# NexentaFusion User Guide

## Contents

<table>
<thead>
<tr>
<th>Preface</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Document Overview</td>
<td>2</td>
</tr>
<tr>
<td>About This Document</td>
<td>2</td>
</tr>
<tr>
<td>Accessing Online Help</td>
<td>3</td>
</tr>
<tr>
<td>Supported Web Browsers</td>
<td>3</td>
</tr>
<tr>
<td>Viewing Online Help</td>
<td>3</td>
</tr>
<tr>
<td>Additional Resources</td>
<td>4</td>
</tr>
<tr>
<td>Terminology</td>
<td>5</td>
</tr>
<tr>
<td>What Comes Next?</td>
<td>6</td>
</tr>
<tr>
<td>2 NexentaFusion Overview</td>
<td>7</td>
</tr>
<tr>
<td>Introducing NexentaFusion</td>
<td>7</td>
</tr>
<tr>
<td>Initially Logging in to NexentaFusion</td>
<td>8</td>
</tr>
<tr>
<td>TLS/SSL Certificate Warning</td>
<td>8</td>
</tr>
<tr>
<td>Next Steps</td>
<td>8</td>
</tr>
<tr>
<td>Getting Started with NexentaFusion</td>
<td>9</td>
</tr>
<tr>
<td>Switching Between Appliance and NexentaFusion Modes</td>
<td>9</td>
</tr>
<tr>
<td>NexentaFusion Icons, Main COG, and Top-Level Tabs</td>
<td>10</td>
</tr>
<tr>
<td>Appliances List Page</td>
<td>10</td>
</tr>
<tr>
<td>NexentaFusion Icons</td>
<td>11</td>
</tr>
<tr>
<td>Main COG</td>
<td>13</td>
</tr>
<tr>
<td>Top-Level Tabs</td>
<td>14</td>
</tr>
<tr>
<td>What Comes Next?</td>
<td>17</td>
</tr>
<tr>
<td>3 Registering NexentaStor Appliances</td>
<td>18</td>
</tr>
<tr>
<td>Registering a NexentaStor Appliance</td>
<td>18</td>
</tr>
<tr>
<td>Confirming Registration</td>
<td>21</td>
</tr>
<tr>
<td>Viewing Appliance Summary</td>
<td>21</td>
</tr>
<tr>
<td>Viewing Appliance Licenses</td>
<td>22</td>
</tr>
<tr>
<td>Viewing Appliance Profile and Version</td>
<td>23</td>
</tr>
</tbody>
</table>
# NexentaFusion User Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Comes Next?</td>
<td>24</td>
</tr>
<tr>
<td><strong>4 Configuring NexentaFusion</strong></td>
<td>25</td>
</tr>
<tr>
<td>NexentaFusion Configuration Overview</td>
<td>25</td>
</tr>
<tr>
<td>Setting the SMTP Mail Server (Email Setup)</td>
<td>26</td>
</tr>
<tr>
<td>Creating, Modifying, and Deleting Local UI User Accounts</td>
<td>28</td>
</tr>
<tr>
<td>Creating a New Local UI User Account</td>
<td>29</td>
</tr>
<tr>
<td>Changing the Login Credentials and Role for a Local UI User</td>
<td>30</td>
</tr>
<tr>
<td>Deleting a Local UI User Account</td>
<td>32</td>
</tr>
<tr>
<td>Adding NexentaFusion to Windows Active Directory (AD)</td>
<td>32</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>32</td>
</tr>
<tr>
<td>Configure NexentaFusion for Windows AD</td>
<td>33</td>
</tr>
<tr>
<td>Setting the Date/Time</td>
<td>33</td>
</tr>
<tr>
<td>Configuring Session Settings</td>
<td>35</td>
</tr>
<tr>
<td>What Comes Next?</td>
<td>35</td>
</tr>
<tr>
<td><strong>5 Managing NexentaStor Appliances</strong></td>
<td>36</td>
</tr>
<tr>
<td>Provisioning Overview</td>
<td>36</td>
</tr>
<tr>
<td>Verifying Enclosure and Disk Information</td>
<td>38</td>
</tr>
<tr>
<td>Enclosure Components Overview</td>
<td>38</td>
</tr>
<tr>
<td>Filtering System Components</td>
<td>40</td>
</tr>
<tr>
<td>Viewing Hardware Components</td>
<td>40</td>
</tr>
<tr>
<td>Managing Network Configurations</td>
<td>43</td>
</tr>
<tr>
<td>Verifying and Modifying IP Links</td>
<td>43</td>
</tr>
<tr>
<td>Creating Aggregates</td>
<td>45</td>
</tr>
<tr>
<td>Adding a VLAN</td>
<td>46</td>
</tr>
<tr>
<td>Adding an Address</td>
<td>48</td>
</tr>
<tr>
<td>Verifying IP Addresses</td>
<td>49</td>
</tr>
<tr>
<td>Creating, Verifying, and Deleting IP Routes</td>
<td>50</td>
</tr>
<tr>
<td>Modifying IP Network Settings</td>
<td>52</td>
</tr>
<tr>
<td>Verifying FC Interfaces</td>
<td>53</td>
</tr>
<tr>
<td>Creating and Managing Pools</td>
<td>54</td>
</tr>
<tr>
<td>Planning for Pools</td>
<td>54</td>
</tr>
<tr>
<td>Viewing Available Disks for a Pool</td>
<td>55</td>
</tr>
</tbody>
</table>
Creating Pools on Single or Clustered Nodes ........................................55
Guided Configuration .................................................................56
Naming and Configuring a Pool .....................................................56
Adding Data Devices to a Pool ......................................................58
Adding Cache, Log, Special, and Spare Devices to a Pool ..................60
Editing an Existing Pool ..............................................................62
Configuring an HA Service for a Shared Pool .................................63
Discovering Pools and Viewing Pool Status .....................................64
Viewing Status Details for a Shared Pool ........................................66
Setting Management Actions .......................................................67
Editing Pool Properties ...............................................................70
Adding an Unshared Pool to HA Service ........................................71
Viewing VIPs Associated with an HA Service ................................72
Moving a Pool under HA Service for Manual Failover ......................73
Removing a Pool From HA Control ...............................................74
Creating and Managing File Systems .........................................75
Creating a File System on a Pool ................................................75
Viewing File Systems .................................................................78
Filtering File Systems ...............................................................81
Sharing File Systems Using NFS ...............................................82
Configuring and Enabling the NFS Server ......................................82
Creating an NFS Share ..............................................................83
Open Shares ........................................................................84
Shares with Security Options .......................................................84
Create an NFS Share for a File System .........................................84
Sharing File Systems Using SMB .................................................87
Configuring and Enabling the SMB Server ....................................87
Creating an SMB Share ..............................................................89
Mapping an SMB Share on Windows .............................................90
Creating and Managing Volume Groups and Volumes .....................91
Creating a Volume Group ..........................................................91
Creating Volumes .......................................................................93
Editing Properties for Volume Groups and Volumes .......................95
Deleting a Volume Group or Volume ................................................. 97
Mapping Volumes ........................................................................ 98
Managing LUNs ........................................................................... 99
Viewing LUN Information .............................................................. 99
Editing and Destroying LUNs ....................................................... 100
Managing iSCSI Host Groups, Targets, and Groups .................... 101
Configuring Secure Authentication ............................................. 102
Unidirectional CHAP Authentication ......................................... 102
Bidirectional CHAP ................................................................. 102
Configuring iSCSI Host Groups ................................................. 102
Creating, Editing, and Destroying iSCSI Targets and Target Groups ......................................................... 105
Creating iSCSI Targets .............................................................. 105
Creating iSCSI Target Groups .................................................... 106
Viewing iSCSI Target Information and Sessions ...................... 107
Editing or Deleting iSCSI Targets .............................................. 108
Removing iSCSI Targets from a Group and Destroying the Target Group ................................................. 109
Managing FC Host Groups, Targets and Target Groups .......... 111
Configuring FC Host Groups ...................................................... 111
Adding FC Targets to a New or Existing FC Target Group ........ 112
Removing FC Targets from a Group ......................................... 113
Viewing Target Group Sessions ................................................. 113
Destroying FC Target Groups .................................................... 114
Protecting Data .......................................................................... 115
Taking a One-Time Snapshot .................................................... 115
Cloning a Snapshot and Promoting a Clone .............................. 116
Rolling Back or Deleting a Snapshot ....................................... 117
Adding a Protection Service ...................................................... 119
Working with Protection Services ........................................... 119
Adding a Scheduled Replication Service ................................. 120
Adding a Scheduled Snapshots Service ................................ 122
Filtering Snapshots and Data Protection Service Data .............. 123
Configuring Continuous Replication ..................................... 124
Editing or Deleting a Schedule ................................................ 125
Manually Executing a Service .......................................................... 126
Disabling and Enabling a Protection Service ...................................... 127
Destroying a Protection Service ......................................................... 128
Flipping the Direction of a Replication Service .................................. 129
Verifying and Querying Data Protection Data .................................... 130
Editing the Data Protection Dedicated Network Interface ................. 132
Managing System and Data Settings .................................................. 134
    Enabling and Disabling System Services ........................................ 134
    Editing System Services ............................................................. 135
    Configuring Data Settings ........................................................... 136
        Configure Logs ................................................................. 136
        Configure Events and Real-Time Analytics ............................... 137
        Set Active Probes ............................................................. 138
        Manage Analytics Aggregation Data ...................................... 140
Managing High Availability ............................................................. 141
    About High Availability and HA Services ..................................... 141
        HA Cluster ................................................................. 141
        HA Service ................................................................. 142
    Managing HA Services .............................................................. 142
        Verifying Service Status ..................................................... 143
        Failing Over Services Manually ............................................ 144
        Adding a VIP ............................................................... 144
        Editing and Deleting a VIP .................................................. 145
        Moving an HA Service ....................................................... 146
        Setting the HA Service Mode ............................................... 146
        Stopping and Starting an HA Service ...................................... 147
        Destroying an HA Service .................................................... 147
        Removing a Pool from HA Service ......................................... 148
        Verifying Cluster Status ....................................................... 148
What Comes Next? ........................................................................ 149

6 Performance Monitoring and Analytics ............................................ 150
Terminology ................................................................................. 150
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>151</td>
</tr>
<tr>
<td>Using the Default Dashboard</td>
<td>152</td>
</tr>
<tr>
<td>What Comes Next?</td>
<td>153</td>
</tr>
<tr>
<td>Using the Analytics Workspace</td>
<td>153</td>
</tr>
<tr>
<td>Understanding the Analytics Workspace</td>
<td>153</td>
</tr>
<tr>
<td>Canvas Workspace: 1</td>
<td>154</td>
</tr>
<tr>
<td>Widget Selection Panel: 2</td>
<td>154</td>
</tr>
<tr>
<td>Canvas Bar: 3</td>
<td>154</td>
</tr>
<tr>
<td>Navigating to the Analytics Workspace</td>
<td>155</td>
</tr>
<tr>
<td>Using a Canvas</td>
<td>155</td>
</tr>
<tr>
<td>Creating a New Canvas</td>
<td>156</td>
</tr>
<tr>
<td>Adding, Moving, Resizing, and Removing Widgets</td>
<td>156</td>
</tr>
<tr>
<td>Managing Canvases</td>
<td>157</td>
</tr>
<tr>
<td>Modifying, Renaming, or Removing a Canvas</td>
<td>157</td>
</tr>
<tr>
<td>Cloning, Importing, and Exporting Canvases</td>
<td>158</td>
</tr>
<tr>
<td>Viewing and Editing the Dashboard Canvas</td>
<td>159</td>
</tr>
<tr>
<td>Viewing the Dashboard Canvas</td>
<td>159</td>
</tr>
<tr>
<td>Customizing the Dashboard Canvas</td>
<td>160</td>
</tr>
<tr>
<td>Resetting Dashboard Canvas Defaults</td>
<td>160</td>
</tr>
<tr>
<td>Using Widgets</td>
<td>161</td>
</tr>
<tr>
<td>Using the Widget Selection Panel</td>
<td>161</td>
</tr>
<tr>
<td>Configuring Widgets</td>
<td>162</td>
</tr>
<tr>
<td>Widget Categories</td>
<td>162</td>
</tr>
<tr>
<td>Cloning Widgets</td>
<td>163</td>
</tr>
<tr>
<td>Editing and Saving Widgets</td>
<td>164</td>
</tr>
<tr>
<td>Removing Configured Widgets</td>
<td>165</td>
</tr>
<tr>
<td>Analyzing Data</td>
<td>166</td>
</tr>
<tr>
<td>Analyzing Performance Data</td>
<td>166</td>
</tr>
<tr>
<td>Analyzing Top N Data</td>
<td>168</td>
</tr>
<tr>
<td>Working with Top N Widgets</td>
<td>168</td>
</tr>
<tr>
<td>Creating a Custom Time Interval</td>
<td>169</td>
</tr>
<tr>
<td>Analyzing Capacity Data</td>
<td>170</td>
</tr>
</tbody>
</table>
Analyzing Health and Utilization Data ............................................. 171
What Comes Next? ........................................................................... 172

7 Fault Management ........................................................................ 173
About Logs, Audit Logs, Events, and Alerts ..................................... 173
Viewing Logs, Audit Logs, and Alerts ............................................. 174
Creating Rules for Logs and Events .............................................. 175
Troubleshooting Data Devices in a Pool ........................................ 176
Locating a Failed Disk ..................................................................... 177
Managing Pool Data Devices .......................................................... 178
  Administering Pool Data Devices .................................................. 178
  Removing a Device from a Pool ..................................................... 179
  Replacing a Device in a Pool ....................................................... 179
  Attaching a New Mirror Device .................................................. 180
  Detaching a Device from a Mirror ............................................... 180
  Setting a Device in a Pool to Offline ............................................ 180
  Setting a Physical Device to Online ............................................ 180
  Clearing Error from a Device ..................................................... 180
Rebooting or Powering Off a NexentaStor Appliance ......................... 181
Preface

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

Intended Audience

This documentation is intended for Storage Administrators and assumes that you have experience with data storage concepts, such as NAS, SAN, NFS, and ZFS; Fibre Channel (FC) and iSCSI interfaces; Microsoft Windows Active Directory.

Documentation History

The following table lists the released version of this documentation.

Table 1: Documentation Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B3000-Fusion-000062-A</td>
<td>October, 2016</td>
<td>GA</td>
</tr>
</tbody>
</table>

Contacting Support

Send your support questions and requests to support@nexenta.com.

Comments

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

- About This Document
- Accessing Online Help
- Additional Resources
- Terminology
- What Comes Next?

About This Document

NexentaFusion is a graphical user interface (GUI) that allows you to intuitively manage NexentaStor appliances. This document demonstrates how to configure NexentaFusion to work with NexentaStor appliances, then provision and manage physical and virtual NexentaStor appliances. We recommend that you use this document in conjunction with the suggested Additional Resources.

This document is organized as follows:

- Chapter 1: Document Overview
  This chapter covers how this document is organized, supported browsers, how to find NexentaFusion online help, and basic terminology.

- Chapter 2: NexentaFusion Overview
  This chapter introduces the NexentaFusion UI that you will use to provision NexentaStor appliances in your environment.

- Chapter 3: Register NexentaStor Appliance
  This chapter covers basic configuration procedures for establishing a connection between NexentaFusion and NexentaStor, as well as how to register an appliance. You can register clustered or single node appliances.

- Chapter 4: NexentaFusion Configuration
  This chapter covers adding NexentaFusion to Windows Active Directory, setting up an SMTP mailer, creating local UI users, and setting the date and time.

- Chapter 5: Managing NexentaStor Appliances
  This chapter demonstrates how to perform management tasks for NexentaStor appliances, such as verifying network interfaces, identifying disks, creating and managing pools, optimizing performance and availability, creating and sharing file systems, and creating and mapping volumes.
• **Chapter 6: Performance Monitoring and Analytics**
  This chapter covers how to use the default dashboard and pre-defined widgets, and how to create custom widgets and canvases for future use. NexentaFusion displays metrics for registered NexentaStor appliances in real time or historical time.

• **Chapter 7: Fault Management (Logs, audit logs, events, and alerts)**
  This chapter explains how to create rules, monitor errors and alerts, identify the status of storage components, remove failed devices, and manage devices in a pool.

**Accessing Online Help**

This section covers the Web browsers and versions that are supported by NexentaFusion 1.0.0, and demonstrates how to view the online help version of this document.

**Supported Web Browsers**

You access NexentaFusion online help with a Web browser. NexentaFusion 1.0.0 supports the following browsers:

- Google Chrome, latest version
- Mozilla Firefox, v47 or later

**Viewing Online Help**

The content in this document is available in NexentaFusion online help. Use the following procedure to access the online help.

❖ **To access NexentaFusion help, do the following:**
  1. Log into NexentaFusion.
     This opens the Appliance List view.
  2. In the upper right corner, click the Main COG.
  3. Select Help from the drop-down list to view the Online Help.
Additional Resources

Use the following resources in conjunction with this document. They can be downloaded from the Nexenta Products Web page: https://nexenta.com/products/downloads/nexentastor

Table 1-1: Documentation Resources

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NexentaStor 5.0 CLI Configuration Guide</td>
<td>This guide demonstrates the basic steps and commands to configure and manage NexentaStor 5.0 appliances. Use this document in conjunction with the NexentaStor 5.0 Command Line Interface Reference Guide, and the NexentaStor 5.0 HA CLI Admin Guide.</td>
</tr>
<tr>
<td>NexentaStor 5.0 Command Line Interface Reference Guide</td>
<td>This reference guide provides a summary of the CLI commands. Use it in conjunction with the companion document, NexentaStor 5.0 CLI Configuration Guide.</td>
</tr>
<tr>
<td>NexentaStor 5.0 HA CLI Admin Guide</td>
<td>This guide demonstrates the basic steps and commands to configure and manage the NexentaStor 5.0 High Availability (HA) cluster using the NexentaStor 5.0 Command Line Interface (CLI).</td>
</tr>
<tr>
<td>NexentaStor Product Guide</td>
<td>This guide provides an overview of NexentaStor and its core components, describes key features, and provides relevant CLI commands. This manual is intended as a guide to NexentaStor concepts and not as a configuration guide.</td>
</tr>
<tr>
<td>NexentaStor 5.0 and NexentaFusion 1.0 Installation QuickStart Guide</td>
<td>This document includes the instructions to install and upgrade NexentaStor and NexentaFusion.</td>
</tr>
<tr>
<td>NexentaStor 5.0 vCenter Plugin Admin Guide</td>
<td>This guide includes instructions to install NexentaStor 5.0 vCenter Web Client Plugin (vCenter Plugin), which enables VMware customers to configure and manage storage and virtualization through a single interface.</td>
</tr>
<tr>
<td>NexentaStor 5.0 VVOL Admin Guide</td>
<td>This guide describes the NexentaStor Virtual Volume (VVOL) solution. It provides instructions on how to deploy VVOL, integrate it with VMware vsphere, and enumerates the storage operations it supports.</td>
</tr>
</tbody>
</table>
Terminology

The following terms are used throughout this document, and utilized in the NexentaFusion UI:

Table 1-2: Terms and Definitions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NexentaFusion</td>
<td>NexentaFusion is a user interface (UI) for a Software-Defined Storage system. NexentaFusion allows for easy configuration and management of appliances, as well as providing an intuitive analytics dashboard for file services and block services.</td>
</tr>
<tr>
<td>NexentaStor Appliance</td>
<td>NexentaStor is a software-based storage appliance that supports file and block services, along with a variety of advanced storage features such as replication, snapshots, and clones.</td>
</tr>
<tr>
<td>Dataset</td>
<td>A dataset is a generic name for the following components: file system, volume group, volume, and snapshots.</td>
</tr>
<tr>
<td>Pool</td>
<td>A pool is a logical space for the creation of datasets that is constructed from virtual devices (vDevs) that are an aggregation of block devices/physical storage. You can manage physical storage by configuring pools based on the needs of your site and available storage space.</td>
</tr>
<tr>
<td>File system</td>
<td>A file system is a specific type of dataset that facilitates the organization and sharing of file data and directories using NFS or SMB protocols. File systems can be nested up to 15 levels in a pool, and can contain other file systems and snapshots.</td>
</tr>
<tr>
<td>vDev</td>
<td>Each top level device in a pool is called a virtual device (vDev), which can be a simple disk or a RAID combination, such as a mirror or RAID-Z1, Z2, Z3 array.</td>
</tr>
<tr>
<td>Volume Group</td>
<td>A volume group is a first level dataset (below the pool) that is a logical grouping of volumes with similar characteristics. Volume groups cannot hold user data and cannot be exposed over protocols.</td>
</tr>
<tr>
<td>Volume</td>
<td>A volume is a dataset that represents a block device. A volume must be created within a volume group under a pool. A volume can be mapped as a LUN using iSCSI or FC protocols.</td>
</tr>
<tr>
<td>NexentaFusion mode</td>
<td>Select Fusion from the pull-down menu in top left of the orange bar. NexentaFusion mode allows you to view, modify, and delete logs, audit logs, alerts, and rules. For more information, see Chapter 7, Fault Management.</td>
</tr>
<tr>
<td>Appliance Mode</td>
<td>Select the Appliance mode from the pull-down menu in the upper left corner of the window to manage NexentaStor appliances. Appliance mode has the necessary UI elements to manage NexentaStor appliances, both single node and clustered.</td>
</tr>
</tbody>
</table>
What Comes Next?

Now that you have read the summary of each chapter, the following chapter acquaints you with the NexentaFusion user interface (UI).
NexentaFusion Overview

This chapter introduces the basic functionality of NexentaFusion, and over the following topics:

- Introducing NexentaFusion
- Initially Logging in to NexentaFusion
- Getting Started with NexentaFusion
- Switching Between Appliance and NexentaFusion Modes
- NexentaFusion Icons, Main COG, and Top-Level Tabs
- What Comes Next?

Introducing NexentaFusion

The NexentaFusion user interface (UI) enables you to intuitively manage NexentaStor appliances. You can create and configure pools, create and share file systems, and access appliance-level summaries of hardware, pools, NICs, file systems, shares, volumes, LUNs, and services. NexentaFusion uses drill-down menus, action COGs, and expand-contract arrows, to provide a full range of administrative functionality for provisioning, monitoring, and optimizing storage appliances.

To watch a short video introduction to NexentaFusion, go to: https://www.youtube.com/watch?v=ryBGX6B0sAA&list=PLlXP6v5WL0ZQRlzhF5ERlq22ReWaAmIE5W.
Initially Logging in to NexentaFusion

After successfully installing NexentaFusion, the system is ready for use with a predefined account with full administrative privileges. This predefined account cannot be deleted.

- To log in to NexentaFusion for the first time, do the following:
  1. Enter the following NexentaFusion default credentials:
     - username: admin
     - password: nexenta
  2. Change the password for this predefined admin user account.

The End User Licence Agreement (EULA) appears.

3. Scroll to the bottom of the EULA and click Accept.

TLS/SSL Certificate Warning

It is possible to receive a warning that your server's TLS/SSL certificate is signed by an Certification Authority (CA) that is not well-known or trusted. This can happen if an intermediate (chain) certificate is missing, expired or has been revoked; the server host name does not match the host name configured in the certificate; the time and date setting is incorrect; or a self-signed certificate is being used.

- Ensure that the common name (CN) reflects the name of the entity presenting the certificate (e.g., the host name).
- If the certificates, or any of the chain certificates, have expired or been revoked, obtain a new certificate from your Certificate Authority (CA), following their documentation.
- If a self-signed certificate is being used, consider obtaining a signed certificate from a CA.

Next Steps

After you have logged in to NexentaFusion for the first time and changed the default admin password, continue with Getting Started with NexentaFusion.
Getting Started with NexentaFusion

This section provides an overview of working with NexentaFusion after Initially Logging in to NexentaFusion and becoming familiar with Switching Between Appliance and NexentaFusion Modes and NexentaFusion Icons, Main COG, and Top-Level Tabs.

Task 1: Register a NexentaStor appliance.
When you first log in to NexentaFusion you are presented with the Appliances List screen. You can now begin Registering a NexentaStor Appliance.

Task 2: Configure NexentaFusion.
Complete the basic configuration to establish the connection between the NexentaFusion and NexentaStor appliances, as described in Configuring NexentaFusion.

Start provisioning an appliance by clicking the name or icon of the appliance in the list, and following the directions described in Managing NexentaStor Appliances.

Switching Between Appliance and NexentaFusion Modes

When you log in to NexentaFusion, the Appliance List screen appears, automatically placing you in Appliance mode. Fusion mode is the other task mode in NexentaFusion.

- Appliance mode—Used to register and manage NexentaStor appliances. For more information, see Registering NexentaStor Appliances and Managing NexentaStor Appliances.
- Fusion mode—Used to monitor and examine logs and alerts. For more information, see Fault Management.

The following task demonstrates how to switch between Appliance mode and Fusion mode.

- To switch to between modes, do the following:
  1. Log in to NexentaFusion.
     The Appliances List page appears.
  2. Click Appliance in the top menu bar.
     A drop-down menu appears.
  3. Select Fusion to switch to NexentaFusion mode.
4. To switch back to Appliance mode, click Fusion and select Appliance from the drop-down menu.

NexentaFusion Icons, Main COG, and Top-Level Tabs

This section covers the following topics:

- Appliances List Page
- Icons and their Functions
- NexentaFusion Icons
- Main COG
- Top-Level Tabs

Appliances List Page

After registering a single-node NexentaStor appliance or a clustered NexentaStor appliance, the Appliances List page displays with the following information:

- Name—Lists the name of the device with an icon representative of a single or clustered node.
- Health—Shows the status of the health for an appliance. Hover the cursor over the health icon to display detailed information on the appliance health.
• Alerts—Shows the number of alerts to the right of the icon. Click an alerts icon to view a pop-up dialog with information on the generated alerts.

