
<tr>
<td></td>
<td>• Disable failovermode</td>
</tr>
<tr>
<td></td>
<td>• Disable arraycommpath</td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION</strong></td>
</tr>
<tr>
<td></td>
<td>To prevent file system corruption, the arraycommpath setting should not be changed while the server is online. The server should be taken offline to change this setting.</td>
</tr>
<tr>
<td><strong>EMC MirrorView™, EMC SnapView™, and EMC SAN Copy™</strong></td>
<td>VNX for block, MirrorView, SnapView, and SAN Copy are not supported on NAS-allocated LUNs.</td>
</tr>
</tbody>
</table>

### VNX for file problem information

For problems with Unisphere or the VNX for file, EMC recommends that before contacting the service provider or EMC for help, you should run log collection promptly. The sooner the collection script is run, the more likely that command output, logs, and dump files that can help correct the problem can be collected.

The tasks for collecting problem information are:

- Enable Automatic Log Transfer from Unisphere on page 105
- Run Log Collection from the CLI on page 105

Use CLI options to perform script operations on page 106 details the command options available to perform script operations for VNX for file.

### Automatically collect and transfer logs

The Automatic Collection and Transfer tool aids in troubleshooting and resolving system errors and other problems with a VNX for file that is configured to issue a call home. When VNX for file services are running, the collection script runs automatically in the background on the Control Station. It collects and saves command output, logs, and dump files related to events that produce a CallHome. Examples of such events include Data Mover panics and Replication session failures. If you enable Automatic Transfer, the Control Station automatically transfers this information to a preconfigured FTP server when it is generated.
As the script does not run during system installations and upgrades, it does not collect events that might occur during those operations.

The tool produces zipped archive files of logs needed to analyze issues, and writes these files to /nas/var/emcsupport. This tool also collects Data Mover panic dumps when they occur with support materials. The Data Mover panic dumps are stored in the directory /nas/var/dump. After collecting logs and files, if the transfer script is enabled, the tool automatically transfers the collected data to EMC by using the configured transport mode (such as Monitoring Station HTTPS). By default, the transfer capability is disabled.

A maximum of 460 MB is used for archiving log collections and a maximum of two Data Mover panic dumps. If the logs and dumps specified in the configuration file have reached the maximum, the tool deletes the oldest log to make room for new logs. However, the tool leaves old dumps in place, so those have to be manually deleted from the dump directory.

When the tool successfully transfers a Data Mover panic dump to /nas/var/dump, it automatically clears the dump partition. If two dumps already exist in the dump area, the tool logs a message to sys_log, indicating that it cannot extract any further dumps to /nas/var/dump until unneeded dumps are manually deleted.

The system logs contain entries each time a dump is transferred by the configured transport mode to EMC Customer Service. If the tool is invoked manually, the command output and any other important messages are logged in /nas/log/sys_log.

If the configuration file has used the entire serial number string to identify dumps, the location of the dump transfer might be truncated in sys_log. If this occurs, even though the system log might not report the complete transfer location, the transfer is successful, as recorded in the log. Administrator or root user privileges are needed to invoke the Automatic Collection and Transfer tool, which is run from the command line interface (CLI). You also might be asked by an EMC Customer Support Representative to run the tool to diagnose and solve system problems.

The first time the master script runs, it creates the configuration file /nas/site/automaticcollection.cfg. This file contains lines that set various parameters to manage the collection and transfer processes. For instance, it determines the location from which the files are transferred, and, in the case of FTP as the configured transport mode, it automatically sets the username and password for transfer files if the automatic transfer capability is enabled. If the configuration file is changed, the automatic collection script does not re-create it. In this case, to return to the default configuration file, rename or remove the edited configuration file from the system.

However, apart from disabling the tool or changing the part of the file related to the transport mode configuration, EMC strongly recommends that you use the default values in this file. Otherwise, it is possible that the tool could consume more Control Station resources than are necessary.

The configuration file manages the following information:

- Whether to disable the automatic transfer capability.
- The number of dumps to retain in the /nas/var/dump directory. The default is 2.
Enable Automatic Log Transfer from Unisphere

The Automatic Log Transfer tool is a support feature in VNX for file. Log Collection is enabled by default. The system automatically collects and compresses logs and dumps when certain events are generated. Support materials, logs, and dumps are saved locally on the Control Station. After collecting logs and files, you can configure the system to automatically transfer the collected data to EMC. The Automatic Transfer option is disabled by default. When you enable Automatic Transfer, the system will automatically transfer the support materials collected—both logs and dumps—from the Control Station to a pre-configured transport mode, such as FTP or Monitoring Station HTTPS.