![Alerts Table](image)

• Configured capacity—Shows the sum of the free capacity, as well as the allocated capacity of the pool after applying the redundancies (raid/mirror).

• Installed capacity—Shows the sum of the disk sizes installed in the appliance.

• Actions—Tasks you can perform using the options on the drop-down list.

**NexentaFusion Icons** explains the icons that appear on the Appliances List page, and throughout the rest of the NexentaFusion UI.

### NexentaFusion Icons

**Table 2-1** lists common icons used throughout NexentaFusion, with an explanation for each. Some of the icons represent the state of an item, while others provide an interactive action.

**Table 2-1: Icons and their Functions**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
</table>
| ![Main COG](image) | Main COG  
Click the Main COG in the orange bar to access a drop-down menu of supported options. Select the desired action from the menu to perform the task. |
| ![Action COG](image) | Action COG  
Click an action COG to display a drop-down menu of supported options. |
| ![Expand, Collapse](image) | Expand, Collapse  
Click an arrow to show or hide all of the entries in a table. |
| ![Expand (Tree view)](image) | Expand (Tree view)  
Click the arrow to display a list of hidden items, such as a file system under a pool. |
| ![Single node](image) | Single node  
This icon represents a single appliance. |
<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
</table>
| ![Clustered nodes](image) | Clustered nodes  
This icon represents a two-node clustered appliance. |
| ![Critical — Health state](image) | Critical — Health state  
This red icon implies there are serious issues. |
| ![Warning — Health state](image) | Warning — Health state  
This yellow icon indicates there is a problem that might be causing performance issues, but it is not yet serious. For example, a degraded pool would display the yellow icon. |
| ![Unknown—Health state](image) | Unknown—Health state  
This icon indicates that health information has not been received from the appliance in a specified time to report the status. |
| ![Good — Health state](image) | Good — Health state  
This green icon implies that there are no issues associated with the associated item. For example, a healthy node or pool etc. |
| ![The shield icon represents the cluster service. Hover the mouse over this shield icon to read the state of the cluster service. A cluster service running on an active node, state OK on both nodes, should be able to fail-over properly.](image) | The shield icon represents the cluster service.  
Hover the mouse over this shield icon to read the state of the cluster service.  
A cluster service running on an active node, state OK on both nodes, should be able to fail-over properly. |
| ![This icon represents a cluster service running on active node that may not be able to failover, or is in flux on the other node. A blinking icon indicates a service is in transition. Click Refresh to see if the transition has completed.](image) | This icon represents a cluster service running on active node that may not be able to failover, or is in flux on the other node.  
A blinking icon indicates a service is in transition. Click Refresh to see if the transition has completed. |
| ![This icon represents a cluster service state that is in flux, and is attempting to get started on a node. A blinking icon indicates a service is in transition. Click Refresh to see if the transition has completed.](image) | This icon represents a cluster service state that is in flux, and is attempting to get started on a node.  
A blinking icon indicates a service is in transition. Click Refresh to see if the transition has completed. |
| ![This icon represents a cluster service that is not running, but should be able to be restarted on a node.](image) | This icon represents a cluster service that is not running, but should be able to be restarted on a node. |
| ![This icon represents a cluster service that is not running on either node due to major problems. Intervention is needed.](image) | This icon represents a cluster service that is not running on either node due to major problems. Intervention is needed. |
Main COG

The **Main COG** appears in the orange bar at the top of NexentaFusion window. Its options apply to NexentaFusion, not a specific appliance. Click the **Main COG** to display a drop-down list with the following options:

- **About**—View NexentaFusion version information, how to contact support and the online community resources, as well as allowing you to review the Nexenta End User License Agreement (EULA) that was accepted upon the initial login to NexentaFusion.
- **Audit Logs**—Search for and view logs of user logins and authentication, and put/post reports that change the appliance.
- **Elasticsearch Overview**—View information on the Elasticsearch DB that is used to persist metrics for analytics, logs, and alerts.
- **Logs**—Search for and view system logs with a tabular display showing Timestamp, Hostname, Message, Severity, Component, HostId, and Origin of the event.
- **Settings**—View and modify NexentaFusion settings, as described in Chapter 4, Configuring NexentaFusion.
- **Help**—Access the NexentaFusion online help, or download the complete help content in a PDF version of the NexentaFusion 1.0 User Guide.

For more information on the Elastic DB, see Creating Rules for Logs and Events in Chapter 7, Fault Management.

- **To view system and audit logs, do the following:**
  1. Log in to NexentaFusion.
  2. Click the **Main COG** and do one of the following:
     - Select **Logs** from the drop-down list to view a list of system logs.
     - Select **Audit Logs** from the drop-down list to view a list of audit logs.

  For more information on logs, audit logs, alerts, and rules, see Chapter 7, Fault Management.

- **To complete basic configuration tasks in NexentaFusion, do the following:**
  1. Log in to NexentaFusion.
  2. Click the **Main COG** and select **Settings** from the drop-down list.
3. Do the following:
   - Click **Active Directory** in the left panel to add NexentaFusion to Windows Active Directory, for authentication and authorization capabilities. For more information, see Adding NexentaFusion to Windows Active Directory (AD).
   - Click **Date/Time** in the left panel to set the date and time for a device. For more information, see Setting the Date/Time.
   - Click **Email Setup** in the left panel to configure an SMTP server for system failure notification. For more information, see Setting the SMTP Mail Server (Email Setup).
   - Click **Local UI User** to create, modify, and delete NexentaFusion Local UI User accounts. For more information, see Creating, Modifying, and Deleting Local UI User Accounts.

For more information on configuring NexentaFusion, see Chapter 4, Configuring NexentaFusion.

**Top-Level Tabs**

After you log in to NexentaFusion, the **Appliances List** appears. You use the functions under the NexentaFusion top-level tabs to manage NexentaStor appliances. This section provides an overview of the functions for each top-level tab.

- **To manage appliances with NexentaFusion top-level tabs, do the following:**
  1. Log in to NexentaFusion, and click **Appliances List** in the top menu bar.
  2. Select an appliance from the drop-down list.

The Dashboard window appears, showing analytics for the selected appliance.
3. Use the following tabs to manage registered NexentaStor appliances:

- **Dashboard**—Monitor performance and utilization metrics for a selected appliance using default and custom widgets. For more information, see [Dashboard](#).
- **Management**—View appliance summaries and manage components, pools, networks, file systems, and volumes. For more information, see [Managing NexentaStor Appliances](#).
- **Analytics**—View performance metrics, configure widgets, create custom canvases, configure the default dashboard. For more information, see [Using the Analytics Workspace](#).
- **Administration**—Enable, view, and disable system services. Configure parameters for logs, events, and analytics for the selected NexentaStor appliance. For more information, see [Managing NexentaStor Appliances](#) and [Rebooting or Powering Off a NexentaStor Appliance](#).

### Table 2-2: Getting Acquainted with Top-Level Tabs

<table>
<thead>
<tr>
<th>Top-Level Tab</th>
<th>Supported Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliances List</td>
<td>View a list of all registered appliances, or register an appliance. For more information, see <a href="#">Chapter 3, Registering NexentaStor Appliances</a>. Provision registered appliances. For more information, see <a href="#">Chapter 5, Managing NexentaStor Appliances</a>.</td>
</tr>
<tr>
<td>Dashboard</td>
<td>View information on the operational status of the appliance and summaries of logical and physical capacity, and performance metrics. For more information, see <a href="#">Dashboard</a>.</td>
</tr>
</tbody>
</table>
| Management | Pools:
- Aggregate available disks into pools, manage pools, and manage shared pools in a clustered appliance.
- Manage physical or logical disk devices for data or reserve as hot spares.
- Assign a cache device to the existing data pool to provide an additional layer of caching, and set a device in a pool to online or offline state.
- Configure an HA service, and add pools to an HA service. For more information, see [Chapter 5, Managing NexentaStor Appliances](#) and [Chapter 7, Fault Management](#). |
<p>| Filesystems | Create and manage file systems with a number of advanced capabilities for configuring data protection and sharing it over the network with NFS or SMB protocols. For more information, see <a href="#">Chapter 5, Managing NexentaStor Appliances</a>. |
| Volumes | Create and manage volume groups and volumes, configure data protection for volumes and volume groups, and share them over the network by mapping to LUNs, iSCSI or FC. For more information, see <a href="#">Chapter 5, Managing NexentaStor Appliances</a>. |</p>
<table>
<thead>
<tr>
<th>Top-Level Tab</th>
<th>Supported Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection:</td>
<td>Verify and query protection service data. For more information, see Protecting Data. For information on creating, editing, and deleting Protection Services, see Chapter 5, Managing NexentaStor Appliances.</td>
</tr>
<tr>
<td>High Availability (HA):</td>
<td>Note: The High Availability tab is only visible when a valid HA license is installed on the selected appliance. Manage HA services and monitor the status of cluster nodes. • Verify service status, and fail over services manually as necessary. • Add, edit, and delete VIPs • Move an HA service, stop, start, and delete an HA service. • View status on shared HA pools, and remove a pool from an HA service. For more information, see Managing High Availability.</td>
</tr>
<tr>
<td>Components:</td>
<td>• View hardware details, such as CPUs, memory, network adapters, disks, enclosures, and host bus adapters. • Verify if a disk under a selected chassis is online or offline, view sensor details of an enclosure, and locate a disk by LED blinking. For more information, see Chapter 5, Managing NexentaStor Appliances, and Chapter 7, Fault Management.</td>
</tr>
<tr>
<td>Networks:</td>
<td>• Manage network interfaces, and aggregate network interfaces. • Configure VLANs, and create network routes. For more information, see Chapter 5, Managing NexentaStor Appliances.</td>
</tr>
<tr>
<td>Analytics</td>
<td>Monitor aspects of appliance components operation and performance. The Analytics workspace has customizable widgets for visualizing real-time or historical performance and capacity metrics. You can change the Dashboard display from the Analytics workspace. For more information, see Chapter 6, Performance Monitoring and Analytics.</td>
</tr>
</tbody>
</table>
Now that you've logged in to NexentaFusion and become familiar with the NexentaFusion UI, continue with Chapter 3, Registering NexentaStor Appliances, and then complete the basic configuration to establish the connection between the NexentaFusion and NexentaStor appliances.

<table>
<thead>
<tr>
<th>Top-Level Tab</th>
<th>Supported Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Enable or disable HA cluster, idmap, NDMP, and STMF services. You can also configure, edit, and check the status of the services: iscsit, nfs, ntp, smb, and snmp.</td>
</tr>
<tr>
<td></td>
<td>• <strong>iSCSI target service</strong>—Configure the iSCSI target service and choose the supported authentication services like CHAP and Radius to share the NexentaStor appliance volume using the iSCSI protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NFS server</strong>—Configure the NFS server according to your IT infrastructure needs before sharing a file system. NFS allows you to share file systems on Linux and UNIX operating systems. Once shared, the file system displays as a local resource on the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NTP client</strong>—Add a reachable NTP server hostname to synchronize the time with the NTP server. Make sure the time is in sync using the same NTP Server for both Domain Controller and NexentaStor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SMB server</strong>—Configure SMB server to provide shared access to files between nodes on a network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SNMP service</strong>—Configure Simple Network Management Protocol (SNMP) to manage devices over an IP network.</td>
</tr>
</tbody>
</table>
Registering NexentaStor Appliances

This section includes the following topics:

- Registering a NexentaStor Appliance
- Confirming Registration
- Viewing Appliance Summary
- Viewing Appliance Licenses
- Viewing Appliance Profile and Version
- What Comes Next?

This chapter covers the procedures for registering a NexentaStor appliance. During the installation of NexentaFusion, you established a connection between NexentaFusion and the NexentaStor appliances by setting up the Web UI Network and Nexenta Management Network interfaces.

- **Web UI Network interface**—Used to access NexentaFusion UI for management purposes.
- **Nexenta Management Network interface**—Used by NexentaFusion to access and manage NexentaStor appliances.

To be able to manage a NexentaStor appliance with NexentaFusion, you must first complete the steps for Registering a NexentaStor Appliance.

### Registering a NexentaStor Appliance

Before you can manage the NexentaStor storage appliances using NexentaFusion, you must register the appliances in NexentaFusion. You can choose to register clustered or single node appliances.

If the appliance being registered has a host name identical to that of a currently registered appliance, an error dialog appears and registration is disallowed. You can change the host name using the CLI, then proceed with registering the appliance.

---

Clustered appliances must be configured using the CLI before they can be registered with NexentaFusion.

**Note:**

Both clustered nodes must be up and running to successfully complete the registration process.
To register a NexentaStor single or clustered node, do the following:

1. Log in to NexentaFusion as a Superuser and select **Appliance** from the drop-down list.
2. In the **Appliances List** page, click **Register Appliance**.
3. For either a single or clustered node, do the following:
   a) Enter the IP of one node in the cluster, or the IP of the single node appliance.
   b) Edit the port number, if not using the HTTPS default of 8443.
   c) Click **Continue**.
4. In the **Connection to Appliance** dialog, enter the credentials, click **I trust this certificate**, and then click **Continue**.
5. For a clustered appliance, after the first node successfully authenticates, a second dialog appears with the pre-filled credentials used to for the first node. If the credentials for the second node are different, enter the appropriate credentials, click I trust the certificate, and then click Continue.

6. Review the appliance settings, and configure Communication settings for the appliance.
For a clustered appliance, the communication settings are assumed to be the same for both nodes. If they are different, uncheck Use Same Settings for Both Nodes and edit the communication settings as needed.
7. Configure the SMTP server setting as necessary, and then click **Confirm**.

Once you have registered the NexentaStor appliance and all the credentials are authenticated, the appliance list displays it under the Appliances List drop-down list and Appliances main window. This Appliances List provides information on the total installed space and available storage.

**Confirming Registration**

The Appliances List provides information for all registered appliances.

- To view the list of registered appliances, do the following:
  1. Log in to NexentaFusion and select **Appliance** from the drop-down list.
  2. From the **Appliances Lists** menu, select **See All Appliances**. The registered appliance appears in the table.

**Viewing Appliance Summary**

After you registered a NexentaStor appliance, review the storage and appliance health. Storage health summarizes information of the pools, if they are online, raw capacity, utilization, and free space. Appliance health summarizes IO services, CPU details, and network details.

The Appliances List page displays the following information in tabular format:

- **Name**—Shows the appliance name, along with an icon that distinguishes it as a single or clustered node.
- **Health**—Describes the health of the appliance and the storage.

**Note:** Immediately after registering an appliance, its health is shown as “unknown” until the background tasks with additional requests to the appliance have completed.
• Alerts—Shows the number of alerts.
• Configured capacity—Shows the sum of free capacity and the allocated capacity of the pool after applying the redundancies (raid/mirror).
• Installed capacity—Shows the sum of disk sizes installed in the appliance.
• Actions—Provides a COG with a drop-down list of actions you can perform.

For more information, see NexentaFusion Icons, Main COG, and Top-Level Tabs.

Viewing Appliance Licenses

You can view the license file with the attributes from NexentaFusion UI.

To view the appliance license, do the following:

1. Log in to NexentaFusion and select Appliance from the drop-down list.
2. From the Appliances Lists menu, select See All Appliances.
3. Click the COG next to the appliance and select License from the drop-down list.

The license details appear, including licensed capacity, issue and expiration date, status of the appliance, license limitations, and licensed features.
Viewing Appliance Profile and Version

Once you select the registered appliance from the **Appliance List** view, the interface displays the Appliance profile and the SW version under the label Profile and Server.

The appliance profile is a collection of default tunables on the NexentaStor appliance. Setting a profile can be done at the initial setup of a NexentaStor appliance during the installation or at a later time using the NexentaStor 5.0 CLI. The default profile is generic. All-flash profiles change kernel settings and storage pool defaults for the best performance of the system configuration based on SSD drives.

See the **NexentaStor 5.0 Configuration QuickStart Guide** to learn about the profiles that can be applied to a NexentaStor appliance.

- **To view the appliance profile, do the following:**
  1. Log in to NexentaFusion and select **Appliance** from the drop-down list.
  2. From the **Appliances Lists** menu, select **See All Appliances**.
3. Select the appliance, and then click **Components**.

The Profile for the appliance appears on the top left side of the window with the NexentaStor version that is running on the appliance just beneath.

**What Comes Next?**

After successfully registering an appliance, continue with the basic configuration, as described in **Chapter 4, Configuring NexentaFusion**.
Configuring NexentaFusion

This chapter covers the following topics:

- NexentaFusion Configuration Overview
- Setting the SMTP Mail Server (Email Setup)
- Creating, Modifying, and Deleting Local UI User Accounts
- Adding NexentaFusion to Windows Active Directory (AD)
- Setting the Date/Time
- Configuring Session Settings
- What Comes Next?

NexentaFusion Configuration Overview

This section provides a process overview for completing an initial NexentaFusion configuration.

Note: NexentaFusion configuration tasks can only be performed by an admin “superuser”. For more information, see NexentaFusion Predefined User Roles.

To perform an initial NexentaStor appliance configuration, do the following:

1. Log in to NexentaFusion, click the Main COG in the top right corner of the window and select Settings from the drop-down list. Network is selected by default.

2. Verify the Web UI Network and Nexenta Management Network settings, that were configured during the NexentaFusion installation. For more information on these network interfaces, see Chapter 3, Registering NexentaStor Appliances.
3. Configure the SMTP server, as described in Setting the SMTP Mail Server (Email Setup).

4. Optional: Add NexentaFusion to Windows Active Directory, as described in Adding NexentaFusion to Windows Active Directory (AD).

5. Create NexentaFusion Local UI User accounts, as described in Creating, Modifying, and Deleting Local UI User Accounts.

6. Configure the date and time for the appliance, as described in Setting the Date/Time.

7. Configure the inactivity time for a user session, as described in Configuring Session Settings.

Setting the SMTP Mail Server (Email Setup)

This section demonstrates how to set up an SMTP mail server for NexentaFusion. The SMTP mail server parameters need to be configured to allow NexentaFusion to generate email notifications for NexentaFusion alerts.

The following table lists the parameters you configure for an SMTP server. Have this information ready before you begin to configure the SMTP parameters.

Table 4-1: SMTP Parameters

<table>
<thead>
<tr>
<th>SMTP parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server</td>
<td>SMTP server hostname or IP address.</td>
</tr>
<tr>
<td>SMTP User Name</td>
<td>Login name for the SMTP server.</td>
</tr>
<tr>
<td>SMTP Password</td>
<td>Password that you use to access your e-mail. Password for the SMTP server login.</td>
</tr>
</tbody>
</table>
To set the SMTP mail server, do the following:

1. Log in to NexentaFusion, click the Main COG in the top right corner and select Settings from the drop-down list.
2. In the left panel, select Email Setup.
   The SMTP setup page appears.
3. Enter the **SMTP server host name**, followed by the **Username** and **Password**, in the respective fields.
4. Specify the **SMTP port** and check the **Use SSL/TLS** check box to activate that feature.
5. Choose an **Authentication method** from the drop-down list, and specify a **Sender email address**.
6. Specify **Recipients** email addresses, separated by semicolons, and a **Local superuser admin email** address.

<table>
<thead>
<tr>
<th>SMTP parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMTP Server Port</strong></td>
<td>Port for the SMTP server. Port 25 is the default, but some IPs deny its use due to the extensive spam and malware traffic this port receives. You can choose to configure another port.</td>
</tr>
</tbody>
</table>
| **SMTP Authentication method** | Use SSL/TLS  
Method of SMTP authentication that your mail server uses:  
Plain (default value) or Login |
| **Sender email address**  | The email address displayed in the Sender field for all emails originating from NexentaFusion.                                             |
| **Recipients**            | One or more existing email addresses to receive all notifications generated by NexentaFusion. Separate multiple email addresses with a semicolon. |
| **Local superuser admin email** | Email address of the superuser admin, required for the recovery of lost passwords.                                                       |
Creating, Modifying, and Deleting Local UI User Accounts

Each user role has specified access privileges that define the tasks the user is allowed to perform. NexentaFusion provides the following predefined User roles, as described in Table 4-2. This section covers the following topics:

- [Creating a New Local UI User Account](#)
- [Changing the Login Credentials and Role for a Local UI User](#)
- [Deleting a Local UI User Account](#)

**Note:** NexentaFusion configuration tasks can only be performed by a “superuser” admin. For more information, see [NexentaFusion Predefined User Roles](#).
Creating a New Local UI User Account

You can create any number of NexentaFusion user accounts. Each account can only be assigned one user role, and each account must have a unique username and password.

When a user enters a username and password on the Login screen, NexentaFusion checks first to see if that username is in the local user list. If the name is not on the local user list, and AD is configured, then AD is checked. When you configure AD users, you must delete any local users that may be duplicates of the AD users. For more information, see Adding NexentaFusion to Windows Active Directory (AD).

To create a Local UI User account, do the following:

1. Log in to NexentaFusion as a superuser admin, click the Main COG in the top right corner of the window and select Settings from the drop-down list.
2. In the left panel, select Local UI User Setup.
3. Click New User +.
4. Enter a Username and Password in the respective fields, and then re-enter the password in the Repeat password field.
5. Select a User role from the drop-down list. For an explanation of the user roles, see Table 4-2.
6. Enter an Email address to allow for the recovery of a username or password.

---

Table 4-2: NexentaFusion Predefined User Roles

<table>
<thead>
<tr>
<th>User Roles</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>A user account has all administrative privileges, with the exception of registering an appliance and managing NexentaFusion settings.</td>
</tr>
<tr>
<td>Superuser</td>
<td>A superuser admin account has complete administrative privileges for NexentaFusion management. A superuser can configure NexentaFusion, view all UI pages, perform all actions, and recover lost passwords.</td>
</tr>
<tr>
<td>Viewer</td>
<td>A viewer account has read-only privileges and no administrative permissions. This user role can view all pages, but is unable to perform create, delete, or modify actions.</td>
</tr>
</tbody>
</table>
7. Click **Save**.

### Changing the Login Credentials and Role for a Local UI User

This section demonstrates how to change the login credentials and role for a Local UI user, as well as ensuring a lost username and password can be retrieved if needed. Local administrators (admin superusers) have the ability to reset credentials for Local UI users, from the Local UI User Setup page. For an explanation of the user roles, see Table 4-2.

- **To change the login credentials for a local user, do the following:**
  1. Log in to NexentaFusion as a superuser admin, click the **Main COG** at the top of the window, and select **Settings** from the drop-down list.
2. Click **Local UI User SetUp** in the left panel, then click the **COG** for the admin user and select **Edit**.

3. Enter a new **Password** in the text field of the dialog, then enter it again in the **Repeat password** field.

4. Optionally, select the **Force password change on next user login** check box.

5. To change the **User role**, make a selection from the drop-down list.

6. To be able to retrieve login credentials in the case of a lost username or password, enter an **Email address** at which to be notified.

   In case of a lost username and password, you can reset the credentials from the Login screen. To do this, you must have configured the SMTP mail server and set up an email address at which to receive notifications. For information on how to configure the SMTP server, see **Setting the SMTP Mail Server (Email Setup)**.

7. Click **Save**.
Deleting a Local UI User Account

You can delete a Local UI user account at any time from the Local UI User Setup page.

- To change a user role or delete a Local UI User account, do the following:
  1. Log in to NexentaFusion as a superuser admin, click the Main COG at the top of the window, and select Settings from the drop-down list.
  2. In the left panel, select Local UI User Setup.
  3. Click the COG for the user you want to delete, and select Destroy from the drop-down list.
  4. In the confirmation dialog, click Destroy to delete the user account.

Adding NexentaFusion to Windows Active Directory (AD)

You can integrate NexentaFusion with Windows Active Directory (AD) to take advantage of Active Directory authentication and authorization. When integrating with an AD server, you can create mappings for AD users and groups with the local UI user roles (superuser, user and viewer).

If you have integrated NexentaFusion with Windows Active Directory (AD), you can login with your AD user credentials. When you enter a username and password, NexentaFusion first checks the local user list. If the user name is not on the local user list and AD is configured, then AD is checked. When you configure AD users, you must first delete local users that are duplicates of the AD users.

Prerequisites

Before you begin integrating NexentaFusion with Active Directory, make sure your environment meets the following prerequisites:

- Windows Server 2012 or 2012R2.
- Active Directory configured on a Windows Server.
- DNS server installed and working in the Active Directory environment.
- NexentaFusion and the Domain Controller use the same NTP Server and the time is in sync on both systems.
- If the NexentaFusion network interface is configured as DHCP, the DHCP server name-server list contains the IP address of the DNS server that is used for the Active Directory domain.
- Ensure that you are logged in to NexentaFusion as superuser to integrate NexentaFusion with AD server.
- If you have a DNS server that is not part of the Active Directory DC, make sure the DNS Server that is used by NexentaFusion has the proper DNS records to locate the AD server. If you use Active Directory as your DNS server, everything is configured by default.
Configure NexentaFusion for Windows AD

You must be logged in to NexentaFusion as superuser to perform the following procedure.

- **To integrate NexentaFusion with a Windows AD server, do the following:**
  1. Log in to [NexentaFusion](https://nexenta.com) as a superuser admin, click the Main COG in the top right corner of the window, and select **Settings** from the drop-down list.
  2. In the left panel, select **Active Directory**.
  3. In the Active Directory window, specify the following:
     - **AD server name**—Enter the name of the Active Directory server.
     - **Port number**—Enter the port number for the AD server.
     - **Use SSL/TLS**—Select this check box to implement Secure Socket Layer (SSL) and Transport Layer Security (TLS).
     - **Base DN**—Enter the base domain name.
     - **AD username**—Enter the AD user name.
     - **AD Password**—Enter the AD password.
     - **FQDN**—Enter a fully qualified domain name (FQDN), such as example.com.
     - **User groups**—Enter the unique ID for each user group.
     - **Viewer groups**—Enter the unique ID for each viewer group.
     
         **Warning!** Changing the following settings will invalidate all sessions.
         - AD server name—Enter the name of the Active Directory server.
         - Port number—Enter the port number for the AD server.
         - Use SSL/TLS—Select this check box to implement Secure Socket Layer (SSL) and Transport Layer Security (TLS).
         - Base DN—Enter the base domain name.
         - AD username—Enter the AD user name.
         - AD Password—Enter the AD password.
         - FQDN—Enter a fully qualified domain name (FQDN), such as example.com.
         - User groups—Enter the unique ID for each user group.
         - Viewer groups—Enter the unique ID for each viewer group.
         
         For more information on local user groups, see the [NexentaStor 5.0 User Guide](https://nexenta.com).
  4. Click **Save**.

Setting the Date/Time

You can synchronize the NexentaFusion time setting with the NTP server, or manually configure the time in the server time zone. To synchronize the NexentaFusion time setting with the NTP server, you must add a reachable NTP hostname. This section demonstrates how to automatically synchronize the NexentaFusion time setting with the NTP server, as well as how to manually configure the date and time.

- **To synchronize with the NTP server, do the following:**
  1. Log in to [NexentaFusion](https://nexenta.com) as a superuser admin, click the Main COG in the top right corner of the window, and select **Settings** from the drop-down list.
  2. In the left panel, select **Date/Time**.
  3. Click the **Daily time synchronization with NTP** check box.
  4. Enter the URL for the NTP server of your choice.
5. Click Save.

To manually configure the date and time, do the following:

1. Log in to NexentaFusion as a superuser admin, click the Main COG in the top right corner of the window, and select Settings from the drop-down list.

2. In the left panel, select Date/Time.

3. To set the date and time, deselect Daily time synchronization with NTP, if it is selected.

4. In the Time in server timezone, enter the hour, minutes and seconds (hh:mm:ss).

5. Click inside the Date field and select a date from the pop-up calendar.

6. Click Save.
Configuring Session Settings

You can configure the inactivity time for user sessions, between 1 to 60 minutes, after which the user will be required to log in again.

- To configure the inactivity time for user sessions, do the following:
  1. Log in to NexentaFusion as a superuser admin, click the Main COG in the top right corner of the window, and select Settings from the drop-down list.
  2. In the left panel, select Session Settings.
  3. In the Session inactivity time field, enter a value between 1 and 60 (minutes).
  4. Click Save.

The system will require a user to log in again whenever their session is inactive longer than the specified time.

What Comes Next?

In the following chapter you learn how to provision NexentaStor appliances and manage them in your environment.
Managing NexentaStor Appliances

This section includes the following topics:

- Provisioning Overview
- Verifying Enclosure and Disk Information
- Managing Network Configurations
- Creating and Managing Pools
- Creating and Managing File Systems
- Sharing File Systems Using NFS
- Sharing File Systems Using SMB
- Creating and Managing Volume Groups and Volumes
- Managing LUNs
- Managing iSCSI Host Groups, Targets, and Groups
- Managing FC Host Groups, Targets and Target Groups
- Protecting Data
- Managing High Availability
- What Comes Next?

Provisioning Overview

With NexentaFusion, you can create a pool on a clustered or a non-clustered appliance. For a clustered appliance, you can configure pools with a High Availability (HA) service to ensure the pools automatically failover to the alternate node in case of a system failure.

You can create file systems and share them for anonymous access or authenticated access in workgroup mode or domain. Likewise, you can create volume groups and volumes, and share the volumes by mapping them as LUNs. NexentaFusion provides data protection capabilities that apply to any dataset, be it a file system, volume group, or volume. Data protection is accomplished through the use of snapshots, and replication that can be scheduled or continuous. For more information, see Protecting Data.

To provision a single node or a clustered NexentaStor appliance using NexentaFusion, complete the tasks in Table 5-1 in the order in which they are presented.
Table 5-1: Provisioning Task Map

<table>
<thead>
<tr>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Identify disks associated with a NexentaStor appliance.</strong></td>
<td>After registering a NexentaStor appliance, and if there are JBODs attached, you may want to review the disks that can be assigned as data, cache, spare, or log devices. This section demonstrates how to view all the enclosures and disks enclosed in a chassis. For information, see Verifying Enclosure and Disk Information.</td>
</tr>
<tr>
<td><strong>2. Update the NexentaStor appliance network, as needed.</strong></td>
<td>This section demonstrates how to do the following:</td>
</tr>
<tr>
<td></td>
<td>- Verify the network interface you configured during NexentaStor appliance installation.</td>
</tr>
<tr>
<td></td>
<td>- Optional: Configure aggregates and VLANs to maximize the network performance and monitor status.</td>
</tr>
<tr>
<td><strong>3. Configure a pool for a single node or clustered appliance.</strong></td>
<td>This section demonstrates how to do the following:</td>
</tr>
<tr>
<td></td>
<td>- Identify the disks that can be used in a pool.</td>
</tr>
<tr>
<td></td>
<td>- Create a pool with the desired redundancy characteristics.</td>
</tr>
<tr>
<td></td>
<td>- Add cache devices and disk logs to optimize performance.</td>
</tr>
<tr>
<td></td>
<td>- Add spares to improve availability.</td>
</tr>
<tr>
<td></td>
<td>- Add unmap support for SSDs to efficiently use the storage.</td>
</tr>
<tr>
<td></td>
<td>- Schedule a scrub service to check the pool integrity.</td>
</tr>
<tr>
<td><strong>4. Configure a shared pool HA service for the failover of HA cluster pools.</strong></td>
<td>A NexentaStor HA Cluster detects system failures and then transfers ownership of shared pools to the alternate appliance. These sections demonstrate how to do the following:</td>
</tr>
<tr>
<td></td>
<td>- Add a shared pool to an HA service.</td>
</tr>
<tr>
<td></td>
<td>- Configure a VIP for clients to access.</td>
</tr>
<tr>
<td><strong>5. Configure a file system, or volume group and volumes.</strong></td>
<td>The file system is managed by multiple properties for maximum performance and optimization. A volume group is a container for managing volume datasets. These sections demonstrate how to do the following:</td>
</tr>
<tr>
<td></td>
<td>- Create and manage file systems.</td>
</tr>
<tr>
<td></td>
<td>- Create and manage volume groups and volumes.</td>
</tr>
</tbody>
</table>

For information, see Configuring an HA Service for a Shared Pool, and Creating and Managing Pools.
Verifying Enclosure and Disk Information

After registering a NexentaStor appliance, you can view the appliance hardware information, such as CPUs, memory, network adapters, disks, enclosures, and host bus adapters. If you have JBODs attached to a NexentaStor appliance, NexentaFusion provides a graphical or tabular view of the JBODs chassis for easy management of the chassis and disks.

This section covers the following topics:

- Enclosure Components Overview
- Filtering System Components
- Verifying and Modifying IP Links

Enclosure Components Overview

Table 5-2 and Table 5-3 explain the parameters for the JBOD Sensor Panel and Disk Panel respectively.
Table 5-2: JBOD Sensor Panel Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Lists the devices in a JBOD: fan, PSU, and JBOD. Sensors that help to monitor JBOD devices state include temperature, voltage, and so on. For every vendor, a sensor (such as jbod_temperature1 or jbod_voltage3) can indicate a different parameter. Refer to the vendor-specific JBOD technical documentation. If sensor readings exceed the predefined JBOD thresholds, an alert is generated and a failure notification is sent to the specified e-mail address. The e-mail notification must be enabled and configured.</td>
</tr>
<tr>
<td>Value, Units, Type</td>
<td>Displays the appropriate value for a sensor type, such as: Temperature - C°.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the device: ONLINE—Device is online and fully functional. OFFLINE—Device is offline. UNAVAIL—Device is unavailable. NO_MEDIA—Removable device has no media, so no logical device is assigned. RETIRED—Device was retired. RETIRING—Device in the process of being retired. ORPHANED—Device discovered but cannot be matched, a rare condition. UNKNOWN—Device state cannot be retrieved, the device may not be responding.</td>
</tr>
</tbody>
</table>

You can view the state of the disk and the occupied disk slots. Green indicates a disk online that can be used for creating a pool, if the disk is not already used in a pool or exported. Red indicates a disk that cannot be used for creating a pool.

Table 5-3: Disk Panel Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Device</td>
<td>Displays the disk name in NexentaFusion. The typical format is c0t0d0, where c is the controller number, t is the target number, d is the logical unit number.</td>
</tr>
<tr>
<td>Pool</td>
<td>Displays the pool name to which the device belongs.</td>
</tr>
<tr>
<td>Model</td>
<td>Displays the model of a disk.</td>
</tr>
<tr>
<td>Serial</td>
<td>Displays the disk serial number.</td>
</tr>
<tr>
<td>State</td>
<td>Displays disk status. The state of the disk can vary according to JBOD model. Refer to the JBOD documentation for more information.</td>
</tr>
<tr>
<td>Exported</td>
<td>Displays the exported value as “yes”, if the device belongs to an exported pool.</td>
</tr>
</tbody>
</table>
Filtering System Components

This section demonstrates how to filter system components in the Chassis display.

To filter hardware components shown in the Chassis display, do the following:

1. Log in to NexentaFusion, and click Appliance if not already in the Appliance view.
2. In the Appliances List, click an appliance and select Management.
3. Click Components.
4. Make selections from the following filter drop-down lists, as appropriate for the appliance:
   - Selected chassis—Select the chassis to be displayed. You can make multiple selections.
   - Selected disks—Select the disks to be shown. The display changes with each selection.
5. Select an option again to remove it from the list, and the display changes accordingly.

Viewing Hardware Components

The Components page displays a list of disks in a chassis, as well as sensors, slotmap image, and information about the devices in a JBOD. To view the information about a disk, hover the cursor over the disk label under Chassis. You can also filter the view by specific chassis and disk type.

To view the hardware components and JBODs of a single or clustered node, do the following:

1. Log in to NexentaFusion, and click Appliance if not already in the Appliance view.
2. In the Appliances List, click an appliance and select Management.
3. Click Components, and select the hardware component. If the appliance is clustered, select the node you want to view.
4. For detailed information, click the triangle on the left to expand the view.

5. To view chassis devices in graphical or tabular mode, select the appropriate icon.

6. Click the **COG** and choose from the following options on the drop-down list:
   - Select **Display enclosure sensors information** to view a table with information on the state of various components.
   - Select **Edit enclosure label** to change the label of a chassis enclosure by entering it in the text field that appears.
• Select **Display enclosure image** (for certain chassis models) to see the physical layout.

7. Do the following, as necessary:
   • To view the connection details of the JBOD, click **View Connection Details**.
   • To locate a disk using the blink feature, click **Show Indicators** and then click the indicator.

This sets the indicator on the JBOD to flash, allowing you to easily locate the disk in a storage rack. Use this functionality to physically locate a failed disk.
8. To view the details for a disk, such as model, serial number, and RPM, hover the cursor over the disk label under Chassis.

Managing Network Configurations

NexentaFusion enables you to manage network interfaces and configurations in the following ways:

- Verifying and Modifying IP Links
- Creating Aggregates
- Adding a VLAN
- Adding an Address
- Verifying IP Addresses
- Creating, Verifying, and Deleting IP Routes
- Modifying IP Network Settings
- Verifying FC Interfaces

Verifying and Modifying IP Links

During NexentaStor 5.0 installation, you set up the network interface card (NIC) for the NexentaStor appliance. This section demonstrates how to verify the network interface is in place and properly configured. You can view existing network (hardware and software) interfaces (NICs), links, and aggregations. The following table describes the network interface tasks you can perform with NexentaFusion.
Table 5-4: Modifying Network Interfaces for NexentaStor Appliances

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add another address</td>
<td>You can add another IP address to a link.</td>
</tr>
<tr>
<td>Destroy</td>
<td>Completely removes any configurations set for this interface and sets Configuration field back to “Unconfigured”.</td>
</tr>
<tr>
<td>View</td>
<td>You may view the list of addresses associated with any link and their detailed information such as name, network mask, address type and their current state. A link remains busy when it has at least one associated address object.</td>
</tr>
<tr>
<td>Delete</td>
<td>When you delete an address object from a specified link, the system that uses this network address will become unreachable after deleting an address.</td>
</tr>
<tr>
<td>Unconfigure</td>
<td>You can unconfigure a NIC interface in order to remove it smoothly from the appliance, or to modify the network.</td>
</tr>
<tr>
<td></td>
<td>Note: If you unconfigure the primary interface, you lose the connection to NexentaFusion over SSH.</td>
</tr>
<tr>
<td>Advanced Settings / Destroy</td>
<td>You can set MTU or destroy a link using the COG menu options.</td>
</tr>
</tbody>
</table>

To verify a network interface, do the following:

1. Log in to NexentaFusion and click **Appliance**, if not already in the Appliance view.
2. In the **Appliances List**, click an appliance and select **Management**.
3. Click **Networks > IP Links**.
   - A tabular display showing link names, state, speed, class, over, IP address, and VLAN tag (as applicable) for the selected appliance appears.
4. Click the triangle to the left of the **Link** name to expand the table and verify the VLANs for network interface cards (NICs) or aggregations for a specific link. Click the triangle again to collapse the view.

   The table shows the addresses associated with links, and related information such as the name of the alias or address object, IP address, and configuration type (static/DHCP).
5. Click the **COG** in the far right column to do the following, as necessary:
   - Select **Advanced Settings** to set the maximum transmission unit (MTU) for the link.
   - Optionally, select **Unconfigure** to unconfigure a NIC interface so you can remove it smoothly from the appliance, or to modify the network.

   **Note:** When you unconfigure the management interface, you lose the SSH connection with NexentaFusion.

   - Select **Destroy** to delete a link, VLAN, or IPMP group, then in the confirmation dialog click **Yes**.

### Creating Aggregates

Link aggregation combines multiple physical Ethernet links into one logical link to increase network performance and protect the appliance against failures. Link aggregations are beneficial in the following ways:

- Administering multiple interfaces as a single port.
- Using one IP address to aggregate multiple interfaces.
- Securing the IP address of an aggregation from external applications.
- Allowing for the automatic failover of IOs from a failed interface to a usable link in the aggregation.
- Increasing the bandwidth within a physical network setup.

Aggregation prevents appliances from being limited to the bandwidth of the largest NIC, increasing the throughput to that of the combined NICs.

When creating an aggregate, you are asked to (optionally) specify Link Aggregation Control Protocol (LACP) mode settings for the aggregations. NexentaStor supports LACP - IEEE 802.3ad. LACP automatically bundles multiple physical ports into a single logical channel, thus providing greater performance and availability. The following LACP modes are supported on NexentaStor Ethernet ports:

- **off**—The port does not participate in link aggregation negotiation.
- **passive**—The port responds to link aggregation control commands and participates in negotiations initiated by the remote switch.
- **active**—The port actively issues link aggregation control commands and tries to negotiate link bundles with the remote switch.

   ✤ **To create an aggregation, do the following:**

   1. Log in to NexentaFusion and click **Appliance**, if not already in the Appliance view.
   2. In the **Appliances List**, click an appliance and select **Management**.
   3. Click **Networks > IP Links**.

      A tabular display showing the link names, state, speed, class, over, IP address, and VLAN tag (as applicable) appears.

   4. Click the check boxes to the left of two or more available links, then click the **Create Aggregate** button that appears at the bottom of the screen.
5. Specify the following information:
   - Aggregate Name—An alphanumeric value that ends with a digit, such as aggr0.
   - LACP Mode—Optional: Default, Off, Active, Passive
   - LACP Policy—Optional: Default, L2, L3, L4
   - LACP Timer—Optional: Default, short, long
   - MAC Address—Optional: MAC address of aggregation

6. Click Create.

Adding a VLAN

Adding a Virtual Local Area Network (VLAN) is recommended for flexibility in managing network traffic. A VLAN is a group of hosts with a common set of requirements that communicate as if they were attached to the broadcast domain, regardless of their physical location.
NexentaFusion allows you to group network hosts together according to resource needs, rather than being limited to grouping hosts that are on the same network switch. Using VLANs with NexentaStor 5.0 provides greater flexibility in managing and responding to network traffic needs.

VLANs provide the segmentation services traditionally provided by routers in LAN configurations. You can configure VLANs to address issues, such as scalability, security, and network management.

To assign a VLAN to a link, do the following:

1. Log in to NexentaFusion and click **Appliance**, if not already in the Appliance view.
2. In the **Appliances List**, click an appliance and select **Management**.
3. Click **Networks > IP Links**.
   
   A tabular display of link names, state, speed, class, over, IP address, and VLAN tag (as applicable) appears.
4. Click the check box next to the link to be assigned to the VLAN, then click the **Assign VLAN** button at the bottom of the screen.
5. In the Assign VLAN dialog, specify the following information:
   - VLAN Name—An alphanumeric value that ends with a digit, such as vlan1
   - VLAN ID—An identification number for the VLAN, a value between 1 and 4096
6. Click **Assign**, and the VLAN automatically appears in the table.
Adding an Address

It is recommended that you create an address object and assign it to a specified network link. When creating an address object, you specify a name, type (static, dhcp, mgmt, addrconf), and network mask. You can have any number of associated addresses in a link.

For a static address, you set the network IP address, network mask and name. For dynamic address configurations ("dhcp" for IPv4 and "addrconf" for IPv6) only a name is required. IPv4 and IPv6 are both for addresses and network masks. The protocol version depends on your input.

You can add additional network interfaces (NIC) to an appliance for use in high availability scenarios, link aggregation, multipath, and so on. You can create a link aggregation or VLAN on top of specified network links. To create an aggregation, at least two physical links are required. To create a VLAN on top of specified links, a unique VLAN identification number (VID) is required.

Note: A link will remain busy when it has at least one associated address object.

To configure a network interface, do the following:

1. Log in to NexentaFusion and click Appliance, if not already in the Appliance view.
2. In the Appliances List, click an appliance and select the Management tab.
3. Click Networks > IP Links.

A tabular display showing the link names, state, speed, class, over, IP address, and VLAN tag (as applicable) appears.

4. To add an IP address to a link, do the following:
   a) Click the check box to the left of the Link name, and then click Add Address at the bottom of the window. The Add Network Address dialog appears.
   b) Enter a Name and select an address Type from the drop-down list. The remaining fields may change depending on the Type of link selected.
   c) Specify the information for the remaining fields, and click Add Address.

The information required varies with the type of address being added. The following example is for a static (IPv4) address.
Verifying IP Addresses

This section demonstrates how to verify information for virtual IP (VIP) addresses and appliance IP addresses. For information on creating a VIP, see Configuring an HA Service for a Shared Pool.

To verify appliance IP address information, do the following:

1. Log in to NexentaFusion and click **Appliance**, if not already in the Appliance view.
2. In the **Appliances List**, click an appliance and select **Management**.
3. Click **Networks > IP Addresses**.

   A tabular display showing appliance addresses appears. For clustered appliances, the virtual IP (VIP) addresses are also shown.

4. For VIPs, verify the following information:
   - IP address—address assigned to the VIP
   - Name—unique name for the VIP
   - Interfaces—health states of the VIP interfaces
   - Service—name of service assigned to the VIP

5. For appliance network interfaces, verify the following information:
   - IP address—addresses assigned to appliance interfaces
   - Name—unique name for the address
   - Address State—current health state for each address
   - Type—interface type, for example: static, dhcp, mgmt, and addrconf
   - Interface State—current health state for the interface

6. To unconfigure an interface, do the following:
   a) Click the COG on the far right.
   b) Select **Unconfigure** from the drop-down list.
   c) In the confirmation dialog, click **Yes**.
Creating, Verifying, and Deleting IP Routes

You can view existing network routes, create new network routes, and delete network routes as necessary. You create a new network route by providing the network or host as destination, and specifying a reachable gateway address through which the packets are to be routed. You can set IPv4 as the default protocol version.

Note: The gateway must be reachable by the network for you to be able to create a route.

To verify and create an IP route, do the following:

1. Log in to NexentaFusion, and click **Appliance** if not already in the Appliance view.
2. In the **Appliances List**, click an appliance, and select **Management**.
3. Click **Networks > IP Routes**.
   A tabular display of information for any existing IP routes appears.
4. Click **Create New Route**, and in the Create Network Route dialog do the following:
   a) Enter a route **Destination** address that is a reachable host or network.
   b) Enter a **Gateway** address, which can be a host, network, or default.
5. Click **Create**.

- **To verify or delete an IP route, do the following:**
  1. Log in to NexentaFusion, and click **Appliance** if not already in the Appliance view.
  2. In the **Appliances List**, click an appliance, and select the **Management** tab.
  3. Click **Networks > IP Routes**.
     
     A tabular display of information for existing IP routes appears.
  4. To view the status of route flags, hover the cursor over the address in the Destination column.

5. Verify the following information for each route:
   - **Destination**—Address assigned as the route destination
   - **Gateway**—Address assigned for the Gateway
   - **Protocol**—Route protocol (IPV4, IPV6)
• Interface—Route interface
• References—Number of references associated with the route
• Static—Check mark appears if it is a static route, and empty if not

6. To delete a static route, click the trash can icon in the far right column.

Modifying IP Network Settings

During NexentaStor 5.0 installation, you may have set up a domain name server (DNS) during the initial NexentaStor installation. This section demonstrates how to verify the established DNS settings, and modify them as needed.

❖ To verify and modify DNS settings, do the following:

1. Log in to NexentaFusion, and click Appliance if not already in the Appliance view.
2. In the Appliances List, click an appliance, and select Management.
3. Click Networks > IP Network Settings.
   The DNS settings for the selected appliance appear.
4. Enter new DNS settings, as necessary, and then click Save.
5. Optional: For clustered nodes, click the Use same settings for all nodes check box to apply the DNS settings to both nodes.
6. Click Save.
Verifying FC Interfaces

This section demonstrates how to verify information for FibreChannel (FC) appliance interfaces.

To verify appliance FC interface information, do the following:

1. Log in to NexentaFusion, and click Appliance if not already in the Appliance view.
2. In the Appliances List, click an appliance, and select Management.
3. Select Networks > FC Interfaces.
   
   A tabular display showing the appliance FC interface information appears.

4. Verify the following information:
   
   - Port WWN—unique World Wide Name (WWN) indicator for the port assigned to the appliance interface
   - State—current health status for the port
   - Current Speed—measured in Gb
   - Mode—initiator or target mode
   - Node WWN—unique WWN indicator assigned to the node
   - HBA—make and model of the Host Bus Adapter (HBA)

Note: Changing the mode of a port can only be done through the CLI, and requires that the node be rebooted to take effect.
Creating and Managing Pools

The following tasks demonstrate how to plan for, create, edit, and configure an HA service for a shared pool:

- Planning for Pools
- Viewing Available Disks for a Pool
- Creating Pools on Single or Clustered Nodes
- Editing an Existing Pool
- Configuring an HA Service for a Shared Pool

The following tasks demonstrate how to manage pools:

- Discovering Pools and Viewing Pool Status
- Setting Management Actions
- Editing Pool Properties
- Adding an Unshared Pool to HA Service
- Viewing VIPs Associated with an HA Service
- Moving a Pool under HA Service for Manual Failover
- Removing a Pool From HA Control

Planning for Pools

A pool is a virtual storage entity consisting of one or more virtual devices (vDevs) comprised of block devices. Pools enable you to manage a collection of devices as a single entity, independent of the storage under the pool. Before you can create a pool, NexentaStor must have virtual or physical disks available.

To begin working with NexentaStor, initially you must create a storage pool. The Pool Creation Process includes selecting disks for one or more data vDevs, then adding cache, log, special, and spare devices as needed. NexentaFusion provides Creating Pools on Single or Clustered Nodes and component filtering capabilities to increase the efficiency of finding specific device types to add to a pool. Consider the following factors before creating a storage pool:

- Determine the capacity and performance for each group.
- Determine if the pool is intended for a clustered or non-clustered environment.
- Analyze and plan the organization of the pools.
- Determine if redundancy is required, and what type is best suited for your site: mirror, RAIDZ1, RAIDZ2, or RAIDZ3. See Creating Pools on Single or Clustered Nodes for disk requirements for each redundancy type.
- Determine the replication requirement based on storage needs.
- You can increase the size and capacity of a pool, but you are not allowed to decrease the size of a pool.
Viewing Available Disks for a Pool

Once you register a NexentaStor appliance with a JBOD attached, you can create a pool. The first step in that process is to review the disks that are available to be assigned to a pool.

To identify disks for usage, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance on which you want to create the pool.
3. Under **Management**, click **Pools > Create Pool**.

   A table appears with the **Available Drives** number of disks that can be added as vDevs, cache, spares, logs, or used for HA.
   - **Total**—Number of drives accessible to both nodes in a cluster and drives accessible by only a single node.
   - **HA**—Number of drives that are accessible to both nodes in an HA cluster, and can be used to create an HA pool.

4. Assess the available devices, estimate the needs for the pool, considering the factors described in **Planning for Pools**, then continue with **Creating Pools on Single or Clustered Nodes**.

Creating Pools on Single or Clustered Nodes

This section explains the advantages of using **Guided Configuration**, and demonstrates how to create a pool on a single node or on a clustered appliance. The following table provides the short list of tasks that comprise the pool creation process. It is recommended that you perform the tasks in the order listed.

Table 5-5: Pool Creation Process

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Naming and Configuring a Pool</strong></td>
<td>Give the pool a name, set high availability (HA) as necessary, and choose a build method.</td>
</tr>
<tr>
<td>2. <strong>Adding Data Devices to a Pool</strong></td>
<td>Add disks to be used as data devices.</td>
</tr>
<tr>
<td>3. <strong>Adding Cache, Log, Special, and Spare Devices to a Pool</strong></td>
<td>Optionally, specify redundancy and add disks to be used as cache, log, special (write back cache), or spare devices.</td>
</tr>
</tbody>
</table>
Guided Configuration

The Guided Configuration tool provides greater efficiency in showing the appropriate available disks when creating a pool. After selecting a redundancy level, available disks are shown from which you can choose. Guided Configuration follows these basic guidelines:

- Disks must be of the same type (HDD or SSD).
- Disks must be of the same capacity.
- Available disks of the same type are shown in bright green with a plus (+) sign.
- After an initial selection of drives, Guided Configuration displays recommended drives, based on the logic (drive type, size, and location) of the previous selection.
- Redundancy configurations must contain the following minimum number of disks:
  - Mirror: Must have at least two (2) devices
  - RAIDZ1: Must have at least three (3) devices
  - RAIDZ2: Must have at least five (5) devices
  - RAIDZ3: Must have at least seven (7) devices

---

**Note:** Though not recommended, you can turn OFF Guided Configuration at any time and select disks of different types and sizes.