To enable automatic transfer:

Procedure
1. Select the system.
3. In the dialog box that appears, select Enable Automatic Transfer and click Apply.

Run Log Collection from the CLI

You might be asked by an EMC Customer Support Representative to run the automatic collection script on the Control Station.

To run the log collection script to create the support materials file, perform the following:

Procedure
1. Log in to the control station as nasadmin and then switch (su) to root.
2. To run the script, type the complete path:
   
   Select `/nas/tools/automaticcollection -getlogs`

3. The script compiles the VNX for file support information into a compressed file and saves the file in the `/nas/var/log` directory. The file is given the name:

   `support_materials_<serial number>.<ymdhhss>.zip`

   where:

   `<serial number>` = the serial number of the VNX for file.

   `<ymdhhss>` = the date and the time the script was run.

   After you finish

   After creating the support materials file, contact the service provider or the EMC Customer Service Center for directions on how to deliver the file for analysis. Use CLI options to perform script operations on page 106 describes how to use the CLI options to perform several script operations.
Disable Automatic Collection and Transfer tool

To completely disable the Automatic Collection and Transfer tool, type:

```
$/nas/tools/automaticcollection -disable -all
```

An alternative method of disabling the entire tool is to edit the configuration file `/nas/site/automaticcollection.cfg` using a text editor such as `vi`, and uncomment the line containing the word `OFF`.

The following is an example of a configuration file output:

```
[nasadmin@bulls-cs ~]$ cat /nas/site/automaticcollection.cfg
# This is the configuration file for automaticcollection.
# Anything after the # character on that line is ignored.  Blank
# lines are also ignored.  Whitespace at the begining and end of each
# line is also ignored.
# To get back to the default configuration file, simply remove this
# file (or rename it, of course), and a new one will be created the
# next time automaticcollection runs.  You may change this file if
# you wish,
# and if you do so, automaticcollection will not recreate it.
# However, you will not receive any updates to this file should you
# choose to upgrade your control station software later.
# Don't modify the following line unless instructed by authorized
# service personnel.
# OFF
# Current version number
VERSION 2
# Uncomment the following line to disable the transfer feature.
# Disable
# Uncomment the following line to control the number of copies of
# panic dumps you would like to keep in /nas/var/dump directory.
# We strongly suggest to keep the default value.  The default is 2.
# MaxCopyDump 2
# Uncomment the following line to control the number of simultaneous
# transfer you will allow from the Control Station.  The default is
# 2, and it should not go any lower.
# MaxTransfer 2
# The following configurations are used by the transfer process.
# Please do not modify these unless instructed by authorized service
# personnel.
host ftp.emc.com
user anonymous
pass APM00055108049@emc.com
# Modify the following line to specify the remote directory where
# the materials should be stored.  The default is on the FTP server
# /incoming/APM00055108049 directory.
remote_directory /incoming/APM00055108049
```

Use CLI options to perform script operations

This section describes the available options, regardless of whether you invoke them yourself or at the request of EMC Customer Service. You must have administrator privileges to use this tool. Consequently, be sure to log in to the Control Station as `nasadmin` before using this tool.

Command options

To display a list of Automatic Collection and Transfer tool command options, type:

```
$/nas/tools/automaticcollection -help
```

Automatic Collection and Transfer tool command options on page 107 lists the Automatic Collection and Transfer tool’s command options and descriptions.
Table 26 Automatic Collection and Transfer tool command options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Displays the complete list of options.</td>
</tr>
<tr>
<td>-getlogs</td>
<td>Runs the collection script which, when complete, causes the logs to be transferred if the transfer script is enabled.</td>
</tr>
<tr>
<td>-filename &lt;filename&gt;</td>
<td>Includes additional information, such as the case number, in the filename.</td>
</tr>
<tr>
<td>-retrievedump</td>
<td>Extracts the most recent dump and then runs the transfer script for dumps if the transfer script is enabled.</td>
</tr>
<tr>
<td>-slot</td>
<td>Indicates the number of the slot from which to retrieve the dump.</td>
</tr>
<tr>
<td>-local</td>
<td>Writes the dump to a local directory.</td>
</tr>
<tr>
<td>-transferlogs</td>
<td>Runs the transfer script for logs. The script reviews timestamps on all collected logs in /nas/var/log and then transfers the most recent set of logs in this partition.</td>
</tr>
<tr>
<td>-config</td>
<td>Displays the current configuration.</td>
</tr>
<tr>
<td>-disable</td>
<td>Turns off the transfer script.</td>
</tr>
<tr>
<td>-enable</td>
<td>Turns on the transfer script.</td>
</tr>
<tr>
<td>-info</td>
<td>Checks the state of the transfer script.</td>
</tr>
</tbody>
</table>