Naming and Configuring a Pool

The first step in the pool creation process is to establish a name, set HA as necessary, and specify the build method for the pool.

- **To name and configure a pool, do the following:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance on which you want to create the pool.
  3. Under **Management**, click **Pools > Create Pool**.
  4. In the **Create Pool** panel on the left, enter a **Pool name** and do one of the following:
5. For a single node, select the **Build Method: Manual**. Auto is only supported in NexentaStor 5.0 CLI.

![CREATE POOL]

For a High Availability cluster, make a selection from the **Select HA mode** drop-down list. If the pool is to be shared across both cluster nodes, select **Enable**. Otherwise, select the cluster node on which the pool is to reside, then select **Build Method: Manual**.

![CREATE POOL]

5. In the **Manual Pool Creation** dialog, click **Continue**, and proceed to **Adding Data Devices to a Pool**.
Adding Data Devices to a Pool

A pool is made up of one or more data devices (vDevs or disks). A vDev can be a single disk, or a group of disks created with configured redundancy. When you use multiple vDevs in a pool, the data is striped across the vDevs to enhance performance and maximize usable space.

Guided Configuration is enabled by default. Though not recommended, you can choose to turn Guided Configuration OFF at any time, and make selections based on your own criteria.

When you create a storage pool, you must explicitly specify the data devices and the data redundancy level.

To add devices to a pool, do the following:

1. Complete Naming and Configuring a Pool.
2. Select redundancy for the pool from the drop-down list:
   - Non-redundant
   - mirror (two-way or three-way)
   - RAID-Z1 (3 or more disks)
   - RAID-Z2 (5 or more disks)
   - RAID-Z3 (7 or more disks)
3. Optionally, filter for available selections, choosing options from the Select chassis and Select disks drop-down lists. The disk display changes to reflect the filter results.
4. Before adding disks to the pool, verify the details of the available drives by hovering the cursor over the disk label in the table.

![Image of disk pool with disk labels showing green and red indicators]

Green indicates a disk that is in a healthy state and can be used for creating or building a pool. Red indicates a disk that is corrupted or failed, and cannot be used for creating or building a pool.

5. Click the plus icon (+) to add a disk to the vDev in the pool. Click the minus (-) icon to remove an incorrectly selected disk from the vDev, and select another.

![Image of vDev configuration with disk icons and plus/minus buttons]

6. To add another device, click **New vDev +**. When Guided Configuration is ON, the vDev is populated with disks similar to those similar to the previous vDev, if available.
7. Click **Next** and continue with Adding Cache, Log, Special, and Spare Devices to a Pool.

**Note:** Guided Configuration is **ON** by default. Though not recommended, you can disable Guided Configuration and choose disks of varying type and capacity.

**Adding Cache, Log, Special, and Spare Devices to a Pool**

To improve the performance, you can also add optional pool devices when creating a pool. For cache and log devices, Nexenta recommends the use of high-performance devices such as SSD. You can also set the Auto Expand property during the pool creation.

- **Cache**—To improve the performance for random-read workloads, you can add an additional layer of caching between main memory and disk with cache devices. You have the option to add more than one cache device when creating a pool. Cache devices can also be removed any time after you create the pool.

- **Log**—To improve the performance, use ZFS Intent Log (ZIL) for non-volatile temporary storage for writes not yet stored on the zpool. ZIL works as a WRITE cache layer in-between main memory and disk storage pool. When adding the log devices, specify the log redundancy too.

- **Special**—To increase performance of hybrid pools, use a special device for write back cache (WBC). A special device can only use SSDs and must be mirrored. A safe rule of thumb is that a special device used for WBC should be 1% of the usable capacity of the pool.

- **Spare**—You can also specify devices to replace a failed device in the storage pool you create. When you designate a device as a hot spare, it automatically replaces the failed device. Spares should be the same device size and type as the data devices.

- **Properties**—Auto Expand: Select this option to automatically increase the size of a pool when the underlying device is grown.
To add cache, log, special, and spare devices to a pool, do the following:

1. Successfully complete the following tasks:
   a) Naming and Configuring a Pool.
   b) Adding Data Devices to a Pool.

2. To add a cache device, select Cache and do one of the following:
   • Click Create, follow the prompts for adding devices, and click Save.
   • Click Skip to continue with the Guided Configuration without adding a cache device.

3. To add an optional log device, select Log and do one of the following:
   • Select log redundancy type from the drop-down list and click Create.
   • Click Skip to continue with the Guided Configuration without adding a log device.

4. To add a write back cache device, select Special, and do one of the following:
   • Click Create, select two or more SSDs, and click Save. A special device can only use SSDs or NVMs.
   • Click Skip to continue with the Guided Configuration without adding a special device.

5. To add a spare device, select Spares and do one of the following:
   • Click Create, then follow the prompt for adding devices and click Save.
   • Click Skip to continue with the Guided Configuration without adding a spare device.

6. Do the following, as necessary:
   • Click Auto expand to allow the pool to automatically increase in size when the underlying device grows.
   • Enter a descriptive Comment for the pool.
   • For an HA cluster node, select the node on which to Activate pool on. After the pool is created, you can configure the High Availability service.

**Note:** The devices that belong to an exported pool are considered to be in use and cannot be used to create a new pool or added to an existing one. Though not recommended, you can override this condition with the CLI.
7. Click **Create Pool**.

8. If you selected Enable High Availability, continue with Configuring an HA Service for a Shared Pool. The screen for configuring HA access to the pool appears.

**Editing an Existing Pool**

It is recommended that you plan for pool capacity prior to creating them. However, you can add to the capacity of a pool later should the need arise.

---

**Note:** You are not allowed to decrease the size of a pool.

---

The following rules apply for increasing the size of redundant pools:

- When increasing the size of a non-redundant pool you are prompted to **Add disks**.
- When increasing the size of a redundant pool, you are prompted to add a **New vDev**.

To edit the capacity of an existing pool, do the following:

1. For an existing pool on the **Management > Pools** page, click the **COG** on the far right and select **Edit** from the drop-down list.

2. In the **Edit Pool** panel on the left, do one of the following:
   - For a redundant pool, click **New vDev**.
   - For a non-redundant pool, click **Add disks**.

3. Select the prompted number of disks from the table on the right and click **Save**.

4. Optionally, to add a cache, log, special, or spare device, do the following:
   a) Select **Cache**, **Log**, **Special** or **Spares**.
   b) Click **Create** and select the prompted number of disks.
   c) Click **Save**.
Configuring an HA Service for a Shared Pool

The primary benefit of an HA Service is to provide high availability access to the user’s data. This is accomplished by detecting Nexenta node failures along with client communication drops and transferring ownership of the shared pools to the alternate NexentaStor node.

A VIP is a virtual address associated with a shared pool service. The network clients use the VIP to connect to the shared pool.

To configure HA service for a shared pool, do the following:

1. Complete the following tasks:
   a) Creating Pools on Single or Clustered Nodes with HA enabled.
   b) Adding Data Devices to a Pool.
   c) Adding Cache, Log, Special, and Spare Devices to a Pool.

   The Add to HA Control screen appears.

2. Do one of the following:
   • Select Use existing service to control pool, select the radio button next to the Service name in the table, and click Save.
   • Select Create a new service to control pool, and continue with the following step.

3. Enter a Service description.

4. Optionally, configure one or more virtual IP addresses in the following way:

   If you choose not to create a VIP, click the trash can icon on the far right to remove the empty row. Otherwise, you will be unable to create the service.

Note:
The VIP name, IP address, and netmask values you enter for the shared pool were configured when the HA cluster was set up using the CLI.

   a) Enter the VIP Name used when the HA cluster was configured.
   b) Select an IP protocol from the drop-down list.
   c) Enter the IP address used for the VIP when the HA cluster was configured.
   d) Enter the Netmask used for the VIP when the HA cluster was configured.
   e) Select the interface for each node from their respective drop-down lists, such as an aggregated link, or a VLAN link, or a physical link.
5. Click **Create Service**.

After associating a pool with an HA service, the pool table appears with a flashing yellow shield.

6. Refresh the screen again, and a flashing yellow shield appears. Refresh the screen again until the green shield appears. The pool begins handling IOs when the green shield is shown.

**Note:** This entire sequence may take a few minutes. If after a refresh and several minutes the shield is not green, mouse over the shield to see if the status indicates a problem.

**Discovering Pools and Viewing Pool Status**

You will want to find pools that are available for use when you need to import a pool, or if you accidentally destroyed a pool and need to recover it. After creating a pool, you can verify its status.

**Note:** Destroying a pool doesn’t erase the data on the disks. The pool can be discovered and re-imported.
To discover pools and view pool status, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance on which you want to create the pool.
3. Under **Management**, click **Pools**. The pools belonging to the appliance are shown.
4. To find an exported pool that is available to import, toggle **Show exported pools** to **Yes**.
5. To perform an import, click the COG to the right of the exported pool.
6. In the Pools table, review the following status:
   - Health—Shows the health of the pool.
   - Node—Shows the node that owns the pool, for a clustered appliance.
   - Raw % Utilized—Shows the percentage of raw capacity used.
   - HA Service State—Shows details of the Cluster service states for the clustered nodes. The first column on the left only appears for a clustered appliance. Hover the mouse over the shield icon to view the pop-up dialog.
   - Configured Capacity—Shows the sum of free capacity and the allocated capacity of the pool after applying the redundancies (RAID/mirror).
7. Continue with **Setting Management Actions**.
Viewing Status Details for a Shared Pool

This section demonstrates how to view the status details of a shared pool under the control of an HA service.

To view the service status for a pool, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
2. Select Management > High Availability.
4. In the Services details table, click the COG for the pool and select status.
   A status dialog appears with the Info tab displaying details on the pool.
5. Click the Disks and Properties tabs to view the respective details.

Note: The Delegation, Failure mode, and Cache file properties should not be changed without consulting Nexenta Support. Otherwise, changes to these properties could result in data corruption.

6. Click Close.
Setting Management Actions

This section covers the management actions available on the Management > Pools page.

- Scrubbing is a resource-consuming operation similar to resilvering. It is preferable to schedule scrubbing during a maintenance window and to do only one operation at a time.

**Note:**
- If a scrub is already in progress, a subsequent start-scrub returns an error.
- If a resilver is in progress, the system schedules the scrub operation to start once the resilver completes.

To perform a management action on a pool, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List page, select the appliance.
4. Select the COG for a pool and choose a management action from the drop-down list.

If the pool belongs to an HA cluster, two HA specific options are also available. See Table 5-6 for detailed descriptions of each of the management actions.
### Table 5-6: Managing Pools

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View pool status</td>
<td>You can view detailed characteristics of a pool, such as the number of disks used, redundancy configuration, trace errors in the disks, the status of a new or replaced disks, and so on.</td>
</tr>
<tr>
<td>Click COG &gt; Status</td>
<td></td>
</tr>
<tr>
<td>Edit an existing pool</td>
<td>Manually change the configuration of a pool. For more information, see <a href="#">Editing an Existing Pool</a>.</td>
</tr>
<tr>
<td>Click COG &gt; Edit</td>
<td></td>
</tr>
<tr>
<td>Export a pool</td>
<td>Exporting a pool from the appliance detaches it from its associated storage. All the devices belonging to the pool are marked as exported and are considered to be in use. Exported pools can be moved between appliances and imported as long as a sufficient number of devices are present. All mounted datasets of the pool are unmounted before the pool is exported.</td>
</tr>
<tr>
<td>Click COG &gt; Export</td>
<td></td>
</tr>
<tr>
<td>Find an Exported pool</td>
<td>You may need to import a pool and don’t know what pools are available. Alternatively, you might have accidentally destroyed a pool and now need to recover it. Destroying a pool doesn't erase the data on the disks, so the pool can still be discovered and restored. To find an exported or an inactive or a destroyed pool available to import, see <a href="#">Creating and Managing Pools</a>.</td>
</tr>
<tr>
<td>Modify pool properties</td>
<td>Modify the available properties of a data pool. For more information, see <a href="#">Editing Pool Properties</a>.</td>
</tr>
<tr>
<td>Click COG &gt; Properties</td>
<td></td>
</tr>
<tr>
<td>Run a scrub service</td>
<td>NexentaFusion enables you to run a scrubbing service automatically to periodically examine all the data in the specified pools to verify that its checksums correctly and also to check for consistency errors. If the pool has a redundant configuration, NexentaFusion corrects any errors it finds. You can manually start a scrub service when replacing a disk to ensure that the replacement device is functional. This also ensures that data is written correctly and verifies the integrity of the pool.</td>
</tr>
<tr>
<td>Click COG &gt; Scrub</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>**View real-time Unmap =(on</td>
<td>off)**&lt;br&gt;Click COG &gt; Unmap</td>
</tr>
<tr>
<td>**Schedule Unmap =(on</td>
<td>off)**&lt;br&gt;Click COG &gt; unmap</td>
</tr>
<tr>
<td>Destroy a pool&lt;br&gt;Click COG &gt; Destroy</td>
<td>Destroying a pool frees its physical devices to be used for other pools. The freed devices can be used to create a new pool or to add to an existing one. If you deleted a pool by mistake, you can re-import it. It is possible to retrieve the deleted pool only if the sufficient number of devices are available. All mounted active datasets are unmounted before the pool is destroyed on the node.  &lt;br&gt;Note: You cannot destroy a pool that is configured as High-Availability. To destroy a pool under a cluster service, remove the cluster service first. For more information, see Removing a Pool From HA Control.</td>
</tr>
<tr>
<td>Import a pool&lt;br&gt;Click COG &gt; Import</td>
<td>You can import a pool that has been exported or destroyed. <strong>Caution:</strong> You can force a pool to be imported even if the pool is potentially active. Force importing a pool that is currently active in another system could result in data corruption and panics since both systems try to access the same storage ID.</td>
</tr>
<tr>
<td>Add to HA Control</td>
<td>Add a pool to an HA service. For more information, see Adding an Unshared Pool to HA Service.</td>
</tr>
<tr>
<td>Remove from HA Control</td>
<td>Delete the pool from an HA service. For more information, see Removing a Pool From HA Control.</td>
</tr>
</tbody>
</table>
Editing Pool Properties

You can edit pool properties anytime after a pool is created. If you edit the pool properties for a clustered appliance, the modifications are made on the node where the pool is active.

To edit pool properties, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance on which you want to create the pool.
3. Under **Management**, click **Pools**.
4. Click the **COG** for the pool and select **Properties** from the drop-down list.
5. On the Edit Pool Properties dialog, modify the option settings as necessary. Table 5-7 explains the available options.

Table 5-7: List of Pool Properties

<table>
<thead>
<tr>
<th>Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-expand=(on</td>
<td>off)</td>
</tr>
<tr>
<td>Delegation=(on</td>
<td>off)</td>
</tr>
<tr>
<td><strong>Note:</strong> Do not change this property without first consulting Nexenta Support. Otherwise, you may experience data corruption.</td>
<td></td>
</tr>
<tr>
<td>Failure-mode=(wait</td>
<td>continue</td>
</tr>
<tr>
<td><strong>Note:</strong> Do not change this property without first consulting Nexenta Support. Otherwise, you may experience data corruption.</td>
<td></td>
</tr>
<tr>
<td>Scrub-schedule=cron_expression</td>
<td>Runs the auto-scrub service on this schedule.</td>
</tr>
<tr>
<td>Cache File</td>
<td>Specifies the pool configuration cache location</td>
</tr>
<tr>
<td><strong>Note:</strong> Do not change this property without first consulting Nexenta Support. Otherwise, you may experience data corruption.</td>
<td></td>
</tr>
<tr>
<td>Comment=TEXT</td>
<td>User-defined pool comment</td>
</tr>
<tr>
<td>Real-time Unmap =(on</td>
<td>off)</td>
</tr>
<tr>
<td>Scheduled Unmap =(on</td>
<td>off)</td>
</tr>
</tbody>
</table>
Adding an Unshared Pool to HA Service

For pools on a clustered appliance that have not been enabled for high-availability, you can add the pools to an HA service at a later time. This section demonstrates how to add an unshared pool to an HA service.

Clicking on **Pools** lists all the pools belonging to an appliance that are part of an HA service, as well as the pools that are not part of an HA service. If the devices in a pool are not available to both the nodes in the cluster, you are unable to add the HA service.

- To add an unshared pool to a cluster service, do the following:
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the clustered appliance on which the HA service exists.
  3. Select **Management > Pools**, click the **COG** of the pool to be added, and select **Add to HA control** from the drop-down list.
  4. Do one of the following:
     - To use an existing service, click **Use existing service to control pool**, select the service, and click **Save**.
     - To use a new service, click **Create new service to control pool**, enter a **Service description**, optionally configure VIPs as described in Configuring an HA Service for a Shared Pool, then click **Create Service**.

  5. Refresh the screen, then wait a few moments and refresh the screen again.
After associating a pool with an HA service, the pool table may redisplay with a red shield. After refreshing the screen, the pool should display a flashing yellow shield after the first refresh, then a green shield on a subsequent refresh. The pool begins handling IOs when a green shield is shown.

---

**Note:** The refresh sequence may take a few minutes. If several minutes have passed after a refresh and the shield is not green, mouse over the shield to see if the status indicates a problem.

---

### Viewing VIPs Associated with an HA Service

A VIP is a virtual address associated with a shared pool service. The network clients use the VIP to connect to the shared pool. When you created an HA Service for a shared pool, as described in Managing HA Services, you may have added one or more VIPs. This section demonstrates how to view the VIPs associated with an HA service.

To view a list of configured VIPs associated with an HA service, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the clustered appliance on which the HA service exists.
3. Select **Management > Pools**.

   For a clustered appliance, the pool view shows the node that owns the pool. The status of the pool is shown in the Health column. The first column in the following figure (only shown for a clustered appliance) represents the Cluster service state.

4. In the first column, hover the cursor over the shield icon to view information on the configured VIP and states of the service.

   The **Unblocked** parameter indicates whether or not the HA Service is enabled to be started on the node, as shown in the following image.

---

**Note:** Clients use the VIP to access an NFS or SMB share on iSCSI LUNs on a clustered appliance.
Moving a Pool under HA Service for Manual Failover

When a pool is configured for HA with NexentaFusion, it is set to failover automatically when the HA cluster detects a system failure. However, you can move a pool (enabled for high-availability) manually, from the active node to the secondary node in a clustered environment. You might do this when the active node is in a maintenance window, or during load or performance balancing.

To manually move an HA pool from one node to another, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List page, select the clustered appliance on which the HA service exists.
   All the pools belonging to the appliance are shown.
4. Click the COG of the pool enabled for high-availability and select Move HA Pool.
   If the HA service manages multiple pools, a dialog appears.
5. To move all pools managed by the service to the designated node, click Yes.

Note: When you migrate a pool, all unwritten data in cache is flushed to the disk before the migration occurs.
Removing a Pool From HA Control

When you remove a pool from HA control, the pool remains on the node where the HA service was running, and all the shares stay accessible from this node but not the VIP address. The HA service takes the name of the first pool with which it is associated. Multiple pools can be managed by one HA service. If the first pool is removed from HA control, all other pools associated with the service are also removed from HA control, and the HA service is destroyed. Likewise, you can remove all pools from HA control and destroy the service from the Destroy HA Service screen.

To remove a pool from HA control, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the clustered appliance on which the HA service exists.
3. Select **Management > Pools**.
   All the pools belonging to the appliance are shown.
4. Click the **COG** of the HA pool enabled for high-availability and select **Remove from HA Control** from the drop-down list.
   The Destroy HA service confirmation dialog appears, which allows you to remove all pools from HA control and destroy the service.
5. To remove all pools from HA control and destroy the service, click **Yes**.
   The pool remains on the node where the service was running and all the shares stay accessible from this node, but not the VIP address.

   The following dialog appears when you remove a pool from HA service that is not the initial pool with which the service was created.

   ![Destroy HA service dialog](image1)

   The following dialog appears when you remove the initial pool with which the HA service was created.

   ![Destroy HA service dialog](image2)
Creating and Managing File Systems

NexentaFusion allows you to see the status of all the file systems, including compression performance, and share a file system using various sharing protocols (SMB, NFS) that enable both Windows and Unix hosts to access the datasets. NexentaFusion also enables virus scanning on the file system, allows you to search for a specified file system and manages Access Control Lists when creating and editing shares. The storage pool is always a root directory for the file system hierarchy. The file system is managed by multiple properties for maximum performance and optimization.

This section covers the following topics:

- Creating a File System on a Pool
- Viewing File Systems
- Sharing File Systems Using NFS
- Sharing File Systems Using NFS

Creating a File System on a Pool

This section demonstrates how to create a file system on a pool, and explains the properties of a file system. A file system is a manageable storage unit that enables you to organize and share data over the network. After creating a storage pool that provides logical space for the creation of datasets, you can create a hierarchy of multiple file systems either on an HA pool (that can be active on either node) or on a non-HA pool.

A file system can contain nested file systems, also known as child file systems. Each nested file system is part of the hierarchy (tree structure), with its mount point being the sub-directory of another file system—the parent file system. The top-most directory, which does not have a parent, is the root directory. You can have up to 15 levels of nested file systems below the parent root directory.

See Table 5-9 for a list of tasks you can perform with the filesystem COG options.

 دون نسخة من النص الأصلي:  

في هذا السطر عنnęت نسخة من النص الأصلي:  

دوال متقاطعات:  

- To create a file system, do the following:
  1. Log in to NexentaFusion and click Appliance in the drop-down list.
  2. In the Appliances List page, select the appliance on which the pool exists, and select Management > Filesystems. The Filesystems tab is selected by default.
     A list of all pools belonging to the appliance is shown.
  3. Click the arrows on the left of the heading bar to expand the view of the hierarchy.
4. Click the COG for a pool or file system and select Add New Filesystem from the drop-down list.

5. Set the necessary properties, as described in Table 5-8 and click Create.

---

**Note:** When you create a file system, unspecified property values are inherited from ZFS. Some properties can only be set when the file system is created.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum space reserved for data and protection</td>
<td>Sets the minimum amount of disk space guaranteed to a dataset and its descendents. When the amount of disk space used is below this value, the dataset is treated as if it were using the amount of space specified by its reservation. Reservations are accounted for in the used disk space of the parent dataset and count against the quotas and reservations for the parent dataset.</td>
</tr>
<tr>
<td>Record Size</td>
<td>Specifies a suggested block size for files in a file system (defaults to 128KB).</td>
</tr>
<tr>
<td>Quota Size</td>
<td>Sets the amount of disk space that a dataset and its descendents can consume. This property enforces a hard limit on the amount of space used.</td>
</tr>
<tr>
<td>Minimum space reserved for data only</td>
<td>Sets the minimum amount of disk space guaranteed to a dataset, not including descendents such as snapshots and clones. When the amount of disk space used is below this value, the dataset is treated as if it were taking up the amount of space specified by the reservation. The reservation is accounted for in the parent dataset's disk space used, and counts against the parent dataset's quotas and reservations. If a reservation is set, a snapshot is only allowed if enough free pool space is available outside of this reservation to accommodate the current number of referenced bytes in the dataset.</td>
</tr>
<tr>
<td>Allow extended attributes</td>
<td>Indicates whether extended attributes are enabled (on) or disabled (off) for the file system.</td>
</tr>
<tr>
<td>Compression mode</td>
<td>Enables the compression algorithm for a dataset (defaults to lz4).</td>
</tr>
<tr>
<td>Dedupe mode</td>
<td>If Dedupe mode is set to on, it enables the deletion of redundant data copies, thereby using the storage capacity more effectively.</td>
</tr>
<tr>
<td>Enable virus scanning</td>
<td>Controls whether regular files should be scanned for viruses when a file is opened and closed. In addition to enabling this property, a virus scanning service must also be enabled for virus scanning to occur, if you have third-party virus scanning software. The default value is off.</td>
</tr>
<tr>
<td>Expose snapshot directory</td>
<td>Controls whether the .zfs directory is hidden or visible in the root of the file system.</td>
</tr>
<tr>
<td>Inherit ACL rules</td>
<td>Controls the inheritance of the ACL settings by new files and subdirectories from the parent directory. You can change the properties at any time, using the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>discard</strong> — Does not inherit the ACL entries.</td>
</tr>
<tr>
<td></td>
<td>• <strong>noallow</strong> — Inherits ACL entries only with <strong>deny</strong> access type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>restricted</strong> — Inherits ACL entries, excluding <strong>write_owner</strong>, <strong>write_acl</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>passthrough</strong> — Defines mode of newly created files with the inherited ACL entries.</td>
</tr>
<tr>
<td></td>
<td>• <strong>passthrough-x</strong> — Assigns a permission to execute to newly created files, if this permission is defined in file creation mode and inherited by the ACL.</td>
</tr>
</tbody>
</table>
Viewing File Systems

This section demonstrates how to view the status of a file system. The file system status shows the available space, quota, and allocated size for all file systems.

When a file system is part of an HA pool, the first column on the far left of the table is shown with an HA service status shield icon. Hover the cursor over a shield icon to display a pop-up dialog with status information for the HA service. A shield icon only appears beside a pool that is part of an HA service on a clustered appliance.

To view file system status, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance on which the pool exists.
3. Select **Management > Filesystems**.
   - A list of all pools belonging to the selected appliance is shown. For a clustered appliance, a list of the pools that are part of an HA service are shown, as well as the pools that are not.
4. To only view data for a specific pool, select a **Pool** from the drop-down list. The default is to show all pools.
5. To view the entire file system structure, click the arrows on the left of the table header.
6. To view the list of file systems in a pool, click the expander arrow next to the pool name.
7. Optionally, sort by a specific column by clicking the column head.
   - If compression was enabled when the file system was created, the **Data Reduction Ratio** column appears showing the correlation of actual storage capacity to uncompressed capacity. This number represents the compression effectiveness.
8. To view file system properties, click the COG for a file system and select **Edit properties**. A dialog appears showing the editable properties. See **Properties of File System** for a description of each property.
### Table 5-9: Managing File Systems Using the COG

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Filesystem</td>
<td>You can create and share file systems within pools. First, you create a pool that will contain the file system. Then you can create a hierarchy of file systems, or nested-file systems, as necessary. File systems enable the logical organization of information, as well as the ability to share information across the network.</td>
</tr>
<tr>
<td>Data Protection</td>
<td>You can create one-time snapshots, schedule snapshots taken at regular intervals, schedule replication at regular intervals either locally or on a remote host, and schedule continuous replication either locally or on a remote host.</td>
</tr>
</tbody>
</table>
| Destroy          | You can choose to destroy a NexentaFusion file system, even if there are open files. If the file system is not busy when you attempt to destroy it, it is automatically unshared and unmounted. When destroying a file system, you can also choose to destroy its snapshots.  
  **Note:** From NexentaFusion, you cannot destroy a file system if it has child file systems nested under it. Using the CLI, you can destroy a parent file system even if it has nested file systems, however. |
| Properties       | You can edit most file system properties any time after the file system is created. For more information, see Table 5-8.                                                                                     |
### View capacity usage summary

You can view the following file system metrics:

- Amount of disk space consumed by a dataset and all its descendents, which is the same as Allocated amount shown in the table.
- Amount of disk space that is used by a dataset itself, which would be freed if the dataset was destroyed, after first destroying any snapshots and removing any reservations.
- Amount of data accessible by a dataset, which might or might not be shared with other datasets in the pool.
- Amount of disk space that is consumed by snapshots of a dataset.
- Compression ratio achieved for a dataset, expressed as a multiplier.
- Amount of disk space used by the children of this dataset.
- Property for cloned file systems or volumes that identifies the snapshot from which the clone was created.

To view file system metrics, select the file system, then select **COG > Properties**, and expand **Usage Data**.

### Share using NFS/SMB

You can share a file system so that users can remotely access its contents. A child file system inherits the sharing protocol of its parent. An individual child file system can also have additional sharing protocols.

For example, if a parent file system uses the SMB protocol, its child file systems must also use SMB, along with any other protocols assigned to the child individually.

To mount a file system in Windows, you must share it first. If you mount a file system in Windows before sharing it, you will not be able to see the file system.

For more information, see: [Sharing File Systems Using NFS](#).

### Remove NFS/SMB share

You can unshare a shared file system at any time. When you unshare a file system, you can leave or remove the shares for child file systems, if any exist.

### Remount

NexentaFusion file systems are arranged in a hierarchical tree of objects. To organize file systems into a unified tree of objects, the file systems must be mounted. When you create a file system, NexentaFusion automatically mounts it. However in some instances, a file system may become unmounted. If this should happen, you can manually remount the file system using the NexentaStor CLI (not the NexentaFusion UI).

When you mount or unmount a file system it may become unavailable for network clients.
Filtering File Systems

You can use filters to narrow the file systems data display, allowing you to view only the information that is needed. You can also filter filesystem snapshots and data protection services. This section demonstrates both procedures.

- To filter data for file systems, do the following:
  1. Log in to NexentaFusion, and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance that contains the pool.
  3. Select **Management > Filesystems**, then select one of the following: **Filesystems** or **Shares**.
  4. To only show data for a specific pool, select a **Pool** from the drop-down list. The default is to show all pools.
  5. To refine the data display, select an option to **Filter by** from the drop-down list.
  6. Specify the desired parameters by making selections from drop-down lists and entering filter values, as needed. Filter criteria varies with the selected option.
  7. Click **Filter** to apply the filter and view the results, or click **Clear** to reset the fields.

The following example specifies a filter for file systems, with a quota greater than 100GiB across all pools.
Sharing File Systems Using NFS

NFS allows you to share file systems on Linux and UNIX operating systems. A shared file system displays as a local resource. NexentaFusion supports NFS v2 and NFS v4.

This section covers the following topics:

- Configuring and Enabling the NFS Server
- Creating an NFS Share

Configuring and Enabling the NFS Server

By default, the NFS server is enabled on the NexentaStor appliance. If the NFS server is not enabled before sharing a file system, enable the NFS server.

**, Note:** You must have superuser privileges are to perform this procedure.

To configure the NFS server, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance that contains the pool.
3. Select **Administration > System Settings**.
4. Under System services, click the COG for an NFS server and do one of the following:
   - To enable NFS, select **Enable**.
   - To modify NFS tunables, select **Edit** and change the following options, as necessary.

You can configure NFS server tunables listed in the following table to meet the IT requirements at your site.
### Table 5-10: NFS Server Tunables

<table>
<thead>
<tr>
<th><strong>NFS Server Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grace Period</td>
<td>Specifies the number of seconds after a server restarts in which the clients have to reclaim both NFS version 3 locks (provided by NLM) and version 4 locks. The default is 90 seconds.</td>
</tr>
<tr>
<td>Max concurrent requests</td>
<td>Specifies the maximum number of concurrent NFS requests. The default is 256.</td>
</tr>
<tr>
<td>Min NFS version</td>
<td>Sets the minimum version of the NFS protocol to be registered and offered by the NFS server. The default is 2.</td>
</tr>
<tr>
<td>Max NFS version</td>
<td>Sets the maximum version of the NFS protocol to be registered and offered by the NFS server. The default is 4.</td>
</tr>
<tr>
<td>NFSv4 delegation</td>
<td>Controls whether the version 4 delegation feature is enabled for the NFS server. Turn the feature On or Off, as necessary for your environment.</td>
</tr>
<tr>
<td>NFSv4 identity domain</td>
<td>Specifies the common domain for NFS clients and servers.</td>
</tr>
<tr>
<td>Max locked threads per client</td>
<td>Specifies the maximum number of concurrent locked requests. The default is 256.</td>
</tr>
</tbody>
</table>

### Creating an NFS Share

Sharing file systems using the NFS protocol provides the following advantages:

- Shared storage
- Simultaneous read/write access to NFS share by multiple clients
- Fast performance, compression, snapshots, ACLs, etc.
- Easy to create and manage, without additional resources.

NexentaFusion provides an intuitive interface for sharing an NFS file system that is accessible to all hosts, or restricted to specific clients:

- **Open share for VMware and Virtualization**—Use this sharing option if the share is to be mounted in a VMware environment for use as a Datastore that is accessible to all hosts. Or, if the share is to be mounted on hosts in other virtualization environments that require full root access.
- **Open share for any NFS client**—Use this sharing option to allow all hosts read and write access to the share.
- **Advanced - share with security options**—Use this sharing option to specify the clients that are allowed access to the share using selected authentication protocols.
Open Shares

Open shares trust the client to perform authentication. The user’s UNIX user-id and group-ids are passed in the clear over the network, unauthenticated by the NFS server.

- Open share for VMware and Virtualization—The share provides full root access to all hosts.
- Open share for any NFS client—The file system ACL is modified to give everyone@ full read, write, and modify permissions.

Shares with Security Options

Authenticated users typically have the appropriate permissions for full access to the network and file systems.

- Authenticated user (AUTH_SYS) access requires that a user sign in with a unique user name and password, and trusts the client to perform the authentication. The user’s UNIX user-id and group-ids are passed in the clear on the network, unauthenticated by the NFS server.
- AUTH_NONE trusts the client to perform authentication. The NFS clients have no identity and are mapped to anonymous user ‘nobody’ by the NFS server. Users have read-write access to the contents of a shared top level file system.

You can also set Anonymous File Access Control permissions:

- Disabled—Sets anon=1. Allows setting the access control element (ACE) for everyone@ with read, write, and modify permissions. This is the default for shares that use the Open share for any NFS client option.
- Nobody—Sets anon=nobody. Allows setting the ACE for user:nobody with read, write, and modify permissions.
- Root—Sets anon=root. Allows root access to all hosts. It is the default setting for shares that use the Open share for VMware and Virtualization option.
- Other—Sets anon=<username>. Allows you to set the ACE for a specified user (username) with read, write, and modify permissions.

Create an NFS Share for a File System

This section demonstrates how to create an NFS share. For more information on NFS sharing options, see Table 5-11.

- To create an NFS share for a file system, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select an appliance.
  2. Select Management > Filesystems.
     The pools belonging to the appliance appear in the table.
  3. To view the hierarchy of file systems in all the pools, click the heading Expand All / Collapse All arrows on the left.
4. Click the COG for a file system and select Share using NFS.

5. To provide open access to the file system for all hosts, do one of the following:
   - Select Open share for VMware and Virtualization, to set the share so that it trusts the client to perform authentication and provides full root access to all hosts. To restrict share access for this option, click the here link and go to the next step.
   - Select Open share for any NFS client, to set the share so that all hosts can have read/write access to this share. To restrict share access for this option, click the here link and go to the next step.

6. To provide restricted access to the file system, click the Advanced share with security options and do one of the following:
   - Click Use AUTH_SYS, then:
     -- click Add Row,
     -- enter Hosts values,
     -- select a host Type,
     -- specify Root access, Read/Write privileges, Read Only, or No access.
     -- Repeat for other hosts, networks, netgroups, and domains.
   - Click Use AUTH_NONE, then:
     -- click Add Row,
     -- enter Hosts values,
     -- select a host Type,
-- specify Root access, Read/Write privileges, Read Only, or No access.
-- Repeat for other hosts, networks, netgroups, and domains.

Click the arrow on the right of Anonymous File Access Control to choose from the following options. Clicking the radio button on the left activates a selection check box on the right.

-- disabled (default)—Anonymous access is disabled. This is the default selection for Open share for any NFS client shares. If not already selected, click the check box to the right to activate this option. Click the check box again to deselect.
-- nobody—Automatically allows access for user:nobody. Click the check box to the right to activate this option.
-- root—Allows root access to the share for all hosts. This is the default selection for Open share for VMware and Virtualization shares. If not already selected, click the check box to the right to activate this option.
-- other—Provides a text field in which you can specify a user (username) that can have read, write, and modify access for the share. Click the check box to the right to activate this option. Click the check box again to deselect.

The access control entries (ACEs) to be added and removed appear below.
7. Click Save.

NFS sharing options are explained in Table 5-11.

Table 5-11: NFS Sharing Options

<table>
<thead>
<tr>
<th>NFS Folder Sharing Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Authentication Protocols  | § AUTH_SYS — In secure authentication, the user name and password are transferred transparently.  
§ AUTH_NONE — Null authentication, where NFS clients are mapped by NFS servers as user nobody. |
| Open share                | Allows all hosts to have read and write access to a share, or the share can be mounted on hosts in VMware or another virtualized environment. An open share trusts the client to perform authentication. |
| Anonymous File Access Control | Grants access to anonymous users and recognizes them as user ‘nobody’. The shared top-level directory is allows read-write access for anonymous user ‘nobody’. If you are using an authentication method, leave these options unchecked. |
| Read-Write                | Users with Read-write access. Overrides the 'Read-Only' field for specified clients. |
| Read-Only                 | Users designated with Read-only access. |
| No Access                 | Users designated with no access at all. |
| Root                      | Designated root users of other computer hosts that have root access to this share. |

Note: Using group ACLs is recommended, as it is more efficient than per-user ACLs.

Sharing File Systems Using SMB

The Server Message Block (SMB) protocol is a network file sharing protocol. Creating an SMB share makes the dataset available to NexentaStor users. SMB 1.0, 2.1 (default), and 3.0 are supported. NexentaFusion provides kernel and ZFS-integrated CIFS stacks, with native support for Windows Access Control Lists (ACL). Mount the file system as a shared drive on each Windows machine allowed access to the file system.

Configuring and Enabling the SMB Server

This section demonstrates how to configure and enable an SMB server. Table 5-12 explains the configurable options for an SMB server. By default, the SMB server is enabled on the NexentaStor appliance. Before you can share a file system using SMB, you first have to enable SMB on the appliance. The procedure that follows demonstrates how to enable SMB and edit tunables for the SMB server.

Note: You must have superuser privileges are to perform this procedure.
To configure the SMB server, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance that contains the pool.
3. Select **Administration > System Settings**.
4. Under System services, click the **COG** for the SMB server and do one of the following:
   - Select **Enable** to activate SMB
   - Select **Edit** to modify the tunables described in **Table 5-12**, make the necessary changes, and click **Save**.

<table>
<thead>
<tr>
<th>SMB Server Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Workgroup</td>
<td>Enter a Workgroup name and click <strong>Save</strong> to change the workgroup name.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>Enter AD credentials and click <strong>Save</strong> to join a Windows domain. The default is Workgroup mode.</td>
</tr>
<tr>
<td>Max SMB protocol level</td>
<td>Sets the maximum version of the SMB protocol to be registered and offered by the SMB server.</td>
</tr>
<tr>
<td>AD site name</td>
<td>Specifies the Active Directory site. Leave this field blank if you do not have a local Active Directory site.</td>
</tr>
<tr>
<td>Preferred domain controller</td>
<td>This property can be used when there are multiple domain controllers to indicate which one is preferred.</td>
</tr>
<tr>
<td>Signing</td>
<td>Enables SMB signing.</td>
</tr>
<tr>
<td>LanMan compatibility level</td>
<td>Specifies the LAN Manager (LM) authentication level. The LM compatibility level controls the type of user authentication for workgroup mode or domain mode.</td>
</tr>
<tr>
<td>Enable IPv6</td>
<td>Enables IPv6 Internet protocol support within the CIFS Service.</td>
</tr>
<tr>
<td>Enable guest access</td>
<td>Enables guest access to shares. When this option is selected, ACLs (with read/write permissions) for Guests@BUILTIN are automatically set. For more information, see the NexentaStor 5.0 CLI Configuration Guide.</td>
</tr>
<tr>
<td>Enable NetBIOs</td>
<td>Enables NetBIOs.</td>
</tr>
<tr>
<td>Restrict anonymous</td>
<td>Disables anonymous access to IPC.</td>
</tr>
</tbody>
</table>
Creating an SMB Share

This section demonstrates how to create an SMB share. **Table 5-13** explains the SMB share options you can set when creating an SMB share.

Selecting a sharing protocol for a parent file system automatically assigns that protocol to all child file systems. However, individual child file systems can be shared using additional sharing protocols.

Table 5-13: SMB Share Options

<table>
<thead>
<tr>
<th>SMB Sharing Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share name</td>
<td>By convention, a file system named <code>&lt;pool_name/filesystem_name&gt;</code> becomes an SMB share named <code>&lt;pool_name/filesystem_name&gt;</code>.</td>
</tr>
<tr>
<td>ABE enumeration</td>
<td>To see only the files and directories for which you have access, select Access-Based Enumeration (ABE) in the SMB share option. You may enable ABE to filter large directories or to hide files.</td>
</tr>
<tr>
<td>Quota management</td>
<td>Enables SMB quota management for this share.</td>
</tr>
<tr>
<td>Allow guest access</td>
<td>Enables guest access with read-only rights to the share.</td>
</tr>
<tr>
<td>Client caching policy</td>
<td>This property specifies how the client should manage client-side caching and access to offline files. The default value is “manual”.</td>
</tr>
</tbody>
</table>
To create an SMB share for a file system, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Filesystems.
   The pools belonging to that appliance are shown in the “Name” column.
3. To view the file systems in a pool, click the expand arrow beside the pool name.
4. Select the file system to be shared and click its COG.
5. Select Share using SMB.

Note: Before you can share a file system using SMB, you must have enabled SMB as described in Configuring and Enabling the SMB Server.

Mapping an SMB Share on Windows

This section demonstrates how to map an SMB share on Windows. To map an SMB share on Windows, you must enable guest access for the SMB file system. Windows users are mapped as guest users. You can enable guest access in SMB file system properties with NexentaFusion.

Note: To access an SMB share as an SMB client when the SMB share exists on a shared pool enabled for high-availability, you must know the VIP address.

To connect to a shared file system with guest access, using Windows:

1. In Windows, select Start > Computer.
2. Click Map network drive.
3. In the Folder field, type the path to the shared file system.
Example:
\\192.168.1.10\data_public

For Windows, you must change all forward slashes (/) in a path to backslashes (\).

4. Click Finish.

Creating and Managing Volume Groups and Volumes

This section demonstrates how to create volume groups and volumes. A volume is a dataset that represents a block device. In essence, a volume is a LUN that can be accessed remotely through protocols supported by SCSI or FC target plugins. A volume must be configured as a member of a volume group below a pool. You can then set volume properties such as compression modes and volume size.

Table 5-14 is a task map that outlines the process for creating volume groups and volumes.

Table 5-14: Task Map: Creating Volume Groups and Volumes

<table>
<thead>
<tr>
<th>Task</th>
<th>For information, see:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create a pool. [Creating Pools on Single or Clustered Nodes]</td>
</tr>
<tr>
<td>2.</td>
<td>Create a volume group. [Creating a Volume Group]</td>
</tr>
<tr>
<td>3.</td>
<td>Create volumes with the same characteristics, to be included in the same volume group. [Creating Volumes]</td>
</tr>
<tr>
<td>4.</td>
<td>Optional: Edit the properties of an existing volume group or volume. [Editing Properties for Volume Groups and Volumes]</td>
</tr>
<tr>
<td>5.</td>
<td>Optional: Deleting a volume group or volume [Deleting a Volume Group or Volume]</td>
</tr>
</tbody>
</table>

Creating a Volume Group

You create a volume group as a container for volumes. You must create a volume group prior to creating a volume, even if you only intend to create a single volume. This section demonstrates how to create a volume group. A volume group resides within a pool. For information on how to create a pool, see [Creating Pools on Single or Clustered Nodes].

Note: Volumes created under a volume group inherit the properties that have been set for that volume group.
To create a volume group, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Volumes > Volumes.
   The pools belonging to that appliance are shown in the “Name” column in bold.
3. To create a volume group in a pool, click the COG at the far right and select Add New Volume Group from the drop-down list.

4. Specify the following characteristics in the Create Volume Group dialog:
   - Name—Enter a unique name for the volume group.
   - Block size—Select a block size from the drop-down list. The block size cannot be changed after the volume has been written, so specify the optimum at this time.
   - Minimum space reserved for data and protection—Specify the minimum amount of disk space guaranteed for the volume group and its descendents. There is no default value. A value of zero means there is no minimum.
   - Minimum space reserved for data only—Specify the minimum amount of disk space guaranteed for the volume group not including descendents, such as snapshots and clones. There is no default value. A value of zero means there is no minimum.

5. Expand the Optional Settings and specify the following characteristics, as necessary:
   - Compression mode—Enables or disables compression mode for the volume group. The default is lz4.
   - Read only—Controls whether or not the volume group can be modified. The default is false.
• Dedupe mode—Controls whether or not compressed data is removed from the file system. The default is off.
• Sync mode—Controls synchronous behavior. The default is standard.

6. Click Create, then continue with Creating Volumes.

Creating Volumes

This section demonstrates how to create a new volume of a specified size. Volumes that are to be included in a volume group inherit the properties for that volume group by default. You can be modify volume properties, if desired.

To create a volume, do the following:
1. Complete the following tasks:
   a) Creating Pools on Single or Clustered Nodes.
   b) Creating a Volume Group.
2. Click the arrow to the left of the pool that contains the volume group, then click the COG for the volume group and select Add New Volume.
3. In the Create Volume dialog, specify the following:
   • Name—Specifies the relative file system or volume path in the following format:
     <pool>/<volume_group_name>/<volume_name>
• Volume size—Specifies the logical size of the volume.
• Block size—Sets the block size. Select a block size from the drop-down list. The block size cannot be changed after the volume has been written, so set the optimum size at this time.
• Thin-provisioned—Controls whether or not a volume is thin-provisioned. Thin provisioning provides the ability to reserve and allocate storage capacity on demand. The default is NO. For a thin-provisioned volume, toggle to YES.
• Minimum space reserved for data only—For thin-provisioned volumes, specify the minimum amount of disk space guaranteed for the volume not including descendants, such as snapshots and clones. There is no default value. A value of zero means there is no quota.
• Minimum space reserved for data and protection—Specify the minimum amount of disk space guaranteed for the volume and its descendants, including snapshots and clones. There is no default value. A value of zero means there is no quota.

4. Expand the Optional Settings and specify the following characteristics, as desired:
   • Compression mode—Enables or disables compression mode for the volume. The default is lz4.
   • Read only—Controls whether or not the volume can be modified. The default is false.
   • Dedupe mode—Controls whether or not compressed data is removed from the volume. The default is off.
   • Sync mode—Controls synchronous behavior. The default is standard.
5. Click Create.

Editing Properties for Volume Groups and Volumes

Volumes created under a volume group inherit the properties that have been set for that volume group. However, you can modify the properties of a volume or volume group at any time. This section demonstrates how to use filters to easily find and view data for volumes, then modify the properties of a volume group and volume.

To filter data for volumes, do the following:

1. Log in to NexentaFusion, and in the Appliances List page, select the appliance.
2. Select Management > Volumes, then select Volumes.
3. To only show data for a specific pool, select a Pool from the drop-down list. The default is to show all pools.
4. To further refine the data display, select an option to Filter by from the drop-down list.

5. Specify parameters by making selections from drop-down lists and entering filter values, as necessary.

Filter criteria options vary with the selected option. The following example specifies a filter for volumes that are greater than 40GiB in size, across all pools.
To modify the properties of a volume group, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance that contains the pool.
3. Select **Management > Volumes > Volumes**.
4. Expand the pool that contains the volume group, then click the **COG** for the volume group and select **Properties** from the drop-down list.

5. In the **Edit Volume Group Properties** dialog, modify the properties set when [Creating a Volume Group](#), as necessary, and click **Save**.

To modify the properties of a volume, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance that contains the pool.
3. Select **Management > Volumes > Volumes**.
4. Expand the pool that contains the volume group, then expand the volume group.
5. Click the **COG** for the volume and select **Properties** from the drop-down list.
6. In the **Edit Volume Properties** dialog, modify the properties set when **Creating Volumes**, as necessary, and click **Save**.

### Deleting a Volume Group or Volume

You can easily delete volumes and volume groups. Delete all the volumes within a volume group before you attempt to delete the group.

- **To delete a volume, do the following:**
  1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
  2. Select **Management > Volumes > Volumes**.
  3. Expand the pool that contains the volume group, then click the **COG** for the volume to be deleted and select **Destroy** from the drop-down list.
  4. In the confirmation dialog, click the **Destroy volume’s snapshots** check box to delete all of the volume’s snapshots, or leave it blank to retain the snapshots and only delete the volume.
  5. Click **Destroy**.

---

**Note:** You cannot destroy a volume group that is not empty. Delete all of the volumes within a volume group before attempting to destroy the group itself.

---

- **To delete a volume group, do the following:**
  1. Delete all of the volumes within the group, as described in the previous task.
  2. Expand the pool that contains the volume group, then click the **COG** for the volume group to be deleted and select **Destroy** from the drop-down list.
  3. In the confirmation dialog, click **Destroy**.
Mapping Volumes

You can map a volume as an iSCSI LUN or FC LUN. LUN mappings enable you to select the iSCSI targets to which to export the current LUN, and the initiators that are allowed to see the LUN. In the simplest configuration, all initiators can see the mapped targets.

Before you begin mapping a volume to a LUN, you should have already completed Creating Volumes, and Managing iSCSI Host Groups, Targets, and Groups, or Managing FC Host Groups, Targets and Target Groups.

To map a volume, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance that contains the pool.
2. Select Management > Volumes > Volumes.
3. Expand the pool and volume group that contains the volume to be mapped, click the COG for the volume, and select Map Volume from the drop-down list.
4. Select a Protocol: iSCSI or Fibre Channel.
5. In the Map Volume dialog click Add Mapping, and do the following:
   a) Select host group from the drop-down list, or select All to allow any host access to the volume. For information on creating host groups, see Configuring iSCSI Host Groups and Configuring FC Host Groups.
   b) Select target group from the drop-down list. For information on creating target groups, see Managing iSCSI Host Groups, Targets, and Groups and Managing FC Host Groups, Targets and Target Groups.

Note: Fibre Channel functionality requires an additional license. If there is no Fibre Channel license, only the iSCSI option is active and is selected by default for mapping.
Managing LUNs

NexentaFusion allows you to map volumes to LUNs, as described in Mapping Volumes. A logical unit number (LUN) identifies a logical unit, a device addressed by protocols, such as Fibre Channel or iSCSI. This section covers how to manage LUNs once the volumes have been mapped.

- Viewing LUN Information
- Editing and Destroying LUNs

Viewing LUN Information

This section demonstrates how to view information about LUNs, including health status, host group, target group and size.

- To view information for a LUN, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
  2. Select Management > Volumes > LUNs.
  3. In the far left column, click the Expand All / Collapse All arrows to show the mappings.
     The volume Name, Status, Serial number, Host Group, Target Group, Size of the LUN, and Protocol are shown in the table.

```c)
Optional: Assign a **LUN #** to the volume. The system assigns a LUN number by default, but you can enter a specific value, if desired.

d) Click **Save**.

6. Additional mappings can be added by repeating step 5.

7. Click **Close** when the mappings are complete.
```
Editing and Destroying LUNs

This section demonstrates how to edit the LUN mappings and destroy a LUN.

To edit LUN mappings, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Volumes > LUNs.
3. In the far right column, click the COG for a LUN and select Edit Mappings.