User examples

The following examples describe the functions you are most likely to perform with the Automatic Collection and Transfer tool:

- To enable automatic transfer of file logs and dumps to EMC Customer Service, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -enable`

- To disable automatic transfer of log files and dumps if they have been previously enabled, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -disable`

- To completely turn off the Automatic Collection and Transfer tool, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -disable -all`

EMC Customer Service and support provider examples

The following examples describe the functions you might perform if asked to do so by EMC Customer Service or an authorized support provider:

- To run the collection script for logs, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -getlogs`

- To run the transfer script for dumps, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -retrievedump -slot <slot ID>`

- To run the transfer script for logs, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -transferlogs`

- To display the current configuration, at the command prompt, type:
  
  `$/nas/tools/automaticcollection -config`
Manage logging and alerting capabilities

- To check the state of the transfer script, at the command prompt, type:
  
  
  ```bash
  $/nas/tools/automaticcollection -info
  ```
As part of an effort to continuously improve and enhance the performance and capabilities of its product lines, EMC periodically releases new versions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, contact your EMC Customer Support Representative.

_Problem Resolution Roadmap for VNX_ contains additional information about using EMC Online Support and resolving problems.

Topics included in this chapter are:

- **EMC E-Lab Interoperability Navigator** ................................................................. 110
- **Error messages** ................................................................................................. 110
- **Error messages for Data Mover** ........................................................................ 110
- **EMC Training and Professional Services** ......................................................... 111
- **Recovery after an VNX SP failure** .................................................................... 111
- **Monitor system activity** ................................................................................... 111
- **System activity output** .................................................................................... 112
EMC E-Lab Interoperability Navigator

The EMC E-Lab™ Interoperability Navigator is a searchable, web-based application that provides access to EMC interoperability support matrices. It is available on EMC Online Support at http://Support.EMC.com. After logging in, in the right pane under Product and Support Tools, click E-Lab Navigator.

Error messages

All event, alert, and status messages provide detailed information and recommended actions to help you troubleshoot the situation.

To view message details, use any of these methods:

- **Unisphere software:**
  - Right-click an event, alert, or status message and select to view Event Details, Alert Details, or Status Details.

- **CLI:**
  - Type `nas_message -info <MessageID>`, where `<MessageID>` is the message identification number.

- **Celerra Error Messages Guide:**
  - Use this guide to locate information about messages that are in the earlier-release message format.

- **EMC Online Support:**
  - Use the text from the error message's brief description or the message's ID to search the Knowledgebase on EMC Online Support. After logging in to EMC Online Support, locate the applicable Support by Product page, and search for the error message.

Error messages for Data Mover

While using the system, various messages can appear indicating successful or unsuccessful command execution. Error messages can appear when there is a fault in a command syntax or a fault with the system. Normally, system messages are reported to the log files. Always check the system log (sys_log), which is produced by `server_log`, and the command error log (cmd_log.err) for message information. In some cases when a problem occurs, no message appears. Instead, system actions occur, which in turn, might indicate a problem. Data Mover problems on page 110 lists two examples that might occur with Data Movers.

Error messages indicating a problem with a Data Mover might also appear in the system log. Therefore, when troubleshooting, periodically check the log for the presence of certain error messages. These error messages appear only in the system log and do not appear on screen during an active session.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Probable cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Mover repeatedly stops responding.</td>
<td>Data Mover might have lost its connection either in its cabling</td>
<td>Restart the Data Mover and then check free space and memory. If</td>
</tr>
</tbody>
</table>
Table 27 Data Mover problems (continued)

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Probable cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>or from the network; or it might be out of memory or free space.</td>
<td></td>
<td>these appear acceptable, verify that all cables are secure. Then ping or view system uptime.</td>
</tr>
<tr>
<td>When attempting to view SCSI devices, the system stops responding.</td>
<td>Storage system is offline.</td>
<td>Verify the storage system is online, and then retry.</td>
</tr>
</tbody>
</table>

EMC Training and Professional Services

EMC Customer Education courses help you learn how EMC storage products work together within your environment to maximize your entire infrastructure investment. EMC Customer Education features online and hands-on training in state-of-the-art labs conveniently located throughout the world. EMC customer training courses are developed and delivered by EMC experts. Go to EMC Online Support at [http://Support.EMC.com](http://Support.EMC.com) for course and registration information.