4. In the Edit Volume using iSCSI dialog, modify LUN mappings in the following ways:
   a) To add a new mapping, click Add Mapping, select a host group and target group from the respective drop-down lists.
   b) To delete a mapping, click the trash can icon for the mapping, then click Yes in the confirmation dialog.
   c) Click Close.
To destroy a LUN, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance that contains the pool.
3. Select **Management > Volumes > LUNs**.
4. In the far right column, click the **COG** for the LUN and select **Destroy**.
5. In the confirmation dialog, click **Yes**.

Managing iSCSI Host Groups, Targets, and Groups

This section covers how to configure and manage iSCSI host groups (initiator groups), iSCSI targets, and iSCSI target groups.

- [Configuring Secure Authentication](#)
- [Configuring iSCSI Host Groups](#)
- [Creating, Editing, and Destroying iSCSI Targets and Target Groups](#)
- [Editing or Deleting iSCSI Targets](#)
Configuring Secure Authentication

Challenge-Handshake Authentication Protocol (CHAP) is a scheme that the PPP protocol uses to authenticate the remote clients in the network. Secure authentication is optional. However, the following CHAP options ensure that only trusted hosts can access specified targets:

- **Unidirectional CHAP**—Unidirectional CHAP is the most commonly used iSCSI security level. It enhances data security and ensures that only authorized initiators access the data with unidirectional CHAP between a particular initiator and the NexentaStor appliance on a peer-to-peer model.

- **Bidirectional CHAP**—Bidirectional CHAP provides a two-layer authentication protection. It requires that the target identifies an initiator, as well as the initiator identifying the target.

**Tip:** Verify that your hardware supports the chosen level of security.

Unidirectional CHAP Authentication

Unidirectional CHAP assumes that an initiator has its own secret, which you specify on the NexentaStor appliance side. When an initiator connects to a target, the SCSI Target verifies the initiator credentials before granting access to data. An initiator logging in to an NexentaStor iSCSI target with unidirectional CHAP enabled must have a CHAP secret set. For more information, see Configuring iSCSI Host Groups.

Bidirectional CHAP

You can establish bidirectional CHAP to provide more secure authentication. Set up a CHAP User name and password on the target side by choosing the CHAP authentication method when you create the iSCSI target. For more information, see Creating, Editing, and Destroying iSCSI Targets and Target Groups.

Configuring iSCSI Host Groups

A host group contains one or more remote initiators. You can use initiator groups to restrict the access of various initiators so they can only see specific targets and datasets. You can choose to allow all hosts to access a LUN, or specify that only select hosts have access privileges.

For enhanced security, you can configure secure authentication for remote initiators that use CHAP authentication. For more information, see Creating, Editing, and Destroying iSCSI Targets and Target Groups.

This section demonstrates how to add, edit, and destroy a host group. iSCSI initiator addresses follow the IQN format:

```
Type  Date       Auth                          "example.com" naming authority
+-----+----------+-----------------------------+----------------------------+
```
To create a host group, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Volumes > Host Groups, then click Add Host Group.
3. In the Create Host Group dialog, enter a unique Host Group name.
   A host group may contain iSCSI and FC initiators, but this is not recommended. Each initiator can only be a member to one host group.
4. Click the iSCSI host initiator.
5. To add Unassigned Host Initiators that have been communicated to the appliance with the CLI iscsiauth command for use with unidirectional CHAP, select an initiator in the table and click Add to Group.
6. To manually add an initiation, in the Manual initiator entry field, do the following:
   a) Enter an IQN or EUI address.
   b) Optional: Enter a CHAP name and CHAP secret. For more information, see Creating, Editing, and Destroying iSCSI Targets and Target Groups.
   c) Click Add to Group.
7. Click Save.
To edit or destroy a host group, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance you want to edit or destroy.
3. Select **Management > Volumes > Host Groups**.
4. Click the **COG** to the right of the host group and select **Remove** from the drop-down list.
5. In the confirmation dialog, click **Destroy**.
Creating, Editing, and Destroying iSCSI Targets and Target Groups

An iSCSI target is a storage resource located on a server that utilizes the iSCSI protocol to link data storage devices over the network. A target group is a container for targets with a set of network portals within an iSCSI node over which an iSCSI session is conducted. This section demonstrates how to create, edit, and destroy targets and target groups, as well as how to view target sessions.

- Creating iSCSI Targets
- Creating iSCSI Target Groups
- Viewing iSCSI Target Information and Sessions
- Editing or Deleting iSCSI Targets
- Removing iSCSI Targets from a Group and Destroying the Target Group

Creating iSCSI Targets

You can create an iSCSI target with a specified authentication method, or no authentication at all. Assigning a target to a target group is optional.

❖ To create an iSCSI target, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance that contains the pool.
2. Select Management > Volumes > iSCSI Targets and Groups.
3. Click Create Target.
4. In the Create Target dialog, specify the following:
   a) Enter a unique Alias, or name, for the target.
   b) Optional: Select an Authentication method from the drop-down list. The default is None. If you choose CHAP, you must enter a CHAP name and secret. For more information, see Configuring Secure Authentication.
   c) Optional: Enter an IQN address. The system auto-generates an IQN address if this field is left blank.
   d) If a clustered appliance, select the Address set from the drop-down list. For example, to map a volume on an HA pool, the target should use the VIP associated with that pool.
   e) Select a Target portal, or portals. If not using the default (3260), enter a port number.
5. Optional: Select a **Target Group** from the drop-down list, or enter a unique name in the text field to create a new target group. For information on how to create a target group at a later time, see [Creating iSCSI Target Groups](#).

![Create Target](image)

6. Click **Save**.

**Creating iSCSI Target Groups**

A target group can contain one or more targets. You must successfully complete [Creating iSCSI Targets](#) before you can create a target group.

- **To create a target group, do the following:**
  1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
  2. Select **Management** > **Volumes**.
  3. Select **iSCSI Targets and Groups**.
  4. In the far left column, select the check boxes of the targets to be included in the target group, then click **Assign To Target Group** at the bottom of the window.
5. In the Add targets to group dialog, do one of the following:
   • Enter a New group name in the text field at the top of the dialog.
   • Select the a Target group from the list.

6. Click Add.

7. Click Refresh to update the display.

Viewing iSCSI Target Information and Sessions

You can view target information, as well as details on specific target sessions.

To view target information and sessions, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Volumes.
3. Select iSCSI Targets and Groups.

Target information appears in a table, showing the Group, Target Alias, Status, Target IQN, Authentication method, and IP Address.
4. To view sessions for a specific target, click the COG on the right and select Show sessions.

The Active sessions dialog appears, showing information for active targets: alias, creation time, and initiators accessing the targets.

5. Click Refresh to update the display.

**Editing or Deleting iSCSI Targets**

You can easily edit iSCSI target properties, or delete a target entirely.

- To edit or remove a target, do the following:
  1. Log in to NexentaFusion, and in the Appliances List page, select the appliance.
  2. Select Management > Volumes.
  3. Select iSCSI Targets and Groups.
  4. In the far right column, click the COG and select Edit Target.
  5. In the Edit Target dialog, modify the target settings, as needed.

In the following example, the target was given a new Alias, and a second Target portal was provided.
6. Click **Save**.

   * **To remove a target, do the following:**
     1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
     2. Select **Management > Volumes**.
     3. Select **iSCSI Targets and Groups**.
     4. In the far right column, click the COG for the target and select **Destroy Target**.

5. In the confirmation dialog, click **Yes**.
6. Click **Refresh** to update the display.

**Removing iSCSI Targets from a Group and Destroying the Target Group**

You can easily remove iSCSI targets from a group and delete a target group entirely.

   * **To remove a target from a group, do the following:**
     1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
     2. Select **Management > Volumes**.
3. Select iSCSI Targets and Groups.
4. In the far right column, click the COG for a target and select Remove Target from Group.
5. In the confirmation dialog, click Yes.
6. Click Refresh to update the display.

To delete a target group, do the following:
1. Log in to NexentaFusion, and in the Appliances List page, select the appliance.
2. Select Management > Volumes.
3. Select iSCSI Targets and Groups.
4. In the far right column, click the COG for a target and select Destroy Target Group.
5. Optional: In the confirmation dialog, select the check box to Also delete member targets.
6. Click Yes.
Managing NexentaStor Appliance

111

Managing FC Host Groups, Targets and Target Groups

A Fiber Channel (FC) target is a storage resource located on a server that utilizes the Fibre Channel Protocol (FCP) to link data storage devices over the network. A target group is a container for targets with a set of network portals within a node over which an FCP session is conducted. This section demonstrates how to perform the following tasks:

- Configuring FC Host Groups
- Adding FC Targets to a New or Existing FC Target Group
- Removing FC Targets from a Group
- Viewing Target Group Sessions
- Destroying FC Target Groups

Configuring FC Host Groups

A host group contains one or more remote initiators. You can use initiator groups to restrict the access of various initiators so they can only see specific targets and datasets. You can choose to allow all hosts to access a LUN, or specify that only select hosts have access privileges.

This section demonstrates how to add, edit, and destroy a host group. FC initiator addresses follow the World Wide Name (WWN) format. A WWN is a unique identifier assigned to a manufacturer and hard-coded into a Fibre Channel device. Each WWN is an 8 or 16 byte number. The most significant four bits are referred to as a NAA (Network Address Authority), the remainder is derived from IEEE OUI (Company Identifier) information, for example: wwn.0x500277a4100c4321

- To create a FC host group, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
  2. Select Management > Volumes.
  3. Select Host Groups, then click Add Host Group.
  4. In the Create Host Group dialog, enter a unique Host Group name.
     A host group may contain iSCSI and FC initiators, though this is not recommended. Each initiator can only be a member to one host group.
  5. Click the Fibre channel host initiators tab, select Unassigned Host Initiators to be added to the group. Optionally, you can filter for an initiator in the list by entering characters for the initiator name in the search field.
  6. Click Add to Group.
  7. To manually add an initiator to the group, enter a WWN address and click Add to Group.
  8. Click Save.
Adding FC Targets to a New or Existing FC Target Group

This section demonstrates how to create FC target group with the available targets.

To add FC targets to a new or existing FC target group, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Volumes.
3. Select FC Targets and Groups.
4. Click the check box to the left of the target or targets to be added, then in the lower right corner of the window click Assign to Target Group. Node columns only appear if the appliance is a cluster. Targets that do not yet belong to a group are shown with a blank Target Group name and an empty check box. A target can only belong to one target group.

5. In the Add targets to group, do one of the following:
   - To create a New group with the FC targets, enter a group name in the text field and click Add.
   - To add the FC targets to an existing Target group, click the radio button for the FC group and click Add.

6. Click Refresh to update the display.
Removing FC Targets from a Group

This section demonstrates how to remove FC targets from an FC target group.

To remove FC targets from a group, do the following:
1. Log in to NexentaFusion, and in the Appliances List page, select the appliance.
2. Select Management > Volumes.
3. Select FC Targets and Groups.
4. To remove a target from a group, in the FC Targets and Groups page click the target COG and select Remove Target from Group in the drop-down list.
5. In the confirmation dialog, click Yes.
6. Click Refresh to update the display.

Viewing Target Group Sessions

This section demonstrates how to view session details for all the FC targets belonging to a group.

To view target group sessions, do the following:
1. Log in to NexentaFusion, and in the Appliances List page, select the appliance.
2. Select Management > Volumes.
3. Select FC Targets and Groups.
4. Click the target COG and select Show sessions in the drop-down list.
   The Active sessions dialog appears.
5. Click Close to return to the FC Targets and Groups page.

Destroying FC Target Groups

This section demonstrates how to delete a FC target group. You must remove all targets from the group before you can delete the actual group.

- To delete a FC target group, do the following:
  1. Log in to NexentaFusion, and in the Appliances List page, select the appliance.
  2. Select Management > Volumes.
  3. Select FC Targets and Groups.
  4. Remove all the targets from the group in the following way:
     a) For each target, click the COG and select Remove Target from Group in the drop-down list.
     b) In the confirmation dialog, click Yes.
  5. Click the target group COG and select Destroy Target Group in the drop-down list.

6. In the confirmation dialog, click Yes.
Protecting Data

Data protection applies to any dataset, be it a file system, volume group, or volume. Data protection is accomplished through the use of snapshots, and replication that can be scheduled or continuous. A snapshot is a read-only point-in-time copy of a dataset that can later be cloned. A clone is a new dataset that is readable and writable. The snapshot from which a clone is created from cannot be deleted as long as the clone exists. Promoting a clone creates a completely independent dataset. Replication creates a new dataset, then copies any changes made to the original dataset to the replication location at specified intervals. A replication dataset can be local or remote.

You can create a one-time snapshot of a dataset, or create a schedule to automatically take snapshots of the data at specified intervals. Replication, by definition, is scheduled to occur at specified intervals. Continuous Replication does not follow a schedule, instead replication is triggered whenever a change is detected in the original dataset.

This section covers the following topics:

- Taking a One-Time Snapshot
- Cloning a Snapshot and Promoting a Clone
- Rolling Back or Deleting a Snapshot
- Adding a Protection Service
- Configuring Continuous Replication
- Editing or Deleting a Schedule
- Manually Executing a Service
- Disabling and Enabling a Protection Service
- Destroying a Protection Service
- Flipping the Direction of a Replication Service
- Verifying and Querying Data Protection Data
- Editing the Data Protection Dedicated Network Interface

Taking a One-Time Snapshot

This section demonstrates how to take a one-time snapshot of a file system, volume, or volume group. A snapshot is a read-only point-in-time representation of a file system, volume or other dataset. Snapshots allow safety across reboots and upgrades.

This section demonstrates how to perform a one-time snapshot of a dataset. To set up automatic snapshots taken at specified time intervals, see Adding a Scheduled Snapshots Service.
To take a one-time snapshot of a dataset, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management and do one of the following:
   - For a volume group or volume, select Volumes > Volumes.
   - For a file system, select Filesystems > Filesystems.
3. Expand the pool, navigate to the dataset, click the COG, and select Data Protection.
4. On the Snapshots page, click Snap Now.
5. Enter a Snapshot name in the text field.
   - For file systems you can optionally select the Recursive check box to take snapshots of all child (multiple layers of nested) datasets. If there are no nested datasets, the Recursive check box does not appear.
6. Click Confirm.

Cloning a Snapshot and Promoting a Clone

A snapshot is a copy of a dataset at a specific point in time. A clone is a new dataset, created from a snapshot, that is readable and writable. A clone has an implicit dependency on the snapshot from which it was created. Even though the clone may be at another location in the dataset hierarchy, the original snapshot cannot be destroyed as long as the clone exists. You can clone a file system or volume, but not a volume group, as a volume group is merely a container for volumes.

Promoting a clone removes the original dependency on the snapshot from which the clone was created, making it a completely independent dataset. This section demonstrates how to clone a snapshot, and then promote the clone.

To create a clone, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select the Management tab and do one of the following:
   - Select Volumes > Volumes.
   - Select Filesystems > Filesystems.
3. Click the COG to the right of the dataset and select Data Protection.
4. On the Snapshots page, click the COG for the snapshot and select Clone from the drop-down list.
5. Enter a Path for clone in the text field that includes the clone name. The clone is automatically generated with the name specified in the path.
   - In the following example, the user-specified name “CloneVol1” becomes the name for the clone.
6. Click **Clone**.

   To promote a clone, do the following:
   1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
   2. In the **Appliances List** page, select the appliance that contains the pool.
   3. Select **Management** and do one of the following:
      - Select **Volumes > Volumes**.
      - Select **Filesystems > Filesystems**.
   4. Click the **COG** to the right of the cloned dataset and select **Promote**.
   5. In the confirmation dialog, click **Yes**.

### Rolling Back or Deleting a Snapshot

This section demonstrates how to roll back a dataset to a previous snapshot, and how to delete a snapshot.

| Warning: | A rollback operation reverts all changes made to the dataset since the time the snapshot was taken. |

To rollback a dataset to a previous snapshot, do the following:

1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
2. Select the **Management** tab and do one of the following:
   - Select **Volumes > Volumes**.
   - Select **Filesystems > Filesystems**.
3. Expand the pool, click the **COG** on the far right of the dataset, and select **Data Protection**.
4. Select **Snapshots**, click the **COG** next to the snapshot you want to roll the dataset back to, and select **Rollback**.
5. In the confirmation dialog, click **Confirm**.

![Confirmation Dialog]

**Note:** You are not allowed to destroy a snapshot that has dependant datasets, such as a clone created from the snapshot. Promote any dependant clones, as described in Cloning a Snapshot and Promoting a Clone, before trying to delete snapshots.

- **To delete snapshots, do the following:**
  1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
  2. Select the **Management** tab and do one of the following:
     - Select **Volumes > Volumes**.
     - Select **Filesystems > Filesystems**.
  3. Expand the pool, click the **COG** to the right of the dataset and select **Data Protection**.
  4. Do one of the following:
     - Click the check boxes to the left of the snapshot Name to select individual snapshots to be deleted. The check box changes color and a check mark appears.
     - At the left of the heading bar, click the check box to automatically select all snapshots to be deleted. The check boxes change color and check marks appear.
5. At the bottom of the window, click **Destroy**.
6. In the confirmation dialog, click **Destroy**.

## Adding a Protection Service

A service (function) performs a specific task on a dataset. A protection service creates a snapshot instance based on a specified schedule and dataset. You establish a protection service as a basis for scheduling snapshots and replication.

This section covers the following topics:

- Working with Protection Services
- Adding a Scheduled Replication Service
- Adding a Scheduled Snapshots Service
- Filtering Snapshots and Data Protection Service Data

### Working with Protection Services

Local replication replicates data to another location on the same host. Remote replication replicates data from one host to another host. Once a replication service is enabled, a heartbeat mechanism keeps the service up to date through synchronization.

**Note:** A service can have more than one schedule.

The icons in Table 5-15 appear in the Protection column for Filesystems and Volumes as a visual indicators for the type and status of the service.
Adding a Scheduled Replication Service

For scheduled replication, snapshots are created on a specified schedule and replicated to a designated destination, either locally or on a remote host.

To create a scheduled replication service, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select the Management tab and do one of the following:
   - Select Volumes > Volumes.
   - Select Filesystems > Filesystems.
3. Expand the pool, click the COG on the far right of the dataset, and select Data Protection.
4. Select Protection Services, click Add New Service +, then in the New Protection Service dialog, do the following:
   a) Enter a Service name that is unique and is made up of only letters, numbers, and any of the following symbols: underscore (_), dash (-), or forward slash (/).
   b) Select Scheduled replication from the drop-down list.
   c) For Local replication, click the check box.
   d) For a Remote host, specify the following:
      - HTTPS (required option)
      - IP address or fully qualified domain name (FQDN) for the destination appliance
      - Port number, the default is 8443
   e) For local and remote replication, enter the complete path to the Secondary dataset to which the snapshots will be replicated.
5. Optional: If there are nested datasets, click the **Recursive** check box to take snapshots of all the nested datasets under the parent dataset, as well as the selected dataset. If there are no nested datasets, the Recursive option is grayed out.

6. **Click Add Schedule**, then in the New Schedule dialog specify the following:
   - **Repeat**—the time interval at which the snapshots should be taken: hourly, daily, weekly, or monthly. The options change in accordance with the selected time interval.
   - **Options that are specific to the selected time interval**.
   - **Run at**—time of day at which to take the snapshots.
   - **Snapshots Keep Policy**—number of latest snapshots to be kept locally and on the secondary server.

7. **Click Add Schedule**, then click **Create**.
Adding a Scheduled Snapshots Service

For scheduled snapshots, snapshots are created on a specified schedule. Schedule services can then replicate data on a given schedule. A service can have multiple schedules.

❖ To create a scheduled snapshot service, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select the Management tab and do one of the following:
   • Select Volumes > Volumes.
   • Select Filesystems > Filesystems.
3. Expand the pool, click the COG to the right of the dataset, and select Data Protection.
4. Select Protection Services, click Add New Service +, then in the New Protection Service dialog, do the following:
   a) Enter a Service name that is unique and is made up of only letters, numbers, and any of the following symbols: underscore (_), dash (-), or forward slash (/).
   b) Select Scheduled snapshots from the Service type drop-down list, if not already selected.
   c) If there are nested datasets, select the Recursive check box to take snapshots of all the nested datasets under the parent dataset, as well as the selected dataset. If there are no nested datasets, the Recursive option is disabled.

5. Click Add Schedule, then in the New Schedule dialog specify the following:
   • Repeat—the time interval at which the snapshots should be taken: hourly, daily, weekly, or monthly. The options change in accordance with the selected time interval.
   • Options that are specific to the selected time interval.
   • Snapshots Keep Policy—number of the latest snapshots to be kept locally.
6. Click **Add Schedule**, then click **Create**.

### Filtering Snapshots and Data Protection Service Data

NexentaFusion provides filtering capabilities that greatly improve efficiency for viewing snapshot and data protection service data.

- **To filter snapshot and data protection service data, do the following:**
  1. Log in to NexentaFusion, and in the **Appliances List** page, select the appliance.
  2. Select the **Management** tab and do one of the following:
     - Select **Volumes > Volumes**.
     - Select **Filesystems > Filesystems**.
  3. Click the **COG** of a file system or volume and select **Data Protection** from the drop-down list.
  4. Do one of the following:
     - Click **Snapshots** and select a **Filter by** option from the drop-down list.
     - Click **Protection Services** and select a **Filter by** option from the drop-down list.
  5. Enter a query string, or make selections as appropriate, then click **Filter**. The results appear in the table below.

The following example filters for **Snapshots** created after August 22, 2016 at 12:36 pm.

The following example filters for **Protection Services** with “repl” in the name.
6. Click Clear to reset the default values for a new query.

Configuring Continuous Replication

Continuous replication provides optimum data protection by continually copying dataset updates, and storing them locally or remotely. Changes to data trigger an automatic snapshot that is immediately replicated to a specified destination.

To configure continuous replication, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select the Management tab and do one of the following:
   - Select Volumes > Volumes.
   - Select Filesystems > Filesystems.
3. Expand the pool, click the COG on the far right of the dataset, and select Data Protection.
4. Select Continuous Replication, then click Configure Continuous Replication.
5. In the New Protection Service dialog, do one of the following:
   - a) For Local replication, click the check box.
   - b) For remote replication, specify the following for the Remote host:
     - HTTPS (required option)
     - IP address or fully qualified domain name (FQDN) for the destination appliance
     - Port number, the default is 8443
   - c) For local and remote replication, enter the complete path to the Secondary dataset to which the snapshots are to be replicated.

Note: Scheduled Replication requires an additional license. Scheduled snapshot functionality is included with the base NexentaStor 5.0 license. For more information, contact your NexentaStor Sales Engineer.
6. Optional: For a file system with nested datasets, click the **Recursive** check box to take snapshots of all the nested datasets under the parent dataset. There is no recursive selection for volume groups. All volumes in a selected group are automatically replicated.

7. In the confirmation dialog, click **Create**.

---

**Editing or Deleting a Schedule**

This section demonstrates how to edit or delete a schedule.

| Note: Continuous Replication requires an additional license. Scheduled snapshot functionality is included with the base NexentaStor 5.0 license. For more information, contact your NexentaStor Sales Engineer. |

الف. **To manually edit or delete a schedule, do the following:**

1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.

2. Select the **Management** tab and do one of the following:
   - Select **Filesystems**, click the **COG** for a file system, and select **Data Protection** from the drop-down list.
   - Select **Volumes**, click the **COG** for a volume or volume group, and select **Data Protection** from the drop-down list.
3. To modify the schedule, do the following:
   a) Select **Protection Services**.
   b) Click the arrow to the right of the service Name to expand the tree, click the COG for the schedule and select **Edit** from the drop-down list.
   c) Modify the dialog fields as described in [Adding a Scheduled Replication Service](#) or [Adding a Scheduled Snapshots Service](#).
   d) Click **Save**.

4. To delete the schedule, do the following:
   a) Select **Protection Services**.
   b) Click the arrow to the right of the service Name to expand the tree, click the COG for the schedule, and select **Destroy** from the drop-down list.
   c) In the confirmation dialog, click **Destroy**.

### Manually Executing a Service

This section demonstrates how to execute a scheduled service manually. For information on how to create a service, see [Adding a Protection Service](#).

To manually execute a service, do the following:

1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
2. Select the **Management** tab and do one of the following:
   - Select **Filesystems**, click the COG for a file system, and select **Data Protection** from the drop-down list.
   - Select **Volumes**, click the COG for a volume or volume group, and select **Data Protection** from the drop-down list.
3. Select **Protection Services**, click the COG for the schedule and select **Execute now** from the drop-down list.
Disabling and Enabling a Protection Service

You can disable a protection service at any time. Disabling a protection service ends replication, overriding the configured replication schedule. Disabling the service on the Primary node of an HA cluster simultaneously disables the service on the Secondary node. Disabling the service on both HA nodes at the same time is important in controlling failover.

You can also choose to destroy a protection service, scheduled replication or continuous replication. When you destroy a replication service, you can destroy the destination dataset and snapshots, as applicable to the protection service.

**Warning:** Forcibly disabling recursive replication can result in data inconsistencies. You must disable a replication service before you are allowed to destroy the service.

- To disable a protection service, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
  2. Select the Management tab and do one of the following:
     - Select Volumes > Volumes.
     - Select Filesystems > Filesystems.
  3. Expand the pool, click the COG to the right of the dataset, and do one of the following:
     - Select Data Protection > Protection Services.
     - Select Data Protection > Continuous Replication.
  4. Select the COG on the far right and do one of the following:
     - Select Disable Protection Service from the drop-down list, then in the confirmation dialog click Yes. If replication is in progress, it will complete and then disable the service.
     - Selecting Force the service to be disabled and stop replications immediately may result in data inconsistencies, if a replication is in progress. It is recommended that this option only be selected in critical situations.

- For Continuous Replication, toggle Service enabled to OFF. To re-enable the service, toggle Service enabled back to ON.
5. In the confirmation dialog, click Yes.

Destroying a Protection Service

You can destroy a protection service, as long as the service is disabled. You have the option of destroying the source snapshots and destination snapshots or dataset, as desired.

To destroy a protection service, do the following:

1. Disable the service, as described in Disabling and Enabling a Protection Service.
2. In the Appliances List page, select the appliance.
3. Do one of the following:
   - Select Management > Volumes > Volumes.
   - Select Management > Filesystems > Filesystems.
4. Expand the pool, click the COG on the far right of the dataset and do one of the following:
   - Select Data Protection > Protection Services.
   - Select Data Protection > Continuous Replication.
5. Click the COG for the service, and do one of the following:
   - Select Destroy from the drop-down list.
   - Select Remove Continuous Replication Service.
6. Choose from the following options:

<table>
<thead>
<tr>
<th>Note: When deleting a Continuous Replication service, Destroy the destination dataset and Force the service to be destroyed under all circumstances are the only available options.</th>
</tr>
</thead>
</table>

- **Destroy source snapshots**—Deletes the source snapshots while destroying the service, leaving the destination snapshots and dataset intact.
- **Destroy destination snapshots**—Deletes the destination snapshots while destroying the service, leaving the source snapshots and destination dataset intact.
• **Destroy destination dataset**—Deletes the destination dataset, which includes the destination snapshots, while destroying the service.

• **Force the service to be destroyed under all circumstances**—Deletes the service under all conditions.

7. Click **Destroy**.

**Flipping the Direction of a Replication Service**

Flipping the direction of the replication service can be used to restore data back to the source site as part of a dataset recovery operation. Flipping the direction of the service does not create a copy of the replication service at the secondary site. This operation can only be performed on disabled replication services.

**Warning:** You must disable a replication service before you are allowed to flip the direction. All clients should be quiesced prior to flipping the direction of the service, otherwise data may be compromised during the process. Clients can resume writing data once the flip process is complete.

The following guidelines apply when flipping the direction of a replication service:

- When replication direction is flipped, keep policy values are flipped as well.
- Two services cannot replicate to the same destination. It is not allowed.
- Quiesce all clients prior to beginning the flip process, to maintain the integrity of the data.
- If a replication service is active when flipping the direction, an error dialog appears.
To flip the direction of a service, do the following:

1. Disable the service as described in Disabling and Enabling a Protection Service.
2. In the Appliances List page, select the appliance.
3. Do one of the following:
   - Select Management > Volumes > Volumes.
   - Select Management > Filesystems > Filesystems.
4. Expand the pool, click the COG on the far right of the dataset and do one of the following:
   - Select Data Protection > Protection Services.
   - Select Data Protection > Continuous Replication.
5. Do one of the following:
   - Click the COG next to the dataset and select Flip direction,
   - Click Flip Replication Direction.
6. Click Yes in the confirmation dialog that appears.

**Verifying and Querying Data Protection Data**

The Management > Data Protection page provides a summary of data protection data, in tabular and graphical formats, from which you can verify the established services and configurations.

The Data Protection page also provides querying capabilities by protection service type.

To verify and query data protection data, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Data Protection.
3. Verify the following information, as necessary:
   - Summary of configured Data Protection services, shown in tabular format.
   - Summary of dedicated network configurations, shown in tabular format.
   - Summary of the capacity for each pool, shown in graph format. Hover the cursor over a graphic bar to view a pop-up with detailed information for that pool.

To query snapshot and protection data, do the following

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Select Management > Data Protection.
3. To query snapshot data, click Snapshots and do the following:
   a) Make a selection from the drop-down list on the far left. The default is Snapshot name. The query fields change in accordance to the selection.
   b) Specify the necessary query options, as appropriate. The following example is set to query for snapshots created after August 10, 2016 at 12:00 pm.
   c) Click Filter. Results appear in tabular form below.
   d) Hover the cursor over a Protection Service icon to view a pop-up with detailed information.
   e) Click a COG to perform related actions for the selected snapshot.
4. To query protection data, click **Protection Services** and do the following:
   
   a) Select a **Service name** from the drop-down list. The resulting query options vary in accordance with the selected service.
   
   b) Enter query parameters or make a selection from the drop-down list, as appropriate for the service. The following example is set to query for services that are in a faulted state.
   
   c) Click **Filter**. The results appear in a table below.
   
   d) Hover the cursor over an icon next to the **Name** of the service, to view a pop-up with detailed information.
   
   e) Click a **COG** to perform related actions for the selected service.

5. Click **Clear** to reset the fields to their defaults, and perform another query.

**Editing the Data Protection Dedicated Network Interface**

This section demonstrates how to specify or change the dedicated network interface for data protection. The network interface dedicated to data protection is used to receive and send replication data. For information on how to configure an IP address, see **Managing Network Configurations**.

| Note: | It is recommended that you not use the mgmt address type for the data protection dedicated network interface. This is because the mgmt address is the communication channel between the appliance and NexentaFusion. |

To change the data protection dedicated network interface, do the following:

1. Log in to NexentaFusion and in the **Appliances List** page, select the appliance.
2. Select **Management > Data Protection**.
3. Under **Dedicated Network Interface**, click the **pencil** icon next to the interface you want to modify.

![Dedicated Network Interface](image)

The Data Protection Dedicate Network Interface Address dialog appears.

4. Select the IP address for use when receiving replication data.

![Data Protection Dedicated Network Interface Address](image)

5. Click **Save**.
Managing System and Data Settings

The Administration page allows you to enable, view, and disable system services, as well as Rebooting or Powering Off a NexentaStor Appliance. Under the Data Settings tab, you can configure parameters for logs, events, and analytics for NexentaStor appliances.

This section covers the following topics:

- Enabling and Disabling System Services
- Editing System Services
- Configuring Data Settings

Enabling and Disabling System Services

The Administration > System Settings page provides a list of all the available system services. This section demonstrates how to enable and disable services.

To enable and disable system services, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.

2. Click Administration, and the System Settings tab is selected by default.

   The System Services table appears. Services that are active are shown as online in the Status column. Inactive services are shown as disabled.

3. To enable an inactive service, click the COG for the disabled service and select Enable from the drop-down list.

4. To disable an active service, click the COG for the enabled service and select Disable from the drop down list, then in the confirmation dialog click Yes.

Note: You must have superuser privileges are to perform this procedure.
Editing System Services

You can edit the properties for the following services from the Administration > System Settings page: iSCSI target service, NFS server, NTP client, SMB server, SNMP service. The remaining services can only be enabled or disabled.

This section demonstrates how to edit service properties and save the changes. The editable properties vary according to the service.

To edit system service properties, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Click Administration, and the System Settings tab is selected by default.

   The System Services table appears. If the appliance is a clustered node, the services status for both nodes is shown.

   Services that are active are shown as online in the Status column. Inactive services are shown as disabled. The state of a service does not affect your ability to edit its properties.

3. To edit a service, click the COG for the service and select Edit from the drop-down list. You can edit a disabled service as well as an enabled service.
4. Modify the properties for the service as necessary. The properties you can set vary with the type of domain.

5. Click Save.

Configuring Data Settings

You can configure data settings for the analysis of system data from the Administration > Data Settings page.

This section demonstrates how to configure data settings for logs, events, real-time analytics, active probes, as well as how to view and manage analytics aggregation data. The following topics are covered:

- Configure Logs
- Configure Events and Real-Time Analytics
- Set Active Probes
- Manage Analytics Aggregation Data

Configure Logs

This section demonstrates how to configure data settings for logs, including setting the severity level, retention, and allocated space for logs.

❖ To configure log data settings, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.

2. Click Administration > Data Settings.

3. In the Logs panel, do the following:

   a) Set the Severity Level select the bar graph and drag it to the desired notification level, then clicking Save. The Severity Level communicates the level of system logs the appliance should send to Fusion and persist in the database for easy retrieval and examination.

   b) Select the Retention time interval from the drop-down list, then clicking Save.

   c) Make some space by choosing to Delete logs older than a date you select on the pop-up calendar, then click Delete # of Logs. Where # is the space to be reclaimed.
Configure Events and Real-Time Analytics

You can set the amount of time to store events and real-time analytics data, as well as specify a date after which stored data is deleted.

- **To configure events and real-time analytics data settings, do the following:**
  1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
  2. Click Administration > Data Settings.
  3. Specify the following Retention policies:
     - Select the length of time to Store events for from the drop-down list and click Save.
     - Select the length of time to Store real-time data for from the drop-down list and click Save.
  4. Make some space for events and real-time analytics data in the following ways:
     - Delete events older than a selected date on the pop-up calendar, then click Delete # of Events.
     - Delete real-time data older than a selected date on the pop-up calendar, then click Delete # of Real-Time Data.
Set Active Probes

Active probes provide metrics that are displayed in a visual format on the dashboard. Thus, changing the Active Probe settings affects the dashboard display.

- **To modify active probe settings, do the following:**
  1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
  2. Click Administration > Data Settings.
  3. Go to the Active Probes panel and do the following:
     a) Review the Active Probe Metrics and decide on which ones to set.
     b) Click an empty probe check box to enable a probe.
     c) Click a box with a check mark to disable a probe.
  4. When your selection is complete, click Save.

---

**Note:** Probes that are not described in Table 5-16 are not utilized by NexentaFusion, and should remain disabled (default).
### Table 5-16: Active Probe Metrics

<table>
<thead>
<tr>
<th>Active Probe</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NFSStat</strong></td>
<td>Overall host I/O statistics for NFS protocols (v3, v4). IOPS, bandwidth and latency for NFS read/write operations, including roll-ups (total bytes transferred, total IOPS performed, average latency). Probe interval: 15 seconds</td>
</tr>
<tr>
<td><strong>arcStats</strong></td>
<td>Adaptive Replacement Cache hits percentage. Probe interval: 15 seconds</td>
</tr>
<tr>
<td><strong>fcLuStats</strong></td>
<td>FibreChannel per-LU I/O statistics. IOPS, bandwidth and average latency for read/write operations, including roll-ups (total bytes transferred, total IOPS performed). Probe interval: 15 seconds</td>
</tr>
<tr>
<td><strong>iscsiLuStats</strong></td>
<td>iSCSI per-LU I/O statistics. IOPS, bandwidth and average latency for read/write operations, including roll-ups (total bytes transferred, total IOPS performed). Probe interval: 15 seconds</td>
</tr>
<tr>
<td><strong>zpoolStats</strong></td>
<td>Per-zpool usage statistics. The following data is exposed: - pool size - used space - available space - compression ratio - bytes used by snapshots; - space available for top-level dataset; - space consumed by top-level dataset and all its children. Probe interval: 30 minutes</td>
</tr>
<tr>
<td><strong>SMBStat</strong></td>
<td>Overall host I/O statistics for SMB protocol. IOPS, bandwidth and latency for SMB read/write operations. Probe interval: 15 seconds</td>
</tr>
<tr>
<td><strong>cpuUtilization</strong></td>
<td>Per-CPU utilization percentage (kernel, user or idle, + overall CPU load percentage). Probe interval: 15 seconds</td>
</tr>
<tr>
<td><strong>fcSummaryStats</strong></td>
<td>Host FC I/O statistics. IOPS and bandwidth for read/write operations, including roll-ups (total bytes transferred, total IOPS performed and average latency). Probe interval: 15 seconds</td>
</tr>
</tbody>
</table>
Manage Analytics Aggregation Data

This section demonstrates how you can manage the amount of saved analytics data.

To manage analytics aggregation data, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select the appliance.
2. Click Administration > Data Settings.
3. Go to the Analytics Data Aggregation panel to view the following information:
   - Total disk space used by analytics data
   - Estimated disk space needed for analytics
   - Data older than: aggregation metrics
4. To make more space, do the following:
   a) Click inside the Delete files older than field.
   b) Select a date from the pop-up calendar.
   c) Click Delete # of data to reclaim the displayed amount of space.
Managing High Availability

NexentaStor High Availability (HA) is an enterprise-proven cluster product that manages the availability of critical storage pools. You initially configure the NexentaStor 5.0 HA cluster using the NexentaStor 5.0 Command Line Interface (CLI), and then manage the clustered nodes with NexentaFusion.

For information on how to initially configure nodes of an NexentaStor 5.0 HA cluster, see the NexentaStor 5.0 HA CLI Configuration Admin Guide. For information on how to configure an HA service in NexentaFusion, see Configuring an HA Service for a Shared Pool.

This section covers the following topics:

- About High Availability and HA Services
- Managing HA Services
- Verifying Cluster Status

About High Availability and HA Services

An HA cluster consists of two servers with shared storage and any number of configured HA services. Each service in the cluster contains one or more storage pools and zero or more associated VIPs. The high availability of the pools is maintained by the cluster software that manages the startup and failover of the HA services within the cluster.

An an example of a High Availability (HA) cluster configuration would consist of two HA services. Each service created independently, then assigned to one or more pools. Under normal operation, each node provides services their designated pools. In the event of either node failing, the surviving node takes over the HA services for both the pools. The pools must be built using the shared storage devices that are accessible from both the nodes.

When a failed node is repaired and restarted, it re-joins the cluster and the administrator controls when the pools are redistributed. The nodes in a cluster communicate with each other node through heartbeat mechanisms. The HA cluster detects a system failure when updates from a node are not received across the heartbeat mechanisms for a specified period of time.

HA Cluster

- A pair of NexentaStor appliances that have the HA feature licensed on both nodes.
- Runs a defined set of services and monitors each cluster member for failures. Clustered NexentaStor appliances are connected through various communication channels, and exchange heartbeats that continually send information about their states.
- Can have multiple pools and services, with at least one dedicated pool per HA service.
- Includes a built-in monitoring mechanism that detects a failure in the interface (for example, Web UI network interface or Fibre Channel interface) between the clients and the datasets that can trigger an automatic failover to the other node in the cluster.
Managing HA Services

An HA service runs on clustered nodes to provide high availability (HA) access to user data. When the HA service detects a node failure, it transfers ownership of the shared storage to the other node in the cluster pair. HA services are managed independently from one another and can be in several possible states.

The Management > High Availability tab only appears when nodes are configured in a HA cluster. An HA cluster must be configured using the NexentaStor 5.0 CLI. For more information, see the NexentaStor 5.0 CLI Configuration Guide.

This section covers the following topics:

- Verifying Service Status
- Failing Over Services Manually
- Adding a VIP
- Editing and Deleting a VIP
- Moving an HA Service
- Setting the HA Service Mode
- Stopping and Starting an HA Service
- Destroying an HA Service
- Removing a Pool from HA Service

For information on how to configure an HA service in NexentaFusion, see Configuring an HA Service for a Shared Pool.
Verifying Service Status

This section demonstrates how to review an overall summary of services running on clustered nodes and view details for each service.

To view service status and details, do the following:

1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
2. Select Management > High Availability.
   - The Services summary and Services details tables appear showing at-a-glance information about the services running on both nodes in the cluster.
4. Click the Shield icon for a service in the Service summary table to view details for the service in a pop-up dialog.
5. To update the data display, click Refresh in the upper right corner.
Failing Over Services Manually

This section demonstrates how to manually failover all services from one node in a cluster to the other.

| Warning: | This procedure moves all services from the source node to the destination (or Secondary) node.

- To manually fail over services, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
  2. Select Management > High Availability.
  4. In the upper right corner of the Services summary panel, click Failover.
  5. In the confirmation dialog, Select the desired direction for the failover, and then click Yes.

Adding a VIP

This section demonstrates how to add a virtual IP (VIP) to an existing service. A VIP is an address associated with a shared pool. Network clients use a VIP to connect to a shared pool. After creating an HA service, you can add a VIP in a cluster-wide fashion on all cluster nodes.

- To add a VIP to a service, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
  2. Select Management > High Availability.
  3. Select Service Management, and then select the desired service.
  4. In the Services details panel, click Add VIP. A row is added to the table.
5. Do the following:
   a) Enter a unique VIP Name in the text field.
   b) Select an IP protocol from the drop-down list. IPv4 is the default.
   c) Enter an IP Address and Netmask in the appropriate fields.
   d) Select an interface for each node from their respective drop-down lists.

6. Click the disk icon on the far right to Add VIP. Or, click the X to Cancel Editing and delete the entries for the new VIP.

Editing and Deleting a VIP

This section demonstrates how to edit and delete HA VIPs with NexentaFusion.

To edit an HA VIP, do the following:
1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
2. Select Management > High Availability.
4. In the Services details panel, click the COG for the VIP and click Edit.
5. Modify the VIP settings as necessary, and click the disk icon to Save Changes.

To delete an HA VIP, do the following:
1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
2. Select Management > High Availability.
4. In the Services details panel, click the COG for the VIP and click Delete.
5. In the confirmation dialog, click Yes.
Moving an HA Service

This section demonstrates how to manually move a selected service to the alternate node in a cluster at any time.

- **To manually move a service to the other cluster node, do the following:**
  1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
  2. Select Management > High Availability.
  4. In the Services summary table, click the COG for the service and select Move.
  5. In the Move HA service to another node confirmation dialog, click Yes.

![Move HA service to another node confirmation dialog]

The service is moved to the alternate node in the cluster.

Setting the HA Service Mode

After creating an HA service, you can set the service mode to start automatically after the service stops, or set the service mode to manual, requiring that the service be started manually. This section demonstrates how to set the service mode to either automatic or manual.

- **To set the mode of a service, do the following:**
  1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
  2. Select Management > High Availability.
  4. In the Services summary table, click the COG for the service and select Set Mode.
  5. In the Set service mode dialog, click the appropriate radio button to set the mode for each node: automatic or manual.
6. Click Set to apply the changes.

Stopping and Starting an HA Service

This section demonstrates how to manually stop and start an HA service at any time with NexentaFusion.

❖ **To stop and start an HA service, do the following:**

1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
2. Select Management > High Availability.
4. In the Services summary table, click the COG for the service and do one of the following:
   - To stop the service, select Stop from the drop-down list.
   - To start the service, select Start from the drop-down list.
5. In the confirmation dialog, click Yes.

Destroying an HA Service

This section demonstrates how you can destroy an HA service with NexentaFusion.

❖ **To destroy an HA service, do the following:**

1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
2. Select Management > High Availability.
4. In the Services summary table, click the COG for the service and select Destroy from the drop-down list.
5. In the confirmation dialog, click Yes.
Removing a Pool from HA Service

This section demonstrates how to remove a pool from HA service with NexentaFusion. To view the status of a shared pool, see Viewing Status Details for a Shared Pool.

| Warning: | The HA service will be destroyed when you remove the initial pool with which the service was created (the pool with same name as the service) from HA control. |

- To remove a service from a pool, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
  2. Select Management > High Availability.
  4. In the Services details table, click the COG for the pool and select Remove.
  5. In the confirmation dialog, click Yes.

Verifying Cluster Status

You can review and verify the details and status of cluster nodes at a glance from the Cluster Status page, including heartbeat and configuration information.

- To verify the status of cluster nodes, do the following:
  1. Log in to NexentaFusion and in the Appliances List page, select a cluster.
  2. Select Management > High Availability.
     The Cluster Status table appears.
4. Click **Refresh** to update the data.

**What Comes Next?**

Chapter 6, *Performance Monitoring and Analytics* covers monitoring and analyzing appliance operations and performance. You perform these tasks with customizable widgets that provide analytics data presented with intuitive graphic metrics.
Performance Monitoring and Analytics

This chapter introduces the NexentaFusion features you can use for monitoring NexentaStor appliances, and covers the following topics:

- Terminology
- Dashboard
- Using the Analytics Workspace
- Using a Canvas
- Using Widgets
- Analyzing Data
- What Comes Next?

Terminology

The following table introduces NexentaFusion terms used for performance monitoring and analytics.

Table 6-1: Terms and Descriptions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics Workspace</td>
<td>The Analytics workspace allows you to monitor and investigate appliance operation and performance. This is accomplished through the use of customizable widgets with visual displays of performance and capacity metrics.</td>
</tr>
<tr>
<td>Dashboard (Top level tab)</td>
<td>The Dashboard tab provides real-time visual data for a selected NexentaStor appliance. The NexentaFusion default dashboard contains multiple widgets that display operational status information. To view the dashboard for an appliance, log in to NexentaFusion, select Appliance, then select an appliance from the Appliances List and click Dashboard. For more information, see Dashboard.</td>
</tr>
</tbody>
</table>

The widgets displayed on the Dashboard can be customized on the Analytics workspace. For more information, see Viewing and Editing the Dashboard Canvas.
Dashboard

The NexentaFusion dashboard provides a visual display of data for NexentaStor appliances. The default NexentaFusion dashboard contains widgets that show the operational status of the appliance. Widget metrics update every few minutes.

To view the default dashboard, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance.
3. Click **Dashboard**.

<table>
<thead>
<tr>
<th>Terms</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard Canvas (Analytics workspace)</td>
<td>The Dashboard canvas in the Analytics workspace is the permanent canvas whose widgets are displayed on the Dashboard. Changes made to the widgets in the Analytics workspace are reflected on the Dashboard (under the Dashboard tab).</td>
</tr>
<tr>
<td>Canvas</td>
<td>A canvas is a container in which you view selected widgets. You can customize the widgets to investigate aspects of the appliance components operation and performance. For more information, see Creating a New Canvas and Managing Canvases.</td>
</tr>
<tr>
<td>Widgets</td>
<td>A widget provides a visual display of information for various aspects of your appliance. Performance widgets chart metric data in real-time or historical time. Capacity and Dashboard widgets provide summaries of capacity and performance metrics. Widgets are grouped by category. For more information, see Adding, Moving, Resizing, and Removing Widgets and Configuring Widgets.</td>
</tr>
</tbody>
</table>
The widgets displayed on the Dashboard can be customized by editing them on the Analytics workspace. For more information, see Using the Analytics Workspace and Viewing and Editing the Dashboard Canvas.

Using the Default Dashboard

The Dashboard tab displays the widgets defined by the Dashboard canvas. You can use the following elements to read the metrics from the Dashboard:

- State icons provide an at-a-glance view of appliance health and performance, as well as the services running on the appliance.

- Graphs display detail pop-ups when you hover the cursor over an area.
• Drop-down lists allow you to select time intervals for statistic aggregation that are displayed in graph form below. Hover the cursor over an area of the graph to view detailed information for a particular point in time.

### What Comes Next?

The following sections demonstrate how to edit the dashboard using the analytics workspace, as well as how to create a canvas, add widgets, and manage widgets and canvases.

### Using the Analytics Workspace

In the Analytics workspace, you can create a canvas to display the combined metrics of NexentaStor appliances in real time or historical time. These metrics can be displayed in an intuitive graphical form.

### Understanding the Analytics Workspace

This section introduces you to the functional areas that make up the Analytics workspace. The Analytics workspace is divided into three major areas, as shown in Figure 6-1.
Performance Monitoring and Analytics

Figure 6-1: Areas of the Analytics Workspace

Canvas Workspace: 1

The canvas is the container for widgets. Drag a widget from the selection panel to the drop zone within the perforated line. Once in the canvas, a widget can be resized and moved around. In this workspace, you can configure the widgets to tailor to your needs with specific query parameters. Configured widgets can be saved for reuse on other canvases, and appear in the Configured Widgets section.

Widget Selection Panel: 2

NexentaFusion includes several sets of widgets that are grouped into categories. The categories include Configured, Top N, Performance, Capacity, and Dashboard widgets. Click the arrow next to the widget title to expand or collapse the list of available widgets. Configured widgets are user-customized widgets saved for reuse. For more information, see Configuring Widgets.

Canvas Bar: 3

Select a canvas you want to use, or add a new canvas:

- Click the [+] icon in the Canvas Bar to create a new canvas, then drag and drop widgets from the Widget Selection Panel onto the new canvas.
- Click a canvas name to activate the canvas for use.

- Use the arrows on the sides of the canvas bar to scroll in the indicated direction.
Click the COG to view a list of supported actions for the current (selected) canvas.

Once a widget is on a specific canvas (Canvas-A), it belongs to that canvas. If you edit the widget on another canvas (Canvas-B), it does not affect the widget on Canvas-A.

Navigating to the Analytics Workspace

The following task demonstrates how to use the Analytics workspace to monitor key aspects of appliance performance.

- To navigate to the Analytics workspace, do the following:
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance.
  3. Click **Analytics**.
  4. Review [Understanding the Analytics Workspace](#) if needed, then continue with [Using a Canvas](#).

Using a Canvas

A canvas is a container on which you select and customize widgets to display specific metrics for appliance operation and performance. This section covers the following topics:

- [Creating a New Canvas](#)
- [Adding, Moving, Resizing, and Removing Widgets](#)
- [Managing Canvases](#)
- [Viewing and Editing the Dashboard Canvas](#)
Creating a New Canvas

NexentaFusion allows you to create custom canvases to monitor specific aspects of appliance health and performance. You can populate a custom canvas with selected widgets to create an optimized view for the needs of your site.

To create a custom canvas, do the following:

1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
2. In the **Appliances List** page, select the appliance.
3. Click **Analytics**, then click Add [+ ] on the **Canvas Bar**.

![Canvas Bar](image)

4. Enter a name for a new canvas in the text field and click **OK**.

![Add new canvas](image)

5. Continue with **Adding, Moving, Resizing, and Removing Widgets**.

Adding, Moving, Resizing, and Removing Widgets

After creating a new canvas, you can add widgets, arrange and resize them on the canvas to meet your needs. This section demonstrates how to perform these tasks.

To add, move, and resize widgets on a canvas, do the following:

1. Complete the steps for **Creating a New Canvas**.
2. To add widgets, from the **Widget Selection Panel** do one of the following:
   - Drag and drop the desired widgets to the **Canvas Workspace**.
   - Click the [+ ] icon **on the widget** to add it to the canvas.
3. To move a widget, select the edge of the title on the left or right, and drag to the desired location.
4. To resize a widget, select the border and drag in the desired size.