EMC Professional Services can help you implement your system efficiently. Consultants evaluate your business, IT processes, and technology, and recommend ways that you can leverage your information for the most benefit. From business plan to implementation, you get the experience and expertise that you need without straining your IT staff or hiring and training new personnel. Contact your EMC Customer Support Representative for more information.

Recovery after an VNX SP failure

If a storage processor (SP) panics (software failure) or must be removed and replaced (hardware failure), perform the following to get the SP back online after it restarts:

**Procedure**

1. Determine if an SP failed over by using the following CLI command:
   
   ```
   $ nas_storage -info -id=<storage_id>
   
   If an SP failed over, its disk volumes were transferred to the other SP.
   ```

2. Transfer the disk volumes back to the default (owning) SP by using the command:
   
   ```
   $ nas_storage -failback -id=<storage_id>
   ```

3. After the SP is backed up, restart any Data Mover that restarted while the SP was down.

   A Data Mover that restarts while one SP is down runs with only a single I/O path, even after both SPs are up again. If this single I/O path fails, the Data Mover panics. This step avoids a Data Mover panic and maintains the server's high-availability operation.

Monitor system activity

System activity monitoring on page 112 describes various statistical outputs to help you monitor system activity.
### Table 28 System activity monitoring

<table>
<thead>
<tr>
<th>Type of display</th>
<th>Output</th>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Packet statistics and connection statuses</td>
<td>`server_netstat &lt;movername&gt; -s -p { tcp</td>
</tr>
<tr>
<td>Routing table</td>
<td>Routing table statistics</td>
<td><code>server_netstat &lt;movername&gt; -r</code></td>
</tr>
<tr>
<td>Interface</td>
<td>Specific interface statistics</td>
<td><code>server_netstat &lt;movername&gt; -i</code></td>
</tr>
<tr>
<td>Active connections</td>
<td>TCP or UDP connections</td>
<td>`server_netstat &lt;movername&gt; -p { tcp</td>
</tr>
<tr>
<td>System</td>
<td>Threads information, memory status, and CPU state</td>
<td><code>server_sysstat &lt;movername&gt;</code></td>
</tr>
</tbody>
</table>

### System activity output

The following sections display samples of the system activity output.

**server_sysstat**

Returns the operating system statistics for the specified Data Mover:

```bash
$ server_sysstat server_2
server_2:
  threads runnable = 2
  threads blocked = 230
  threads I/J/Z = 1
  memoryfree(kB)=412359
  cpu idle_% = 57
```

**server_netstat**

Retrieves the network statistics for the specified Data Mover. You can also retrieve the information for the sockets, physical interfaces, and routing table. The following command returns the network statistics for each protocol:

```bash
$ server_netstat server_2 -s
ip:
  ***
  1054053 total packets received
  0 bad header checksums
  0 with unknown protocol
  9 fragments received
  0 fragments dropped (dup or out of space)
  0 fragments dropped after timeout
  9 packets reassembled
  2 packets forwarded
  80824 packets not forwardable
  80824 no routes
  973235 packets delivered
  493572 total packets sent
  0 packets fragmented
  0 packets not fragmentable
  0 fragments created

icmp:
  ****
  0 calls to icmp_error
```
Output histogram:

- echo reply: 260861
- destination unreachable: 56
- echo: 0

Input histogram:

- echo reply: 0
- destination unreachable: 0
- routing redirect: 0
- echo: 260861
- time exceeded: 0
- address mask request: 0260908

messages received

260917 messages sent

tcp:

- 123708 packets sent
- 23 data packets retransmitted
- 0 resets
- 118192 packets received
- 7 connection requests
- 14 connections lingered

udp:

- 0 incomplete headers
- 249390 bad ports
- 345047 input packets delivered
- 98126 packets sent

You can also retrieve routing table and interface information, as displayed in the next two commands:

\$ server_netstat server_2 -r

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Mask</th>
<th>Type</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.245.56.1</td>
<td>0.0.0.0</td>
<td>DIRECT</td>
<td>LOCAL</td>
</tr>
<tr>
<td>cge-1-0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.245.56.0</td>
<td>10.245.56.22</td>
<td>255.255.252.0</td>
<td>DIRECT</td>
<td>LOCAL</td>
</tr>
<tr>
<td>cge-1-0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.221.252.0</td>
<td>128.221.252.2</td>
<td>255.255.255.0</td>
<td>DIRECT</td>
<td>LOCAL</td>
</tr>
<tr>
<td>mge0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>128.221.253.0</td>
<td>128.221.253.2</td>
<td>255.255.255.0</td>
<td>DIRECT</td>
<td>LOCAL</td>
</tr>
<tr>
<td>mge1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Gateway       | Metric | IsValid | Interface | VLAN |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>::1</td>
<td></td>
<td>true</td>
<td>LOCAL</td>
<td>LOCAL</td>
</tr>
<tr>
<td>4294967295</td>
<td></td>
<td></td>
<td>LOCAL</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

\$ server_netstat server_2 -i

<table>
<thead>
<tr>
<th>Name</th>
<th>Mtu</th>
<th>Ibytes</th>
<th>Ierror</th>
<th>Obytes</th>
<th>Oerror</th>
<th>PhysAddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>cge-1-0</td>
<td>9000</td>
<td>1765361334</td>
<td>0</td>
<td>381528</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0:60:48:1b:eb:86</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cge-1-1</td>
<td>9000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0:60:48:1b:eb:87</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cge-1-2</td>
<td>9000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0:60:48:1b:eb:98</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cge-1-3</td>
<td>9000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0:60:48:1b:eb:99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
server_stats

server_stats provides real-time statistics for the specified Data Mover. Statistics are displayed in a time-series fashion at the end of each interval. The statistics are organized as a hierarchy of families that replaces the summary and table collections. Previously defined summary and table collections have been converted to system-defined statistics groups that can be used as arguments with the new -monitor option:

Table 29 Sample of Statistics Group names

<table>
<thead>
<tr>
<th>System-defined Statistics Group name</th>
<th>server_stats collection name</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic-std</td>
<td>-summary basic</td>
</tr>
<tr>
<td>caches-std</td>
<td>-summary caches</td>
</tr>
<tr>
<td>cifs-std</td>
<td>-summary cifs</td>
</tr>
<tr>
<td>nfs-std</td>
<td>-summary nfs</td>
</tr>
<tr>
<td>cifsOps-std</td>
<td>-table cifs</td>
</tr>
<tr>
<td>diskVolumes-std</td>
<td>-table dvol</td>
</tr>
</tbody>
</table>

Statistics Groups are managed by the newly available nas_stats command.

To monitor a Statistics Group or Statistics Path, use the following syntax:

```
$ server_stats <movename> -monitor <statpath/statgroup_name> -interval <seconds> -count <count>
```

where:
- `<movename>`= name of the Data Mover
- `<statpath/statgroup_name>`= a comma-separated list of statpath and statgroup names.
- `<seconds>`= the number of seconds between samples.
- `<count>`= the number of reports that are generated.

Example:

```
$ server_stats server_2 -monitor cifs-std -i 3 -c 5
```

Troubleshooting
<table>
<thead>
<tr>
<th></th>
<th>CIFS</th>
<th>CIFS</th>
<th>CIFS</th>
<th>CIFS Avg</th>
<th>CIFS</th>
<th>CIFS</th>
<th>CIFS Avg</th>
<th>CIFS</th>
<th>CIFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Total</td>
<td>Read</td>
<td>Read</td>
<td>Read</td>
<td>Write</td>
<td>Write</td>
<td>Write</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ops/s</td>
<td>Ops/s</td>
<td>KiB/s</td>
<td>Size KiB</td>
<td>Ops/s</td>
<td>KiB/s</td>
<td>KiB/s</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connections</td>
<td>Files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**nas_stats**

nas_stats allows the user to manage Statistics Groups. There are two types of Statistics Groups: System and User-defined groups. These groups are the same groups that server_stats will display with –monitor, -list, and –info. nas_stats can be used to modify existing System-defined Statistic Groups or it can be used to create new Userdefined Statistics groups.

For more information about the syntax and usage of the nas_stats command, refer to the *VNX Command Line Interface Reference for File*.  