5. To edit a widget, click the COG in the upper corner and select Edit, modify the settings as needed, then click Apply. For more information, see Using Widgets.

6. To delete a widget, click the COG in the upper corner and select Remove.

The canvas saves automatically. For information on how to save a configured widget for reuse on other canvases, see Configuring Widgets.

---

**Managing Canvases**

You can customize a canvas in a number of ways. This section demonstrates how perform the following tasks:

- Modifying, Renaming, or Removing a Canvas
- Cloning, Importing, and Exporting Canvases

**Modifying, Renaming, or Removing a Canvas**

After creating a custom canvas, it is easy to modify widgets, change the canvas name, or remove the canvas entirely.

- To modify, rename, or remove a canvas, do the following:
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the Appliances List page, select the appliance.
  3. Select an appliance and click **Analytics**.
4. To modify the canvas, in the **Canvas Bar**, select the canvas name, then modify the canvas widgets as described in **Adding, Moving, Resizing, and Removing Widgets**.

5. In the **Canvas Bar**, click the **COG** and do one of the following:
   - To rename the canvas, select **Edit Canvas Name**, enter a new canvas name in the text field of the dialog, and click **Save**.
   - To delete the canvas, select **Remove Canvas**, in the confirmation dialog click **Continue** to remove the canvas, or **Cancel** to exit the procedure without deleting the canvas.

6. To remove a widget from a canvas, see **Configuring Widgets**.

---

**Note:** NexentaFusion also has a Dashboard canvas with pre-defined widgets. The Dashboard canvas can be edited, but not deleted. For more information, see **Viewing and Editing the Dashboard Canvas**.

---

**Cloning, Importing, and Exporting Canvases**

NexentaFusion makes it easy to leverage your custom canvases. This section demonstrates how to clone an existing canvas, import a previously saved canvas file, or export a canvas for future use.

- **To clone, import, or export a canvas, do the following:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance.
  3. Click **Analytics**.
4. In the Canvas Bar, select the canvas name, click the COG, and do one of the following:

- To clone a canvas, select Clone Current Canvas from the drop-down list, enter a new name for the (clone) canvas in the text field, and click OK.
- To export a canvas, select Export Canvas Blueprint from the drop-down list. A .json blueprint file containing the definitions of the widgets in the canvas is downloaded to the local system.
- To import a canvas, select Import Canvas Blueprint from the drop-down list, Choose a File to Import, and click Import.

Viewing and Editing the Dashboard Canvas

From the Analytics page, you can view the default Dashboard canvas with pre-defined widgets that allow you to monitor appliance operational status. The side-by-side placement of widgets makes it easy to see the correlation between different metrics. You can customize the Dashboard for your specific needs.

Viewing the Dashboard Canvas

This section shows you how to view the dashboard canvas from the Analytics page.

To view the dashboard canvas from the Analytics workspace, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List page, select the appliance.
3. Click Analytics.
4. To view current data on NexentaStor appliances, click the **Dashboard** link in the **Canvas Bar**. A canvas with a pre-defined set of widgets appears. For information on how to customize the widgets, see **Configuring Widgets**.

Customizing the Dashboard Canvas

You can customize the Dashboard canvas by adding, rearranging.

- **To add widgets to the Dashboard canvas, do the following:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance.
  3. Click the **Analytics** tab, and then click the **Dashboard** link in the Canvas Bar. The Dashboard canvas displays.
  4. To add widgets, from the **Widget Selection Panel**, select widgets and drag them onto the canvas.
  5. To rearrange and resize widgets, see **Adding, Moving, Resizing, and Removing Widgets**.
  6. To configure widget settings, see **Using Widgets**.

---

**Note:** You can edit the widgets on the Dashboard canvas, but the canvas cannot be deleted. When you customize the widgets of the Dashboard canvas from the Analytics workspace, the changes are reflected on the default Dashboard canvas (Dashboard tab).

Resetting Dashboard Canvas Defaults

This section demonstrates how to reset the Dashboard canvas to its default settings.

- **To revert the Dashboard canvas to default settings, do the following:**
  1. Log in to NexentaFusion and click **Appliance** in the drop-down list.
  2. In the **Appliances List** page, select the appliance.
  3. Click **Analytics**.
  4. Click the **Dashboard** link in the **Canvas Bar**. The Dashboard canvas displays.
  5. Click the **COG** in the **Canvas bar** and select **Reset to Defaults**.
Using Widgets

This section covers the Using the Widget Selection Panel and the different types of widgets, then demonstrates Configuring Widgets.

Note: The Using a Canvas section demonstrates Adding, Moving, Resizing, and Removing Widgets after Creating a New Canvas.

Using the Widget Selection Panel

NexentaFusion provides a set of widgets on the Widget Selection Panel that are grouped in functional categories. For more information, see Configuring Widgets.

To bring up the Widget Selection Panel, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List page, select the appliance.
3. Click Analytics.
4. Click the Dashboard link in the Canvas Bar, then click the expansion arrow (>) on the far left.
5. Use the arrow on the Widget Selection Panel to hide (<) and re-display (>) the panel.
6. Continue with Adding, Moving, Resizing, and Removing Widgets and Configuring Widgets.

Configuring Widgets

This section demonstrates how to configure and save widgets for reuse on other canvases, and covers the following topics:

- **Widget Categories**
- **Cloning Widgets**
- **Editing and Saving Widgets**
- **Removing Configured Widgets**

**Widget Categories**

The Widget Selection Panel is divided into the following functional categories:

- **Configured** widgets—Provides easy access to user-customized widgets that have been saved for reuse.
- **Top N** widgets—Provides aggregated data for selected metrics for you to analyze, showing the highest values in a specified set of data collections over a set period of time. For more information, see Analyzing Top N Data.
- **Performance** widgets—Provides real-time/historical IO metrics for pools, NFS or SMB shares, iSCSI or FC LUNs, and the cache hit rate of the appliance. You can load and save widgets with specific parameters to fine tune the monitoring of appliance performance. For more information, see Analyzing Performance Data.
Capacity widgets—Provides information that allow you to make capacity management decisions. Capacity widgets provide detailed information for a NexentaStor appliance. For more information, see Analyzing Capacity Data.

Dashboard widgets—Provides a summary of the appliance health, appliance IO performance, CPU utilization, cache hit rate, high priority events (alerts), and data reduction ratio by pool. For more information, see Analyzing Health and Utilization Data.

Cloning Widgets

This section demonstrates how to create a copy, or clone, of a widget.

To clone and save a widget, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List page, select the appliance.
3. Click Analytics.
4. Click the COG in the upper right corner of the widget and select Clone from the drop-down list.

After making a cloned copy, you can change the metrics being displayed on the widget, so you can compare the relationships of metrics for similar objects. For more information, see Editing and Saving Widgets.

5. On a performance graph, hover the cursor over a point on the graph to view specific metrics for that point in time.
Editing and Saving Widgets

This section demonstrates how to edit a widget, and then save it as a new custom widget for reuse on a custom canvas.

- To edit a widget and save it as a custom widget, do the following:
  1. Log in to NexentaFusion and click Appliance in the drop-down list.
  2. In the Appliances List page, select the appliance.
  3. Click Analytics.
  4. To change the name of a widget, double-click the title, enter a new name in the text field, and click Save.
  5. To edit the widget display, click the COG in the upper right corner of the widget and select Edit from the drop-down list. The options and values you can edit, vary with the function of the widget.
  6. Make the desired modifications and click Apply.
  7. To permanently save the changes and create a new custom widget, click the COG and select Save.
8. Enter a title for a new custom widget in the text field and click OK.

The name of the new custom widget appears under Configured Widgets in the Widget Selection Panel of the canvas.

Removing Configured Widgets

This section demonstrates how to remove a configured widget from the Widget Selection Panel. You are not allowed to remove NexentaFusion default widgets.

To remove a configured widget from the Widget Selection Panel, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.
2. In the Appliances List page, select the appliance.
3. Click Analytics and click the canvas name in the Canvas Bar.
4. Hover the cursor to the right of the widget name and click the trash can icon when it appears.

The widget disappears from the Widget Selection Panel. However, the widget remains on any canvases on which it has been placed.

Analyzing Data

This section describes how to use the widgets of the Widget Selection Panel in the following ways:

- Analyzing Performance Data
- Analyzing Top N Data
- Analyzing Capacity Data
- Analyzing Health and Utilization Data

For information on how to save customized widgets, see Editing and Saving Widgets.

Analyzing Performance Data

Performance widgets provide a visual display of appliance performance metrics aggregated over a specified period of time. Performance Widgets include the following:

- Cache Hit Rate
- FC LUN Performance
- iSCSI LUN Performance
- NFS Share IO Performance
- Pool IO Performance
- SMB Share IO Performance

The following procedure demonstrates how to view performance metrics aggregated for a specified time interval.
To use the Performance widget to view historical data, do the following:

1. To select a time range to filter over, do one of the following:
   - Click the time interval in the widget title and select a different interval from the drop-down list.
   - Select a time interval from a drop-down list beneath the widget title.

2. Optionally, double-click the title to bring up a dialog to rename the widget.

3. Select query parameters from the drop-down lists to customize the data displayed.

4. Hover the cursor over the chart to view details about the IOs for that specific point in time.

5. Move the brush to view a detailed segment of the total time range. This allows you to interactively zoom in for a more granular view of the data for that time segment, then zoom out again.

Figure 6-2: Using a Performance Widget to View Historical Data
You can specify the following performance parameters by selecting Edit from the widget COG drop-down list:

- Minimum and maximum values for the y-axis
- Threshold line to indicate whether the IO level is above or below the threshold value
- Line mode or area mode display
- Chart color for free and allocated space
- Graph color for threshold settings, when used space reaches a warning or error level

Analyzing Top N Data

Top N widgets allow you to analyze aggregated data for selected metrics, viewing the highest values in a specified collection of data over a set period of time. Top N widgets can help you to identify elements that are under or overutilized. Top N widgets include the following:

- Top FC LUNs by
- Top iSCSI LUNs by
- Top NFS shares by
- Top SMB shares by

You can select from the following metrics for analysis over a specified time period:

- IOPS: Total, Read, Write
- Latency: Average, Read, Write
- Bandwidth: Total, Read, Write

Working with Top N Widgets

For Top N widgets, you can select the type of metrics and time interval over which the data is aggregated. If the pre-defined time intervals are not sufficient, you can specify a custom time interval. Aggregation data is updated at 20% of the selected time interval, with a maximum refresh rate of 1 minute. For example:
• 5 min interval, refreshes every (1) minute
• 15 min interval, refreshes every 3 minutes
• 30 min interval, refreshes every 6 minutes

The Top N widgets provide the following metric options:

Creating a Custom Time Interval

You can specify a custom time interval over which Top N data is aggregated. When you select the Custom time interval option from the time interval drop-down list, two month calendars appear. Select the start and end dates on the respective months.

Click the navigation arrows (< >) at the top of each calendar, to page forward or back for a starting and ending month. Select the time at which to start and stop data aggregation on the specified dates (hours and minutes) from the drop-down lists. Click Apply to finalize the custom Top N aggregation schedule.

In the following example, the aggregation of Top N data is scheduled to start on 08/23/2016 at 12:00 noon and end on 09/30/2016 at 12:00 noon.
Analyzing Capacity Data

The following Capacity widgets provide visual summaries of logical and physical capacities:

- **Configured Capacity**—Shows the sum of the free capacity and the allocated capacity of the pool after applying redundancies (raid/mirror).
- **Installed Capacity**—Shows the sum of the disk sizes installed in the appliance.
- **Data Reduction**—Shows the data reduction ratio for pools, not including dedupe reduction.
- **Pools Configured Capacity**—Displays a graphical summary of the free capacity and the allocated capacity of all configured pools on the appliance. Hover the cursor over a pool graph to view the allocated capacity and available free space for the pool.
- **Pools % Allocated Capacity**—Shows the allocated capacity, and capacity used for data protection, for each individual pool in the appliance. Pool absolute capacity values are shown as a percentage of the total values.
The following figure shows the configurable options for the Pools Configured Capacity widget, when you select Edit from the COG drop-down list:

- Set Chart colors for free and allocated space.
- Set Capacity Threshold graph colors (threshold percentage) for when used space reaches warning or error levels.
- Click the COG and select Save to apply the customizations.

### Analyzing Health and Utilization Data

Dashboard widgets are used to monitor appliance health and performance. Dashboard widgets include the following:

- Alerts—Displays warning and error alerts in easy-to-read tabular format. You can customize the widget to specify the type of alert displayed.
- Appliance Health—Shows the health status for all NexentaStor appliances and their pools, conveying good health, warnings, and critical alerts with at-a-glance icons.
- CPU Utilization —Displays CPU usage for all NexentaStor appliances. You can edit settings to display alerts when the CPU usage reaches a certain threshold in a specified time interval.
- Cache Hit Rate—Shows real-time data for the percentage of accesses that result in cache hits.
- Data Reduction Ratio by Pool—Displays the compression ratio for pools, not including dedupe reduction. The display is ordered from highest to lowest compression ratio value.
- NAS IO Performance—Displays performance metrics for OPS, Latency, and Bandwidth. You can set IO thresholds for a specific time interval and configure alert displays for when thresholds are exceeded.
- SAN IO Performance—Displays SAN performance metrics for iSCSI and FC, as desired. You can select options from drop-down lists at the top of the widget to customize the information displayed.
What Comes Next?

The following chapter covers the following details:

Where to find alerts and logs; how to monitor and investigate key aspects of appliance; how to configure display parameters for threshold alerts; how to configure the system to respond to certain types of alerts and logs.
Fault Management

This chapter covers the following topics:

- About Logs, Audit Logs, Events, and Alerts
- Viewing Logs, Audit Logs, and Alerts
- Creating Rules for Logs and Events
- Troubleshooting Data Devices in a Pool
- Locating a Failed Disk
- Managing Pool Data Devices
- Rebooting or Powering Off a NexentaStor Appliance

About Logs, Audit Logs, Events, and Alerts

The Elasticsearch database (GSDB) is the NexentaFusion database used to persist logs, alerts, and metrics for analytics. By default, the Elasticsearch database server is placed on the same machine as NexentaFusion with port 9200, when NexentaFusion is installed.

Logs include system events, process information, and errors that may disrupt the normal provisioning of the storage appliance. The following examples of actions are recorded as logs:

- NexentaFusion fails to join the Windows AD server
- License compliance violations
- Lost connection between NexentaFusion and NexentaStor appliances

Audit Logs record user activities of NexentaFusion actions that change a NexentaStor appliance. An audit log also records user authentication, when they log in and out of NexentaFusion or a NexentaStor appliance.

Events are captured changes in NexentaFusion and the storage appliance environment. Both logs and events are listed under the Logs tab in the UI. When an event occurs that requires immediate attention or a critical system health monitor threshold has been exceeded, an alert occurs.

Alerts are notifications of high priority events. Once you have reviewed an alert, you have the option to acknowledge that the alert has been reviewed. Acknowledging an alert removes it from the alerts shown on the Alerts Widget, as well as from the alert count shown on the Appliance List view. The following actions are recorded as alerts:

- A system component fails
- A capacity reaches a threshold warning or error level
Viewing Logs, Audit Logs, and Alerts

NexentaFusion displays the logs, audit logs, and alerts in a tabular format. All messages are displayed in reverse chronological order. You can search for specific messages using wildcard and text searches, or by narrowing the scope with the time range filter.

Some notifications include a + option to display information about the metric. Entries in the table can be exported to CSV format and automatically downloaded to your local system.

To view and download logs, audits, and alerts, do the following:

1. Log in to NexentaFusion.
2. Select FUSION from the drop-down list in the top left corner of the window.
3. Under Notifications, click one of the following:
   - Logs—to view system event logs.
   - Audit—to view audit logs of user authentication and activities that modified an appliance with NexentaFusion.
   - Alerts—to view notifications of high priority events.
4. Click the Expand all messages plus (+) option to expand all messages.
5. To download logs, audits, or alerts, click Export as CSV.
Creating Rules for Logs and Events

NexentaFusion Rules are used to display alerts and generate email notifications. NexentaFusion provides the following default rules:

<table>
<thead>
<tr>
<th>Default Rule Name</th>
<th>Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance alert resolved</td>
<td>Generates an alert when a specified resolved alert message appears in the log.</td>
<td>Warning</td>
</tr>
<tr>
<td>Appliance error alert generated</td>
<td>Generates an alert when a specified error message appears in the log.</td>
<td>Error</td>
</tr>
<tr>
<td>Appliance reboot needed — firmware change</td>
<td>Generates an alert when there is an firmware update, and the appliance must be rebooted.</td>
<td>Warning</td>
</tr>
<tr>
<td>Appliance reboot needed — sysconfig change</td>
<td>Generates an alert when there is a sysconfig change, and the appliance must be rebooted.</td>
<td>Warning</td>
</tr>
<tr>
<td>Appliance warning alert generated</td>
<td>Generates an alert when a specified warning message appears in the log.</td>
<td>Warning</td>
</tr>
<tr>
<td>Appliance went offline</td>
<td>Generates an alert when a lost appliance connection message appears in a log.</td>
<td>Error</td>
</tr>
<tr>
<td>Appliance worker went offline</td>
<td>Generates an alert when a lost appliance connection message appears in a log.</td>
<td>Error</td>
</tr>
<tr>
<td>Data Protection service faulted</td>
<td>Generates an alert when a specified HPR service faulted message appears in the log.</td>
<td>Error</td>
</tr>
<tr>
<td>Data Protection service scheduled start failed</td>
<td>Generates an alert when a specified HPR service scheduled start failed message appears in the log.</td>
<td>Warning</td>
</tr>
<tr>
<td>Low free space warning</td>
<td>Generates an alert when a specified low free space message appears in a log.</td>
<td>Warning</td>
</tr>
<tr>
<td>Pool configuration changed</td>
<td>Generates an alert when a pool configuration changes.</td>
<td>Warning</td>
</tr>
<tr>
<td>Syslog entry—alert emergency</td>
<td>Generates an alert when an emergency message appears in a log. This rule can be disabled.</td>
<td>Error</td>
</tr>
<tr>
<td>Syslog entry—alert severity</td>
<td>Generates an alert when an alert severity message appears in a log.</td>
<td>Error</td>
</tr>
<tr>
<td>Syslog entry—critical severity</td>
<td>Generates an alert when a critical severity message appears in a log. This is disabled by default.</td>
<td>Warning</td>
</tr>
</tbody>
</table>

You can create rules in NexentaFusion that generate alerts and email notifications in response to a specified event or occurrence. NexentaFusion continuously watches the Elastic DB for events that match rule criteria, and immediately generates an alert with the specified severity of error or warning when one occurs.

You can modify default rules to generate email notifications, and disable rules as needed. Disabling rules can be useful during system maintenance, to prevent unnecessary alerts from being generated.
To create log or event rules, do the following:

1. Log in to NexentaFusion and select FUSION from the drop-down list in the upper left corner of the window.

2. Under Notifications > Rules, do one of the following:
   - To create a new log rule, click Add Logs Rule.
   - To create a new event rule, click Add Events Rule.

3. Enter a Name for the rule, select Warning or Error for the Severity level, then specify YES for Enabled (default) or NO to leave the rule disabled until a later time.

4. Enter the rule criteria in the text field.

5. Optional: Select Enable e-mail notifications, enter an email address and subject line for the message in their respective text fields.

6. Click Save.

Troubleshooting Data Devices in a Pool

When hardware is unreliable or not functioning properly, you may need to temporarily disconnect storage devices. To do this, first identify the type of failure. Then, take the device offline to fix or replace it.

To identify a device failure, do the following:

1. Log in to NexentaFusion and click Appliance in the drop-down list.

2. In the Appliances List menu, select an appliance.
3. Under **Management**, click **Pools**.
   A list of all pools belonging to the appliance appears.

4. Click the **COG** for the pool, and select **Status** from the drop-down list.

5. To view health status and potential errors, click **Disks** to bring the panel forward.
   The Health column can display any of the following values:
   - ONLINE, AVAIL—Displays in Green text.
   - DEGRADED, IN USE—Displays in yellow (warning) text.
   - OFFLINE, FAULTED, REMOVED, UNAVAIL—Displays in red (error) text.
   - N/A, SPLIT—Displays in regular text color.
   The Physical State column can display any of the following values:
   - ONLINE—There are no current problems.
   - UNAVAIL, NO_MEDIA, RETIRED, RETIRING, ORPHANED, UNKNOWN, OFFLINE—Disk is not functioning and must be repaired or replaced.
   - Blank—This field is blank for vDev entries.

6. Click **Close**.

7. After identifying the type of error in the device, do the following:
   a) Locate the disk using the blink feature, as described in **Locating a Failed Disk**.
   b) Take the required actions, as described in **Managing Pool Data Devices**.

**Locating a Failed Disk**

The Blink feature enables you to make the indicator for a specific disk bay blink. This functionality can be used to physically locate a failed disk.

- **To locate a failed disk, do the following:**
  1. Log in to NexentaFusion, and click **Appliance** in the drop-down list.
  2. In the **Appliances List** menu, select an appliance.
  3. Under **Management**, click **Pools**.
  4. Click the **COG** for the pool, and select **Edit** from the drop-down list.
  5. Navigate to the corresponding enclosure and click **Show Indicators**.
     NexentaFusion brings up the indicators in the enclosure bay that have indicators set.
  6. Click the LED icon to enable the LED on the JBOD to physically flash.
This function allows you to easily locate the disk in a storage rack.

7. Perform the necessary operations on the blinking device, such as removing or replacing the disk.

Managing Pool Data Devices

This section covers the following topics:

- Administering Pool Data Devices
- Removing a Device from a Pool
- Replacing a Device in a Pool
- Attaching a New Mirror Device
- Detaching a Device from a Mirror
- Setting a Device in a Pool to Offline
- Setting a Physical Device to Online
- Clearing Error from a Device

Administering Pool Data Devices

The Management > Pools allows you to perform a number of administrative tasks should a data device become unreliable or stop functioning properly.

❖ To manage data devices in a pool, do the following:

1. Log in to NexentaFusion, and click Appliance in the drop-down list.
2. In the Appliances List menu, select an appliance.
   A list of pools belonging to the appliance appears.
4. Click the COG for the pool, and select Edit from the drop-down list.
5. Click the device in the left panel, and select the appropriate action from the drop-down list:
   - Clear errors—See Clearing Error from a Device.
   - Attach—See Attaching a New Mirror Device and Setting a Physical Device to Online.
• Replace—See Replacing a Device in a Pool.
• Offline—See Setting a Device in a Pool to Offline.
• Detach—See Detaching a Device from a Mirror.

Removing a Device from a Pool

Only cache, hot spare, and log devices can be removed from a pool. After removing a disk from the pool, the
disk remains online in the system.

| Caution: | You cannot remove data devices from a pool unless you destroy the entire pool. |

Replacing a Device in a Pool

Replacing a device in a pool with another physical device is equivalent to attaching a new device. The device
that is being replaced starts to resilver, detaching the old device. When the resilvering is complete, you can
remove the device from the array and use it for another purpose.

For optimal performance, NexentaStor recommends that the new disk be the same size, speed, and media
type as the disk it replaces. If the intent is to grow the pool, you can increase the size of a pool as described in
Creating Pools on Single or Clustered Nodes. However, if there are many disks, this would require multiple
operations.

| Note: | Nexenta recommends planning for future expansion up-front before creating pools, rather than replacing multiple disks to increase the size of the pool at a later date. |
Attaching a New Mirror Device

NexentaStor enables you to manually attach a new mirror device to an existing data pool on a node. For optimal performance, the disk you are attaching should be the same size, speed, media type as the existing device. The existing device cannot be part of a RAIDZ configuration. If the existing device is not currently part of a mirrored configuration, when you add a new device it automatically transforms into a two-way mirror of the existing device and the new device. If device is part of a two-way mirror, attaching a new device creates a three-way mirror, and multiple-way mirror to the existing data pool to supply more mirrored redundancy on the node.

Detaching a Device from a Mirror

You can detach a device or spare from a mirrored storage data pool on the node. This is helpful if you need to use the device in another pool, or if the disk is corrupted. A spare can also be detached from a RAIDZ storage pool if an existing device was physically replaced.

Caution: The operation is refused if there are no other valid replicas of the data.

Setting a Device in a Pool to Offline

You can set a device in a pool offline if there are hardware issues. When a disk shows hardware errors, bad blocks, or other issues, you can take the device offline, replace it, and then online the new disk. This prevents writing to or reading from the device.

Setting a Physical Device to Online

You can bring a device in a pool back online after being offline to address device issues. When you set a device in a pool to online, the specified device on the node can once again be accessed by read and write operations. You can also expand the device to use all the available spaces.

Note: You do not set spares or cache devices to online.

Clearing Error from a Device

When you check the status of a disk and find any transient errors, you can get rid of them with the Clear option. Only choose this option if the errors do not indicate a potential failure and have not caused unrecoverable data errors in the pool.
Rebooting or Powering Off a NexentaStor Appliance

If required, a NexentaStor appliance can be rebooted or powered down from the NexentaFusion.

Note: You must have superuser privileges are to perform this procedure.

❖ To power off or reboot a NexentaStor appliance, do the following:

1. Log in to NexentaFusion, and click **Appliance** in the drop-down list.
2. In the **Appliances List** menu, select a clustered or non-clustered appliance.
3. Under **Administration**, click **System Settings**.
4. Under **Node Management**, select the appropriate action:
   - **Reboot**—Rebooting a node interrupts services for the duration of the reboot. When rebooting a node that is part of a cluster, HA pools fail-over to the other node. You must manually fail a node back after a failover.
   - **Power Off**—Powering off a node causes all the shared file systems to become unavailable.

5. Verify the action in the confirmation dialog, in one of the following ways:
   - Enter the name of the node and click **Reboot Now**.
   - Enter the name of the node and click **Power Off Now**.