System activity output
INDEX

A
analyzing log data 101
Audit VNX 66
Automatic Collection and Transfer tool
command examples 107
command options 106
configuring 104
described 103
disabling 106
problem reporting 103
running from CLI 106
user command examples 107

C
collecting event log data 101
configuring 86
connect home
configuring 86
Control Station
change hostname value 67
configure for IPv6 80
connect home, configuring 86
enabling daemons 69
halting locally 60
IP aliasing 82
IPv4 networking
avoid conflicts 82
restarting locally 61
set time zone 77
setting date and time 76

D
daemon
Control Station 69
HTTPD 69
Data Mover
halting 62
rebooting
cold 63
warm 63
set time zone 78
setting date and time 76
date setting
Control Station 76
Data Mover 76

E
EMC E-Lab Navigator 110
Emergency shutdown
powering up after 58
VNX series 58
error messages 110

H
Halt Control Stations 59
Halt Data Movers 59
HALTing
Data Mover 62
dual Control Station
Locally 60
Remotely 60
single Control Station
Locally 60
Remotely 60
HTTPD daemons
restarting 69

I
IP aliasing
create 83
delete 83
IP networking
change VNX management port values 84
configure IPv6 on Control Station 80
IPv6
configure IPv6 on Control Station 80

L
Linux security alerts
between software installations 68
new software installations 68
log files
automatic collection and transfer 103
problem reporting 103

M
messages, error 110

N
nas_cel 67
nas_checkup
check system status 67
nas_config
IP aliasing
create 83
delete 83
nas_cs
configure IPv6 on Control Station 80
setting date and time 76
setting timezone 77
nas_version 66
NTP service
configure 77
Planned powerdown

VNX VG10 Gateway 12
VNX VG50 Gateway 12
VNX-F5000 for Block 15
VNX-F7000 for Block 23
VNX5200 for Block 15
VNX5200 for File 18
VNX5200 Unified 18
VNX5400 for Block 15
VNX5400 for File 18
VNX5400 Unified 18
VNX5600 for Block 15
VNX5600 for File 18
VNX5600 Unified 18
VNX5800 for Block 23
VNX5800 for File 26
VNX5800 Unified 26
VNX7600 for Block 23
VNX7600 for File 26
VNX7600 Unified 26
VNX8000 for Block 30
VNX8000 for File 33
VNX8000 Unified 33

Powering up

VNX VG10 Gateway 38
VNX VG50 Gateway 38
VNX-F5000 for Block 40
VNX-F7000 for Block 45
VNX5200 for Block 40
VNX5200 for File 42
VNX5200 Unified 42
VNX5400 for Block 40
VNX5400 for File 42
VNX5400 Unified 42
VNX5600 for Block 40
VNX5600 for File 42
VNX5600 Unified 42
VNX5800 for Block 45
VNX5800 for File 47
VNX5800 Unified 47
VNX7600 for Block 45
VNX7600 for File 47
VNX7600 Unified 47
VNX8000 for Block 50
VNX8000 for File 52
VNX8000 Unified 52

Powerup after emergency shutdown 58
private LAN
  avoid address conflicts 82
problem reporting
  automatic collection and transfer of logs 103
  collecting log files 103

R
reason codes 60, 61
rebooting
  Data Mover 63
Restart Control Stations 59
Restart Data Movers 59
restarting

dual Control Station
  Locally 61
  Remotely 61
single Control Station
  Locally 61
  Remotely 61

S
SCSI devices
  discovering 72
  saving 72
securing event log data 101
server_cpu
  halt Data Mover 62
  reboot Data Mover 63
server_date
  setting Data Mover time zone 78
  setting time and date 76
server_devconfig
  discovering SCSI devices 72
  saving SCSI devices 72
server_snmpd
  view SNMP status 80
server_version 66
setting
  date
    Control Station 76
    Data Mover 76
  time
    Control Station 76
    Data Mover 76
setting time zone
  Control Station using CLI 77
  Data Mover using CLI 78
Shutdown in emergency 58
SNMP
  about 80
  view 80

time service
  Control Station
    set using CLI 77
  Data Mover
    set using CLI 78
setting
  Control Station time and date 76
  Data Mover time and date 76
time setting
  Control Station 76
  Data Mover 76
troubleshooting 109

V
verifying Control Station software version 66
verifying Data Mover software version 66
VNX database
  backup
    automatic 70
manual 70